บันทึกข้อความ

ส่วนราชการ สสพ. โทร ๐๒-๒๔๑๐๗๗๗ ต่อ ๑๖

ที่ ๑๙๐ /๒๕๖๖ **วันที่** ๒๕ กรกฎาคม ๒๕๖๖

เรื่อง ผลการทบทวนแผนการดำเนินงานตามตัวชี้วัด ที่ ๕ ๖ และ ๗

เรียน หัวหน้าฝ่ายอำนวยการ

ตามเกณฑ์การประเมินรัฐวิสาหกิจทางด้านการพัฒนาเทคโนโลยีดิจิทัล ที่กำหนดโดยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) และบริษัท ทริส คอร์ปอเรชั่น จำกัด กำหนดตัวชี้วัดเป็น ๘ ข้อ พร้อมกำหนดเกณฑ์น้ำหนักแต่ละหัวข้อไว้ดังนี้

หัวข้อ	น้ำหนัก (ร้อยละ)
๑. การกำกับดูแลด้านเทคโนโลยีดิจิทัลและแผนปฏิบัติการดิจิทัลขององค์กร (Digital Governance and Roadmap)	๒๕
๒. การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation)	๒๕
๓. การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration)	๑๐
๔. การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)	๑๐
๕. การบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)	๑๐
๖. การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ (Business Continuity and Availability Management)	๑๐
๗. การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management)	๑๐
รวม	**๑๐๐**

โดยในเดือน กรกฎาคม ๒๕๖๖ ส่วนสารสนเทศได้ดำเนินการทบทวนแผนการดำเนินงานตามตัวชี้วัดข้อ ๕ การบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) ตัวชี้วัดที่ ๖ การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ (Business Continuity and Availability Management)และตัวชี้วัดที่ ๗ การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม(Resource Optimization Management) ตามกระบวน และแนวทางปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) ครบถ้วนเรียบร้อยสมบูรณ์แล้ว

จึงเรียนมาเพื่อโปรดเสนอผู้อำนวยการพิจารณาเห็นชอบและแจ้งเวียนผู้เกี่ยวข้องต่อไป

เรียน ผู้อำนวยการ
เพื่อโปรดพิจารณาเห็นชอบ
และแจ้งเวียนผู้เกี่ยวข้อง

(นางสาววิมลรัตน์ บุณโยดม)
หัวหน้าฝ่ายอำนวยการ

ปชาดา บุตรครุธ
(นางสาวปชาดา บุตรครุธ)
หัวหน้าส่วนสารสนเทศและพัฒนาระบบ
27/07/66

• เห็นชอบและสั่งเวียนผู้เกี่ยวข้อง

พันโท
(นราวิทย์ เปาอินทร์)
ผู้อำนวยการโรงงานไพ่
๒๗ ก.ค. ๒๕๖๖

KPI 5 การบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)

KPI 5.1 การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management)

เอกสารโดย

ส่วนสารสนเทศและพัฒนาระบบ
โรงงานไพ่ กรมสรรพสามิต

รหัสเอกสาร IT-DOC-KPI5-001
ปรับปรุงล่าสุด 3 กรกฎาคม 2566

บทนำ

บทนำ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดทำขึ้นเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ผ่านเครือข่ายคอมพิวเตอร์ขององค์การ เป็นไปตามมาตรา 5 มาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และ เพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO/IEC 27001:2018 ให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้

เนื่องจากปัจจุบันแนวทางการดำเนินงานด้านความมั่นปลอดภัย ของโรงงานไพ่ มีการอ้างอิงมาตรฐาน ISO/IEC 27001:2018 ดังกล่าวได้มีการอัพเดท Version เป็น ISO/IEC 27001:2022 ช่วงปลายปี 2565 ที่ผ่านมาโดยสามารถสรุปจุดต่าง Version 2018 และ 2022 ดังนี้

1. Security control in Annex A ที่อ้างอิงจาก ISO/IEC 27002:2013 มี Security control 14 domain , 114 Control อันประกอบด้วย
    - Annex A.5 Information security policy
    - Annex A.6 Organization of information security
    - Annex A.7 Human resource security
    - Annex A.8 Asset management
    - Annex A.9 Access control
    - Annex A.10 Cryptography
    - Annex A.11 Physical and environmental security
    - Annex A.12 Operation security
    - Annex A.13 Communication security
    - Annex A.14 System acquisition development and maintenance
    - Annex A.15 Supplier relationships
    - Annex A.16 Information security incident management
    - Annex A.17 Information security aspects of business continuity management
    - Annex A.18 Compliance

แต่ในเวอร์ชั่น ISO/IEC 27001:2022 ได้มีการจัด categories ใหม่ โดยจัดเรียงเป็น 4 categories ดังนี้

1. Organizational controls มี 37 มาตรการควบคุม
2. People controls มี 8 มาตรการควบคุม
3. Physical controls มี 14 มาตรการควบคุม
4. Technological controls มี 34 มาตรการควบคุม

โดยการจัดกลุ่มนี้ใหม่นี้ ยังมีการลดจำนวนของมาตรการควบคุม (controls) จาก 114 มาตรการควบคุม เหลือทั้งสิน 93 มาตรการควบคุม โดยมีมาตรการควบคุมที่เพิ่ม ทั้งหมด 11 มาตรการควบคุม ดังนี้

- A.5.7 Threat intelligence
- A.5.23 Information security for use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring

A.8.9 Configuration management

A.8.10 Information deletion

A.8.11 Data making

A.8.12 Data leakage prevention

A.8.16 Monitoring activities

A.8.23 Web filtering

A.8.28 Secure coding

นอกจากนี้มาตรการควบคุมอื่นๆ ได้มีการเปลี่ยนชื่อใหม่ เช่น Controls 7.10 Storage media เป็น control ที่รวมเอาข้อกำหนดของ ISO 27001:2018 ในข้อ 8.3 Media handling และ A.11.2.5 Removal of asset ไปรวมไว้ด้วยกัน

นอกเหนือจากนี้ในแต่ละมาตรการควบคุมที่ระบุอยู่ใน ISO/IEC 27002:2022 ยังมีการเพิ่มรายละเอียดเพื่อให้ผู้ใช้งานสามารถพิจารณาเลือกใช้งานได้ง่าย ดังนี้

1. Control type
2. Information security properties
3. Cyber security concept
4. Operational capabilities
5. Security domain

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Eco-system #Resilience

ซึ่งการระบุดังกล่าวจะช่วยให้ผู้ใช้งานสามารถแยกประเภทของมาตรการควบคุมให้สอดคล้องกับวัตถุประสงค์ได้อย่างถูกต้อง

จากประเด็นดังกล่าวนี้ โรงงานไพ่ได้มีการประเมินแล้วพบว่า ISO/IEC 27001:2018 ยังมีการใช้งานได้ในปีงบประมาณ 2567 สอดคล้องตามแนวทางการประเมินผลรัฐวิสาหกิจ หัวข้อเทคโนโลยีดิจิทัล หลักความมั่นคงปลอดภัยตาม พรบ.ไซเบอร์ พรบ. คุ้มครองข้อมูลส่วนบุคคล และยังเพียงพอสำหรับการบริหารควบคุมทางด้านความมั่นคงปลอดภัยในปัจจุบันของโรงงานไพ่ และในปีงบประมาณ 2567 ดังกล่าวโรงงานไพ่ จะเริ่มมีการนำมาตราฐาน ISO/IEC 27001:2022 ประกอบการพิจารณาในทบทวนต่อไป

วัตถุประสงค์

1) เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยสงขลานครินทร์เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

2) เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของและทำให้การดำเนินงานต่างๆ เป็นไปอย่างมีประสิทธิภาพ

3) เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหารและเจ้าหน้าที่ทุกระดับ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

4) เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอทุกปี

องค์ประกอบของการจัดทำคู่มือการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management)

1. แนวทางการจัดทำนโยบายการบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร

1) จัดทำแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

2) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอ้างอิงตามมาตรฐาน ISO/IEC 27001:2018 และมีการปรับปรุงอย่างต่อเนื่อง

3) แนวปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์การได้รับทราบและเจ้าหน้าที่ ทุกคนจะต้องยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

4) แนวปฏิบัตินี้ต้องมีการดำเนินการตรวจสอบ ทบทวนและประเมินตามระยะเวลา 1 ครั้ง ต่อปี

2. กรอบนโยบายการบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร (IT Management)

1) นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)
3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)
4) การจัดหมวดหมู่และควบคุมทรัพย์สินองค์กร (Asset Management)
5) การควบคุมการเข้าถึง (Access Control)
6) การเข้ารหัสข้อมูล (Cryptography)
7) ความมั่นคงทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)
8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)
9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
10) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
11) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
13) การบริหารจัดการความมั่นคงปลอดภัยเพื่อสร้างความต่อเนื่องขององค์กร (Information security aspects of business continuity management)
14) ความสอดคล้อง (Compliance)

สารบัญ

สารบัญ

บทที่ 1
แนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ในบทนี้จะอธิบายถึงแนวในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามเกณฑ์การประเมินผลการดำเนินงานรัฐวิสากิจตามระบบประเมินผลใหม่ (State Enterprise Assessment Model: SE-AM) ของสำนักงานคณะกรรมการนโยบายรัฐวิสากิจ (สคร.) ที่ได้กำหนดให้มีกรอบหลักเกณฑ์ด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้โรงงานไพ่ฯ ภายใต้การกำกับดูแลของสำนักงานคณะกรรมการนโยบายรัฐวิสากิจ (สคร.) ใช้เป็นแนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศได้อย่างมีระบบและครบถ้วน ตามองค์ประกอบดังนี้

กรอบแนวทางบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

- กระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ (Information Security Management) ของรัฐวิสาหกิจ
- รัฐวิสาหกิจมีการกำหนดนโยบายหรือแผนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศครอบคลุมประเด็น ดังนี้

1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)
2) การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information security)
3) การควบคุมการเข้าถึง (Access control)
4) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)
5) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security)
6) การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)
7) การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System acquisition and development)
8) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)
9) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
10) การบริหารจัดการผู้ให้บริการภายนอก (Third party management)
11) การป้องกันโปรแกรมไม่ประสงค์ดี (Malicious Software Prevention)
12) การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต (Website and Internet Security)
13) การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)
14) การบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ (Cryptography) และการบริหารจัดการกุญแจ (Key management)

- รัฐวิสาหกิจมีการสื่อสารนโยบายหรือแผนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) ขององค์กร
- รัฐวิสาหกิจมีการกำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) ขององค์กร

โดยระบบการประเมินผลนี้จะมีหลักเกณฑ์การพิจารณาความสมบูรณ์ของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) ตามหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM จากการประเมินในรูปแบบระดับวุฒิภาวะ (Maturity

Level) โดยพิจารณาจากการจัดการกระบวนการให้มีแนวทางปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) มีการถ่ายทอดแนวทางปฏิบัติแบบเดียวกันทั่วทั้งองค์กร โดยมีการวัด วิเคราะห์ และประเมินประสิทธิผลของกระบวนการอย่างเป็นรูปธรรม เพื่อนำมาปรับปรุงและพัฒนากระบวนการอย่างต่อเนื่อง โดยแบ่งระดับการให้คะแนนตามตามคู่มือการประเมินผลการดำเนินงานรัฐวิสาหกิจ (ฉบับปรับปรุงปี 2566) ดังนี้

ระดับคะแนน	หลักเกณฑ์
ระดับ 1	เริ่มมีแนวทางในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ
ระดับ 2	รัฐวิสาหกิจมีกระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย • การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ • การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ • การควบคุมการเข้าถึง • การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม • การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร • การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ • การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ • การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ • การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ • การบริหารจัดการผู้ให้บริการภายนอก • การป้องกันโปรแกรมไม่ประสงค์ดี • การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต • การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน • การบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศและการบริหารจัดการกุญแจ
ระดับ 3	รัฐวิสาหกิจมีการถ่ายทอดกระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
ระดับ 4	รัฐวิสาหกิจมีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ
ระดับ 5	รัฐวิสาหกิจมีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวนการกำกับดูแลด้านการบริหารจัดการดิจิทัล / จัดทำแผนปฏิบัติการดิจิทัลขององค์กร(ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

ตารางที่ 1 เกณฑ์แบ่งระดับคะแนนตามระบบ SE-AM

โดยมีรายละเอียดของการจัดทำเอกสารคู่มือ การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management) ปรากฏในบทถัดไปตามลำดับ

บทที่ 2
นโยบายและแนวปฏิบัติการบริหารความมั่นคงปลอดภัยสารสนเทศ

นโยบายและแนวปฏิบัติ การบริหารความมั่นคงปลอดภัยสารสนเทศ ดังนี้ :

1. นโยบายการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

- ด้านหน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets) มีวัตถุประสงค์ เพื่อให้ระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

1.1 นโยบายบัญชีสินทรัพย์ (Inventory of assets)

1) ต้องจัดทำและเก็บทะเบียนสินทรัพย์สารสนเทศ เพื่อเป็นข้อมูลสำหรับการนำไปวิเคราะห์และประเมินความเสี่ยง และบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

2) ต้องตรวจสอบสินทรัพย์ตามระยะเวลาที่กำหนด เช่น ปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ

1.2 นโยบายผู้ถือครองสินทรัพย์ (Ownership of assets)

ระบุให้สินทรัพย์ในทะเบียนสินทรัพย์ต้องกำหนดผู้รับผิดชอบให้ชัดเจน

1.3 นโยบายด้านการใช้สินทรัพย์อย่างเหมาะสม (Acceptable use of assets)

อนุญาตให้ใช้สินทรัพย์สารสนเทศให้เป็นไปตามข้อกำหนด ดังนี้

1) ข้อกำหนดการใช้งานเครือข่าย
2) ข้อกำหนดการใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์
3) ข้อกำหนดการใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)

1.4 นโยบายการคืนสินทรัพย์ (Return of assets)

กำหนดให้พนักงานที่สิ้นสุดการจ้างงาน หรือสิ้นสุดโครงการต้องคืนสินทรัพย์สารสนเทศ ที่รับผิดชอบทั้งหมด รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้าออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือและอุปกรณ์ต่างๆ

- ด้านการจัดชั้นความลับของสารสนเทศ (Information classification) มีวัตถุประสงค์เพื่อให้สินทรัพย์สารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

1.5 นโยบายชั้นความลับของสารสนเทศ (Classification of information)

.....1) ต้องทำการจัดหมวดหมู่สินทรัพย์ กำหนดระดับความสำคัญ และกำหนดชั้นความลับ เพื่อป้องกันสารสนเทศให้มีความมั่นคงปลอดภัย โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ.2544

..2) สินทรัพย์สารสนเทศ ซึ่งทำซ้ำมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ให้ถือว่ามีชั้นความลับเดียวกับต้นฉบับ

1.6 นโยบายการบ่งชี้สารสนเทศ (Labeling of information)

ต้องจัดให้มีวิธีการจัดทำ และจัดการป้ายชื่อสินทรัพย์

1.7 นโยบายการจัดการสินทรัพย์ (Handling of assets)

1) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงาน

2) ข้อมูลที่เป็นข้อมูลลับต้องไม่เปิดเผยต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

3) หากส่งผ่านข้อมูลที่เป็นข้อมูลลับผ่านเครือข่ายต้องป้องกันข้อมูลอย่างเหมาะสม ได้แก่ การปกป้องด้วยรหัสผ่าน หรือ การเข้ารหัสข้อมูล

4) ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานขององค์กรทั้งหมด ทั้งที่เก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ใช้งาน ต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใด ๆ เกิดขึ้น ตัวอย่างเช่น การติดมัลแวร์ ฮาร์ดดิสก์เสีย เป็นต้น

- ด้านการจัดการสื่อบันทึกข้อมูล (Media Handling) เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้ายการลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

1.8 นโยบายการบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)

สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่างๆ (เช่น PDA, Thumb- Drive, CD –Rom เป็นต้น) ที่มีข้อมูลลับขององค์กรบันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

1.9 นโยบายการทำลายสื่อบันทึกข้อมูล (Disposal of media)

ข้อมูลลับขององค์กรที่สำเนามาเก็บอยู่บนสื่อบันทึกข้อมูล หากไม่ใช้งานแล้วต้องทำลายให้สิ้นซากตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

1.10 การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)

หากต้องขนย้ายสื่อบันทึกข้อมูลจะต้องป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การล็อคกุญแจการปิดผนึก การเข้ารหัส เป็นต้น

แนวปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

1) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียก คืนทรัพย์สิน

2) จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำ ปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยี สารสนเทศ และบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศ สิ้นสุดตามอายุการใช้งาน (End of Life) หรือสิ้นสุดการให้บริการ (End of Support) จากผู้ผลิตได้อย่าง เหมาะสม

3) มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Inventory List) ของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่รองรับระบบเทคโนโลยีสารสนเทศของบริษัทอย่างครบถ้วนและ เป็นลายลักษณ์อักษรโดยครอบคลุมอย่างน้อย ดังนี้

- ชื่อเครื่องแม่ข่าย
- ชื่อระบบปฏิบัติการ (Operating System) และเวอร์ชัน (Version)
- ชื่อระบบงาน (Application) และเวอร์ชัน (Version)
- เจ้าของทรัพย์สิน (Owner)
- ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (Specification)
- หมายเลขอ้างอิงของฮาร์ดแวร์ (Serial Number) และหมายเลขอ้างอิงของซอฟต์แวร์ (Software license)
- สถานที่ตั้ง
- วันที่เริ่มติดตั้ง
- ประเภทการครอบครอง (ซื้อหรือเช่า)
- รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา
- วันที่บำรุงรักษาล่าสุด

– วันสิ้นสุดการใช้งานตามสัญญา (Warranty) และวันสิ้นสุดการรับประกันการใช้งาน (Support Contract)

– วันสิ้นสุดการให้บริการจากผู้ผลิต (End of Support)

4) มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมี การตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

5) มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในบริษัทและกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของบริษัท ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

6) รายงานการเปลี่ยนแปลงของทรัพย์สินในความรับผิดชอบของตนต่อผู้อำนวยการอาวุโสฝ่ายดิจิทัล เพื่อรับทราบ

7) กำหนดหน้าที่ความรับผิดชอบและควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control) ดังนี้

7.1) ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัทต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน

– ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้าหรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม

– ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัทเว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของ หน่วยงาน

– ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่อง คอมพิวเตอร์ รวมถึงอุปกรณ์ต่อพ่วงให้มีสภาพเดิม

– ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ

– ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

– ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยนไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่

– หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบ หมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

– ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน

– การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติ ตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท

– ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางอุปกรณ์ทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

8) มีการควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License) ให้ถูกต้องลิขสิทธิ์ และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและ สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมาย

2. นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security)

มีวัตถุประสงค์เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์กร โดยให้มีการกำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities) โดยผู้บริหารระดับสูงสุดต้องแต่งตั้งกลุ่มหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ และมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

2.1 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

1) ผู้บริหารด้านไอทีต้องกำหนดตำแหน่งด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดความรับผิดชอบให้เหมาะสม พร้อมทั้งควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

2) ผู้บริหารด้านไอทีเป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

3) ผู้บริหารต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

4) ผู้ใช้งาน และหน่วยงานภายนอกต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติขององค์กรในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

2.2 นโยบายการติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

ต้องกำหนดรายชื่อ และข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) ศูนย์ประสานงาน การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) การไฟฟ้า เพื่อใช้สำหรับติดต่อประสานงานด้านความมั่นคงปลอดภัย

2.3 นโยบายการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษเรื่องเดียวกัน (Contact with special interest groups)

ต้องกำหนดรายชื่อ และข้อมูลสำหรับติดต่อกลุ่มที่มีความสนใจเป็นพิเศษเรื่องเดียวกัน

2.4 นโยบายความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

ต้องระบุความมั่นคงปลอดภัยสารสนเทศสำหรับโครงการที่เกี่ยวข้องกับสารสนเทศ

2.5 นโยบายการควบคุมคอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

วัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและสินทรัพย์สารสนเทศจากการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา รวมทั้งการปฏิบัติงานนอกหน่วยงานจากระยะไกล

1) การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy) ต้องกำหนดวิธีการป้องกันข้อมูลและสินทรัพย์สารสนเทศที่อยู่ในอุปกรณ์คอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารอื่นๆ โดยให้เป็นไปตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

2.6 นโยบายการปฏิบัติงานภายนอกหน่วยงาน (Teleworking)

1) อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานโดยต้องใช้งานผ่านช่องทางที่จัดเตรียมไว้ให้ และต้องตรวจสอบตัวตนก่อนการใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

2) ต้องไม่นำข้อมูลลับขององค์กรไว้บนอุปกรณ์ส่วนตัว หรือหากมีความจำเป็นต้องใช้งาน เมื่อใช้เสร็จแล้วควรลบทิ้งไป

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

1) การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติดังนี้

– ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก 3 เดือน หรือเมื่อระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน

– เลือกรหัสผ่านที่ปลอดภัยและรักษารหัสนั้นให้เป็นความลับอยู่ตลอดเวลา

– ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ

– ไม่ลักลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

– รายงานการล่วงละเมิดความมั่นคงปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

2) การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล ผู้ใช้งานต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ใช้ดูแล เพื่อป้องกันข้อมูลสำคัญสูญหาย

– ผู้ดูแลระบบมีอำนาจที่จะยุติหรือเพิกถอนสิทธิการใช้คอมพิวเตอร์และเครือข่ายโดยทันที หากตรวจพบผู้ใช้ที่ฝ่าฝืนระเบียบหรือกระทำการใดที่อาจสร้างความเสียหายให้กับระบบ

– เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องติดตั้งระบบ screen saver โดยกำหนดรหัสในการเข้าใช้

– การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานจะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานนั้น

3) ต้องไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

– ผู้ดูแลระบบต้องกำหนดให้มีข้อปฏิบัติในการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลการพิสูจนตัวตนที่เหมาะสมก่อนเข้าใช้งานและต้องกำหนดให้ผู้ใช้งาน ออกจากระบบโดยทันทีเมื่อเสร็จสิ้นงาน

– เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

– ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

– การป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา, smart mobile device เมื่อปฏิบัติงานอยู่นอกสถานที่ ได้แก่

ก. ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

ข. ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา

ค. ต้องเข้ารหัสข้อมูลที่สำคัญไว้

ง. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ได้แก่

จ. การสำรองข้อมูลที่เป็นข้อมูลลับต้องเข้ารหัสด้วยเทคโนโลยี Transport Layer Security (TLS) Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ 128 bits (128-bits Encryption) เป็นอย่างน้อยเพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง

ฉ. การอนุญาตให้เข้าถึงข้อมูลลับผ่านเครือข่ายต้องเข้ารหัสด้วยรหัสผ่าน กำหนดวันหมดอายุของการเข้าถึง และระบุให้เข้าถึงได้เฉพาะผู้มีสิทธิ

ช. ไม่อนุญาตให้ส่งผ่านข้อมูลลับผ่านเครือข่าย หากต้องส่งผ่านเครือข่ายต้องขออนุญาตจากผู้บังคับบัญชาทุกครั้ง และในกรณีที่เป็นไฟล์แนบต้องเข้ารหัสด้วยรหัสผ่านทุกครั้ง

ซ. การสำเนาข้อมูลชั้นความลับต้องจดบันทึกจำนวนชุดที่สำเนา รายละเอียดผู้ดำเนินการทุกครั้ง

4) การทำลายสื่อบันทึกข้อมูลหรือข้อมูลลับให้เป็นไปตามแนวปฏิบัติในการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล ดังนี้

– ต้องมีการลบข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรืออุปกรณ์บันทึกข้อมูลอื่นโดยการฟอร์แมตอุปกรณ์ดังกล่าวให้ไม่สามารถเรียกร้องข้อมูลกลับมาได้ ก่อนทำการเปลี่ยน ทดแทน ทำลายหรือจำหน่าย

– ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายอุปกรณ์บันทึกข้อมูลหรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

3. นโยบายการควบคุมการเข้าถึง (Access Control)

3.1 นโยบายความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

มีวัตถุประสงค์เพื่อจำกัดการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต โดยนโยบายควบคุมการเข้าถึง (Access control policy) เป็นการกำหนดมาตรฐานแนวทางปฏิบัติที่มีความสอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอกเพื่อควบคุมให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต โดยมีมาตรการควบคุมการเข้าถึง ตามแนวปฏิบัติดังต่อไปนี้

1) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ
2) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย
3) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
4) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ
5) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
6) แนวปฏิบัติการควบคุมการเข้าถึงระบบกล้องวงจรปิด

3.2 นโยบายการเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

กำหนดการป้องกันทางเครือข่ายให้มีความมั่นคงปลอดภัย ตามแนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย และ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

3.3 นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

มีวัตถุประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้ ดังนี้

1) การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration) การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งานระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่ผู้ใช้งานสิ้นสุดสถานภาพต้องยกเลิกออกจากระบบทันที ตามแนวปฏิบัติการจัดการการเข้าถึงข้อมูลผู้ใช้

3.4 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access Provisioning)

ผู้ดูแลระบบต้องมีกระบวนการกำหนดสิทธิให้ครอบคลุมผู้ใช้งานให้ครบทุกประเภทและทุกบริการ

3.5 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

.....ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่รับผิดชอบด้วย โดยให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงข้อมูลผู้ใช้

3.6 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of privileged access right)

..... การส่งมอบข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังนั้นต้องมีกระบวนการป้องกันและการปกปิดโดยให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงข้อมูลผู้ใช้

3.7 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

3.8 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)

เมื่อเจ้าหน้าที่ลาออก เปลี่ยนแปลงข้อตกลงหรือหรือสัญญา ผู้ดูแลระบบต้องทำการถอดถอนหรือปรับปรุงสิทธิให้ถูกต้อง

- หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) วัตถุประสงค์เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

3.9 นโยบายการใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information)

1) ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศองค์กร การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย หัวข้อ การใช้งานรหัสผ่าน

2) รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย

3) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตนทั้งหมด

4) รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้

การควบคุมการเข้าถึงระบบ (System and application access control) เพื่อป้องกันการเข้าถึงระบบสารสนเทศและข้อมูลบนระบบสารสนเทศโดยไม่ได้รับอนุญาต

3.10 นโยบายการจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

1) ต้องควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน ได้แก่ เขียนอ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้งาน ที่สามารถใช้งานได้ ตรวจสอบว่า สารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

2) บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

3) บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบสารสนเทศขององค์กร ตามแนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

3.11 นโยบายขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

การเข้าถึงระบบปฏิบัติการจะต้องผ่านการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัยตาม แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

3.12 นโยบายการใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

ต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

1) ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
2) ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
3) จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
4) ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้

3.13 นโยบายการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code) อนุญาตเฉพาะผู้รับผิดชอบสามารถเข้าถึงซอร์สโค้ดของโปรแกรม

แนวปฏิบัติการควบคุมการเข้าถึง

เพื่อควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต และรวมความถึงการกำหนดหน้าที่ของผู้ใช้งาน การเข้าถึงเครือข่าย การใช้งานระบบสารสนเทศ การเฝ้าดูการใช้งานระบบสารสนเทศ และอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศขององค์กร เป็นต้น

1) ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

– กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

– กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่ สิทธิอ่านอย่างเดียว สิทธิการเพิ่มข้อมูล สิทธิการแก้ไขข้อมูล สิทธิการลบข้อมูล สิทธิการอนุมัติ/อนุญาต และ ไม่มีสิทธิ

– กำหนดการระงับสิทธิ มอบอำนาจ ให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน ที่ได้กำหนดไว้

2) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย

– การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และการรักษาความมั่นคงปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการ และกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้ 1) ข้อมูลทั่วไปที่เปิดเผยได้ 2) ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ได้แก่

ก. ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำร้อง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

ข. ข้อมูลสารสนเทศตามพันธกิจ ได้แก่ ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

3) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 4 ระดับ

– ข้อมูลที่มีระดับความสำคัญมากที่สุด ได้แก่ ข้อมูลผลการเรียนนิสิต ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านการวิจัย

– ข้อมูลที่มีระดับความสำคัญมาก ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคล ข้อมูลบุคลากร

– ข้อมูลที่มีระดับความสำคัญปานกลาง

– ข้อมูลที่มีระดับความสำคัญน้อยหากข้อมูลที่นอกเหนือจากที่กำหนด การจัดระดับความสำคัญของข้อมูล ให้พิจารณาในระดับฐานข้อมูล ด้วยการประเมินมูลค่าความเสียหายต่อหน่วยงานหากข้อมูลมีปัญหา ไม่สมบูรณ์ แนวปฏิบัติในการพิจารณาจัดลำดับความสำคัญของข้อมูลมีดังนี้

ระดับความสำคัญของข้อมูล การประเมินมูลค่าความเสียหายหากข้อมูลมีปัญหา หรือไม่สมบูรณ์

ความสำคัญมาก มีผลกระทบรุนแรงต่อการดำรงอยู่ของหน่วยงาน หรือปิดหน่วยงาน

ความสำคัญปานกลาง มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย

ความสำคัญน้อยไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ

4) จัดแบ่งลำดับชั้นความลับของข้อมูล

– **ข้อมูลลับที่สุด** หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

– **ข้อมูลลับมาก** หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

– **ข้อมูลลับ** หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

– **ข้อมูลทั่วไป** หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

5) จัดแบ่งระดับชั้นการเข้าถึง ดังนี้

– เข้าถึงได้ทุกกลุ่มผู้ใช้งาน ได้แก่ ข้อมูลทั่วไปที่เปิดเผยได้

– เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ ได้แก่ ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ข้อมูลลับ

– เข้าถึงได้เฉพาะผู้มีสิทธิในการบริหารจัดการระบบสารสนเทศ ได้แก่ ข้อมูลระบบ

6) กำหนดช่องทางในการเข้าถึงข้อมูล

– ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายภายใน ได้ตลอด 24 ชั่วโมง

– ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายอินเตอร์เน็ตที่อยู่ภายนอก ผ่านระบบ VPN ได้ตลอด 24 ชั่วโมง

7) กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล

– ระบบงานบริการสำหรับผู้ใช้งานทั่วไปเข้าถึงได้ตลอดเวลา

– ระบบงานภายในสำหรับผู้ใช้งานสามารถเข้าถึงระบบตามช่วงเวลา ดังนี้

ก. เวลาราชการ (8.30น. – 16.30 น.)

ข. นอกเวลาราชการ (นอกช่วงเวลา 8.30น. – 16.30 น.)

ค. ช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

ง. ช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุช่วงเวลา ระยะเวลาการเข้าถึง

8) มีข้อกำหนดการใช้งานตามภารกิจ

เพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

– มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

– มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

9) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและแก้ไขเปลี่ยนแปลงสิทธิต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

10) ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

11) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย

– ผู้ดูแลระบบต้องออกแบบและแบ่งแยกระบบเครือข่าย (Segregation in networks) โดยแบ่งออกเป็น 2 เครือข่าย คือเครือข่ายภายในหน่วยงาน และเครือข่ายภายนอกองค์การ เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ และกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตเท่านั้น

– ผู้ดูและระบบต้องกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

– มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้นพร้อมทั้งจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงสุด หรือผู้บริหารด้านดิจิทัลก่อนที่จะใช้งานในทุกกรณี

– กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยผู้ดูแลระบบต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

12) การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User authentication for external connections) ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศขององค์กร โดยจะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคล ดังนี้

– วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน จะต้องได้รับการอนุมัติจากผู้บริหารระดับสูงสุด หรือผู้บริหารด้านดิจิทัลก่อนทุกครั้ง และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานจะต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการขออนุญาต อย่างเพียงพอ

– ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (User Name) ทุกครั้ง และผู้ดูแลระบบจะต้องตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของโรงงานไพ่กรมสรรพสามิต อย่างน้อย 1 วิธี เช่น มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม เป็นต้น

– ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

– การเข้าสู่ระบบสารสนเทศของโรงงานไพ่ กรมสรรพสามิตจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

– การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่ควรเปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น โดยการเชื่อมต่อระยะไกลนั้นจะอนุญาตเข้าผ่านทางช่องทาง VPN หรือผ่านการทำงานของระบบซอฟท์แวร์ใดๆ ที่ผ่านการตรวจสอบของผู้ดูแลระบบเรียบร้อยแล้วว่ามีความปลอดภัย และสามารถดำเนินการได้ตามแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของโรงงานไพ่ กรมสรรพสามิต เท่านั้

– การเข้าสู่ระบบจากระยะไกล เพื่อเพิ่มความมั่นคงปลอดภัยของการรับส่งข้อมูล ต้องมีการใช้การเข้ารหัสข้อมูล ได้แก่ TLS1.2

13) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ผู้ดูและระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

– การควบคุมการใช้งานอย่างเหมาะสม และจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้โดยผู้ขอใช้บริการจะต้องได้รับการอนุญาตจากผู้บริหารระดับสูงสุด หรือผู้บริหารด้านดิจิทัลก่อนทุกครั้ง

– ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์โดยผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย เช่น รายชื่อผู้ขอใช้บริการ IP Address Mac Address และผังเครือข่ายเป็นต้น

– อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางได้

14) การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายขององค์กรและเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

15) ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย ผู้ดูแลระบบต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างองค์กรกับหน่วยงานภายนอก

16) การควบคุมผู้ใช้งานในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ได้แก่

– ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย
– มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย
– ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

17) การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อ

ควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น โดยผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายและการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ ดังนี้

- ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address)
- กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย
- กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

18) ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

19) ผู้ดูแลระบบจะต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port) ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายดังนี้

- ผู้ดูแลระบบ ต้องกำหนดการเปิด - ปิด พอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงของอุปกรณ์เครือข่ายต่างๆ และปิดพอร์ตที่เสี่ยงต่อการก่อให้เกิดความเสียหายต่อระบบเครือข่ายและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน
- ผู้ดูแลระบบต้องกำหนดช่วงเวลาในการตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ
- ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (firewall) ของระบบเครือข่าย
- ผู้ดูแลระบบต้องปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้บริหารด้านดิจิทัล เป็นลายลักษณ์อักษร
- ผู้ดูแลระบบต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต
- บุคคลภายนอกที่มีความประสงค์ต้องการใช้งานพอร์ตของอุปกรณ์เครือข่าย ต้องได้รับการอนุญาตจากผู้ดูแลระบบ หรือผู้บริหารด้านดิจิทัล หรือผ่านช่องทางที่องค์กรจัดเตรียมไว้ให้

20) การควบคุมการเชื่อมต่อเครือข่าย (Network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างกัน ดังนี้

- ผู้ดูแลระบบต้องมีการตรวจสอบการเชื่อมต้อระบบเครือข่าย
- จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเครือข่าย
- ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย
- ผู้ดูแลระบบต้องมีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับคอมพิวเตอร์แม่ข่าย
- ผู้ดูแลระบบต้องควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย โดยไม่ได้รับอนุญาต

21) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

22) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

– ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องลงทะเบียน MAC Address ผ่านระบบลงทะเบียนเครื่องคอมพิวเตอร์โดยใช้รหัสบัญชีผู้ใช้ที่ออกโดยส่วนสารสนเทศและพัฒนาระบบ

– ผู้ใช้งานต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

23) ผู้ดูแลระบบต้องดำเนินการดังต่อไปนี้

– ต้องลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

– ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

– ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

– เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

– เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดา หรือ เจาะรหัสได้โดยง่าย

– ต้องกำหนดค่าใช้ WPA2 (Wi-Fi Protected Access) หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

– เลือกใช้วิธีการควบคุม MAC Address ชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้และรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

– ติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

– ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้บริหารด้านดิจิทัลทราบโดยทันที

24) การจัดการการเข้าถึงข้อมูลผู้ใช้

– จัดทำแบบฟอร์มคำขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานโดยยื่นแบบฟอร์มคำขอต่อผู้บริหารด้านดิจิทัลหรือผู้ดูแลระบบที่ได้รับมอบหมาย

– มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

– การกำหนดชื่อผู้ใช้งาน (User Name) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานอื่น

– จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

– มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

– จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

– มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

– มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้บริหารด้านดิจิทัลหรือผู้ดูแลระบบที่ได้รับมอบหมาย

– มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน โดยหัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลในแบบฟอร์ม และยื่นคำขอต่อผู้บริหารด้านดิจิทัล เช่น เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

– ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบที่เกี่ยวข้องทั้งหมด

25) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

– ต้องมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานที่เหมาะสมต่อสถานภาพหรือหน้าที่ความรับผิดชอบ

– ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

– ต้องมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

– ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

26) การบริหารจัดการรหัสผ่าน (User password Management)

– กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

– ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ และไม่เปิดเผยให้ผู้อื่นทราบ

– กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

– ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

– ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

– ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

27) เจ้าของระบบ จะต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เข้า มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง หรือผู้ใช้งานเข้าถึงข้อมูลหรือกระทำการไม่เหมาะสม เป็นต้น เพื่อให้มั่นใจว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

28) ต้องกำหนดหลักสูตร และฝึกอบรมเกี่ยวกับการสร้างความรู้ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ และความตระหนักเรื่องความมั่นคงปลอดภัย และกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

29) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

– กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับระบบที่มีความความสำคัญสูงหรือมีความเสี่ยงสูง การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวสำหรับระบบสารสนเทศ ดังนี้

– ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

– ต้องกำหนดระยะเวลาสำหรับการป้อนรหัสผ่าน

– จำกัดเข้าถึงระบบปฏิบัติการเฉพาะอินทราเน็ต

30) การพิสูจน์ตัวตนสำหรับผู้ใช้งาน (User identification and authentication)

ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบสารสนเทศ ได้แก่

– ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อผู้ใช้ (Username) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

– ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันเกิดจากการใช้ชื่อผู้ใช้ (Username) เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

31) การบริหารจัดการรหัสผ่าน (Password management system)

ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ได้แก่

– กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

– ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ และไม่เปิดเผยให้ผู้อื่นทราบ

– กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

– ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

– ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

– ผู้ใช้งานสามารถดำเนินการปรับเปลี่ยน password ได้ด้วยตนเอง

– ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

32) กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย

ผู้ดูแลระบบต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง เป็นต้น

33) การพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์

ผู้ดูแลระบบต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์

34) การตัดเวลาการใช้งานเครื่องคอมพิวเตอร์

ผู้ดูแลระบบต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์เมื่อเครื่องคอมพิวเตอร์ นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

35) การควบคุมการใช้งานโปรแกรมยูทิลิตี้ (Use of system utilities)

ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้งานโปรแกรมยูทิลิตี้ต้องพิสูจน์ตัวตนก่อน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้
- โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

36) การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง ผู้บริหารต้องจัดให้ติดตั้งระบบเตือนภัยให้กับผู้ใช้ที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

37) การใช้งานระบบเทคโนโลยีสารสนเทศต้องกำหนดให้ตัด และหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานเกิน 15 นาที (Session time-out)

38) ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ของผู้ใช้งานไปยังเครื่องปลายทาง เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง ได้แก่ ระบบบัญชีเงินเดือน ระบบฐานข้อมูลบุคคล โดยสามารถเข้าใช้งานระบบในช่วงวันเวลาราชการตั้งแต่เวลา 8.30น.–16.30น. และวันหยุดราชการตั้งแต่เวลา 8.30น.-12.00น. โดยการเชื่อมต่อ 1 ครั้งอนุญาตให้ใช้งานได้ไม่เกิน 2 ชั่วโมง ในกรณีมีความจำเป็นเร่งด่วนให้ทำการขออนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายเพื่ออนุมัติให้เข้าใช้งานระบบเป็นครั้งคราว

39) การควบคุมการเข้าถึงระบบกล้องวงจรปิด

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบกล้องวงจรปิดและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ โดยการจำกัดการเข้าถึงระบบกล้องวงจรปิด มีดังนี้

- ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบได้ กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าระบบกล้องวงจรปิดที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน
- ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ เพื่อติดต่อกับระบบกล้องวงจรปิดโดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

– เครื่องบันทึกระบบกล้องวงจรปิด ต้องมีการติดตั้งอยู่ในตู้หรือ อุปกรณ์อื่นที่ต้องมีกุญแจล็อค และตั้งอยู่ในพื้นที่ห้องควบคุมระบบ เพื่อความมั่นคงปลอดภัย ตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

– ต้องตัดเวลาการใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานไม่ได้ใช้งานเกิน 60 นาที

– การเข้าถึงระบบสารสนเทศที่มีความสำคัญสูง อนุญาตให้ทำผ่านช่องทางที่กำหนดให้บันทึกข้อมูลการใช้งานไว้เป็น Log File โดยแบ่งเป็น 2 แนวปฏิบัตินี้

ก. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

ข. การป้องกันข้อมูลและสินทรัพย์สารสนเทศที่อยู่ในอุปกรณ์สื่อสารประเภทพกพา

– ผู้ใช้งานต้องมีวิธีป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศในอุปกรณ์สื่อสารประเภทพกพาเมื่อปฏิบัติงานนอกสถานที่ ได้แก่

ก. ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

ข. ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา

ค. ต้องเข้ารหัสข้อมูลที่สำคัญไว้

40) การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายขององค์กร ต้องพิสูจน์ตัวตนก่อนเข้าใช้งาน

– การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

– การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)

– การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่เปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว กำหนดการเชื่อมต่อเข้าสู่ระบบไม่เกิน 2 ชั่วโมง

– การปฏิบัติงานนอกองค์กร ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด

41) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ดังนี้

– การจำกัดการเข้าถึงระบบสารสนเทศ

ก. ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบได้ กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

ข. ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

ค. ต้องตัดเวลาการใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานไม่ได้ใช้งานเกิน 60 นาที

ง. การแยกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง ได้แก่

– การจัดทำบัญชีรายชื่อแยกประเภทโดยแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในองค์กร

– ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ได้แก่ ระบบสารสนเทศทางการบัญชี (ERP) ระบบฐานข้อมูลกลางขององค์กร ต้องได้รับการแยกออกจากระบบงานอื่นๆ ขององค์กร

– ระบบซึ่งไวต่อการรบกวน ต้องควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

– การเข้าถึงระบบสารสนเทศที่มีความสำคัญสูง อนุญาตให้ทำผ่านช่องทางที่

– บันทึกข้อมูลการใช้งานไว้เป็น Log File

42) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กรการป้องกันข้อมูลและสินทรัพย์สารสนเทศที่อยู่ในอุปกรณ์สื่อสารประเภทพกพา ผู้ใช้งานต้องมีวิธีป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศในอุปกรณ์สื่อสารประเภทพกพาเมื่อปฏิบัติงานนอกสถานที่ ได้แก่

– ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง
– ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา
– ต้องเข้ารหัสข้อมูลที่สำคัญไว้

43) การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายขององค์กร ต้องพิสูจน์ตัวตนก่อนเข้าใช้งาน

– การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)
– การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)
– การเข้าสู่ระบบสารสนเทศขององค์กร จะต้องตรวจสอบผู้ใช้งานอีกครั้ง
– การเข้าสู่ระบบจากระยะไกลต้องใช้การเข้ารหัสข้อมูล ได้แก่ TLS1.2 เพื่อเพิ่มความมั่นคงปลอดภัยของการรับส่งข้อมูล

44) การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่เปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว กำหนดการเชื่อมต่อเข้าสู่ระบบไม่เกิน 2 ชั่วโมง

– การปฏิบัติงานนอกองค์กร ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด

45) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงานผู้ดูแลระบบต้องกำหนดขั้นตอนการขออนุมัติการปฏิบัติงานจากภายนอกหน่วยงาน กำหนดสิทธิ์หรือยกเลิก การเข้าถึงระบบงาน ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งการปฏิบัติงานจากภายนอกหน่วยงานหากปรากฏความเสียหายร้ายแรง ผู้ปฏิบัติงานจากภายนอกหน่วยงานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นนั้น ดังนี้

– มีการกรอกแบบฟอร์มการขอใช้งานจากภายนอก
– มีการชี้แจงแผนงานและขั้นตอนปฏิบัติ เพื่อเสนอการขออนุมัติการขอใช้งานจากภายนอก
– ตรวจสอบการทำงานอย่างเคร่งครัด

46) ในกรณีที่โรงงานไพ่ กรมสรรพสามิตได้มีการว่าจ้างกับบริษัทต่าง ๆ เพื่อดำเนินโครงการของการพัฒนาระบบสารสนเทศ ของโรงงานไพ่ กรมสรรพสามิตและต้องลงนามในสัญญาการว่าจ้างกับบริษัทต่างๆ ให้มีการจัดทำเอกสารแนบท้ายสัญญาว่าด้วยการรักษาข้อมูลที่เป็นความลับด้านระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลกับบริษัทคู่สัญญา โดยมีการกำหนดมาตรการ ดังนี้

– ผู้รับจ้างมีหน้าที่ในการคัดสรรพนักงานที่เข้ามาดำเนินโครงการของการพัฒนาระบบสารสนเทศของโรงงานไพ่กรมสรรพสามิตจะต้องไม่เคยเป็นผู้มีความผิดเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ระหว่างการจ้าง ผู้รับจ้างมีหน้าที่และความรับผิดชอบในการควบคุมดูแลพนักงานของผู้รับจ้างให้รักษาข้อมูลที่เป็นความลับเช่นเดียวกับที่ผู้รับจ้างต้องปฏิบัติ

– ผู้รับจ้างจะต้องใช้ความระมัดระวังอย่างที่สุดตามที่ผู้ประกอบวิชาชีพจะพึงมีในการรักษาข้อมูลที่เป็นความลับอย่างเคร่งครัด โดยไม่บอกหรือเปิดเผยข้อมูลทีเป็นความลับแก่บุคคลภายนอกรู้ไม่ว่ากรณีใดๆ ทั้งสิ้น เว้น

แต่เพื่อความจำเป็นในการปฏิบัติงานตามหน้าที่ของผู้รับจ้างตามสัญญาหลักเท่านั้นต้องเสริมสร้างความเข้าใจอันดีต่อพนักงานทุกคน เพื่อให้การปฏิบัติและการบริหารงานด้านการรักษาข้อมูลบังเกิดผลมากที่สุด

– เมื่อสิ้นสุดการปฏิบัติงานตามสัญญาหลักหรือสัญญาหลักสิ้นสุดลงไม่ว่าด้วยเหตุใดๆ ผู้รับจ้างต้องคืนเอกสาร แบบแปลน พิมพ์เขียว หรือคู่มือปฏิบัติงานเกี่ยวกับงานที่ว่าจ้างที่ได้รับไปจากผู้ว่าจ้างทันที และมิให้ทำสำเนาไว้ไม่ว่าในรูปของเอกสารหรือข้อมูลอิเล็กทรอนิกส์อื่นใดทั้งสิ้น

4. นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)

เกี่ยวกับพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas) วัตถุประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร ดังนี้

4.1 นโยบายด้านขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

1) ต้องแบ่งพื้นที่อย่างชัดเจน และกำหนดระดับการควบคุมเพื่อป้องกันการเข้าถึงสินทรัพย์สารสนเทศที่มีความสำคัญ

2) ต้องจัดทำแผนผังแสดงตำแหน่งและพื้นที่แต่ละชนิดและประกาศให้ผู้เกี่ยวข้องทราบ

3) ต้องดูแลรักษาสภาพแวดล้อมของพื้นที่ให้เป็นไปตาม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

4.2 นโยบายการควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

1) ต้องควบคุมให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่

2) ต้องกำหนดสิทธิ และช่วงเวลาในการผ่านเข้าออกพื้นที่

3) ต้องบันทึกการผ่านเข้าออกในพื้นที่ที่สำคัญ

4) ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

4.3 นโยบายการรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)

1) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก

2) เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

3) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

4) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

5) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่ บุคคลผู้นั้นเป็นเจ้าหน้าที่ ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

4.4 นโยบายการป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external end environmental threats) ต้องมีวิธีป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น

4.5 นโยบายการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

1) หากพบสิ่งผิดปรกติ หรือการละเมิดความมั่นคงปลอดภัย จะต้องแจ้งให้ผู้บังคับบัญชาทราบ

2) ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น ”ห้ามเข้าก่อนได้รับอนุญาต”

4.6 นโยบายเกี่ยวกับพื้นที่สำหรับรับส่งของสิ่งของ (Delivery and loading areas) ต้องแยกจุดที่รับส่งสิ่งของ ออกจากพื้นที่ที่มีอุปกรณ์ประมวลผลสารสนเทศ และดำเนินการแกะหีบห่อหรือตรวจสอบให้เสร็จสิ้น ก่อนนำเข้าสู่พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

- ด้านอุปกรณ์ (Equipment) วัตถุประสงค์เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อสินทรัพย์และป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

4.7 นโยบายการจัดตั้งและป้องกันอุปกรณ์ (Equipment siting and protection)

การจัดตั้ง หรือการจัดวางอุปกรณ์สินทรัพย์สารสนเทศ อุปกรณ์ใดที่มีความสำคัญสูงต้องจัดวางในที่ที่เข้าถึงได้ยาก

4.8 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

อุปกรณ์ที่มีความสำคัญสูงควรติดตั้งระบบป้องกันความล้มเหลวของอุปกรณ์ เช่น ระบบสำรองไฟฟ้า ระบบปรับอากาศ เป็นต้น

4.9 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

1) การเดินสายสัญญาณต้องแยกท่อเพื่อป้องกันสัญญาณรบกวน

2) ต้องมีการทำป้ายสายสัญญาณชัดเจน และเมื่อมีการเปลี่ยนแปลงต้องมีการปรับปรุงป้ายสายสัญญาณให้ถูกต้อง

4.10 นโยบายการบำรุงรักษาอุปกรณ์ (Equipment maintenance)

ต้องจัดให้มีการบำรุงรักษาอุปกรณ์เพื่อให้มีสภาพพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง หรือมากกว่าตามระดับความสำคัญ

4.11 นโยบายการนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of assets)

ห้ามนำสินทรัพย์สารสนเทศออกนอกพื้นที่ก่อนได้รับอนุญาตจากผู้รับผิดชอบ และต้องมีขั้นตอนในการตรวจสอบและติดตาม

4.11 ความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off- premises)

สินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยตามความเสี่ยง

4.12 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล หากไม่มีการใช้งานแล้วต้องทำลายให้สิ้นซาก โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

4.13 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)

ต้องป้องกันให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สินทรัพย์สารสนเทศที่ไม่มีผู้ดูแล

4.14 การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear desk and clearscreen policy)

เจ้าหน้าที่ต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญอันหนึ่งของระบบรักษาความมั่นคงปลอดภัย ความมั่นคงทางกายภาพรวมถึงการป้องกันสถานที่และอุปกรณ์ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติเช่น แผ่นดินไหว น้ำท่วมเป็นต้น การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจรอุณหภูมิ หรือความชื้น ในห้องควบคุมที่สูงเกินขีดจำกัด หรือการกระทำโดยประมาท เช่น การทำน้ำกรดโดนเครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ ดังนั้นจึงมีความจำเป็นในการป้องกันอาคารและอุปกรณ์โดยกำหนดเป็นนโยบายเพื่อถือปฏิบัติ ในเรื่องการสร้างห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายรวมถึงมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

1) จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ

เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้ โดยจัดแบ่งพื้นที่ ดังนี้

ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

– พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีเซิร์ฟเวอร์ ระบบเครือข่ายคอมพิวเตอร์ติดตั้งอยู่

2) การเข้าไปในพื้นที่ควบคุม

1. ผู้ยื่นคำขอ (พนักงานโรงงานไพ่) จะต้องกรอกแบบฟอร์มคำขอเข้าถึงห้องเครื่องคอมพิวเตอร์แม่ข่ายก่อนล่วงหน้าอย่างน้อย 1-2 วันทำการ เว้นในแต่กรณีเร่งด่วนดังนี้

- กรณีเกิดเหตุการณ์ฉุกเฉิน เช่น ภัยธรรมชาติ เหตุการณ์ทางการเมือง การขอเข้าตรวจตามกฎหมาย เป็นต้น
- เหตุขัดข้องทางไฟฟ้า
- เหตุขัดข้องด้านการสื่อสารของอุปกรณ์
- เหตุขัดข้องอุปกรณ์ภายในห้องเกิดความเสียหาย
- เหตุอื่น ๆ นอกเหนือจากนี้ หากเป็นกรณีเร่งด่วน อยู่ในดุลพินิจของผู้ดูแล

2. ผู้ยื่นคำขอ (พนักงานโรงงานไพ่) และผู้มาติดต่อ (บุคคลภายในหรือภายนอก) จะต้องรายงานตัวตามรายชื่อที่ระบุไว้ในแบบฟอร์ม โดยแสดงเอกสารประจำตัวที่ระบุตัวตนตามรายชื่อผู้ติดต่อ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับรถ หนังสือเดินทาง โดยเอกสารดังกล่าวจะต้องมีสถานะปกติ ไม่หมดอายุ พร้อมลงลายมือชื่อในเอกสารยืนยันการเข้าห้องเครื่องคอมพิวเตอร์แม่ข่าย นอกเหนือจากรายชื่อดังกล่าวจะไม่สามารถเข้าได้

3. ผู้ยื่นคำขอและผู้มาติดต่อ จะต้องนำสิ่งของต่าง ๆ และอุปกรณ์ที่ไม่เกี่ยวข้องฝากไว้ที่ห้องส่วนสารสนเทศและพัฒนาระบบ รวมถึงที่สิ่งของที่เข้าข่ายต้องห้ามดังนี้

- Smart Phone Tablet Smart Watch Smart Glasses
- หูฟัง ไมโครโฟนหรือชุดหูฟังที่มีไมโครโฟน หรืออุปกรณ์ที่มีความเกี่ยวข้อง
- อุปกรณ์สื่อสารด้วยคลื่นวิทยุทุกชนิด
- อุปกรณ์บันทึกภาพ เสียงและวิดีโอ หรืออุปกรณ์ที่มีความเกี่ยวข้อง
- อุปกรณ์บันทึกข้อมูลทุกชนิด หรืออุปกรณ์ที่มีความเกี่ยวข้อง
- คอมพิวเตอร์แบบพกพาทุกขนาด อุปกรณ์ต่อพ่วงอื่น ๆ หรืออุปกรณ์ที่มีความเกี่ยวข้อง
- อาวุธ ปืน ของแหลมหรือมีคม เชื้อเพลิง สเปรย์ฉีดพ่น สารที่ก่อให้เกิดก๊าซ วัตถุที่ก่อให้เกิดประกายไฟ
- อุปกรณ์ที่มีคลื่นแม่เหล็ก รังสี หรืออุปกรณ์ที่มีความเกี่ยวข้อง
- เครื่องมือช่างทุกชนิด หรืออุปกรณ์ที่มีความเกี่ยวข้อง
- อาหาร หมากฝรั่ง เครื่องดื่มหรือของเหลวทุกชนิด
- บุหรี่หรือบุหรี่ไฟฟ้า สารเสพติด สิ่งของผิดกฎหมาย
- แบตเตอรี่ ประเภทแบตเตอรี่สำรอง (Power Bank)
- ปรอทวัดความดันอากาศหรือปรอทวัดอุณหภูมิ
- สัมภาระทุกขนาด ทุกชนิด
- กระดาษ ปากกา สมุดบันทึก สติกเกอร์ เทปกาว หรืออุปกรณ์เครื่องเขียนที่เกี่ยวข้อง
- สิ่งของอื่น ๆ ให้อยู่ในดุลพินิจของผู้ดูแล

ข้อยกเว้นอื่น ๆ

- สัมภาระขนาดเล็กประเภทกระเป๋าเงินที่ไม่มีอุปกรณ์อิเล็กทรอนิกส์ และเก็บเหรียญเงิน บัตรต่าง ๆ ได้อย่างมิดชิด
- เครื่องประดับชิ้นเล็กจนถึงชิ้นใหญ่ เช่น ตุ้มหู แหวน สร้อยคอ เป็นต้น

- บัตรพนักงานที่มีสายคล้องคอ ต้องเก็บใส่กระเป๋าเสื้อด้านหน้า

ทั้งนี้หากสิ่งต้องห้ามดังกล่าว ไม่ได้ระบุอยู่ในคำขอพิเศษและได้รับการอนุมัติ จะไม่สามารถนำเข้าห้องได้ทุกกรณี

4. ห้ามแตะต้องหรือเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายโดยไม่ได้รับอนุญาตจากผู้ดูแล เว้นเฉพาะงานติดตั้งหรือบำรุงรักษาระบบเท่านั้น หากเกิดความเสียหายใด ๆ ผู้ยื่นคำขอและผู้มาติดต่อจะต้องเป็นผู้รับผิดชอบเพียงผู้เดียว

5. ระยะเวลาการใช้งานห้องเครื่องคอมพิวเตอร์แม่ข่าย

- วันและเวลาราชการ 8.30น. – 16.30น.
- กรณีมีความจำเป็นต้องเข้าใช้งานนอกช่วงเวลา ผู้ยื่นคำขอจะต้องระบุลงในแบบฟอร์มและระบุรายละเอียดของแผนงานพร้อมแนบเอกสารให้ครบถ้วน
- กรณีที่มีเหตุเร่งด่วนและจำเป็นตามข้อที่ 1 จะต้องแจ้งผู้ดูแลโดยทันที และขอให้บันทึกลงแบบฟอร์มตามภายหลังเป็นรายกรณี (หากไม่ดำเนินการ จะไม่สามารถเข้าครั้งต่อไปได้)

6. ผู้ยื่นคำขอและผู้มาติดต่อ จะต้องรักษาความสะอาด ความเป็นระเบียบเรียบร้อยภายในพื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่ายก่อนออกจากห้อง

7. ส่วนสารสนเทศและพัฒนาระบบ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงวิธีการ/ระเบียบการเข้าห้องเครื่องคอมพิวเตอร์แม่ข่าย โดยจะแจ้งให้ทราบผ่านช่องทาง Intranet ของโรงงานไพ่

3) การเข้าไปในพื้นที่จำกัดการเข้าถึง

– ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบหรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย และต้องมีผู้ดูแลระบบที่ได้รับมอบหมายอย่างน้อย 1 คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้งและให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

– ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า 15 ปี เข้าไปในพื้นที่จำกัดการเข้าถึง

– ไม่อนุญาตให้เข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

4) ด้านกายภาพของห้องควบคุมระบบ

– แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้เช่น router, switch, server, UPS เป็นต้น

– มี rack ในการจัดเก็บอุปกรณ์ต่างๆที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

– ตำแหน่งของการวางอุปกรณ์ต่างๆ ไม่ควรวางใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น

– การจัดวางสาย cable network สายไฟฟ้าควรติดป้ายชื่อสายต้นทางปลายทาง และเก็บสายให้เรียบร้อยเพื่อป้องการการเดินสะดุด

– ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

– มีระบบรักษาความมั่นคงปลอดภัยในห้องเช่น กล้อง CCTV ระบบการเข้าออกห้องโดยระบบ fingerprint scan หรือ RFID เป็นต้น

– มีระบบสังเกตการณ์อุณหภูมิภายใน rack ระบบแจ้งเตือนและป้องกันอัคคีภัย

– มีระบบสำรองไฟฟ้าเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติ และระบบสำรองไฟฟ้าอัตโนมัติ เป็นต้น

– มีระบบป้องกันกระแสไฟฟ้าจากฟ้าผ่า

– ระบบปรับอากาศแบบควบคุมอุณหภูมิ (50-80°F)

– ติดตั้งฉนวนกันไฟไหม้ ที่ฝ้าเพดานและกำแพง

5) การบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

– กรณีติดตั้งเซิร์ฟเวอร์หรืออุปกรณ์ต่างๆ ให้แกะหีบห่อและประกอบให้แล้วเสร็จจากภายนอกพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงก่อนนำไปติดตั้งเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

– กรณีที่จำเป็นต้องทำงานก่อสร้าง แก้ไข และติดตั้ง ในพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงต้องมีอุปกรณ์ควบคุม ฝุ่น ความร้อน เพื่อป้องกันความเสียหาย โดยผ่านความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนการปฏิบัติงาน

– ตรวจสอบความพร้อมของระบบรักษาความมั่นคงปลอดภัยทุก 3 เดือน

– ร่างขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟฟ้าลัดวงจร ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือมีผู้บุกรุก เป็นต้น

– ซ้อมการปฏิบัติงานตามแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน ทุก 1 ปี

– มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

6) แนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

– เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูล

– กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้ หรือใช้มาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายใช้ใหม่ได้	วิธีทำลาย	ระยะเวลาทำลาย
กระดาษ		- ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร	เก็บรักษาไว้อย่างน้อย 1 ปีหรือตามที่กฎหมายกำหนด
Flash Drive	ใช้วิธีการ Format	- ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย 1 ปีหรือตามที่กฎหมายกำหนด
แผ่น CD/DVD	ใช้วิธีการ Format	- ใช้การหั่น ตัด เผา ให้สิ้นสภาพการใช้งาน	เก็บรักษาไว้อย่างน้อย 1 ปีหรือตามที่กฎหมายกำหนด
เทป		- ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย	เก็บรักษาไว้อย่างน้อย 1 ปีหรือตามที่กฎหมายกำหนด

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายใช้ใหม่ได้	วิธีทำลาย	ระยะเวลาทำลาย
ฮาร์ดดิสก์	ใช้วิธีการ Format	- ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย 1 ปีหรือตามที่กฎหมายกำหนด

5. นโยบายความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

นโยบายการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management) วัตถุประสงค์เพื่อให้มีการป้องกันสารสนเทศในเครือข่าย และอุปกรณ์ประมวลผลสารสนเทศดังนี้

- ด้านมาตรการเครือข่าย (Network controls) กำหนดนโยบายการควบคุมการเข้าถึงเครือข่าย และบริการเครือข่ายให้มีความมั่นคงปลอดภัยโดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย และ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

5.1 นโยบายความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services) ผู้บริหารต้องมีการกำหนดระดับความต้องการสำหรับบริการเครือข่าย

5.2 นโยบายการแบ่งแยกเครือข่าย (Segregation in networks) ผู้ดูแลระบบต้องจัดแบ่งเครือข่ายระหว่างการใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับองค์กร โดยพิจารณาจากบริการเครือข่าย ระบบสารสนเทศ กลุ่มของผู้ใช้งานของทั้งสองฝ่าย

- ด้านการถ่ายโอนสารสนเทศ (Information transfer) วัตถุประสงค์เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

5.3 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures) การใช้บริการสารสนเทศจากหน่วยงานภายนอก ให้เป็นไปตามแนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

5.4 นโยบายข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer) การทำข้อตกลงต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

5.5 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements) ต้องจัดให้มีการลงนามในสัญญาระหว่างหน่วยงานและหน่วยงานภายนอก ว่าจะไม่เปิดเผยความลับ ของหน่วยงาน (Non-Disclosure Agreement : NDA)

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร

1) สิทธิการใช้เครือข่าย

– สิทธิการใช้เครือข่ายเป็นสิทธิพิเศษเฉพาะ (privilege) ที่องค์กร มอบให้บุคคลหรือหน่วยงานที่ได้รับสิทธิไม่สามารถโอนสิทธิให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

– ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้รายอื่น

– ผู้ใช้ต้องใช้ระบบเครือข่ายคอมพิวเตอร์ตามมารยาทและจรรยาบรรณของการใช้เครือข่ายตามที่องค์กรกำหนดและตามวิถีสากล

2) การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

– การใช้ระบบเครือข่ายคอมพิวเตอร์เพื่อกระทำสิ่งที่ผิดกฎหมาย
– การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี
– การเข้าถึงข้อมูลของผู้อื่นเพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต
– การเผยแพร่ข้อมูลของผู้ใช้หรือของหน่วยงานโดยไม่ได้รับอนุญาต
– การใช้งานที่เป็นสาเหตุให้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหายหรือมีผลต่อประสิทธิภาพการทำงานของระบบ
– การพยายามทำลายหรือทำลายระบบรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์
– การใช้หรือเผยแพร่ซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์
– การลักลอบดักจับข้อมูลในระบบเครือข่ายคอมพิวเตอร์
– การปลอมแปลงเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิดให้แก่ระบบคอมพิวเตอร์และผู้ใช้อื่น
– การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์หรือเครือข่ายอื่น
– การเผยแพร่และ/หรือการเข้าถึงสื่อลามกอนาจาร
– การเข้าใช้งานระบบเครือข่ายเพื่อความบันเทิง ส่วนบุคคลอันไม่เกี่ยวข้องกับหน้าที่การปฏิบัติงาน
– การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อเปิดให้บริการใดๆ โดยไม่ได้รับอนุญาต
– การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจ
– การนำไอพีแอดเดรสขององค์กรไปจดทะเบียนชื่อโดเมนอื่นนอกเหนือจากชื่อโดเมน playingcard.or.th โดยไม่ได้รับอนุญาต
– การใช้ระบบเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบายและระเบียบขององค์กร

3) การฝ่าฝืนระเบียบและการพิจารณาโทษ

– องค์กรจะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้นจากผู้ใช้และ/หรือบัญชีผู้ใช้
– ผู้ใช้ที่ฝ่าฝืนระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์จะถูกพิจารณาระงับและ/หรือยกเลิกบัญชีผู้ใช้
– ส่วนสารสนเทศและพัฒนาระบบจะแจ้งหน่วยงานต้นสังกัดเพื่อพิจารณาโทษแก่ผู้ใช้ที่ฝ่าฝืนระเบียบ

6. นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

- เกี่ยวกับขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities) มีวัตถุประสงค์เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

6.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

ต้องจัดทำคู่มือหรือขั้นตอนปฏิบัติงานที่เกี่ยวกับสารสนเทศที่สำคัญของหน่วยงาน เพื่อป้องกันการปฏิบัติงานด้านสารสนเทศที่ผิดพลาด

6.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)

กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ

6.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบ เช่น CPU Memory Hard disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต

6.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

ในระบบที่มีความสำคัญสูงควรแยกระบบการพัฒนา ออกจากระบบการให้บริการจริง เพื่อป้องกัน การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

- ด้านการป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware) วัตถุประสงค์เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

6.5 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

1) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องติดตั้งโปรแกรมป้องกันมัลแวร์และอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์

2) ผู้ใช้ต้องปรับปรุง Patch และ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลด Patch และ HotFix ต่างๆ จากเว็บไซต์เจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่ เป็นต้น

3) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องทดสอบมัลแวร์ (Virus Scanning) โดยโปรแกรมป้องกันมัลแวร์ก่อนการรับส่งข้อมูลทุกครั้ง

- ด้านการสำรองข้อมูล (Backup) วัตถุประสงค์เพื่อป้องกันการสูญหายของข้อมูล และให้มั่นใจว่าระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน

2.6.6 นโยบายการสำรองและกู้คืนข้อมูล (Information backup and recovery policy)

1) หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการสำรองข้อมูล ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

2) ต้องสำรวจข้อมูล และจัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล

3) ข้อมูลที่มีความสำคัญสูงต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกสำนักงาน

4) ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

5) ต้องทดสอบข้อมูลที่สำรองอย่างสม่ำเสมอ

6) ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

7) หากต้องมีการกู้คืนข้อมูลให้ดำเนินการกู้คืนข้อมูลตาม ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

- ด้านการบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring) วัตถุประสงค์เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

2.6.7 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging) สำนักบริการคอมพิวเตอร์ต้องจัดเก็บข้อมูลบันทึกกิจกรรมของผู้ใช้งาน เพื่อใช้ติดตามกรณีเกิดเหตุความมั่นคงปลอดภัย

2.6.8 การป้องกันข้อมูลล็อก (Protection of log information) อุปกรณ์บันทึกล็อกและข้อมูลการล็อกสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

2.6.9 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs) ต้องมีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ และมีการทบทวนอยู่เสมอ

2.6.10 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization) เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องต้องตั้งเวลาให้ตรงกันโดยเทียบเวลาจากระบบปรับเทียบเวลาขององค์กร

- ด้านการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)วัตถุประสงค์เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

2.6.11 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems) ต้องติดตั้งเฉพาะที่ซอฟต์แวร์ที่จำเป็นในการให้บริการ

- การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management) วัตถุประสงค์เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

2.6.12 นโยบายการจำกัดการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Restrictions on software installation)

1) ระบบที่ให้บริการต้องทำการ Patch ซอฟต์แวร์อย่างสม่ำเสมอ
2) ต้องทำการลบ User ที่ไม่จำเป็นออกจากระบบ เช่น Test
3) ต้องปิด Service ที่ไม่ได้ใช้งาน
4) ซอฟต์แวร์ใดไม่ได้ใช้งานต้องลบออก

2.6.13 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)ต้องติดตามข้อมูลทางด้านเทคนิคของช่องโหว่อย่างสม่ำเสมอ

- สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)วัตถุประสงค์เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบที่ให้บริการสารสนเทศ

2.6.14 มาตรการการตรวจประเมินระบบ (Information systems audit controls) ต้องวางแผนการตรวจสอบระบบ โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

1) การจัดสรรไอพีแอดเดรส

– ไอพีแอดเดรส 124.109.29.192/29 ของระบบเครือข่ายคอมพิวเตอร์เป็นสินทรัพย์ขององค์กร โดยองค์กร มอบอำนาจให้ส่วนสารสนเทศและพัฒนาระบบทำหน้าที่บริหารจัดการ

– ให้ส่วนสารสนเทศและพัฒนาระบบทำหน้าที่จัดสรรไอพีแอดเดรสให้กับหน่วยงานตามที่ร้องขอเพื่อให้ใช้งานได้อย่างเพียงพอและมีประสิทธิภาพ โดยส่วนสารสนเทศและพัฒนาระบบสามารถปรับเปลี่ยนไอพีแอดเดรสที่ได้จัดสรรให้กับหน่วยงานจากหมายเลขเดิมเป็นหมายเลขใหม่ได้ตามหลักวิชาการ เพื่อให้สามารถบริหารและจัดการได้อย่างมีประสิทธิภาพ

2) การจัดการชื่อโดเมน

– องค์กร ได้ขึ้นทะเบียนชื่อโดเมนขององค์กรภายใต้ชื่อ “playingcard.or.th” โดยส่วนบัญชีและการเงินรับภาระชำระค่าธรรมเนียม การขึ้นทะเบียนและค่าบำรุงรักษาชื่อโดเมน

– หน่วยงานมีสิทธิในการใช้ชื่อโดเมน playingcard.or.th โดยยื่นเรื่องขออนุมัติต่อผู้บริหารดิจิทัลหรือผู้บริหารระดับสูงสุด คำขออนุมัติจะต้องลงนามรับรองโดยผู้บริหารระดับสูงสุด

– โครงการพิเศษหรือโครงการใด ๆ ที่ได้รับอนุมัติจากองค์กรสามารถขอจดชื่อโดเมนประจำโครงการได้ โดยหากเป็นโครงการระดับหน่วยงานให้จดทะเบียนภายใต้ชื่อโดเมนย่อยประจำหน่วยงานนั้น หรือในกรณีที่เป็นโครงการระดับองค์กรจะสามารถยื่นขอจดชื่อโดเมนภายใต้ชื่อโดเมนขององค์กรได้

– กลุ่มกิจกรรมมีสิทธิในการขอใช้ชื่อโดเมนประจำกลุ่มกิจกรรมได้ โดยต้องมีหัวหน้ากลุ่มกิจกรรมและหัวหน้าหน่วยงานระดับฝ่ายหรือเทียบเท่าที่หัวหน้ากลุ่มกิจกรรมนั้นสังกัดอยู่ลงนามเห็นชอบ และยื่นเรื่องขออนุมัติต่อผู้บริหารระดับสูงสุด

– การใช้ไอพีแอดเดรสขององค์กร เพื่อจดทะเบียนชื่อโดเมนนอก สาระบบชื่อโดเมนขององค์กร โดยมิได้รับอนุญาตเป็นสิ่งต้องห้าม ยกเว้นกรณีมีเหตุผลความจำเป็นอย่างยิ่ง ทั้งนี้ให้หัวหน้าหน่วยงาน ดำเนินการยื่นคำร้องต่อผู้บริหารดิจิทัล หรือผู้บริหารระดับสูงสุด โดยชี้แจงเหตุผลและความจำเป็นที่ต้องขอจดทะเบียนชื่อโดเมนนอกสารระบบ การอนุมัติจดทะเบียนให้อยู่ในดุลยพินิจของผู้บริหารระดับสูงสุด

3) ข้อกำหนดการใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)

– ผู้ใช้มีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ ผู้ใช้ต้องรักษารหัสผ่านเป็นความลับเฉพาะตัวและไม่อนุญาตให้ผู้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี ผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์ และการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเอง

– ผู้ใช้พึงทราบว่าไม่มีสิทธิที่จะถามหรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

– ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

– การใช้จดหมายอิเล็กทรอนิกส์ ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

ก. การใช้จดหมายอิเล็กทรอนิกส์ เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น

ข. การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่จดหมายลูกโซ่

ค. การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลชั้นความลับขององค์กร

ง. การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลการประชุมของที่ประชุมผู้บริหารองค์กรหรือในการประชุมอื่นๆ โดยที่มิได้มีหน้าที่ หรือมิได้รับมอบหมายจากประธานในที่ประชุม

จ. การปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นๆ ส่งมาจากบุคคลอื่น

ฉ. การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

ช. การปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง

ซ. การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล

ฌ. การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโด เสียง ที่ดูหมิ่น เหยียดหยามหรือแบ่งแยกทาง ศาสนา เชื้อชาติ หรือเพศ

ญ. การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่มีลักษณะหยาบคายหรือลามกอนาจาร

ฎ. การส่งจดหมายอิเล็กทรอนิกส์ เพื่อเผยแพร่โปรแกรมหรืองาน หรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองาน ในลักษณะที่ละเมิดลิขสิทธิ์

ฏ. การส่งจดหมายอิเล็กทรอนิกส์ กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

ฐ. การส่งจดหมายอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบให้ระบบจดหมายอิเล็กทรอนิกส์ หรือเครือข่ายลดทอนประสิทธิภาพลง

ฑ. การส่งจดหมายอิเล็กทรอนิกส์ กระจายมัลแวร์หรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

4) การจัดการรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (Mailing List)

ส่วนสารสนเทศและพัฒนาระบบจัดให้มีระบบรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ เพื่อสร้างช่องทางการส่งจดหมายอิเล็กทรอนิกส์แบบกลุ่ม รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ที่บรรจุรายชื่อบัญชีผู้ใช้ที่ขึ้นทะเบียนในเครือข่ายขององค์กร หรือรายชื่อแยกตามกลุ่มขององค์กรเป็นข้อมูลปกปิดที่ไม่เผยแพร่ให้ผู้ใช้หรือหน่วยงานใดๆ การใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ดังกล่าวมีข้อกำหนดเฉพาะดังนี้

– หน่วยงานที่ได้รับมอบหมายจากผู้บริหารระดับสูงสุด ใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่ข่าวสารและประชาสัมพันธ์ภารกิจขององค์กร

– ส่วนสารสนเทศและพัฒนาระบบใช้เพื่อแจ้งเตือน หรือแจ้งข่าวที่เกี่ยวข้องกับความมั่นคงปลอดภัยหรือการรักษาประสิทธิภาพของระบบคอมพิวเตอร์และเครือข่าย

– ส่วนสารสนเทศและพัฒนาระบบจัดให้มีระบบรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์เพื่อรับข่าวสาร และผู้ใช้สามารถถอนการเป็นสมาชิกเพื่องดรับข่าวสารนั้นได้ตลอดเวลา ทั้งนี้ องค์กรไม่อนุญาตให้สร้างบริการรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์อื่นใดเอง เพื่อป้องกันการใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ที่บรรจุรายชื่อบัญชีจดหมายอิเล็กทรอนิกส์ โดยผู้ใช้ไม่สมัครใจบอกรับ ทั้งนี้ ส่วนสารสนเทศและพัฒนาสงวนสิทธิในการอนุมัติการขอจดทะเบียนชื่อกลุ่ม ตลอดจนการตั้งชื่อกลุ่ม ตามความเหมาะสม

5) โควตาบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีจดหมายอิเล็กทรอนิกส์ ของผู้ใช้แต่ละรายจะมีโควตากำหนดการใช้งานดังนี้

– ขนาดข้อมูลรวมที่เก็บในเซิร์ฟเวอร์
– ขนาดของไฟล์แนบต่อการส่งจดหมายอิเล็กทรอนิกส์ หนึ่งฉบับ
– จำนวนบัญชีผู้รับต่อการส่งจดหมายอิเล็กทรอนิกส์ หนึ่งฉบับ
– อัตราส่งจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนด
– จำนวนจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนด
– โควต้าเหล่านี้อาจแตกต่างกันตามประเภทและภารกิจของผู้ใช้ การกำหนดโควตาให้อยู่ในดุลยพินิจของผู้บริหารดิจิทัล โดยสามารถเพิ่มหรือลดค่าแต่ละบัญชีจดหมายอิเล็กทรอนิกส์ตามความเหมาะสมเพื่อให้การใช้งานและการบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ

6) การตรวจระวังระบบ

องค์กรมีนโยบายปกป้องข้อมูลส่วนบุคคลและให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนภารกิจขององค์กร โดยไม่ตรวจดูจดหมายอิเล็กทรอนิกส์ที่รับส่งตามปกติ แต่องค์กรมีภาระผูกพันตามกฎหมายที่ต้องติดตั้งระบบบันทึกข้อมูลจราจรและการเฝ้าระวังเพื่อคงไว้ซึ่งบริการที่มั่นคงปลอดภัยและมีประสิทธิภาพ องค์กรสงวนสิทธิในการใช้ระบบเฝ้าระวังเพื่อตรวจเนื้อหาจดหมายอิเล็กทรอนิกส์ที่เป็นภัยต่อระบบคอมพิวเตอร์และกลั่นกรองหรือระงับการเผยแพร่นั้นโดยอัตโนมัติ ตลอดจนสงวนสิทธิการเข้าถึงจดหมายอิเล็กทรอนิกส์เพื่อสืบสวน สอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้จดหมายอิเล็กทรอนิกส์ใดๆ หรือการร้องขอจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

7) การระงับบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่องค์กรเอื้ออำนวยให้ผู้ใช้ ซึ่งผู้ใช้ไม่สามารถโอนสิทธิให้แก่ผู้อื่นใช้ได้องค์กรคงไว้ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิให้แก่ผู้ใช้โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหา ความมั่นคงปลอดภัยหรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์ มีแนวปฏิบัติ ดังนี้

8) เมื่อผู้ใช้พ้นสภาพการอยู่ในสังกัดขององค์กร ส่วนสารสนเทศและพัฒนาระบบสามารถระงับบัญชีผู้ใช้ ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย

9) ผู้ใช้สามารถร้องขอการขยายสิทธิการใช้บัญชีผู้ใช้เพื่อคงสิทธิการใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้ เมื่อต้องพ้นสภาพการอยู่ในสังกัดขององค์กร โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัดพร้อมแนบเหตุผลความจำเป็นส่งถึงส่วนสารสนเทศและพัฒนาระบบ การอนุญาตและระยะเวลาการขยายสิทธิให้เป็นอำนาจของผู้บริหารดิจิทัล หรือผู้บริหารระดับสูงสุด

10) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งาน โดยคำร้องขอจากผู้บริหาร หากพบว่ามีการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้

11) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งานโดยทันทีโดยหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบให้ประสิทธิภาพระบบเครือข่ายด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้หรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้ ส่วนสารสนเทศและพัฒนาระบบมีสิทธิระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้นๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

12) สำรองและการกู้คืนข้อมูล การสำรองข้อมูล หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการคัดเลือกและจัดทำระบบสำรองข้อมูล โดยผู้ดูแลระบบมีหน้าที่ ดังนี้

- ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และจัดระดับความสำคัญของข้อมูล
- สำรวจข้อมูล และ จัดระดับความสำคัญในการสำรองข้อมูล ดังนี้

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
1	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
2	กระทบปานกลาง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
3	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
4	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

- ต้องจัดให้มีความถี่ในการสำรองให้พอเพียง ในระบบที่มีความสำคัญสูง เครื่องที่มีความสำคัญสูงควรเพิ่มความถี่การสำรองให้มากขึ้น ดังนี้

ก. เครื่องคอมพิวเตอร์แม่ข่าย (Server Computer)

ลำดับ	ระบบงาน	ข้อมูลที่สำรองข้อมูล	ความถี่ในการสำรองข้อมูล
1	ระบบสารบรรณอิเล็กทรอนิกส์	ค่า Configure ของระบบ E-doc , และฐานข้อมูล	1 เดือน/ครั้ง
2	ระบบ Windows Active Directory	ค่า configure ของระบบ AD	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
3	ระบบ Windows Active Directory สำรอง	ค่า configure ของระบบ AD (สำรอง)	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
4	ระบบบริหารทรัพยากรองค์การ (Production)	ค่า Configure ของระบบ Dynamic AX , และฐานข้อมูล	1 วัน/ครั้ง สำหรับฐานข้อมูล 1 เดือน/ครั้ง สำหรับ Full Backup
5	ระบบบริหารทรัพยากรองค์การ (Development)	ค่า Configure ของระบบ Dynamic AX , และฐานข้อมูล	1 วัน/ครั้ง สำหรับฐานข้อมูล 1 เดือน/ครั้ง สำหรับ Full Backup
6	ระบบสำรองข้อมูล VMware	Windows for VM	1 เดือน/ครั้ง
7	ระบบตรวจสอบ	ค่า configure , Logs	1 เดือน/ครั้ง

ข. อุปกรณ์ระบบเครือข่าย (Network)

ลำดับ	Network	ข้อมูลที่สำรองข้อมูล	ความถี่ในการสำรองข้อมูล
1	Router Mikrotik RB2011UiAS-RM	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
2	Router Mikrotik RB951Ui-2HnD	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
3	Router Cisco RV130W	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
4	Router TP LINK TL-WA801ND	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
5	Router Cisco 1921	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
6	Load Balance Murhroom Truffle	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
7	Wireless Access Point Cisco Aironet 1830	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
8	Core Switch Amer Switch SS3GR1050i	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
9	FireWall Hillstone SG-6000-T1860	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง

ลำดับ	Network	ข้อมูลที่สำรองข้อมูล	ความถี่ในการสำรองข้อมูล
10	FireWall Clavister E80	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
11	Corero IPS5500-500EC External IPS / Hillstone S1060	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
12	Corero IPS5500-150EC Internal IPS / Hillstone S600	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง
13	WapApp Firewall WAPPLES 100 Eco	ค่า configure , Logs	หลังการเปลี่ยนแปลง , 1 เดือน/ครั้ง

– ต้องจัดทำผังหรือขั้นตอนการสำรองข้อมูล
– ต้องทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
– ต้องจัดทำบันทึกการสำรองข้อมูล และตรวจสอบว่าการสำรองข้อมูลสำเร็จหรือไม่ แก้ไข และรายงานต่อผู้บังคับบัญชา
– ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานในระบบที่มีความสำคัญระดับสูง
– ต้องจัดให้มีการเข้ารหัสข้อมูลที่มีระดับความสำคัญสูง (Encrypted backup) โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
– ต้องดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา หรือ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้
– เป็นผู้กำหนดชนิด เช่น Full หรือ Incremental และช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล
– ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

13) การกู้คืนข้อมูล ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ผู้ดูแลระบบมีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงาน ต่อผู้บังคับบัญชา ดังนี้
– ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ
– หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์
– สาเหตุและวิธีการกู้คืน

สาเหตุ	วิธีการ
กรณีที่ 1 เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับ (Source code) ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด
กรณีที่ 2 เกิดความเสียหายขึ้นกับฐานข้อมูล (Database)	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด
กรณีที่ 3 เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ฮาร์ดแวร์ยังคงทำงานปกติ	ดำเนินการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจากโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด
กรณีที่ 4 เกิดความเสียหายขึ้นกับฮาร์ดแวร์	ให้บริษัทผู้ดูแลแก้ไขเบื้องต้นให้ฮาร์ดแวร์สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับระบบปฏิบัติการและระบบงาน ให้บริษัทหรือผู้ได้รับมอบหมายดำเนินการติดตั้งระบบปฏิบัติการและระบบงานนั้นใหม่ โดยใช้โปรแกรมต้นฉบับ ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

14) การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) หน่วยงานที่รับผิดชอบระบบสารสนเทศมีหน้าที่

– ต้องจัดทำแผนความพร้อมกรณีฉุกเฉิน โดยแผนความพร้อมกรณีฉุกเฉินต้องได้รับการเห็นชอบจากผู้บริหาร ประกอบด้วย

ก. การกำหนดชนิดของภัยพิบัติ

ข. ประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีระดับความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้

ค. กำหนดขั้นตอนรับมือภัยพิบัติ

ง. มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

จ. มีการกำหนดช่องทางในการติดต่อกับผู้ใช้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่ต้องติดต่อผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วนเป็นต้น

ฉ. การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่

– ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

– ทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ 1 ครั้ง

15) การดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศหากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องตอบสนองต่อเหตุการณ์อย่างทันท่วงที ดังนั้นจึงต้องมีแนวปฏิบัติเมื่อเกิดเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

16) ระบบไฟร์วอลล์

– ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละครั้ง

– ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ สิ่งที่ต้องตรวจสอบ มีดังต่อไปนี้

ก. กลุ่มข้อมูล (Packet) ที่ไฟล์วอลล์ได้ปิดกั้น

ข. ลักษณะของกลุ่มข้อมูล (Packet) ที่ถูกปิดกั้น

ค. หมายเลขไอพี ของเครือข่ายใดที่ถูกปิดกั้น เป็นจำนวนมาก

– หากตรวจสอบพบการโจมตี หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศให้แจ้งผู้บังคับบัญชาเพื่อตัดสินใจดำเนินการแก้ไขปัญหา หากไม่สามารถแก้ไขปัญหาได้ให้รายงานต่อบริหารด้านดิจิทัล

– กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

17) เครื่องคอมพิวเตอร์แม่ข่าย ต้องตรวจสอบความมั่นคงปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายก่อนเปิดให้บริการ โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

– ติดตั้งไฟล์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เปิดเฉพาะ port ที่ใช้งาน

– ปิด Service ที่ไม่ได้ใช้งาน

– ติดตั้ง NTP เพื่อเทียบเวลาให้ถูกต้อง

– จำกัดการเข้าถึงจาก root หรือ Administrator โดยตรง

– หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และกำหนดผู้ดูแลรับผิดชอบหลัก และผู้รับผิดชอบสำรอง

– หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบความมั่นคงปลอดภัย ต้องจดบันทึก ตรวจสอบแก้ไขและรายงาน เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยต่อผู้บังคับบัญชา

– ต้องตรวจสอบ แก้ไข และรายงานช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายต่อผู้บังคับบัญชา

– กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ต้องดำเนินการแจ้งไปยังผู้รับผิดชอบหน่วยงาน หรือผู้มีอำนาจที่ได้รับมอบหมาย ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

18) ภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต ประกอบด้วย มัลแวร์ หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

– องค์กรต้องดำเนินการจัดหาซอฟต์แวร์เพื่อป้องกัน

– หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต ต้องดำเนินการติดตั้งโปรแกรมป้องกันภัยคุกคามทางอินเทอร์เน็ต และต้องตั้งให้ Update อย่างน้อยสัปดาห์ละครั้ง

– ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของของอุปกรณ์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

ก. การคุกคามทางอินเทอร์เน็ตใดที่มีเป็นจำนวนมาก

ข. ถูกส่งมาจากที่ใด และถูกส่งไปยังที่ใด

– ต้องศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่มีภัยคุกคามทางอินเทอร์เน็ต โดยเฉพาะที่ตรวจพบว่ามีการกระจายภายในเครือข่ายองค์กร

– กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที โดยแบ่งระดับความรุนแรงดังนี้

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
1	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
2	กระทบปานกลาง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
3	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
4	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

7. นโยบายการจัดหาและการพัฒนา ระบบเทคโนโลยีสารสนเทศ (System acquisition and development)

เพื่อให้สามารถนำเทคโนโลยีดิจิทัลมาสนับสนุนการดำเนินงานด้านธุรกิจ (Business) ของโรงงานไพ่ฯ ให้เกิดประสิทธิภาพและประสิทธิผลอย่างสูงสุดต่อองค์กร สามารถช่วยแก้ไขปัญหาในการลงทุนด้านเทคโนโลยีดิจิทัลที่ซ้ำซ้อน เกิดความจำเป็น ไม่สอดคล้องกับทิศทางการดำเนินงานขององค์กร ข้อมูลที่ไม่เป็นมาตรฐานเดียวกัน และขาดการบูรณาการทำงานร่วมกันอย่างเป็นระบบ โรงงานไพ่ฯ ขอออกประกาศแนวทางปฏิบัติเพื่อให้ส่วนงานต่าง ๆ ดำเนินงานได้อย่างเป็นเอกภาพ และเกิดผลสัมฤทธิ์ที่ดี ดังนี้

1) การพัฒนาด้านเทคโนโลยีดิจิทัลในด้านต่าง ๆ จะต้องมีความสอดคล้องกับวิสัยทัศน์ (Vision) พันธกิจ (Mission) และวัตถุประสงค์เชิงยุทธศาสตร์ (Strategy Objective) ของโรงงานไพ่ฯ รวมทั้งเป็นไป ตามกรอบสถาปัตยกรรมองค์กรในอนาคตของโรงงานไพ่ฯ ตามที่กำหนด

2) การลงทุนด้านเทคโนโลยีดิจิทัลจะต้องไม่เป็นการลงทุนที่ซ้ำซ้อน มีความคุ้มค่า และเกิดประโยชน์ต่อองค์กรอย่างสูงสุด

3) การบริหารจัดการด้านเทคโนโลยีดิจิทัลจะต้องคำนึงถึงความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล

4) การรักษาข้อมูลส่วนบุคคล การรักษาความลับของทางราชการ การไม่ละเมิดทรัพย์สินทางปัญญาและการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งผลกระทบในด้านอื่น ๆ ที่จะส่งผลต่อองค์กร

แนวปฏิบัติการจัดหาและการพัฒนา ระบบเทคโนโลยีสารสนเทศ

ในการจัดทำนโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีดิจิทัล มีวัตถุประสงค์เพื่อให้มั่นใจว่าทรัพยากรเทคโนโลยี สารสนเทศ มีความเพียงพอ รวมทั้งการจัดการความเสี่ยงอันเกี่ยวเนื่องจากการขาดทรัพยากร ในการดำเนินงานทางด้านเทคโนโลยีดิจิทัล โรงงานไพ่ มีแนวปฏิบัติดังนี้

1) พิจารณาและกำหนดกลยุทธ์ทางด้านเทคโนโลยีดิจิทัลสำหรับปัจจุบัน และในอนาคตทางเลือกต่าง ๆ สำหรับการจัดหาทรัพยากรทางด้านเทคโนโลยีดิจิทัล และการพัฒนาทรัพยากรสารสนเทศให้เพียงพอต่อ ความต้องการในปัจจุบันและอนาคต รวมทั้งทางเลือกเกี่ยวกับแหล่งที่มาของทรัพยากรสารสนเทศ และกลยุทธ์ ในการจัดหาทรัพยากร

2) กำหนดหลักเกณฑ์เพื่อใช้เป็นแนวทางในการจัดสรรและบริหารทรัพยากรสารสนเทศ รวมทั้งขีดความสามารถ เพื่อให้หน่วยงานเทคโนโลยีดิจิทัลสามารถตอบสนองตามความต้องการขององค์กรตามระดับขีดความสามารถ และสมรรถนะที่ต้องการ ระดับความเร่งด่วนในการใช้งาน และข้อจำกัดด้านงบประมาณ

3) เพื่อเป็นการวางแผนในการจัดสรรทรัพยากรอย่างคุ้มค่า และลดความเสี่ยงที่อาจเกิดขึ้น การจัดทำแผนการจัดสรรทรัพยากรสารสนเทศ ต้องพิจารณาให้เหมาะสมกับโครงสร้างองค์กร และสอดคล้องกับจัดสรรทรัพยากรขององค์กร รวมทั้งการบริหารทรัพยากรบุคคลโดยรวมขององค์กรด้วย

8. นโยบายการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident problem Management)

การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) มีวัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

2.8.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures) ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน และมีความเป็นระบบระเบียบที่ดี โดยให้เป็นไปตามแนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

2.8.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events) ต้องกำหนดช่องทางการติดต่อเพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยอย่างชัดเจน

2.8.3 การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses) หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องรายงานเหตุการณ์ดังกล่าวต่อผู้รับผิดชอบ

2.8.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events) ก่อนการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยต้องตรวจสอบให้ชัดเจน

2.8.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents) กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

2.8.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents) ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อจะได้เรียนรู้และเตรียมการป้องกัน

2.8.7 การเก็บรวบรวมหลักฐาน (Collection of evidence) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

แนวปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ

การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศหน่วยงานที่รับผิดชอบระบบสารสนเทศมีหน้าที่

1) ต้องจัดทำแผนความพร้อมกรณีฉุกเฉิน โดยแผนความพร้อมกรณีฉุกเฉินต้องได้รับการเห็นชอบจากผู้บริหารประกอบด้วย

- การกำหนดชนิดของภัยพิบัติ
- ประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีระดับความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้
- กำหนดขั้นตอนรับมือภัยพิบัติ
- มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

– มีการกำหนดช่องทางในการติดต่อกับผู้ใช้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่ต้องติดต่อผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

– การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่

– ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

– ทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ 1 ครั้ง

2) แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

– ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

– ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่าย ผ่านระบบอินเทอร์เน็ต (Internet)

– ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

– ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

– ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

– การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

ก. ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

ข. ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

ค. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

– ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security audit and assessment) ที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ 1 ครั้ง

– ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายใน (Internal Auditor) ขององค์กร

– กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

3) มาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

– ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

– ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น สำหรับให้ผู้ตรวจสอบใช้งาน และควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้แหล่งจัดเก็บข้อมูลอื่นที่มีข้อกำหนดการเข้าถึงข้อมูล

– กำหนดให้ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

– กำหนดให้เฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อก แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

– ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาตโดยมีการป้องกันเป็นอย่างดี

4) ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ “ผู้บริหารระดับสูงสุด” เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นโดยตรง รวมถึงในกรณีที่มีการร้องเรียน และฟ้องร้องภายใต้กฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

5) ต้องสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันที่เหมาะสม

6) รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศปีละ 1 ครั้ง เสนอต่อคณะอนุกรรมการด้านเทคโนโลยีสารสนเทศ และแจ้งคณะกรรมการบริหารความเสี่ยงขององค์กรเพื่อดำเนินการต่อไป

7) แสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศผ่านเว็บไซต์ ให้ประชาคมขององค์กรทราบ ตามนโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

9. นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

- การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) มีวัตถุประสงค์เพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์กรที่เป็นผลมาจากวิกฤตหรือภัยพิบัติหนึ่ง

2.9.1 นโยบายการวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity policy)

ผู้ดูแลระบบต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

2.9.2 นโยบายตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk assessment information policy)

ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง ตามแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.9.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ 1 ครั้ง

2.9.4 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ต้องกำหนดสถานการณ์หรือสภาวะฉุกเฉิน และจัดระดับความรุนแรงภัยพิบัติ พร้อมแผนรองรองรับเพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย

- การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies) วัตถุประสงค์เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

2.9.5 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities) อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

แนวปฏิบัติการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

1) การวิเคราะห์เหตุการณ์ภัยพิบัติ คือการวิเคราะห์เหตุการณ์ภัยพิบัติภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศ หรือส่งผลให้องค์กรไม่สามารถดำเนินกิจการได้อย่างปกติ จำแนกเป็น 2 กลุ่มหลักๆ ได้แก่

– ภัยพิบัติจากภายนอก

ก. ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องแม่ข่าย ได้แก่ ภัยพิบัติอัคคีภัย อุทกภัย การจลาจล ชุมนุมประท้วง แผ่นดินไหว ฯลฯ

ข. ระบบเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

ค. การบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยีสารสนเทศจากภายนอก เพื่อสร้างความเสียหายหรือทำลายระบบข้อมูล

ง. ระบบกระแสไฟฟ้าขัดข้อง /ไฟฟ้าดับ /ไฟกระชาก

จ. มัลแวร์คอมพิวเตอร์

ฉ. เหตุการณ์โรระบาด หรือโรคติดต่อร้ายแรง ที่ส่งผลกระทบต่อการปฏิบัติงาน

– ภัยพิบัติจากภายใน

ก. ระบบเครื่องแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย ถูกทำลาย

ข. มัลแวร์คอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

ค. เจ้าหน้าที่หรือบุคลากรขององค์กร ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย

2) การประเมินสถานการณ์และกำหนดระดับความรุนแรง

เมื่อองค์กร มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรง ภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัยจัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ โดยเจ้าหน้าที่ศูนย์สารสนเทศนำมาสรุปเป็นข้อมูล ดังนี้

สถานการณ์หรือสภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)			จัดเรียงลำดับ	
	ต่อระบบงาน	ต่อพันธกิจ	ต่อประชาชน	รวม	จัดลำดับ
กรณีไฟไหม้	5	5	5	15	1
กรณีอุทกภัย	5	5	3	13	2
กรณีโดนแทรกแซงระบบ	5	4	3	12	3
กรณีไฟฟ้าดับ	5	3	2	10	4
กรณีแผ่นดินไหว	3	2	3	8	5
กรณีจลาจล การชุมนุม / เหตุการณ์ความไม่สงบ	2	2	3	7	6
โรคระบาด	2	2	1	5	7

3) ขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินหรือผิดปกติ

ส่วนงานสารสนเทศและพัฒนาระบบ ได้จัดเตรียมคู่มือเมื่อเกิดเหตุการณ์ฉุกเฉินหรือผิดปกติในองค์กร โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆ ที่เกิดขึ้น รวบรวมเหตุการณ์การระบุที่มาของผู้บุกรุก เพื่อให้

สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองงานเพื่อใช้งาน และเพื่อใช้ในการกู้คืนระบบ ดังนี้

– การจัดเตรียมอุปกรณ์ โดยส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นหน่วยงานหลักที่ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย คอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ดังนี้

ก. เครื่องคอมพิวเตอร์ PC/เครื่องคอมพิวเตอร์ Notebook
ข. แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการของเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
ค. อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ
ง. โปรแกรมการประชุมออนไลน์
จ. โปรแกรม antivirus
ฉ. Driver อุปกรณ์ต่างๆ
ช. ระบบสำรองไฟฟ้าอัตโนมัติ
ซ. อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

– การสำรองข้อมูล เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหายถูกทำลายจากมัลแวร์หรือผู้บุกรุก แทรกแซง เปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้โดยองค์กรมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์และแผนการสำรองข้อมูล ดังนี้

ก. การสำรองข้อมูลเว็บไซต์และระบบงานต่างๆ
ข. การสำรองข้อมูลเครือข่าย (Configuration)

– การป้องกันและกำจัดมัลแวร์ มีการติดตั้งซอฟต์แวร์ป้องกันและกำจัดมัลแวร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ ลูกข่ายที่เชื่อมต่อในระบบเครือข่าย โดยผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะใน การเชื่อมต่ออินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

– การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

ก. กำหนดมาตรการควบคุมการเข้า – ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้องควบคุมจะมีกุญแจ และ keycard ส่วนกลางเพียง 1 ชุดเท่านั้น กรณีที่ผู้เกี่ยวข้องต้องการเข้าไปใน ห้องควบคุมต้องลงชื่อเบิกกุญแจ และ keycard ในสมุดควบคุมการเข้า - ออก ห้ามบุคคลที่ไม่มีอำนาจหน้าที่ เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้ผู้ดูแลระบบ เป็นผู้รับผิดชอบพาเข้าไปในห้องควบคุมมีการติดตั้งกล้องโทรทัศน์วงจรปิด

ข. มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้โดยกำหนดให้ Firewall ควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ในระบบเครือข่าย และเปิดใช้งานตลอดเวลา

ค. มีการติดตั้ง IPS (Intrusion Prevention System) เพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้ายๆกับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้อง อาศัยโปรแกรมหรือ Hardware ตัวอื่นๆ

ง. มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติเพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป

จ. การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์โดยได้จัดหาระบบบริหาร จัดเก็บ

ข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้า ระวังในครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายขององค์กร คุณภาพสิ่งแวดล้อมให้ดียิ่งขึ้น

– การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว จลาจล ชุมนุมประท้วง โดยเตรียมอุปกรณ์ดังนี้

ก. เตรียมอุปกรณ์ยังชีพ เช่น ยารักษาโรคฯลฯ และแจ้งให้ทุกคนทราบถึงแหล่งที่เก็บ

ข. ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

ค. ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน

– การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยี สารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ได้กำหนดแนวทาง ดังนี้

ก. ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่าย ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 120 นาที ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์ ส่วนบุคคล ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 15 นาที

ข. เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

ค. เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

– การจัดเตรียมอุปกรณ์และระบบเพื่อสนับสนุนการปฏิบัติงานนอกสถานที่ หรือปฏิบัติงานจากที่บ้าน

ก. จัดทำทะเบียนผู้ปฏิบัติงานที่สามารถปฏิบัติงานจากที่บ้าน หรือนอกสถานที่ได้

ข. จัดเตรียมอุปกรณ์ ที่รองรับการปฏิบัติงานนอกสถานที่ประกอบด้วยโน้ตบุ๊ค และอุปกรณ์ต่อพ่วง

ค. จัดเตรียมทะเบียนระบบเครือข่าย ที่สามารถให้ผู้ปฏิบัติงานนอกสถานที่สามารถเข้าถึงการใช้งานได้ พร้อมระบุระบบงานที่อนุญาตให้ผู้ใช้งาน เข้าถึงระบบปฏิบัติการจากนอกสถานที่ได้

ง. ทดสอบความพร้อมของระบบเครือข่าย ที่ใช้ในการปฏิบัติงานนอกสถานที่

4) การเตรียมความพร้อม และแผนปฏิบัติ ฉุกเฉิน

– การเตรียมความพร้อมกรณีเกิดการแทรกแซงเว็บไซต์ เมื่อเกิดเหตุโจมตี บุกรุก ผ่านทางเว็บไซต์ มีขั้นตอนการดำเนินการดังนี้

ก. สกัดกั้นการเข้าถึงเครื่องให้บริการ เพื่อไม่ให้เกิดการเปลี่ยนแปลงของข้อมูล ด้วยการถอดสาย Network ออกจากเครื่อง

ข. ตรวจสอบความเปลี่ยนแปลงของข้อมูลในระบบ

ค. ตรวจสอบ Log File หรือ แฟ้มกิจกรรมของระบบ เพื่อดูพฤติกรรมที่น่าสงสัย

ง. ดำเนินการปิดช่องโหว่บนหน้าเว็บไซต์โดยให้คำนึงถึงสิ่งต่างๆ ประกอบด้วย การตรวจสอบการป้อนข้อมูล SQL Injection XSS (Cross Site Scripting)

หากไม่สามารถดำเนินการแก้ไขได้โดยเร็ว ให้ทำการปิดการใช้งานในส่วนที่เกิดปัญหาก่อนปรับปรุงซอฟต์แวร์ที่เกี่ยวข้องให้เป็นรุ่นล่าสุดที่มีความมั่นคงปลอดภัยสูง

– แผนปฏิบัติกรณีเกิดการแทรกแซงเว็บไซต์

ก. เจ้าหน้าที่ได้รับแจ้งทางอีเมลหรือโทรศัพท์ว่า เว็บไซต์ ถูกแทรกแซงเปลี่ยน หน้าเว็บไซต์

ข. ทดลองเข้าเว็บไซต์ เพื่อตรวจสอบหน้าเว็บไซต์อีกครั้ง

ค. หลังจากตรวจสอบเป็นที่แน่ชัดว่าหน้าเว็บไซต์ถูกเปลี่ยนแปลง ให้รีบเก็บหลักฐานโดยการ copy หน้าเว็บไซต์ไว้

ง. ติดต่อส่วนสารสนเทศและพัฒนาระบบ เพื่อแจ้งเหตุและดำเนินการตัดการเชื่อมต่อจาเครือข่ายอินเตอร์เน็ตชั่วคราวเพื่อดำเนินการแก้ไข

จ. ตรวจสอบหาร่องรอยการเข้าโจมตี ตรวจสอบ log เพื่อหา IP ที่เข้าเปลี่ยนหน้าเว็บไซต์

ฉ. แก้ไขข้อบกพร่อง ช่องโหว่ทางเครือข่าย ที่เป็นสาเหตุให้ถูกโจมตี เปลี่ยน Password การเข้าใช้เครื่องแม่ข่ายหากจำเป็น

ช. เปลี่ยนหน้าเว็บไซต์กลับเป็นแบบเดิมพร้อมเชื่อมต่อเครือข่ายอินเตอร์เน็ต เข้ากับเครื่องให้บริการเว็บไซต์ เปิดการเชื่อมต่อให้สามารถใช้งานเครื่องแม่ข่ายได้ตามปกติ

ซ. กรณีเกิดความเสียหายร้ายแรง ให้นำหลักฐานที่ได้ทั้งหมดเข้าแจ้งความกับตำรวจ

5) การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากกรณีไฟฟ้าดับ ไฟกระชาก กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศฯดังนี้

– เปิดเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ 120 นาที

– เปิดเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ลูกข่าย ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ 15 นาที

– เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และ บำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

– เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกขอมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

– กำหนดให้มีการสำรองฐานข้อมูล และระบบงานต่างๆ ทุก 1 เดือนเป็นอย่างน้อย

6) การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว เตรียมความพร้อม โดยติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น ดังนี้

– ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้องและข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์/แอปพลิเคชั่น ของหน่วยงานต่างๆ เช่น กรมอุตุนิยมวิทยา ศูนย์เตือนภัยพิบัติแห่งชาติกรมป้องกันและบรรเทาสาธารณภัย

– การเตรียมบุคลากร วัสดุอุปกรณ์สถานที่อพยพ

ก. ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหว

ข. ประสานการเตรียมการกับหน่วยงานที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุอุปกรณ์ต่างๆ ตามความจำเป็นและเหมาะสม

ค. สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวกอาหาร และน้ำดื่ม สาหรับบุคลากรขององค์กร

ง. จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่างๆ

– การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางองค์กรให้ดำเนินการแก้ไขเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน อบรม ให้ความรู้เกี่ยวกับการปฏิบัติเมื่อเกิดแผ่นดินไหว แก่เจ้าหน้าที่ บุคลากรภายในองค์กร

7) การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจลเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล

– ดำเนินการค้นหาข่าวจากแหล่งข่าวต่างๆ เช่น ตำรวจ นักข่าว โทรทัศน์วิทยุและหน่วยงานที่เกี่ยวข้อง

– จัดเตรียมกำลังเจ้าหน้าที่ วัสดุอุปกรณ์เครื่องมือเครื่องใช้ระบบการสื่อสาร ยานพาหนะ และมอบหมายหน้าที่ความรับผิดชอบ

– ติดตั้งระบบกล้องวงจรปิดเพื่อรักษาความปลอดภัย

8) การเตรียมความพร้อมในการเสริมสร้างความมั่งคงปลอดภัยให้กับระบบระบบเครือข่าย ติดตั้งโปรแกรมสำหรับติดตามการทำงานของระบบคอมพิวเตอร์ และบริหารจัดการอุปกรณ์เครือข่าย เพื่อตรวจสอบสถานะของอุปกรณ์เครือข่ายในระบบ ซึ่งจะช่วยให้ผู้ดูแลระบบนั้นสามารถที่จะพบปัญหาหรือตรวจสอบปัญหาได้อย่างรวดเร็ว

– การใช้งานโดยทั่วไปสำหรับผู้ใช้งานเครือข่าย

ก. จัดให้มีการอบรมเพื่อเสริมสร้างสมรรถนะในการใช้งานเทคโนโลยีสารสนเทศ เพื่อพัฒนาทักษะความรู้ ความเข้าใจ ในด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรของกรมส่งเสริมคุณภาพสิ่งแวดล้อม เพื่อให้เจ้าหน้าที่ที่ได้รับการฝึกอบรมสามารถนำไปใช้ในการปฏิบัติงานได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น

ข. สร้างความรู้ ความเข้าใจ แก่เจ้าหน้าที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ให้มีความตระหนักในการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย โดยกำหนดให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ดังนี้

- ผู้ใช้งาน ปฏิบัติตามแนวทางการใช้งานหรือห้ามใช้งานโปรแกรมคอมพิวเตอร์
- ผู้ใช้งาน ปฏิบัติตามเงื่อนไขการใช้งานและไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น
- ผู้ใช้งาน ต้องกำหนดหรือใช้งานรหัสผ่าน
- ผู้ใช้งาน ต้องตรวจสอบและป้องกันมัลแวร์
- ผู้ใช้งาน ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การขโมย การสูญหาย หรือการเสียหายของข้อมูล เอกสาร คอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ขององค์กร
- ผู้ใช้งานป้องกันอุปกรณ์หรือเครื่องคอมพิวเตอร์แบบพกพาซึ่งสินtเป็นขององค์กร
- ผู้ใช้งานทำบันทึกข้อความขอใช้งาน VPN เพื่อขออนุมัติจาก ผู้บริหารด้านดิจิทัล สำหรับการเข้าถึงระบบงานขององค์กร จากระยะไกล โดยต้องแสดงเหตุผลหรือความจำเป็นในการใช้งาน พร้อมระบุระยะเวลาการใช้งานตามที่ต้องการ
- ผู้ใช้งาน ห้ามใช้งานระบบเทคโนโลยีสารสนเทศ อินเทอร์เน็ต และเครือข่ายขององค์กร ในลักษณะที่ผิดวัตถุประสงค์
- ผู้ใช้งาน ใช้ระบบงานอีเมล์ในการจัดการกับข้อมูลขององค์กร ตามชั้นความลับ
- ผู้ใช้งานข้อมูล ปฏิบัติตามแนวปฏิบัติในการบริหารจัดการข้อมูลตามระดับชั้นความลับ ที่องค์กร ได้กำหนดไว้

- เมื่อผู้ใช้งานพบเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัย ให้รีบแจ้งไปยังส่วนสารสนเทศโดยทันทีที่พบเห็น
- ผู้บังคับบัญชา ต้องดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ลาออกก่อนวันที่มาปฏิบัติงานวันสุดท้ายเพื่อดูว่ายังอยู่ในสภาพที่ใช้งานได้ตามปกติหรือไม่ หากเกิดการชำรุดหรือเสียหาย ให้ตรวจสอบว่าเป็นการเสียหายตามสภาพการใช้งานหรือไม่ หากเป็นการชำรุดหรือเสียหายโดยประมาทหรือเลินเล่อ ให้แจ้งหน่วยงานพัสดุเพื่อดำเนินการสอบสวนต่อไป

– การใช้งานเครือข่าย สำหรับผู้ดูแลระบบ กำหนดให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย สารสนเทศ ดังนี้

ก. ผู้รับผิดชอบระบบสารสนเทศ ต้องบริหารจัดการความมั่นคงปลอดภัยบนเครือข่ายขององค์กร

ข. ผู้รับผิดชอบระบบสารสนเทศ กำหนดมาตรการความมั่นคงปลอดภัยสำหรับการใช้งาน VPN เพื่อเข้าถึงระบบงานขององค์กร จากระยะไกล

ค. ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการเข้าถึงและใช้งานระบบเครือข่ายไร้สายภายใน องค์กรควรตรวจสอบข้อมูลที่รับ-ส่ง มาจากระบบเครือข่าย

– การใช้งานเครือข่าย สำหรับผู้ใช้งาน ส่วนสารสนเทศและพัฒนาระบบได้ดำเนินการติดตั้งโปรแกรมป้องกันและกำจัดมัลแวร์ให้กับเครื่องคอมพิวเตอร์ลูกข่ายภายในองค์กรโปรแกรมป้องกันและกำจัดมัลแวร์จะทำการสแกนข้อมูลที่มีการรับ ส่งผ่านเครือข่ายก่อนมีการใช้งาน โดยแจ้งให้ผู้ใช้งานปฏิบัติดังนี้

ก. ไม่ควรเปิดให้ผู้อื่นสามารถเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์

ข. ไม่ควรเปิดการเข้าถึงข้อมูลในเครื่องแบบ Full Control

ค. ควรตรวจสอบข้อมูลที่รับ-ส่ง มาจากระบบเครือข่าย

ง. ไม่ควรทำการ Download ข้อมูลใดๆ จากเครือข่ายภายนอก

– การเตรียมความพร้อมในการดำเนินการเกี่ยวกับโปรแกรมป้องกันและกำจัดมัลแวร์

ก. ดำเนินการติดตั้งโปรแกรมป้องกันและกำจัดมัลแวร์ โดยติดตั้งโปรแกรมป้องกันและกำจัดมัลแวร์ให้กับเครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องภายในองค์กรอย่างเพียงพอและได้ต่ออายุลิขสิทธิ์ของโปรแกรมทุกปี

ข. ดำเนินการปรับปรุงรุ่นของโปรแกรมให้เป็นปัจจุบันอยู่เสมอ

ค. ดำเนินการปรับปรุงฐานข้อมูลของมัลแวร์อย่างสม่ำเสมอ

ง. โปรแกรมป้องกันและกำจัดมัลแวร์ที่ใช้งานอยู่ต้องมีการตรวจสอบแบบทันทีทันใด

จ. โปรแกรมป้องกันและกำจัดมัลแวร์ที่ใช้งานอยู่ มีความสามารถในการตรวจสอบการโจมตีจากมัลแวร์ในรูปแบบ ต่างๆ ได้แก่ ตรวจสอบเมื่อเข้าใช้งานแฟ้มข้อมูล, ตรวจสอบเมื่อเข้าใช้งานโปรแกรมดูเว็บไซต์และตรวจสอบเมื่อมีการใช้งาน E-mail

– การเตรียมความพร้อม แผนปฏิบัติกรณีเกิดไฟไหม้/การทดสอบแผนปฏิบัติกรณีเพลิงไหม้ ห้อง Server เจ้าหน้าที่ศูนย์สารสนเทศสิ่งแวดล้อม ได้เข้าร่วมฝึกอบรมหลักสูตรป้องกันและระงับอัคคีภัยประจำปีของหน่วยงานเพื่อให้เจ้าหน้าที่ที่ปฏิบัติงานภายในอาคารมีความรู้ ความเข้าใจเกี่ยวกับความปลอดภัยในอาคารพร้อมรับสถานการณ์ฉุกเฉินกรณีเกิดเหตุเพลิงไหม้ โดยกรณีเกิดเหตุไฟไหม้ห้อง Server ให้ปฏิบัติดังนี้

ก. เมื่อได้รับแจ้งเหตุไฟไหม้ในกรณีปฏิบัติงานอยู่ในห้อง Server ควรรีบออกจากห้อง Server และลงจากอาคารอย่างเป็นระเบียบโดยเร็วที่สุด และไม่ควรกลับเข้าไปในอาคารอีก

ข. ในกรณีอพยพออกจากห้อง Server ควรใช้มือสัมผัสบริเวณผนังหรืออังใกล้ๆ ประตูถ้ามีความร้อนสูง แสดงว่าเกิดเพลิงไหม้บริเวณใกล้เคียง

ค. ให้หนีไฟลงด้านล่างของอาคาร โดยใช้บันไดหนีไฟด้านนอกอาคาร เนื่องจากลักษณะบันไดภายในอาคารเป็นเหมือนช่อง โพรง ที่เสริมให้เปลวไฟพุ่งขึ้น และลุกลามอย่างรวดเร็ว แต่ถ้าลงทางบันไดไม่ได้ให้ลงทางหน้าต่างโดยใช้เชือก หรือผ้ายาวผูกโรยตัวลงมา ส่วนการกระโดดลงจากอาคาร ควรมีเบาะหรือฟูกที่นอนรองรับ

ง. ห้ามใช้ลิฟต์เพราะขณะเกิดเพลิงไหม้ไฟฟ้าจะดับ ทำให้ลิฟต์ค้างจะทำให้ด้านในของตัวลิฟต์ไม่มีอากาศ

จ. หากเส้นทางหนีไฟเต็มไปด้วยกลุ่มควัน ให้ใช้ผ้าชุบน้ำมาคลุมตัว และปิดจมูกป้องกันการสำลักควันแล้วหมอบคลานเนื่องจากอากาศบริสุทธิ์จะอยู่ด้านล่าง (เหนือพื้น)

ฉ. ห้ามหนีไฟเข้าไปหลบในห้องต่างๆ ที่เป็นจุดอับภายในอาคาร เช่น ห้องน้ำ ที่แม้ในช่วงแรกจะปลอดภัยแต่เมื่อไฟลุกลาม น้ำที่อยู่ในห้องอาจไม่เพียงพอสำหรับดับไฟ และความร้อนของไฟจะส่งผลให้น้ำมีความร้อนสูงขึ้นจนสามารถลวกให้เสียชีวิตได้ สิ่งสำคัญที่สุดของการหนีรอดจากเหตุอัคคีภัย คือการมีสติเป็นอันดับแรกเพราะจะทำให้เจ้าหน้าที่องค์กร สามารถหนีเอาตัวรอด และช่วยเหลือผู้อื่นได้อย่างปลอดภัย ซึ่งองค์กร อยู่ในเขตพื้นที่ของสถานีดับเพลิงดุสิต 41/11 ถนนเศรษฐศิริ แขวงถนนนครไชยศรี เขตดุสิต กรุงเทพมหานคร 10300

– การทดสอบแผนปฏิบัติกรณีเพลิงไหม้ห้อง Server

ก. หลังได้ยินกริ่งสัญญาเพลิงไหม้ดังขึ้น รีบตรวจสอบที่มาของกริ่งสัญญา

ข. เจ้าหน้าที่รีบออกจากห้อง Sever ตามผู้นำถือธงไป

ค. เจ้าหน้าที่ทุกคนรีบวิ่งไปทางบันไดหนีไฟและลงบันได

ง. ผู้นำตรวจสอบอีกครั้งว่าไม่มีผู้ตกค้าง และลงบันไดเป็นคนสุดท้าย เมื่อทุกลงมารวมตัวกันบริเวณชั้นล่างของอาคาร เริ่มทำการตรวจนับเจ้าหน้าที่แต่ละกอง หลังตรวจนับเจ้าหน้าที่ และแจ้งจำนวนเรียบร้อยเป็นอันเสร็จขั้นตอนการซ้อมหนีไฟ

– การเตรียมความพร้อมกรณีเกิดโรคระบาด หรือโรคติดต่อร้ายแรง จำเป็นต้องปฏิบัติงานนอกสถานที่

ก. จัดทำทะเบียนผู้ปฏิบัติงานที่สามารถปฏิบัติงานจากที่บ้าน หรือนอกสถานที่ได้

ข. จัดเตรียมอุปกรณ์ฮาร์ดแวร์ ที่รองรับการปฏิบัติงานนอกสถานที่

ค. จัดเตรียมทะเบียนระบบเครือข่าย ที่สามารถให้ผู้ปฏิบัติงานนอกสถานที่สามารถเข้าถึงการใช้งานได้

ง. ทดสอบความพร้อมของระบบเครือข่าย ที่ใช้ในการปฏิบัติงานนอกสถานที่

9) การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน จัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบ ดังนี้

– ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้คำเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

1) ผู้อำนวยการ นายภูมิจิตต์ พงษ์พันธุ์งาม โทร.02-2436493 ต่อ 10

– ระดับปฏิบัติด้านเทคโนโลยีสารสนเทศและเครือข่าย ให้เจ้าหน้าที่ผู้ดูแลระบบของหน่วยงานรับผิดชอบการปฏิบัติงาน การบริหารจัดการศึกษา ทบทวน วางแผน ติดตาม และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยแบ่งทีมงาน ดังนี้ ทีมกู้คืนระบบ ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนระบบต่างๆ ให้สามารถกลับมาใช้งานได้ ตามปกติ

ก. ทีมกู้คืนระบบ ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนระบบต่างๆ ให้สามารถกลับมาใช้งานได้ตามปกติ

1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886

2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005

ข. ทีมกู้คืนเครือข่าย ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนให้เครือข่ายกลับมา ใช้งานได้ตามปกติ

1) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
2) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665

ค. ทีมกู้คืนระบบปฏิบัติการ ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งานได้ตามปกติ รวมถึงประสานงานเพื่อให้ผู้ใช้งานที่ปฏิบัติงานนอกสถานที่ สามารถปฏิบัติงานได้อย่างต่อเนื่อง

1) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
2) นายกวีศิลป์ นันทิพัฒน์สถิต โทร. 095-1558885
3) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665

ง. ทีมแก้ไขกรณีถูกแทรกแซงระบบ ทำหน้าที่ค้นหาสาเหตุและวิธีอุดช่องโหว่ในระบบเครือข่าย และแก้ไขให้ระบบสามารถใช้งานได้เป็นปกติ

1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886
2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
3) นายกวีศิลป์ นันทิพัฒน์สถิต โทร. 095-1558885
4) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665

จ. ทีมประเมินความเสียหาย ทำหน้าที่ประเมินความเสียหายและให้ข้อมูลความเสียหายทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน

1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886
2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005

– ระดับปฏิบัติด้านอาคารสถานที่ : ทำหน้าที่ควบคุม ประสานงาน แก้ไขปัญหาเบื้องต้นจัดเตรียมสถานที่สำหรับปฏิบัติงานสำรอง ระบบไฟฟ้า ระบบการสื่อสาร ระบบปรับอากาศ ให้พร้อมใช้งานกรณีเกิดภัยพิบัติฉุกเฉิน และการจลาจลต่างๆ

1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886
2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
3) นายกวีศิลป์ นันทิพัฒน์สถิต โทร. 095-1558885
4) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665
5) นางสาววชิราภรณ์ เพ่งบุญ โทร 062-6623549

ก. ทีมแก้ไขกรณีเกิดไฟไหม้(ห้องควบคุมระบบ) ทำหน้าที่แจ้งเหตุ ประสานงาน ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ศูนย์สารสนเทศสิ่งแวดล้อมได้จัดหาไว้

1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886
2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
3) นายกวีศิลป์ นันทิพัฒน์สถิต โทร. 095-1558885
4) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665

ข. ทีมแก้ไขกรณีไฟฟ้าดับ ไฟกระชาก (ห้องควบคุมระบบ) ทำหน้าที่แจ้งเหตุ ประสานงาน ดำเนินการ แก้ไขปัญหาเบื้องต้น จัดหาระบบป้องกันไม่ให้เกิดความเสียหายต่อระบบและอุปกรณ์เครือข่าย

1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886
2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
3) นายกวีศิลป์ นันทิพัฒน์สถิต โทร. 095-1558885
4) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665

ค. ทีมแก้ไขกรณีแผ่นดินไหว ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

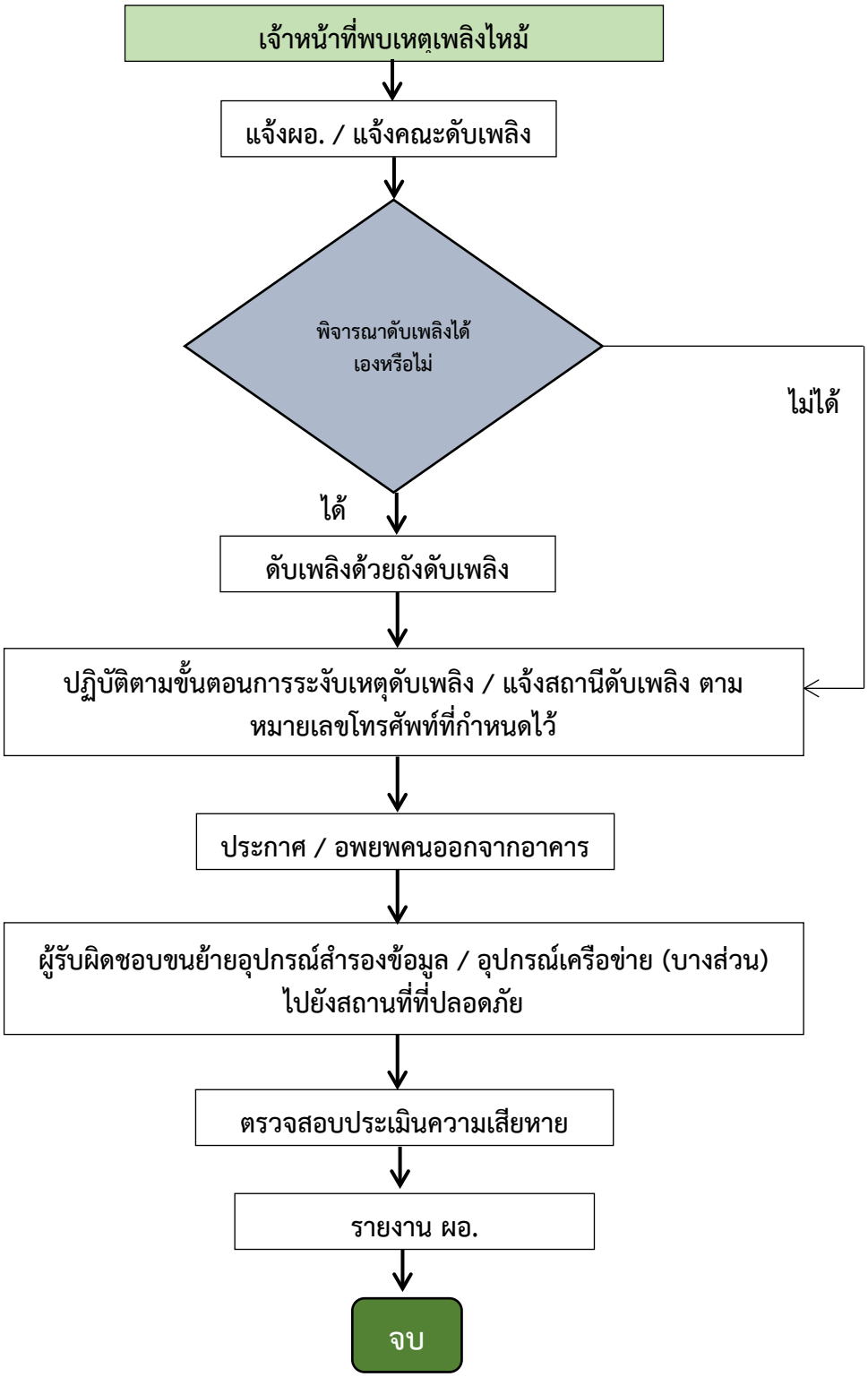
1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886
2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
3) นายกวีศิลป์ นันทิพัฒน์สถิต โทร. 095-1558885
4) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665

ง. ทีมแก้ไขกรณีเกิดการจลาจล ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

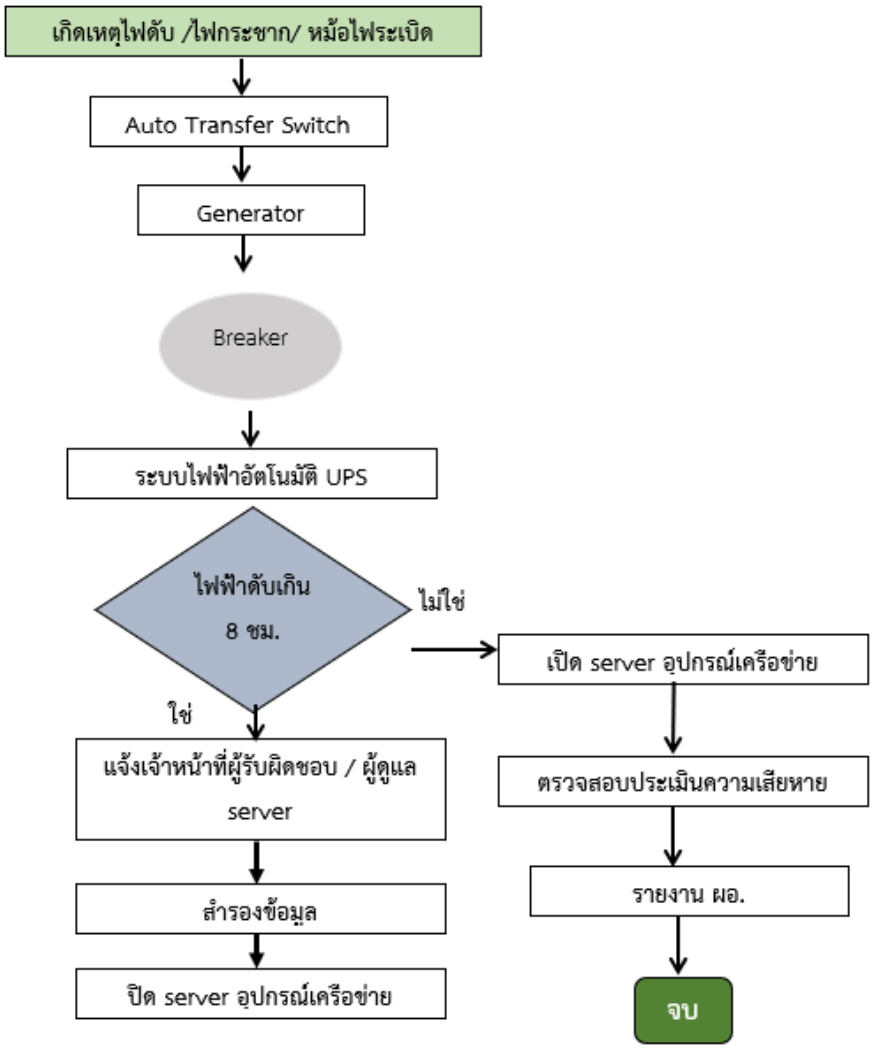
1) นางสาวปชาดา บุตรครุธ โทร. 063-2718886
2) นายวสุพล วงษ์วิโรจน์ โทร. 083-5554005
3) นายกวีศิลป์ นันทิพัฒน์สถิต โทร. 095-1558885
4) นายทวีวัฒน์ จันทร์แดง โทร 097-0855665

10) ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ

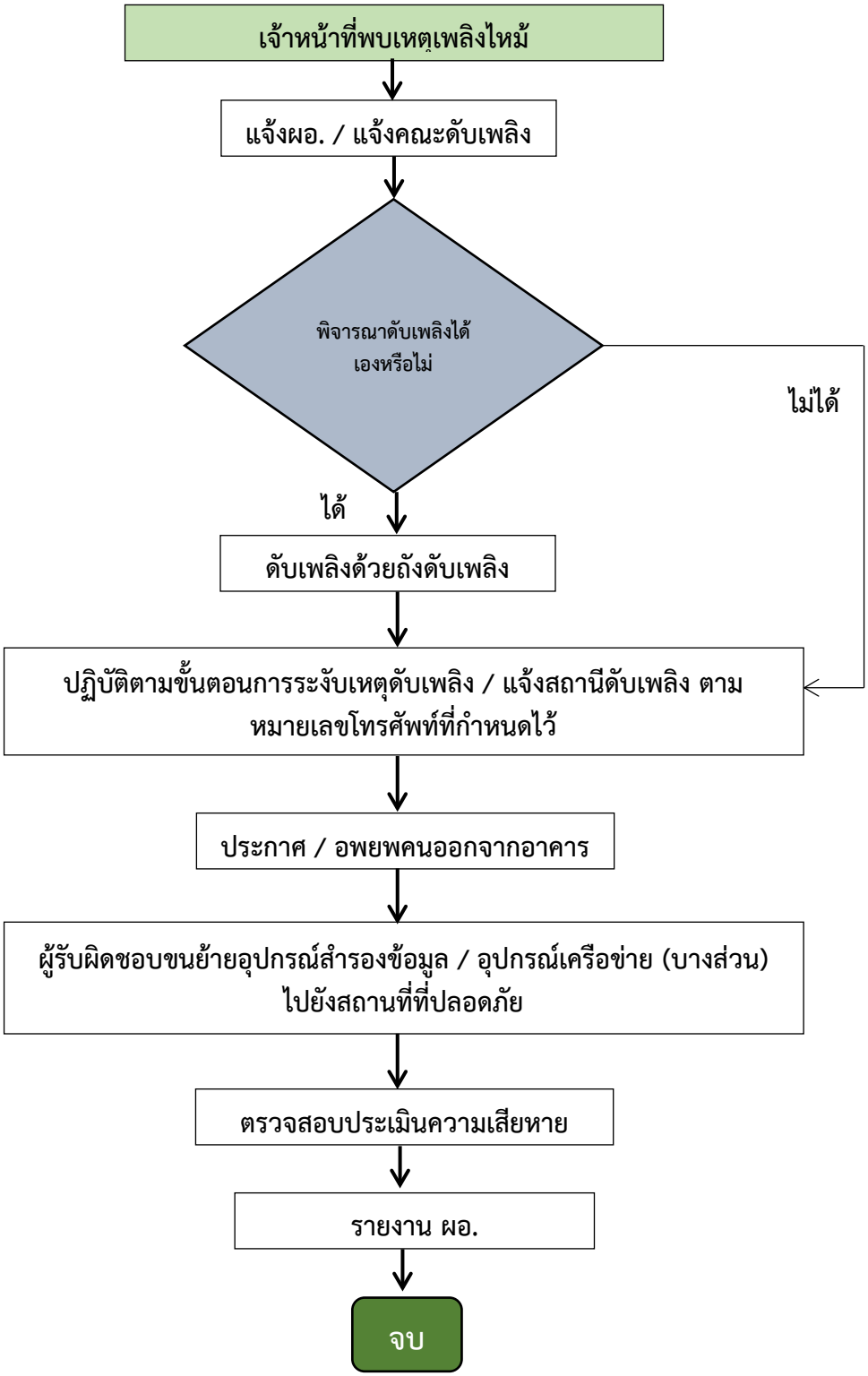
– ขั้นตอนการปฏิบัติงานกรณีไฟไหม้ (ห้องควบคุมระบบ)


เจ้าหน้าที่พบเหตุเพลิงไหม้
แจ้งผอ. / แจ้งคณะดับเพลิง
พิจารณาดับเพลิงได้เองหรือไม่
ไม่ได้
ได้
ดับเพลิงด้วยถังดับเพลิง
ปฏิบัติตามขั้นตอนการระงับเหตุดับเพลิง / แจ้งสถานีดับเพลิง ตามหมายเลขโทรศัพท์ที่กำหนดไว้
ประกาศ / อพยพคนออกจากอาคาร
ผู้รับผิดชอบขนย้ายอุปกรณ์สำรองข้อมูล / อุปกรณ์เครือข่าย (บางส่วน) ไปยังสถานที่ที่ปลอดภัย
ตรวจสอบประเมินความเสียหาย
รายงาน ผอ.
จบ

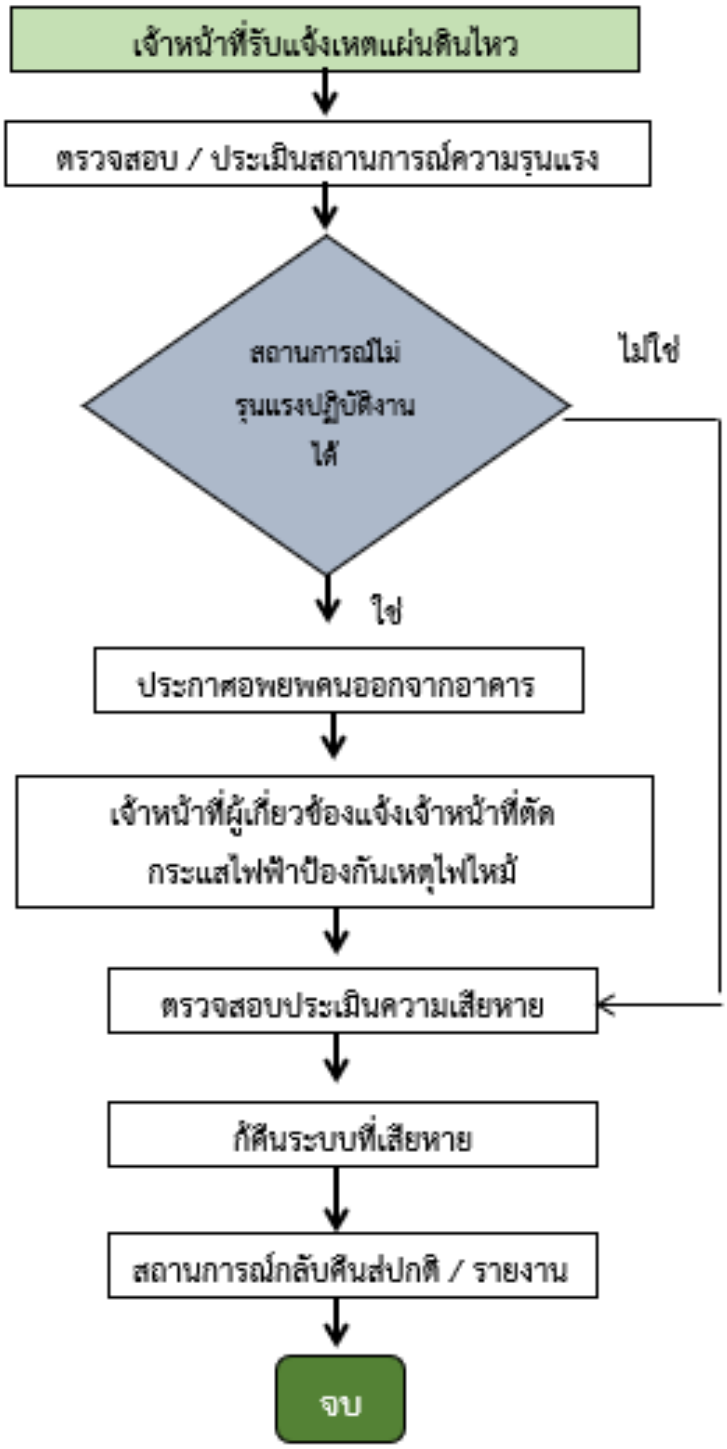
– ขั้นตอนการปฏิบัติงานกรณีเกิดเหตุไฟดับ ไฟกระชาก หม้อไฟระเบิด



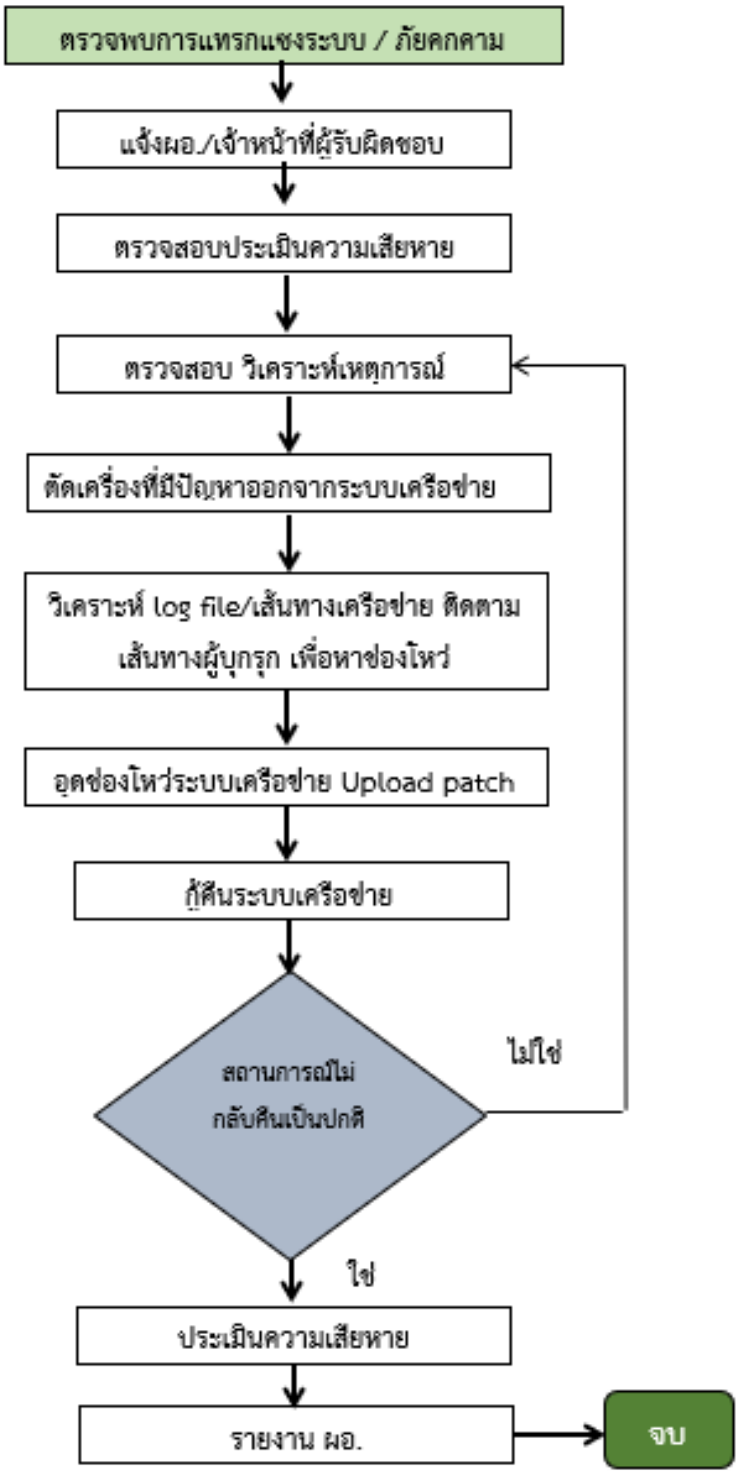
– ขั้นตอนการปฏิบัติงานกรณีเกิดเหตุจราจล



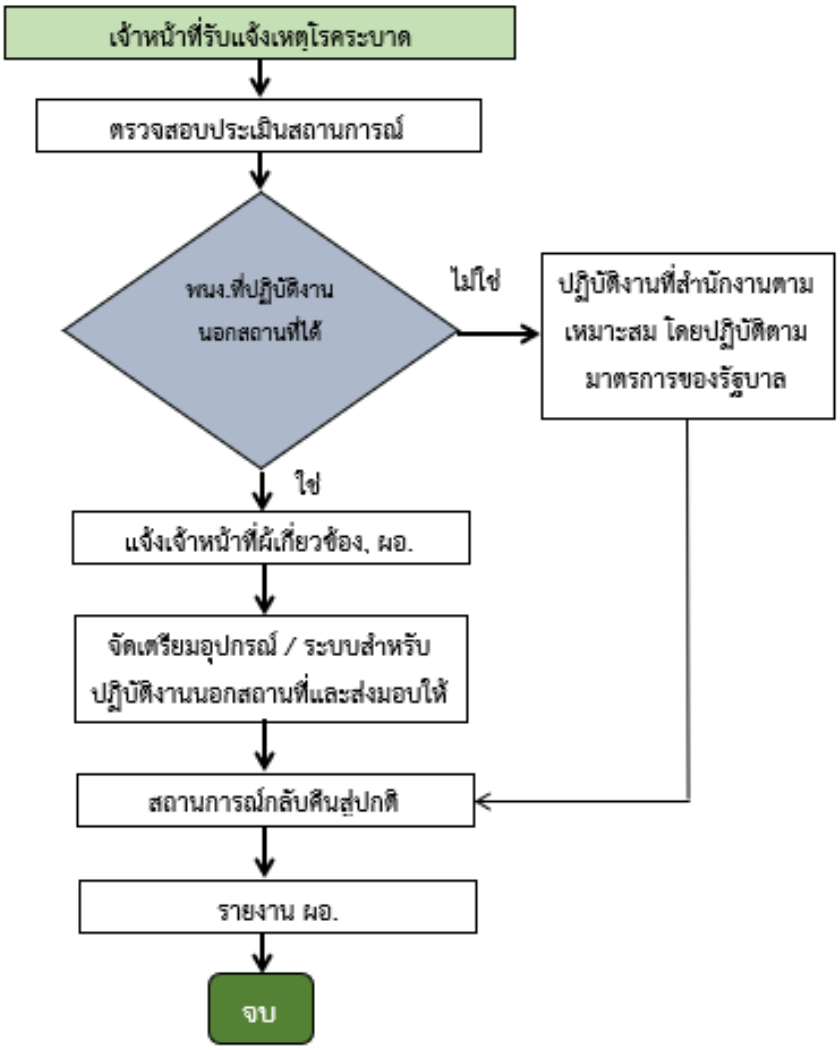
– ขั้นตอนการปฏิบัติงานกรณีเกิดแผ่นดินไหว



– ขั้นตอนการปฏิบัติงานกรณีโดนแทรกแซงระบบ


ตรวจพบการแทรกแซงระบบ / ภัยคุกคาม
แจ้งผอ./เจ้าหน้าที่ผู้รับผิดชอบ
ตรวจสอบประเมินความเสียหาย
ตรวจสอบ วิเคราะห์เหตุการณ์
ตัดเครื่องที่มีปัญหาออกจากระบบเครือข่าย
วิเคราะห์ log file/เส้นทางเครือข่าย ติดตาม
เส้นทางผู้บุกรุก เพื่อหาช่องโหว่
อุดช่องโหว่ระบบเครือข่าย Upload patch
กู้คืนระบบเครือข่าย
สถานการณ์ไม่
กลับคืนเป็นปกติ
ไม่ใช่
ใช่
ประเมินความเสียหาย
รายงาน ผอ.
จบ

– ขั้นตอนการปฏิบัติงานกรณีสถานการณ์โรคระบาด



10. นโยบายการบริหารจัดการผู้ให้บริการภายนอก (Third party management)

ด้านความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship) มีวัตถุประสงค์เพื่อให้มีการป้องกันสินทรัพย์ขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก(Information security policy for supplier relationships)

ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือสินทรัพย์สารสนเทศขององค์กร

2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements) ต้องระบุและบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ผู้ใช้งานเข้าถึงสารสนเทศหรือสินทรัพย์สารสนเทศขององค์กร ก่อนที่ จะอนุญาตให้สามารถเข้าถึงได้

3) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain) ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรต้องสื่อสารถึงห่วงโซ่ผู้ให้บริการภายนอกทั้งหมดที่เข้าถึงสารสนเทศหรือสินทรัพย์สารสนเทศขององค์กร

- ด้านการบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management) วัตถุประสงค์เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

4) การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services) ในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ

5) การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services) หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องจัดทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

แนวปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก

การใช้บริการด้านไอซีทีจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไขเปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของหน่วยงานภายนอกเพื่อความมั่นคง ปลอดภัย ของระบบสารสนเทศขององค์กร โดยนโยบายและแนวปฏิบัตินี้ต้องตรวจสอบ และประเมินตามระยะเวลา 1 ครั้งต่อปี ดังนี้

1) หน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศและการสื่อสารขององค์กร จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารด้านดิจิทัล

2) จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

- เหตุผลในการขอใช้งาน
- ระยะเวลาในการใช้งาน
- การตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

3) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

4) ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

5) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ(Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ(Availability)

6) องค์กรมีสิทธิในการตรวจสอบตามสัญญาการใช้บริการด้านไอซีทีเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

7) ในการจ้างเหมาพัฒนา บำรุงรักษาระบบผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ปฏิบัติงานจากภายนอก ได้แก่

– ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

– ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศได้แก่ การกำหนดชื่อผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

– ต้องบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File

– ในระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารด้านดิจิทัลก่อน

11. นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี (Malicious Software Prevention)

วัตถุประสงค์ เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ และเพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการ บัญชีผู้ใช้สารสนเทศของโดยเคร่งครัด โดยอ้างอิงมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งมีผู้รับผิดชอบคือ

1. ส่วนสารสนเทศและพัฒนาระบบ
2. ผู้ดูแลระบบที่ได้รับมอบหมาย
3. เจ้าหน้าที่ที่ได้รับมอบหมาย โดยมีนโยบายดังนี้

1) คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่ ผู้บริหารสหกรณ์กำหนดให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บริหารสหกรณ์ก่อน

2) บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

3) ผู้จัดการ/ผู้ดูแลระบบงานต้องทำการปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์และปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

4) ผู้ใช้งานต้องพึงระวังไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้จัดการ/ผู้ดูแลระบบ ทราบ

5) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้า สู่เครือข่าย และต้องแจ้งแก่ผู้จัดการ/ผู้ดูแลระบบ

6) ห้ามลักลอบเปลี่ยนแปลง ลบทิ้ง โปรแกรมป้องกันไวรัสคอมพิวเตอร์ ในระบบของสหกรณ์ โดยไม่ได้รับอนุญาตจากผู้บริหารสหกรณ์หรือผู้ที่ได้รับมอบหมาย

7) ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของสหกรณ์

แนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี

1) หลังจากผู้ดูแลระบบติดตั้งระบบปฏิบัติการแล้ว ให้ทำการติดตั้งโปรแกรมป้องกันไวรัสตามที่ได้มีการจัดซื้อลิขสิทธิ์

2) ผู้ดูแลระบบจะต้องตั้งค่าให้เครื่องทำการสแกนไวรัส โดยแบ่งออกเป็น 2 รูปแบบคือ

– การสแกนแบบกำหนดตารางเวลา (Time Schedule) ให้สแกนในช่วง 12.00น. ของทุกวันที่เปิดเครื่อง

– สแกนไวรัสจากสื่อบันทึกภายนอก เช่น CD/DVD, External Harddisk, Flash Drive, SD Card ฯลฯ เมื่อเสียบเข้าเครื่องทุกครั้ง

12. การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเทอร์เน็ต (Website and Internet Security)

1) ไม่ใช้ระบบอินเทอร์เน็ต (Internet) เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อการรักษาความต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

2) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่าง เป็นทางการผ่านระบบอินเทอร์เน็ต

3) ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

4) หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการ เข้าใช้งานโดยบุคคลอื่น

5) ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่ส่วนสารสนเทศและพัฒนาระบบจัดสรรไว้ตามสิทธิ์ที่ได้รับ

6) ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเทอร์เน็ต

1) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ส่วนสารสนเทศและพัฒนาระบบจัดสรรไว้ ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจาก หัวหน้าศูนย์เทคโนโลยีสารสนเทศ เป็น ลายลักษณ์อักษรแล้ว

2) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ต ผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของ ระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

3) ในการรับ-ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ-ส่งข้อมูลทุกครั้ง

4) ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของส่วนสารสนเทศและพัฒนาระบบ เพื่อหาประโยชน์ในเชิง ธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อ ชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

5) ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพ ของเครือข่ายและความปลอดภัยทางข้อมูลของส่วนสารสนเทศและพัฒนาระบบ

6) ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับส่วนสารสนเทศและพัฒนาระบบ

7) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของส่วนสารสนเทศและพัฒนาระบบ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

8) ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความ มั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการ เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

9) ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้าง ขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

10) ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือขอ งข้อมูลคอมพิวเตอร์ที่อยู่บน อินเตอร์เน็ต ก่อนนำข้อมูลไปใช้งาน

11) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเตอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

12) ในการเสนอความคิดเห็นผ่านเว็บบอร์ด (Webboard) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับของส่วนสารสนเทศและพัฒนาระบบ และต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อม เสียต่อชื่อเสียงของส่วนสารสนเทศและพัฒนาระบบ การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

13) หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งาน โดยบุคคลอื่น

13. นโยบายและแนวปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Secuity)

1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

2) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการ เข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

3) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

4) ซอฟต์แวร์ที่ส่วนสารสนเทศและพัฒนาระบบใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็น ความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

5) ซอฟต์แวร์ที่ส่วนสารสนเทศและพัฒนาระบบจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งาน ทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

6) ห้ามผู้ใช้ระบบเทคโนโลยีสารสนเทศของส่วนสารสนเทศและพัฒนาระบบ เพื่อควบคุมคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

14. นโยบายการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ (Cryptography) และการบริหารจัดการ และการบริหารจัดการกุญแจ (Key management)

2.14.1 โรงงานไพ่ต้องจัดให้มีนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูล ที่คำนึงถึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูล ที่เป็นความลับหรือมีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการดำเนินนโยบายและบริหารจัดการกุญแจ เพื่อการเข้ารหัสข้อมูล (key management)

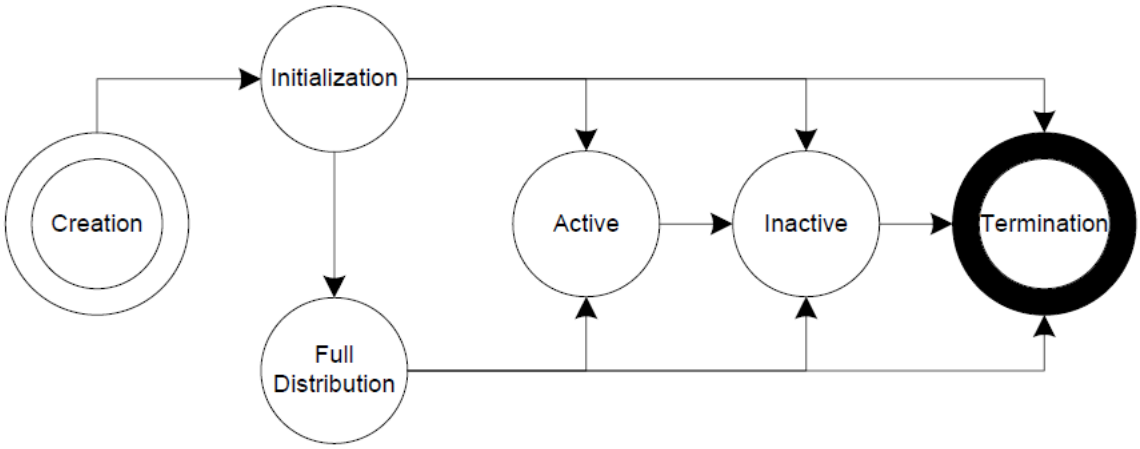
2.14.2 โรงงานไพ่ต้องจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูล ตลอดช่วงเวลาการใช้งาน (key management whole life cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ

แนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ และการบริหารจัดการกุญแจ

การจัดการวงจรชีวิตคีย์ (Key Lifecycle Management) หมายถึงการสร้างและการเลิกใช้คีย์การเข้ารหัส โดยทั่วไปเรียกว่า "Key rollover." คีย์ที่สร้างขึ้นใหม่มักถูกเก็บไว้ในที่เก็บคีย์พร้อมกับคีย์เก่า เนื่องจากการวางคีย์ในที่เก็บแบบกระจายไม่ใช่การดำเนินการแบบ Atomic คีย์การเข้ารหัสแบบใหม่จะพร้อมใช้งานเฉพาะกับชุดย่อยของตัวควบคุมโดเมนเท่านั้น ขึ้นอยู่กับนโยบายการจำลองแบบของที่เก็บ คีย์จะถูกจำลองแบบในที่สุดไปยังตัวควบคุมโดเมนที่เหลืออยู่ในช่วงระยะเวลาหนึ่ง ข้อมูลที่ปกป้องโดยคีย์ใหม่อาจไม่สามารถใช้งานได้กับไคลเอ็นต์ทั้งหมดจนกว่าคีย์ใหม่จะทำซ้ำทั่วทั้งที่เก็บ ตัวอย่างเช่น สิ่งนี้อาจเกิดขึ้นหากข้อมูลที่ได้รับการป้องกันถูกจัดเก็บในที่เก็บข้อมูลบนคลาวด์ที่มีความพร้อมใช้งานสูงซึ่งไม่ขึ้นกับที่เก็บคีย์ ระบบของเราจะเปิดใช้งานคีย์ใหม่ (เริ่มใช้งาน) เฉพาะหลังจากที่สร้างคีย์ดังกล่าวแล้วเพื่อบรรเทาปัญหานี้

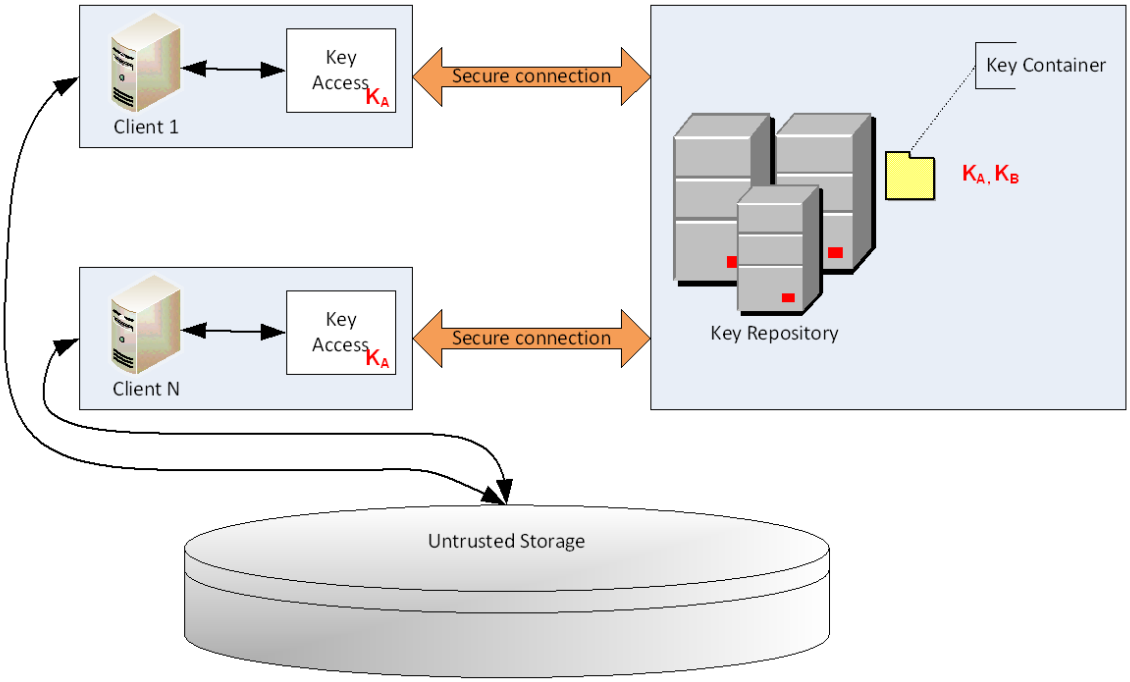
บทความนี้พิจารณาถึงวงจรชีวิตที่สำคัญตามอายุ กระบวนทัศน์อีกประการหนึ่งคือการกำหนดวงจรชีวิตตามจำนวนการใช้คีย์ (หรือตัวนับที่เพิ่มขึ้นแบบจำเจ) อย่างไรก็ตาม การรักษาตัวนับที่เพิ่มขึ้นแบบโมโนโทนเป็นเรื่องยากในระบบแบบกระจาย สิ่งนี้จะยิ่งท้าทายมากขึ้นไปอีก หากเราต้องการใช้ประโยชน์จากที่เก็บแบบกระจายที่มีอยู่ในขณะที่ทำการเปลี่ยนแปลงน้อยที่สุด ดังนั้นเราจึงเลือกวิธีการตามอายุที่เหมาะสมที่สุดสำหรับระบบของเรา
ระบบของเราจะจัดการวงจรชีวิตที่สำคัญให้กับผู้ใช้ปลายทางอย่างโปร่งใส สร้าง เปิดใช้งาน และเลิกใช้คีย์โดยอัตโนมัติเมื่อผู้ใช้ปกป้องและดึงข้อมูล ความสามารถในการทำเช่นนี้ขึ้นอยู่กับสิทธิ์การเข้าถึงของผู้ใช้ เราให้ตัวเลือกแก่ผู้ใช้ปลายทางในการกำหนดค่าบางแง่มุมของนโยบายวงจรชีวิตที่สำคัญ แต่ระบบจะรับผิดชอบในการบังคับใช้นโยบายนี้โดยไม่ได้รับความช่วยเหลือจากผู้ใช้

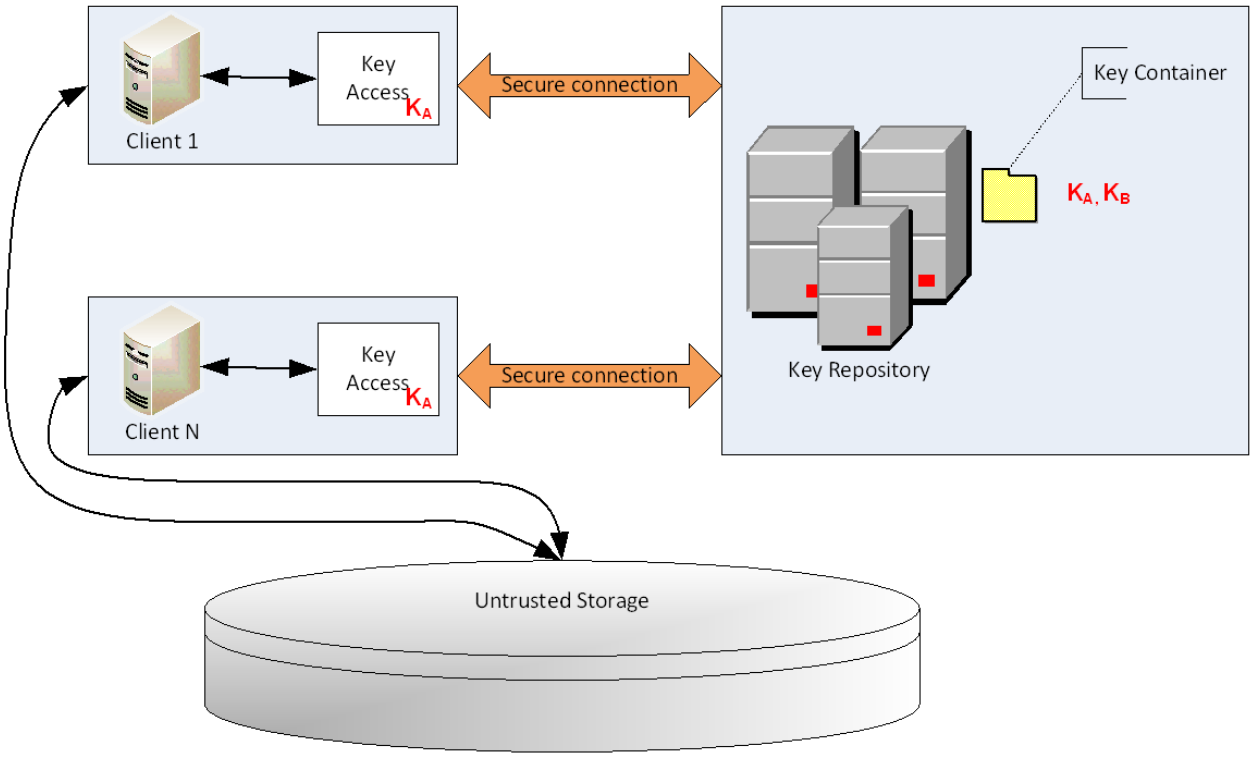
สถานะในวงจรชีวิตของคีย์การเข้ารหัส ผู้ที่คุ้นเคยกับขั้นตอนเหล่านี้อยู่แล้ว และมีความคล้ายคลึงกับขั้นตอนที่ระบุในระบบ Information Lifecycle Management (ILM) เราระบุสถานะที่มีรายละเอียดหลายอย่างในช่วงอายุของคีย์ที่ส่งผลต่อการทำงานภายในของระบบการจัดการคีย์แบบกระจาย ซึ่งการกำหนดมี 6 สถานะ ได้แก่

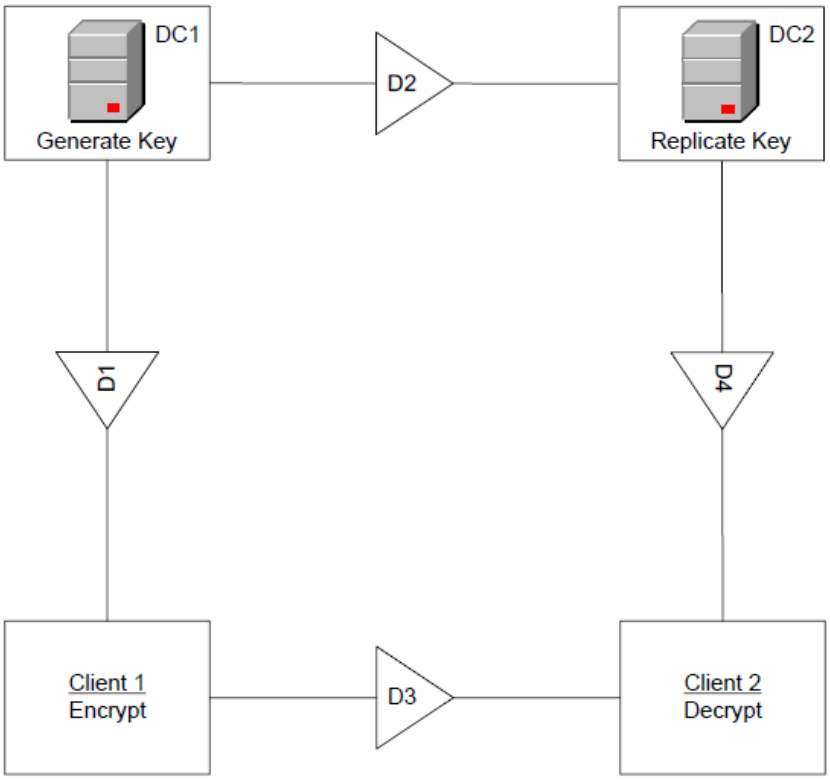


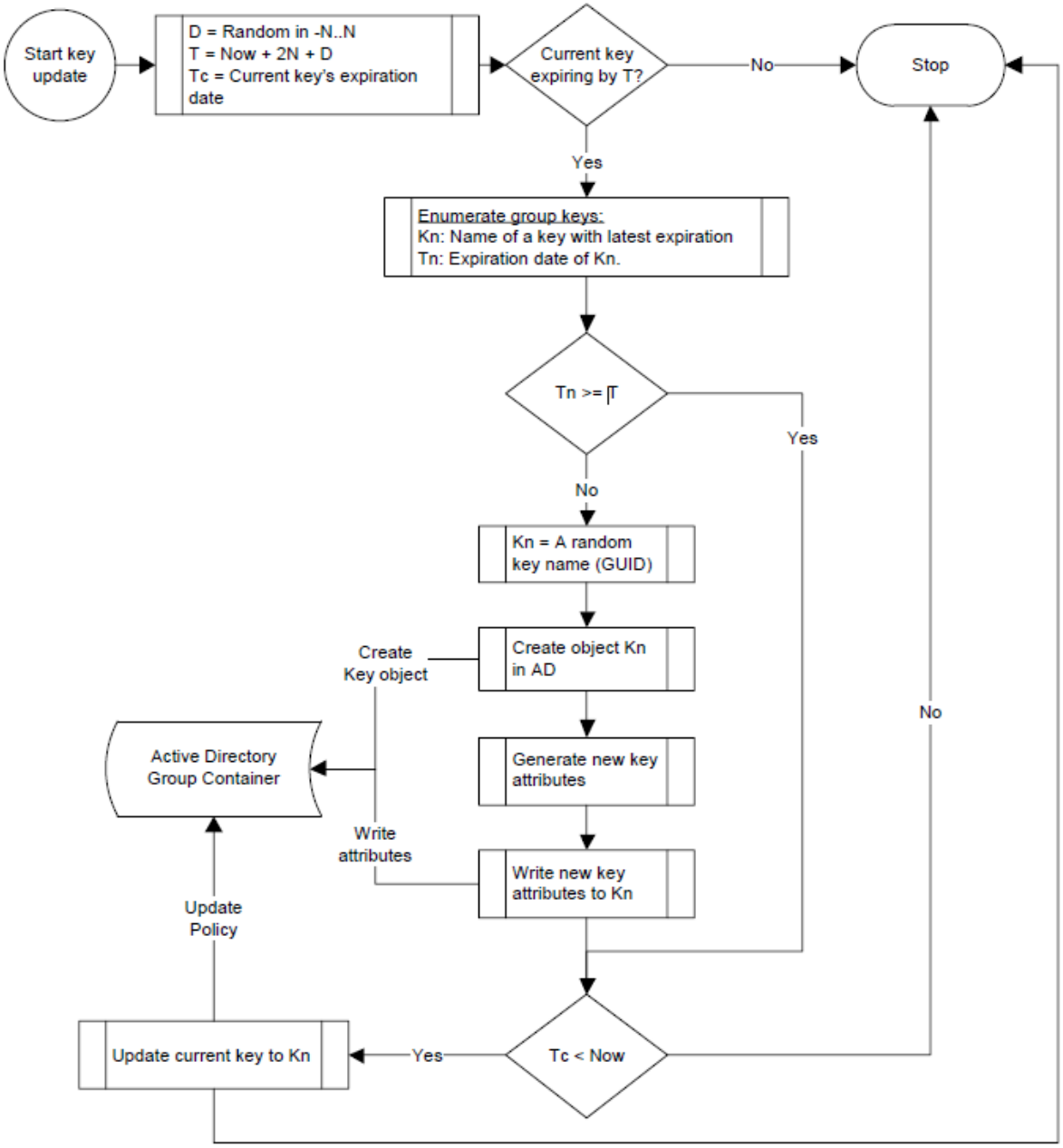
- Creation อ็อบเจ็กต์คีย์ถูกสร้างขึ้นบนตัวควบคุมโดเมนอย่างน้อยหนึ่งตัว แต่ไม่มีการตั้งค่าแอตทริบิวต์
- Initialization ออบเจ็กต์คีย์มีแอตทริบิวต์คีย์หลักทั้งหมดที่ตั้งค่าไว้บนตัวควบคุมโดเมนอย่างน้อยหนึ่งรายการ
- Full Distribution คีย์เริ่มต้นสามารถใช้ได้กับตัวควบคุมโดเมนทั้งหมด
- Active คีย์เริ่มต้นพร้อมใช้งานสำหรับการดำเนินการเข้ารหัสทั้งหมดบนตัวควบคุมโดเมนอย่างน้อยหนึ่งตัว
- Inactive คีย์เริ่มต้นไม่พร้อมใช้งานสำหรับการดำเนินการเข้ารหัสลับบางอย่างบนตัวควบคุมโดเมนทั้งหมด
- Termination คีย์เริ่มต้นจะถูกลบออกอย่างถาวรจากตัวควบคุมโดเมนทั้งหมด

ภาพกระบวนการจัดการ Key Lifecycle Management


Client 1
Key Access
K_A
Secure connection
Key Container
K_A, K_B
Client N
Key Access
K_A
Secure connection
Key Repository
Untrusted Storage


Client 1
Key Access
K_A
Secure connection
Key Container
K_A, K_B
Client N
Key Access
K_A
Secure connection
Key Repository
Untrusted Storage


DC1
Generate Key
D2
DC2
Replicate Key
D1
D4
Client 1
Encrypt
D3
Client 2
Decrypt



กฎที่สำคัญที่สุดสำหรับกลยุทธ์การจัดการคีย์คือผู้ใช้ต้องไม่แก้ไขคีย์ที่ไม่ได้สร้างขึ้น หัวใจสำคัญของระบบการจัดการวงจรชีวิตที่สำคัญของเราคืออัลกอริธึมการอัพเดทที่สำคัญของเราซึ่งมีลักษณะดังต่อไปนี้

– ไคลเอนต์ในเครือข่ายย่อยที่แยกออกมาสามารถอัปเดตคีย์บนตัวควบคุมโดเมนภายในเครื่องได้อย่างปลอดภัย

– เมื่อตัวควบคุมโดเมนบนเครือข่ายย่อยที่แยกออกมาเชื่อมต่อกับส่วนที่เหลือของที่เก็บอีกครั้ง คีย์ที่อัปเดตจะถูกรวมโดยอัตโนมัติโดยเป็นส่วนหนึ่งของกระบวนการจำลอง/การกระทบยอด Active Directory มาตรฐาน

– ผู้ใช้ไม่ต้องกังวลกับอัลกอริธึม กำหนดการ หรือกลไกการอัพเดทคีย์

– ไม่ต้องประสานงานการกระทำกับรายอื่น แต่ละรายสามารถเรียกใช้อัลกอริทึมการอัปเดตคีย์ได้อย่างปลอดภัยบนตัวควบคุมโดเมนภายในเครื่องโดยไม่ต้องกังวลว่าไคลเอ็นต์อื่นจะปรับเปลี่ยนคอนเทนเนอร์บริการเดียวกันบนตัวควบคุมโดเมนอื่น

– การอัปเดตคีย์จะค่อยๆ ดำเนินการเมื่อเวลาผ่านไป ซึ่งจะเพิ่มโอกาสในการแจกจ่ายทั้งหมดก่อนที่คีย์จะเปิดใช้งาน

– อัลกอริธึมการอัพเดตคีย์สามารถทนต่อความล้มเหลวได้ทุกจุดในอัลกอริธึมและรับประกันว่าข้อมูลจะไม่สูญหาย

บทที่ 3
การถ่ายทอดกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

การนำนโยบายไปปฏิบัติเป็นสิ่งสำคัญในการผลักดันให้นโยบายได้รับการรับรู้เข้าใจ ยอมรับและสร้างทัศนคติที่ดีต่อผู้ปฏิบัติตามนโยบาย เพื่อให้เกิดการปฏิบัติอย่างมีประสิทธิภาพ จึงต้องมีการสื่อสารถ่ายทอดนโยบาย และกระบวนการอย่างชัดเจนเป็นลายลักษณ์อักษรให้ครอบคลุมในทุกๆ ช่องทาง

1. วัตถุประสงค์

1) เพื่อให้ผู้เกี่ยวข้องและผู้มีส่วนได้เสีย ทั้งภายในและภายนอกองค์กร ยึดถือเป็นกรอบแนวทางปฏิบัติอย่างสอดคล้องกัน

2) เพื่อให้นโยบายการบริหารความมั่นคงปลอดภัยของสารสนเทศทุกข้อกำหนด ถูกนำไปใช้ในทุกภาคส่วนอย่างมีระบบ

3) เพื่อให้การบริหารความมั่นคงปลอดภัยของสารสนเทศ มีประสิทธิภาพสูงสุด

2. ช่องทางการสื่อสาร

ส่วนสารสนเทศฯ ถ่ายทอดกระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ การกำกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) โดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ

1) ผู้ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการวิเคราะห์และจัดทำการกำกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้ผู้อำนวยการพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

2) ข้อมูลข่าวสาร (Message)

ข้อมูลข่าวสาร ได้แก่ กระบวนการวิเคราะห์และจัดทำการกำกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) ที่ผ่านการพิจารณาจากผู้อำนวยการ โดยได้รับการรับรองความถูกต้องเป็นที่เรีย

3) ช่องทางการสื่อสาร (Channel)

ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้ สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารระบบอินทราเน็ต และจดหมายอิเล็กทรอนิกส์

พร้อมมีการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) ของโรงงานไพ่ฯ โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ จัดทำการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) ที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงาน

ในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่ง ในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) ให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องจำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ

และเพื่อให้สอดคล้องกับการดำเนินการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ การใช้โซเชียลมีเดีย เช่น เฟซบุ๊ก จึงเป็นอีกหนึ่งช่องทางที่สามารถเผยแพร่ข่าวสารในเรื่องดังกล่าวนี้ได้ โดยเลือกเฉพาะข้อมูลที่มีสาระสำคัญต้องการสื่อสารในเชิงสร้างภาพลักษณ์ให้กับโรงงานไพ่ กรมสรรพสามิต

3. การถ่ายทอดกระบวนการและการวิเคราะห์การดำเนินการด้านการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

การถ่ายทอดกระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ มีกระบวนการดำเนินงานดังนี้

3.1 กำหนดวัตถุประสงค์ของการถ่ายทอดกระบวนการการบริหารจัดการความมั่นคงปลอดภัย

1) เพื่อสร้างการรับรู้ในกระบวนการการบริหารจัดการความมั่นคงปลอดภัยให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ

2) เพื่อสร้างความเข้าใจในกระบวนการการบริหารจัดการความมั่นคงปลอดภัยให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

3) เพื่อนำข้อมูลที่ได้รับ (Feedback) จากผู้มีส่วนได้ส่วนเสียต่าง ๆ มาปรับปรุงและพัฒนากระบวนการการบริหารจัดการความมั่นคงปลอดภัยให้มีประสิทธิภาพมากยิ่งขึ้น

3.2 วิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความมั่นคงปลอดภัย

1) กำหนดมีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders) ที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความมั่นคงปลอดภัย

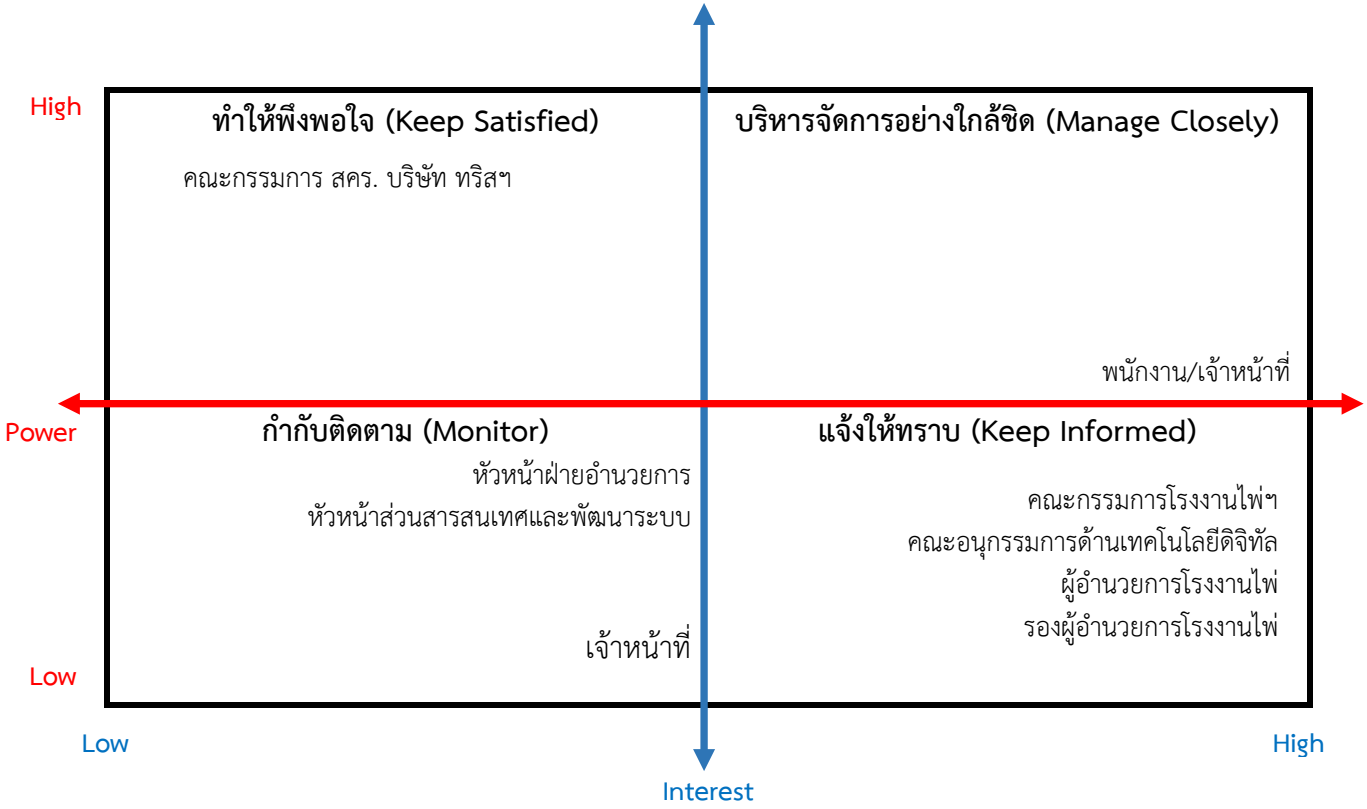
ผู้มีส่วนได้ส่วนเสียที่สำคัญต่อกระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ ประกอบด้วย คณะกรรมการ คณะทำงาน ผู้บริหารและเจ้าหน้าที่ ซึ่งในแต่ละกลุ่มนั้นมีบทบาทหน้าที่ที่ส่งผลกระทบต่อกระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ ที่เหมือนและแตกต่างกันออกไป โดยสามารถสรุปได้ ดังนี้

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
1. คณะกรรมการโรงงานไพ่ กรมสรรพสามิต	• กำกับดูแล (Governance) การดำเนินการด้านการแนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ
2. คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	• กำกับดูแล (Governance) การดำเนินการด้านการแนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
3. ผู้อำนวยการโรงงานไพ่ฯ	• พิจารณาเห็นชอบแนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศเพื่อสนับสนุนการดำเนินงานด้านสารสนเทศ • กำกับดูแล (Governance) การดำเนินการด้านการแนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ • การดำเนินการด้านการบังคับใช้แนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ • กำหนดและถ่ายทอดนโยบายการประยุกต์ใช้แนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ
4. รองผู้อำนวยการโรงงานไพ่ฯ	• กำกับดูแล (Governance) การดำเนินการด้านการแนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ • การดำเนินการด้านการบังคับใช้แนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ • กำหนดและถ่ายทอดนโยบายการประยุกต์ใช้แนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ
5. หัวหน้าฝ่าย/ส่วนงานต่าง ๆ	• บริหารจัดการการดำเนินงานในส่วนงานที่รับผิดชอบให้มีความสอดคล้องกับนโยบายองค์กรของโรงงานไพ่ฯ ที่กำหนด • ให้ความคิดเห็น ข้อเสนอแนะ และข้อวิพากษ์ต่าง ๆ ที่เกี่ยวข้องกับสถาปัตยกรรมองค์กร เพื่อนำไปปรับปรุงกระบวนการการบริหารจัดการความมั่นคงปลอดภัย • สื่อสารและถ่ายทอดข้อมูลข่าวสารต่าง ๆ ที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรไปยังพนักงานในฝ่าย/ส่วน
6. พนักงาน/เจ้าหน้าที่	• ดำเนินงานตามนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ • ให้ความคิดเห็น ข้อเสนอแนะ และข้อวิพากษ์ต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อนำไปปรับปรุงกระบวนการการบริหารจัดการความมั่นคงปลอดภัย

3.3 กำหนดเครื่องมือในการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่สำคัญ

โรงงานไพ่ฯ ได้กำหนดตำแหน่งของผู้มีส่วนได้ส่วนเสียที่สำคัญกับกระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ ในรูปแบบของตารางเส้น (Grid) ได้แบ่งออกเป็นแกน X หมายถึง ผู้ที่มีอำนาจ (Power) และแกน Y หมายถึง ผู้ที่ได้รับผลประโยชน์ (Interest) จำแนกออกเป็น 4 กลุ่ม ได้แก่ กลุ่มที่ควรทำให้พึงพอใจ กลุ่มที่ควรบริหารจัดการอย่างใกล้ชิด กลุ่มที่ต้องกำกับติดตาม และกลุ่มที่ต้องแจ้งข้อมูลข่าวสารให้ทราบ โดยสามารถสรุปได้ดังนี้



ภาพตำแหน่งของผู้มีส่วนได้ส่วนเสียที่สำคัญ จำแนกตามกลุ่มต่าง ๆ

3.4 กำหนดบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญ

โรงงานไพ่ฯ ได้กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ ในรูปแบบตาราง RACI (RACI Matrix) โดยในแต่ละกระบวนการผู้มีส่วนได้ส่วนเสียหลักจะมีบทบาทหน้าที่ที่เหมือน และแตกต่างกันออกไป ประกอบด้วย ผู้รับผิดชอบงาน (A) ผู้ที่ทำงานนั้น ๆ (R) ผู้ที่มีหน้าที่ให้คำปรึกษา (C) และผู้ที่โรงงานไพ่ฯ จะต้องแจ้งข้อมูลข่าวสารที่เกี่ยวข้องกับการดำเนินงานให้ทราบเป็นระยะ ๆ (I) โดยสามารถสรุปได้ ดังนี้

ตารางบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญกับกระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ

การจัดทำกระบวนการบริหารจัดการการบริหารจัดการความมั่นคงปลอดภัย	R = Responsible A = Accountable C = Consulted I = Informed						
กิจกรรม	คณะกรรมการโรงงานไพ่	คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	ผู้อำนวยการโรงงานไพ่	รองผู้อำนวยการโรงงานไพ่	หัวหน้าฝ่ายอำนวยการ	หัวหน้าส่วน/เจ้าหน้าที่สารสนเทศและพัฒนาระบบ	พนักงาน
กำหนดเป้าหมายการจัดทำกระบวนการฯ	I	I	C	I	R	A	I
ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง	I	I	C	I	R	A	I
สำรวจปัญหา อุปสรรค และความต้องการ	I	I	C	I	R	A	R
วิเคราะห์ข้อมูล	I	I	C	I	R	A	I
ออกแบบกระบวนการ	I	I	C	I	R	A	I
กำหนดแนวทางการใช้แนวนโยบายและแนวปฏิบัติฯ	I	I	C	I	R	A	I
วิเคราะห์ผู้มีส่วนได้ส่วนเสีย	I	I	C	I	R	A	I
ถ่ายทอดกระบวนการวิเคราะห์และจัดทำ	I	I	C	I	I	A	I
กำกับดูแลแนวนโยบายและแนวปฏิบัติฯ	I	I	C	I	R	A	I
บริหารจัดการแนวนโยบายและแนวปฏิบัติฯ	I	I	C	I	R	A	I

3.5 จัดทำกระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ

กระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯใช้วิธีการวิเคราะห์กระบวนการทำงานด้วยแบบจำลอง SIPOC หรือ “SIPOC Model” ประกอบด้วยองค์ประกอบต่าง ๆ ได้แก่ ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier) ปัจจัยนำเข้า (Input) กระบวนการ (Processes) ผลผลิต (Outputs) และผู้ที่นำผลผลิตไปใช้งาน (Customers) ซึ่งสามารถแสดงให้เห็นโดยภาพรวม ดังนี้

ชื่อกระบวนการ : กระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ	**วันที่จัดทำ/ปรับปรุงกระบวนการ :** 3 กรกฎาคม 2566
ผู้รับผิดชอบ : ส่วนสารสนเทศและพัฒนาระบบ	**จัดทำครั้งที่ :** 2

ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	ปัจจัยนำเข้า (Input)	กระบวนการ (Process)	ผลผลิต (Outputs)	ผู้ที่นำผลผลิตไปใช้งาน (Customers)
S1: หัวหน้าส่วนสารสนเทศฯ	I1: งบประมาณในการดำเนินงาน I2: บุคลากร ประกอบด้วย ● ผู้อำนวยการ ● รองผู้อำนวยการ ● หัวหน้าฝ่ายอำนวยการ ● หัวหน้าส่วนสารสนเทศฯ ● เจ้าหน้าที่สารสนเทศ I3: เทคโนโลยี ได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ของระบบคอมพิวเตอร์ I4: วัสดุอุปกรณ์ ได้แก่ เครื่องใช้สำนักงาน I5: เครื่องมือที่ใช้ในการวิเคราะห์ ได้แก่ ● แผนภูมิก้างปลา ● SWOT Analysis ● TOWS Matrix ● Gap Analysis	**P1: กำหนดแนวนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ** ↓ **P2: ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง** ↓ **P3: สำรวจปัญหา อุปสรรค ความต้องการ** ↓ **P4: วิเคราะห์ข้อมูล** ↓ **P5: จัดทำแนวโยบายและแนวปฏิบัติ** ↓ **P6: ประกาศใช้** ↓ **P7: ติดตามผลการดำเนินงาน**	แนวนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ	C1: ภายในองค์กร ● ฝ่ายอำนวยการ ● ฝ่ายโรงพิมพ์ ● ฝ่ายผลิตไพ่

ชื่อกระบวนการ : กระบวนการการบริหารจัดการความมั่นคงปลอดภัยของโรงงานไพ่ฯ			**วันที่จัดทำ/ปรับปรุงกระบวนการ :** 3 กรกฎาคม 2566	
ผู้รับผิดชอบ : ส่วนสารสนเทศและพัฒนาระบบ			**จัดทำครั้งที่ :** 2	
ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	**ปัจจัยนำเข้า (Input)**	**กระบวนการ (Process)**	**ผลผลิต (Outputs)**	**ผู้ที่นำผลผลิตไปใช้งาน (Customers)**
S2: เจ้าหน้าที่สารสนเทศ				C2: ภายในองค์กร ● ผู้ติดต่อ ● บริษัท
S6: คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล				

3.6 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการกำหนดแนวนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ

เป็นกระบวนการกำหนดเป้าหมาย หรือสิ่งที่โรงงานไพ่ฯ ต้องการจะเป็นในอนาคต ซึ่งได้แก่ การเป็นผู้นำด้านสิ่งพิมพ์ปลอดการปลอมแปลง และดิจิทัลปริ้นติ้งโซลูชั่นภาครัฐ ทั้งนี้ ในการจะบรรลุวัตถุประสงค์และเป้าหมายดังที่กำหนดได้นั้น แนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ตามมาตรฐาน ISO:IEC/27001 : 2018 จึงมีบทบาทสำคัญอย่างยิ่งในการช่วยสนับสนุนการดำเนินงานในด้านต่าง ๆ ขององค์กร ให้มีมาตรฐานการดำเนินงานที่น่าเชื่อถือ ปลอดภัย โดยจะสังเหตุเห็นได้ว่า ISO:IEC/27001 : 2018 เป็นเรื่องที่ว่าด้วยมาตรฐานความมั่นคงปลอดภัย ของสารสนเทศทั้งหมด ทั้งในส่วนของข้อมูล การปฏิบัติที่มีมาตรฐานมีการควบคุมภายในที่ดี สอดรับวิสัยทัศน์และพันธกิจของโรงงานไพ่ ที่จะมุ่งสู่การเป็นผู้นำด้านสิ่งพิมพ์ปลอดการปลอม และการดำเนินงานทางด้านโซลูชั่น และสอดคล้องตาม พรบ. ไซเบอร์ และ พรบ. คุ้มครองข้อมูลส่วนบุคคล ดังนั้น การบริหารความมั่นคงปลอดภัยของสารสนเทศ ตามมาตรฐาน ISO:IEC/27001 : 2018 จึงมีความสัมพันธ์อย่างยิ่งกับเป้าหมายขององค์กรในอนาคต ดังนั้นผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการนี้ จึงประกอบด้วยทั้งบุคลากรภายในตั้งแต่ระดับการบริหาร ถึงระดับปฏิบัติงาน และผู้เกี่ยวข้องที่มีการใช้บริการ ติดต่อสื่อสาร กับโรงงานไพ่ เพื่อช่วยกันให้ข้อเสนอแนะข้อสังเกต และช่วยกันกำหนดเป้าหมาย และทิศทางการดำเนินงานขององค์กรในอนาคต เพื่อที่จะสามารถออกการบริหารความมั่นคงปลอดภัยของสารสนเทศ ตามมาตรฐาน ISO:IEC/27001 : 2018 ที่มีความสอดคล้องกับเป้าหมายตามที่กำหนดได้ หรืออาจกล่าวได้ว่า หากเป้าหมายหรือวิสัยทัศน์ขององค์กรเปลี่ยน ก็จะส่งผลต่อการบริหารความมั่นคงปลอดภัยของสารสนเทศที่ต้องปรับเปลี่ยนไปเพื่อรองรับเป้าหมายใหม่ตามที่กำหนด ดังนั้น การบริหารความมั่นคงปลอดภัยของสารสนเทศจึงได้ถูกกำหนดให้มีการทบทวนเป็นประจำทุกปี

3.7 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการศึกษาทบทวนเอกสารที่เกี่ยวข้อง

การศึกษาทบทวนเอกสารที่เกี่ยวข้องจะแบ่งออกเป็น 2 ส่วน ได้แก่ เอกสารสำคัญที่เกี่ยวข้องกับการดำเนินงานของโรงงานไพ่ฯ ประกอบด้วย

1) วิสัยทัศน์ ยุทธศาสตร์ พันธกิจ และเป้าหมายขององค์กร

2) แนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศที่มีความเหมาะสมกับบริบทของโรงงานไพ่ ในกระบวนการนี้เนื่องจากการกำหนดวิสัยทัศน์ ยุทธศาสตร์ พันธกิจ และเป้าหมายขององค์กร ได้ผ่านการพิจารณาในกระบวนการกำหนดเป้าหมายในอนาคตขององค์กรแล้ว การกำหนดการบริหารความมั่นคงปลอดภัยของสารสนเทศที่มีความเหมาะสมกับบริบทของโรงงานไพ่ฯ จึงเป็นหน้าที่ของผู้เชี่ยวชาญที่จะต้องทำการศึกษาการบริหารความมั่นคงปลอดภัยของสารสนเทศที่เป็นมาตรฐานสากล โดยการวิเคราะห์เชิงเปรียบเทียบพิจารณาถึงข้อดี – ข้อจำกัดขององค์ประกอบต่างๆ เพื่อคัดเลือก และกำหนดการบริหารความมั่นคงปลอดภัยของสารสนเทศที่มีความเหมาะสมกับโรงงานไพ่ฯ โดยในการกำหนดผู้เชี่ยวชาญนั้น จะต้องกำหนดผู้เชี่ยวชาญที่เกี่ยวข้องและครอบคลุมการดำเนินงานในด้านต่าง ๆ ขององค์กร ไม่เพียงแต่เฉพาะด้านเทคโนโลยีดิจิทัลเท่านั้น แต่จะต้องครอบคลุมการดำเนินงานในด้านต่าง ๆ ขององค์กรด้วย เพื่อให้การศึกษา วิเคราะห์ และออกแบบการบริหารความมั่นคงปลอดภัยของสารสนเทศสามารถช่วยสนับสนุนการดำเนินงานในด้านต่าง ๆ ขององค์ได้อย่างเหมาะสม

3.8 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการสำรวจข้อมูล

การสำรวจข้อมูลเป็นการเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการดำเนินงานขององค์กรได้เข้ามามีส่วนร่วมในการแสดงความคิดเห็น ให้ข้อเสนอแนะ และวิพากษ์กในประเด็นที่เกี่ยวข้องกับการดำเนินงานขององค์กรที่ผ่านมา ในกระบวนการนี้จึงทำให้ทราบถึงบริบทการดำเนินงานของโรงงานไพ่ฯ ในปัจจุบัน ช่วยสะท้อนให้เห็นถึงปัญหา อุปสรรค และข้อจำกัดต่าง ๆ ทั้งด้านเทคโนโลยีดิจิทัล และการดำเนินงานขององค์กร ซึ่งจะมีผลต่อการ

บริหารความมั่นคงปลอดภัยของสารสนเทศที่เหมาะสมกับโรงงานไพ่ฯ ทั้งนี้เพราะในการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ที่มีความเหมาะสมกับโรงงานไพ่ฯ นั้น ไม่เพียงแต่จะพิจารณาเฉพาะกรอบการบริหารความมั่นคงปลอดภัยของสารสนเทศ องค์กรที่เป็นมาตรฐานเท่านั้น แต่จะต้องพิจารณาบริบทการดำเนินงานขององค์กรในปัจจุบันร่วมด้วย เพื่อให้ได้รับแนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ที่เป็นมาตรฐานและสามารถประยุกต์ใช้กับการดำเนินงานได้อย่างเหมาะสม ดังนั้น ในกระบวนการนี้นอกจากจะมีผู้มีผู้เชี่ยวชาญเข้ามาร่วมดำเนินการแล้ว ยังมีบุคลการของโรงงานไพ่ฯ ที่เป็นผู้รับผิดชอบในส่วนงานต่าง ๆ ซึ่งเป็นผู้ที่มีความรู้ความเข้าใจในส่วนงานที่ตนเป็นผู้รับผิดชอบเป็นอย่างดี โดยใช้วิธีการสัมภาษณ์เชิงลึก หรือการประชุมกลุ่มย่อย

3.9 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลจะประกอบไปด้วยการนำข้อมูลมาเปรียบเทียบกับแม่แบบของแนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตราฐานสากล ISO:IEC 27001:2018 พร้อมนำผลการดำเนินงานที่ผ่านมาร่วมกันวิเคราะห์ข้อมูลเพื่อหา ช่องว่าง (Gap) ต้องปรับปรุงแก้ไขเพื่อให้บรรลุเป้าหมายขององค์กรได้ในอนาคต จนนำไปสู่การสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัย ให้กับองค์กร คู่ค้า บุคคล หรือองค์กรภายนอกอื่นๆ และสร้างความยั่งยืนในการพัฒนาองค์กรให้สำเร็จตามวิสัยทัศน์ และกลยุทธ์ ขององค์กร

3.10 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการจัดทำแนวโยบายและแนวปฏิบัติ

แนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ มีการจัดทำตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO:IEC/27001:2018 ซึ่งมาตราฐานดังกล่าวจะมีแม่แบบในการดำเนินงานแต่ละขั้นตอนที่ชัดเจน ทั้งสิ้น 14 Domain โดยสามารถกำหนดเป็นกรอบนโยบายการบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร (IT Management) ดังนี้

1) นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)
3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)
4) การจัดหมวดหมู่และควบคุมทรัพย์สินองค์กร (Asset Management)
5) การควบคุมการเข้าถึง (Access Control)
6) การเข้ารหัสข้อมูล (Cryptography)
7) ความมั่นคงทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)
8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)
9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
10) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
11) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
13) การบริหารจัดการความมั่นคงปลอดภัยเพื่อสร้างความต่อเนื่องขององค์กร (Information security aspects of business continuity management)
14) ความสอดคล้อง (Compliance)

นอกจากนั้นแล้ว ยังต้องพิจารณาถึงหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสากิจ ตามระบบประเมินผลรัฐวิสาหกิจ (SE-AM) หัวข้อการพัฒนาเทคโนโลยีดิจิทัล ประเด็นด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ได้กำหนดหลักเกณฑ์การการบริหารจัดการความมั่นคงปลอดภัย ในด้านต่าง ๆ ทั้งในด้านของแนวทาง กระบวนการ การถ่ายทอดกระบวนการ การกำหนดตัววัด ติดตาม วิเคราะห์ และประเมินตัววัดผลลัพธ์ รวมทั้งการนำผลลัพธ์ที่ได้เข้าสู่กระบวนการการการบริหารจัดการความมั่นคงปลอดภัย ดังนั้น ในกระบวนการนี้จึงมีความเกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียต่าง ๆ หลายส่วน โดยเฉพาะอย่างยิ่ง ผู้เชี่ยวชาญด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ที่ต้องเป็นผู้รับผิดชอบหลักในการกำหนดรูปแบบ และออกแบบการบริหารความมั่นคงปลอดภัยของสารสนเทศในอนาคตที่มีความเหมาะสมกับโรงงานไพ่ฯ

3.11 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศองค์กรอย่างเป็นรูปธรรม

กระบวนการกำหนดกรอบแนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นรูปธรรม เป็นกระบวนการกำหนดการบริหารความมั่นคงปลอดภัยของสารสนเทศของโรงงานไพ่ฯ ไปปรับใช้กับการดำเนินงานในด้านต่าง ๆ เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องดำเนินงานภายใต้การบริหารความมั่นคงปลอดภัยของสารสนเทศที่กำหนดขึ้น โดยมีการกำหนดแนวทางที่ชัดเจน ภายใต้หลักการกำกับดูแลด้านดิจิทัล (Digital Governance) ประกอบด้วยแนวทางต่าง ๆ ได้แก่ กำหนดผู้รับผิดชอบในการบริหารความมั่นคงปลอดภัยของสารสนเทศ ประกาศนโยบาย กำหนดเป้าหมายในการดำเนินงาน และตัวชี้วัดผลการดำเนินงานการบริหารความมั่นคงปลอดภัยของสารสนเทศ กำหนดความสอดคล้องในการดำเนินงาน และสื่อสารให้ผู้มีส่วนได้ส่วนเสียในองค์กรได้รับทราบ ในกระบวนการนี้ผู้ที่ได้เข้ามามีบทบาทสำคัญ นอกจากนั้นแล้ว โรงงานไพ่ฯ ยังได้เปิดโอกาสให้ผู้บริหาร และพนักงานทุกคนในองค์กรได้เข้ามามีส่วนร่วมกับกระบวนการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นรูปธรรม ผ่านช่องทางการสื่อสารต่าง ๆ ได้แก่ ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ เว็บไซต์ของโรงงานไพ่ฯ ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ จดหมายอิเล็กทรอนิกส์ และแอพลิเคชั่นไลน์ (LINE) ทั้งนี้เพราะสถาปัตยกรรมองค์กรของโรงงานไพ่ฯ จะต้องถูกนำไปใช้กับทุกคนในองค์กร ดังนั้น จึงได้เปิดโอกาสให้ทุกคนในองค์กรได้เข้ามามีส่วนร่วมในการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศเพื่อให้มีความเหมาะสมกับบริบทการดำเนินงานของบุคลากรในโรงงานไพ่ฯ

3.12 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการถ่ายทอดกระบวนการการบริหารจัดการความมั่นคงปลอดภัย

การถ่ายทอดแนวนโยบายและแนวปฏิบัติด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความมั่นคงปลอดภัยได้เข้ามามีส่วนร่วมในการพิจารณาให้ข้อเสนอแนะ วิพากษ์ และร่วมแสดงความคิดเห็น เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับมาปรับปรุงและพัฒนากระบวนการฯ ให้มีประสิทธิภาพมากยิ่งขึ้นต่อไป จนเกิดการพัฒนาที่มีแนวทางการปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) โดยโรงงานไพ่ฯ ได้กำหนดให้มีการทบทวนปรับปรุงกระบวนการการบริหารจัดการความมั่นคงปลอดภัยเป็นประจำทุกปี ทั้งนี้ ผู้มีส่วนได้ส่วนเสียที่มีความเกี่ยวข้องกับกระบวนการนี้ จะประกอบด้วย ผู้อำนวยการโรงงานไพ่ฯ และผู้แทนในระดับหัวหน้าฝ่ายและหัวหน้าส่วนงานต่าง ๆ ของโรงงานไพ่ฯ ได้แก่ ฝ่ายอำนวยการ ฝ่ายโรงพิมพ์ ฝ่ายผลิตไพ่ ฝ่ายตรวจสอบภายใน ส่วนพัฒนาธุรกิจและการตลาด รวมทั้งส่วนสารสนเทศและพัฒนาระบบ จึงทำให้ได้รับมุมมองที่มีความหลากหลายครอบคลุมในมิติต่าง ๆ ในการดำเนินงานขององค์กร ผ่านช่องทางการสื่อสาร คือ การประชุมแบบเผชิญหน้า (Face to Face) หรือการประชุมออนไลน์ผ่านระบบการประชุมทางไกล (Video Conference)

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
1. กำหนดเป้าหมาย	1.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1.1.1 ผู้อำนวยการโรงงานไพ่ฯ 1.1.2 รองผู้อำนวยการโรงงานไพ่ฯ หัวหน้าฝ่ายอำนวยการ 1.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 1.2.2 เจ้าหน้าที่สารสนเทศฯ	การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management)	ส่วนสารสนเทศและพัฒนาระบบ
2. ศึกษาทบทวนเอกสารที่เกี่ยวข้อง	2.1 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 2.1.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2.1.2 เจ้าหน้าที่สารสนเทศ	ข้อมูลพื้นฐานที่สามารถนำมาช่วยในการออกแบบกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสารสนเทศที่เหมาะสมกับโรงงานไพ่ฯ ประกอบด้วย ● แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	ส่วนสารสนเทศและพัฒนาระบบ
3. สำรวจปัญหา อุปสรรค และความต้องการ	3.1 หัวหน้าฝ่ายงาน และส่วนงานต่าง ๆ หรือผู้แทนในแต่ละฝ่ายงาน ผู้ใช้ติดต่อ กับโรงงานไพ่	ผลการสำรวจข้อมูลของโรงงานไพ่ฯ ที่ทำให้ทราบถึง ● ปัญหา อุปสรรค การใช้งานระบบสารสนเทศ	ส่วนสารสนเทศและพัฒนาระบบ

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
		● ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	
4. วิเคราะห์ข้อมูล	4.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 4.1.1 ผู้อำนวยการโรงงานไพ่ฯ 4.1.2 รองผู้อำนวยการโรงงานไพ่ฯ 4.1.3 หัวหน้าฝ่ายอำนวยการ 4.1.4 หัวหน้าฝ่ายโรงพิมพ์ 4.1.5 .หัวหน้าส่วนแผนงานและกลยุทธ์ 4.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 4.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 4.2.2 เจ้าหน้าที่สารสนเทศ	ข้อเสนอแนะ คำแนะนำ และแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ
5. จัดทำแนวโยบายและแนวปฏิบัติฯ	5.1 การจัดทำแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วย 5.1.1 หัวหน้าฝ่าย / หัวหน้าส่วน 5.1.2 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 5.1.3 เจ้าหน้าที่สารสนเทศ	ร่างแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
6. พิจารณาแนวนโยบายและแนวปฏิบัติฯ	6.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 6.1.1 ผู้อำนวยการโรงงานไพ่ฯ 6.1.2 รองผู้อำนวยการโรงงานไพ่ฯ 6.1.3 หัวหน้าฝ่ายอำนวยการ 6.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 6.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 6.2.2 เจ้าหน้าที่สารสนเทศฯ	แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	ผู้บริหารและพนักงานของโรงงานไพ่ฯ ทุกคน
7. ประกาศใช้แนวนโยบายและแนวปฏิบัติฯ	7.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 7.1.1 ผู้อำนวยการโรงงานไพ่ 7.1.2 รองผู้อำนวยการโรงงานไพ่ 7.1.3 หัวหน้าฝ่ายอำนวยการ	แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	ผู้บริหารและพนักงานของโรงงานไพ่ฯ ทุกคน
8. ติดตามผลการดำเนินงาน	8.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 8.1.1 ผู้อำนวยการโรงงานไพ่ 8.1.2 รองผู้อำนวยการโรงงานไพ่ 8.1.3 หัวหน้าฝ่ายอำนวยการ 8.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 8.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 8.2.2 เจ้าหน้าที่สารสนเทศฯ	ผลการประเมิน ความคิดเห็น และข้อเสนอแนะต่าง ๆ	ส่วนสารสนเทศและพัฒนาระบบนำข้อมูลที่ได้มาปรับปรุงกระบวนการการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4. ถ่ายทอดกระบวนการการบริหารจัดการความมั่นคงปลอดภัย

โรงงานไพ่ฯ ได้กำหนดวิธีการถ่ายทอดกระบวนการการบริหารจัดการความมั่นคงปลอดภัย โดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ ทั้งนี้ โรงงานไพ่ฯ ได้ประยุกต์ใช้แบบจำลองการสื่อสารดังกล่าว สำหรับการถ่ายทอดกระบวนการการบริหารจัดการความมั่นคงปลอดภัย ดังนี้

4.1 ผู้ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการการบริหารจัดการความมั่นคงปลอดภัย โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล และคณะทำงานกำกับดูแลและการบริหารจัดการสถาปัตยกรรมองค์กรพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

4.2 ข้อมูลข่าวสาร (Message)

ข้อมูลข่าวสาร ได้แก่ กระบวนการการบริหารจัดการความมั่นคงปลอดภัย ที่ผ่านการพิจารณาจากคณะอนุกรรมการฯ และคณะทำงานฯ โดยได้รับการรับรองความถูกต้องเป็นที่เรียบร้อยแล้ว

4.3 ช่องทางการสื่อสาร (Channel)

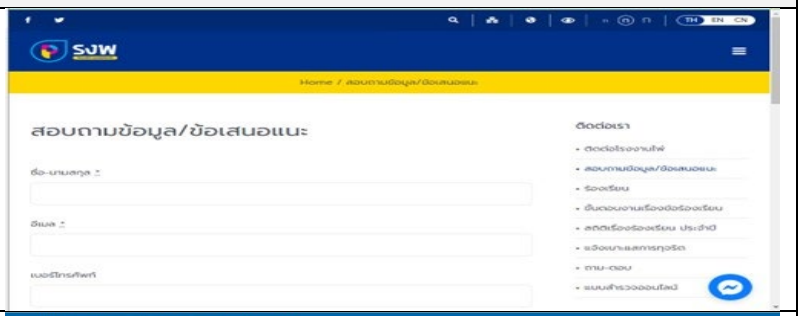
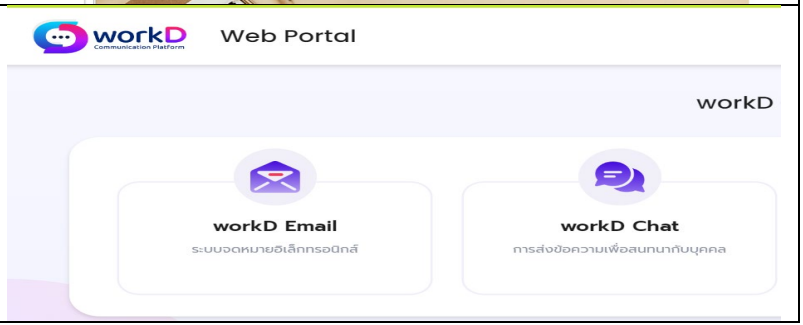
ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้

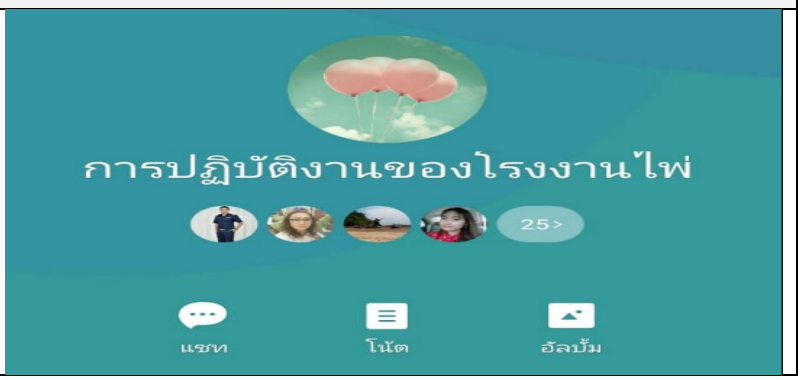
1) สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการ และหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารผ่านที่ประชุมคณะอนุกรรมการด้านเทคโนโลยีดิจิทัล

ตำแหน่ง	ภาพประกอบ
หน้าทางเข้าโรงงานไพ่ฯ	
ห้องสันทนาการ	

ตำแหน่ง	ภาพประกอบ
หน้าห้องส่วนบริหารงานกลาง	

2) สื่อสมัยใหม่ ประกอบด้วย เว็บไซต์ของโรงงานไพ่ฯ ได้แก่(https://www.playingcard.or.th/) ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)และแอพลิเคชั่นไลน์ (LINE) โดยในช่องทางดังกล่าว ได้เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถให้ความคิดเห็น และข้อเสนอแนะต่าง ๆ ที่เกี่ยวข้องกับกระบวนการวิเคราะห์และการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อมที่สามารถเข้าถึงได้จากอุปกรณ์การอิเล็กทรอนิกส์ต่าง ๆ ทั้งสมาร์ทโฟน และคอมพิวเตอร์ เพื่อที่จะสามารถนำข้อมูลต่าง ๆ เหล่านั้นมาปรับปรุงและพัฒนากระบวนการฯ ให้มีประสิทธิภาพมากขึ้นต่อไป

สื่อที่ใช้	ภาพประกอบ
เว็บไซต์ของโรงงานไพ่ฯ (https://www.playingcard.or.th/)	
ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ	
ระบบการสื่อสารแบบรวมศูนย์ (workD Platform) -workD Mail ระบบจดหมายอิเล็กทรอนิกส์ (saraban@playingcard.mail.go.th) -workD Chat การส่งข้อความเพื่อสนทนา	

สื่อที่ใช้	ภาพประกอบ
แอพลิเคชั่นไลน์ (LINE)	

4.4 ผู้รับสาร (Receiver)

ผู้รับสาร หรือผู้ที่มีความเกี่ยวข้องกับข้อมูลข่าวสารในกระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศ ได้แก่ บุคลากรของโรงงานไพ่ฯ ทั้งในระดับผู้บริหาร พนักงาน และผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้อง

5. ประเมินการรับรู้จากผู้ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ

ในขั้นตอนนี้เป็นกระบวนการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และการดำเนินการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศของโรงงานไพ่ฯ ที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่ง ในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุงแก้ไข และพัฒนากระบวนการวิเคราะห์และการดำเนินการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศของโรงงานไพ่ฯ ให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องกับกระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศ จำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ ได้ดังนี้

วิธีการประเมินการรับรู้

กระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศ	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
1. กำหนดเป้าหมาย	1.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ 1.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	ผู้บริหารในระดับต่างๆ ได้เข้ามามีส่วนร่วมกับการกำหนดเป้าหมายของกระบวนการบริหารความมั่นคงปลอดภัยของสารสนเทศของสารสนเทศผ่านการประชุม	● รายงานการประชุม
2. ศึกษาทบทวนเอกสารที่เกี่ยวข้อง	2.1 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ และเจ้าหน้าที่สารสนเทศได้ศึกษา ทบทวนทั้งปัจจัยภายนอก และปัจจัยภายในเพื่อพิจารณาทบทวนเอกสารต่าง ๆ ที่เกี่ยวข้อง	● ผลการศึกษาทบทวนเอกสารที่เกี่ยวข้อง
3. สำรวจปัญหา อุปสรรค และความต้องการ	3.1 หัวหน้าฝ่าย/ส่วนงานต่าง ๆ หรือผู้แทนในแต่ละฝ่ายงาน	นัดสัมภาษณ์เชิงลึกกับหัวหน้าฝ่าย/ส่วนงานต่าง ๆ	● รายงานสรุปผลการสำรวจข้อมูล ● แบบสัมภาษณ์
4. วิเคราะห์ข้อมูล	4.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ 4) หัวหน้าฝ่ายโรงพิมพ์	● ทำหนังสือเวียนถึงผู้บริหาร เพื่อพิจารณาผลการวิเคราะห์ข้อมูล	● รายงานผลการวิเคราะห์ข้อมูล ● หนังสือเวียน

กระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศ	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
	5) หัวหน้าส่วนแผนงานและกลยุทธ์ 4.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศ		
5. จัดทำแนวโยบายและแนวปฏิบัติฯ	5.1 การจัดทำแผนการดำเนินการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศขององค์กร ประกอบด้วย 1) หัวหน้าฝ่าย/ส่วนงานต่าง ๆ ของโรงงานไพ่ฯ 2) หัวหน้าส่วนสารสนเทศ 3) เจ้าหน้าที่ส่วนสารสนเทศ	ผู้มีส่วนเกี่ยวข้องร่วมกันเพื่อพิจารณาออกแบบกระบวนการบริหารความมั่นคงปลอดภัยของสารสนเทศของสารสนเทศของโรงงานไพ่ฯ	● กระบวนการบริหารความมั่นคงปลอดภัยของสารสนเทศของสารสนเทศของโรงงานไพ่ฯ ● เอกสารสรุปรายงานประชุม
6. พิจารณาแนวนโยบายและแนวปฏิบัติฯ	6.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ 6.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	ทำบันทึกข้อความถึงผู้อำนวยการ เพื่อพิจารณาเห็นชอบผลการทบทวนการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)	● การบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) ● บันทึกข้อความ
7. ประกาศใช้แนวนโยบายและแนวปฏิบัติฯ	7.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 1) ผู้อำนวยการโรงงานไพ่ 2) รองผู้อำนวยการโรงงานไพ่ 3) หัวหน้าฝ่ายอำนวยการ	● นำกระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศเข้าสู่ที่ประชุม	● หนังสือเวียน ● การบริหารความมั่นคงปลอดภัยของสารสนเทศ

กระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศ	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
	7.2 หัวหน้าฝ่าย/ส่วนต่างๆ 7.3 พนักงานโรงงานไพ่ 7.4 ผู้ติดต่อประสานงานกับโรงงานไพ่	คณะอนุกรรมการด้านเทคโนโลยีดิจิทัลเพื่อพิจารณา ● ใช้แบบสอบถามประเมินการรับรู้ด้านกระบวนการวิเคราะห์และการดำเนินการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศของโรงงานไพ่ฯ	(Information Security Management)
8. ติดตามผลการดำเนินงาน	8.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 1) ผู้อำนวยการโรงงานไพ่ 2) รองผู้อำนวยการโรงงานไพ่ 3) หัวหน้าฝ่ายอำนวยการ 8.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	● ติดตามผลการประเมินจาก ตัวชี้วัดการดำเนินกิจกรรม โครงการต่างๆ ทางด้านเทคโนโลยีดิจิทัล ว่าสอดคล้อง เป็นไปตามแผนทางการบริหารจัดการใช้ทรัพยากรอย่างเหมาะสมหรือไม่	● การดำเนินกิจกรรมโครงการต่าง ๆ ทางด้านเทคโนโลยีดิจิทัลสอดคล้อง เป็นไปตามแผนทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

สรุปโรงงานไพ่ฯ ได้กำหนดวิธีการประเมินผลการรับรู้กระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศด้วยรูปแบบที่แตกต่างกัน จำแนกตามผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการต่าง ๆ ซึ่งได้ผ่านการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการมาเป็นที่เรียบร้อยแล้ว ทั้งนี้เพราะผู้มีส่วนได้ส่วนเสียต่าง ๆ เหล่านั้น ล้วนเป็นส่วนหนึ่งของการจัดทำ พัฒนา และยกระดับกระบวนการบริหารความมั่นคงปลอดภัยของสารสนเทศของสารสนเทศของโรงงานไพ่ฯ ให้ดียิ่งขึ้น ดังนั้น การจัดทำสถาปัตยกรรมองค์ในครั้งนี้ จึงเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้เข้ามามีส่วนร่วมในการแสดงความคิดเห็น และให้ข้อเสนอแนะสำหรับการปรับปรุงกระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งสอดคล้องกับหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยโรงงานไพ่ฯ ได้กำหนดให้การประเมินการรับรู้ดำเนินการควบคู่กับการจัดทำกระบวนการวิเคราะห์และการบริหารความมั่นคงปลอดภัยของสารสนเทศเป็นประจำทุกปี เพื่อให้กระบวนการมีแนวทางปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice)

หมายเหตุ : บันทึกข้อความที่ 180/2566 วันที่ 4 กรกฎาคม 2566

บทที่ 4
การวัดผล ติดตาม และประเมินผล การบริหารความมั่นคงปลอดภัยของสารสนเทศ

1. วัตถุประสงค์

1) เพื่อให้การบริหารความมั่นคงปลอดภัยของสารสนเทศได้รับการดูแล และติดตาม อย่างต่อเนื่อง

2) เพื่อวางแผนทบทวน ผลการดำเนินการบริหารความมั่นคงปลอดภัยของสารสนเทศ และหาแนวทางปรับปรุงพัฒนาให้มีประสิทธิภาพ

2. ขั้นตอนการวัดผล และติดตาม

ส่วนงานเทคโนโลยีสารสนเทศ มีการกำหนดขั้นตอนการวัดผล ติดตาม และประเมินผล ของนโยบายทุกหมวดหมู่ที่เกี่ยวข้องกับงานด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ดังนี้

ด้านผู้ใช้งานระบบ

1) ผู้ใช้งานระบบของโรงงานไพ่ กรมสรรพสามิต ร้องขอให้ส่วนงานเทคโนโลยีสารสนเทศดำเนินการในเรื่องต่างๆ โดยส่งคำร้อง ผ่านระบบ ezSUPPORT ซึ่งระบบดังกล่าวมีการจัดหมวดหมู่ และประเภทคำร้องขอให้เลือกอย่างเป็นระบบ

2) ส่วนงานเทคโนโลยีสารสนเทศ รับคำร้องขอตามข้อ (1) และดำเนินการตามคำร้องขอในกรอบระยะเวลา และแนวทางการให้บริการที่วางไว้

3) ผู้ใช้งานระบบ สามารถติดตาม และเช็คสถานะคำร้องขอได้เองผ่านระบบ ezSUPPORT

4) ผู้ใช้งานระบบ ต้องทำการประเมินผลความพึงพอใจในการใช้บริการ ผ่านระบบออนไลน์หลังคำร้องขอได้รับการดำเนินการแล้วเสร็จ

5) เจ้าหน้าที่ส่วนงานเทคโนโลยีสารสนเทศ มีการทำรายงานสรุปปัญหาประจำเดือน ส่งให้หัวหน้างานรับทราบ เพื่อวิเคราะห์ปริมาณปัญหาหรือคำรอง พร้อมวิเคราะห์ผลการประเมิน

ด้านผู้ดูแลระบบ

1) ติดตาม ตรวจสอบ ระบบฮาร์ดแวร์ ซอฟท์แวร์ รวมถึงระบบต่างๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ อย่างต่อเนื่องและสม่ำเสมอ หรือตามกรอบระยะเวลาที่กำหนดไว้

2) กำหนดเป้าหมาย และประเมินผลงานด้านระบบ ตามกรอบระยะเวลา

3. หลักเกณฑ์การประเมิน

3.1 จากผลคะแนนความพึงพอใจ โดยตั้งเป้าหมายสำฤทธิ์ผลโดยรวมไม่ต่ำกว่าร้อยละ 80 ทั้งนี้แบ่งกรอบการประเมินความพึงพอใจเป็น 4 หมวดหลัก ดังนี้

- ด้านเทคโนโลยีการให้บริการ
- ด้านขั้นตอน / กระบวนการให้บริการ
- ด้านเจ้าหน้าที่ผู้ให้บริการ
- ด้านคุณภาพ

ภายใต้หลักเกณฑ์ด้านนโยบายการบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งเล็งเห็นแล้วว่าทุกหมวดของหัวข้อการประเมินความพึงพอใจจะเชื่อมโยงเกี่ยวกับนโยบายในทุกหัวข้อของโรงงานไพ่ โดยแบ่งวิธีการให้คะแนนสำหรับผู้ประเมินในแต่ละหัวข้อเป็น 3 ระดับ (ตั้งแต่ระดับ 1 ถึง ระดับ 3) และเมื่อวิเคราะห์ผลการประเมินแล้ว นำมากำหนดกรอบเป้าหมายเป็นร้อยละดังนี้

ผลคะแนนเฉลี่ย	ค่าการประเมิน	ความหมาย
2.34 – 3.00	มากที่สุด	อยู่ในเกณฑ์ดีมาก / ควรมีแผนในการรักษามาตรฐานให้ "คงอยู่" ต่อไป
1.68 – 2.33	ปานกลาง	อยู่ในเกณฑ์ดี / ควรมีแผนในการพัฒนามาตรฐานเพื่อให้ขึ้นสู่ระดับ "ดีมาก"
1.00 – 1.67	น้อยที่สุด	อยู่ในเกณฑ์ต่ำกว่ามาตรฐาน / ควรมีแผนในการเร่งปรับปรุงโดยด่วน

3.2 จากการวิเคราะห์ตัวเลขเคสในหมวด “[OSC] แจ้งปัญหาการใช้งาน” และ “[ASK] สอบถามข้อมูลทั่วไป” จากระบบ ezSUPPORT โดยวิเคราะห์ตัวเลขเคสในสองหมวดดังกล่าวจากสรุปรายงานประจำเดือน และกำหนดกรอบการสัมฤทธิ์ผลโดยให้เป้าหมายปริมาณตัวเลขเคสทั้งสองหมวดต้องลดลงไม่ต่ำกว่าร้อยละ 3 ในแต่ละไตรมาส

3.3 จากการติดตามดูแลระบบจากฝ่ายเทคโนโลยีสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศตั้งเป้าหมายเพื่อควบคุมการทำงานของทีมเป็นการภายใน โดยกำหนดเป้าหมายการสัมฤทธิ์ผลจากการดำเนินการปิดเคสผ่านระบบ ezSUPPORT ทั้งสามหมวด ประกอบด้วย [OSC] แจ้งปัญหาการใช้งาน, [REQ] ยื่นคำร้อง/คำขอ และ “[ASK] สอบถามข้อมูลทั่วไป” ซึ่งพิจารณาวัดผลในภาพรวมทุกหัวข้อ เนื่องจากเป็นเรื่องที่เกี่ยวโยงกับมาตรการบริหารความมั่นคงปลอดภัยของสารสนเทศทั้งสิ้น โดยมีเป้ามายต้องดำเนินการปิดเคสให้แล้วเสร็จภายในเวลาที่กำหนดไม่ต่ำกว่าร้อยละ 80 จากจำนวนเคสทั้งหมด

4. ผลการประเมินประจำปีงบประมาณ 2566

4.1 จากผลการประเมินจากคะแนนความพึงพอใจ

จากการวิเคราะห์ความพึงพอใจ พบว่า ปีงบประมาณ 2566 มีผู้ใช้บริการทางด้านสารสนเทศที่แก้ไขแล้วเสร็จทั้งสิ้น จำนวน 56 เคส โดยส่วนสารสนเทศฯ ได้ดำเนินการสอบถามความพึงพอใจของผู้ใช้บริการพบว่า

ผู้ใช้งานมีความพึงพอใจลำดับที่ 1 ด้านเจ้าหน้าที่ผู้ให้บริการ ที่ร้อยละ 93.90

ลำดับที่ 2 ด้านเทคโนโลยีการให้บริการ ที่ร้อยละ 93.25

ลำดับที่ 3 ด้านคุณภาพ ที่ร้อยละ 92.26

และลำดับที่ 4 ด้านขั้นตอน/กระบวนการให้บริการ ที่ร้อยละ 88.99 รายละเอียดตามตารางดังนี้

สรุปผลการประเมินความพึงพอใจโดยรวมในแต่ละหมวดเป็นไปตามเป้าหมายที่ไม่ต่ำกว่าร้อยละ 80 เห็นควรรักษามาตรฐานให้คงอยู่ต่อไป รวมถึงสามารถพัฒนาให้ดียิ่งขึ้นในลำดับถัดไป

รายการประเมิน	ระดับความพึงพอใจ (จำนวนคน)			คิดเป็นร้อยละความพึงพอใจ
	มากที่สุด	ปานกลาง	น้อยที่สุด	
1. ด้านเทคโนโลยีการให้บริการ (ร้อยละ 93.25)				
- ความสะดวกในการเข้าใช้งาน	46	9	1	93.45
- รูปแบบการใช้งานระบบ ความยาก - ง่าย	44	10	2	91.67
- ความสะดวกในการติดตามสถานะของงานอย่างต่อเนื่อง	49	5	2	94.64
2. ด้านขั้นตอน/กระบวนการให้บริการ (ร้อยละ 88.99)				
- มีกระบวนการและขั้นตอนการให้บริการที่เหมาะสม	44	7	5	89.88
- ระยะเวลาการให้บริการที่เหมาะสม	41	10	5	88.10
3. ด้านเจ้าหน้าที่ผู้ให้บริการ (ร้อยละ 93.90)				
- ให้บริการด้วยความสุภาพ เป็นมิตร	45	10	1	92.86
- มีความตั้งใจและกระตือรือร้นในการให้บริการ	50	5	1	95.83
- ให้คำแนะนำและตอบข้อซักถามได้เป็นอย่างดี	51	5	0	97.02
- ความพร้อมของเจ้าหน้าที่ในการให้บริการ	45	5	6	89.88
4. ด้านคุณภาพ (ร้อยละ 92.26)				
- ได้รับบริการที่ครบถ้วน	47	5	4	92.26
- ได้รับบริการที่ถูกต้อง	41	9	6	87.50
- ได้รับบริการที่เป็นประโยชน์ต่อการดำเนินงาน	43	9	4	89.88

4.2 จากผลการประเมินจากการวิเคราะห์ตัวเลขเคสในหมวด “[OSC] แจ้งปัญหาการใช้งาน” และ “[ASK] สอบถามข้อมูลทั่วไป” จากระบบ ezSUPPORT

จากการวิเคราะห์ตัวเลขเคสหมวด “แจ้งปัญหาการใช้งาน” พบว่าปริมาณตัวเลขไตรมาส 1 ปี พ.ศ. 2565 เพิ่มขึ้นจากไตรมาส 4 ปี พ.ศ.2564 ร้อยละ 50, ปริมาณตัวเลขไตรมาส 2 ปี พ.ศ.2565 ลดลงจากไตรมาส 1 ร้อยละ 54 และปริมาณตัวเลขไตรมาส 3 เพิ่มขึ้นจากไตรมาส 2 ร้อยละ 36

สำหรับไตรมาส 2 และ 4 พบว่าปริมาณตัวเลขเพิ่มขึ้น ส่งผลให้ประสิทธิผลไม่เป็นไปตามเป้ามายที่กำหนดไว้ จึงเห็นควรพิจารณาทบทวนหาแนวทางปรับปรุงแก้ไขในไตรมาสถัดไป โดยเฉพาะอย่างยิ่งเรื่อง “[ZHW-PCM] คอมพิวเตอร์และอุปกรณ์ต่อพ่วง” ซึ่งเป็นหัวข้อปัญหาหาหลักที่ส่งผลให้ปริมาณตัวเลขเพิ่มขึ้น

หมวด [OSC] แจ้งปัญหาการใช้งาน

หัวข้อปัญหา	ปริมาณปัญหา			
	ไตรมาส 1 ต.ค.-ธ.ค.65	ไตรมาส 2 ม.ค.-มี.ค.66	ไตรมาส 3 เม.ย.-มิ.ย.66	ไตรมาส 4 ก.ค.-ก.ย.66
[MS-O365] Office 365	1	0	0	0
[WORKD] ระบบการสื่อสารแบบรวมศูนย์ workD Platform	0	0	0	1
[ERP-ACP] ระบบจ่ายเงิน	0	1	1	1
[ERP-ACR] ระบบรับเงิน	0	2	0	0
[ERP-BUD] ระบบควบคุมงบประมาณ	0	1	0	0
[ERP-FIX] ระบบสินทรัพย์ถาวร	2	0	0	0
[ERP-GEN] ระบบบัญชีแยกประเภท	3	7	3	1
[ERP-HRM] ระบบทรัพยากรบุคคล	0	2	0	1
[ERP-INV] ระบบควบคุมสินค้าคงคลัง	0	0	2	1
[ERP-MNF] ระบบควบคุมการผลิต	0	0	0	0
[ERP-PUR] ระบบจัดซื้อจัดจ้าง	0	0	1	2
[ERP-SAL] ระบบงานขาย	0	0	1	0
[MSP-ABI] ระบบสารสนเทศสำหรับผู้บริหาร,	0	0	0	0
[VNC-EDC] ระบบสารบรรณอิเล็กทรอนิกส์	0	0	0	0
[WEB-ECM] ระบบ E-Commerce	0	0	0	0
[WEB-INT] เว็บไซต์ภายในองค์กร	0	0	0	0
[WEB-PCF] เว็บไซต์หลัก	0	0	0	0
[ZHW-PCM] คอมพิวเตอร์และอุปกรณ์ต่อพ่วง	1	1	0	2
[ZNW-INT] ระบบเครือข่ายและอินเทอร์เน็ต	0	2	0	1
[ZSW-APP] ซอฟต์แวร์อื่น ๆ	7	1	4	3
รวม	14	17	12	13
ร้อยละ (+ / -)		17.65	-41.67	7.69

หมวด [ASK] สอบถามข้อมูลทั่วไป

จากการวิเคราะห์ตัวเลขการสอบถามข้อมูลทั่วไปพบว่ามีปริมาณที่น้อยมาก จึงยังไม่นำเข้าสู่กระบวนการวิเคราะห์ แต่ควรเฝ้าติดตามดูแล และหากพบว่ามีแนวโน้มที่เพิ่มขึ้นสามารถปรับปรุงคู่มือหรือสร้างเป็น Knowledge base เพื่อให้ผู้ใช้งานศึกษาข้อมูลในเรื่องที่เกี่ยวข้องเองได้บนอินทราเน็ตในลำดับถัดไป

4.3 จากการติดตามดูแลระบบจากฝ่ายเทคโนโลยีสารสนเทศ

จากปริมาณเคสทั้งหมดที่แจ้งผ่านระบบ ezSUPPORT ในปีงบประมาณ 2566 จำนวนทั้งสิ้น 56 เคส แก้ไขและปิดเคสได้ภายในระยะเวลาที่กำหนด จำนวนทั้งสิ้น 49 เคส คิดเป็นร้อยละ 87.5 ซึ่งเป็นไปตามเป้าหมายที่กำหนดไว้ (ไม่ควรต่ำกว่าร้อยละ 80)

บทที่ 5
การทบทวน ปรับปรุง แผนการบริหารความมั่นคงปลอดภัยของสารสนเทศ

1. แผนระดับองค์กร

มีการทบทวน ปรับปรุง และวางแผน เป็นประจำทุก 1 ปี โดยนำคะแนนผลการประเมินจากผู้ใช้งานมาวิเคราะห์และทบทวนร่วมกับผลการประเมินผ่านการเฝ้าติดตามจากผู้ดูแลระบบสารสนเทศ และดำเนินการศึกษาทบทวนเอกสารที่เกี่ยวข้อง ตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ อันได้แก่

ปัจจัยภายนอก

- นโยบายรัฐบาลด้านเทคโนโลยีดิจิทัล, ยุทธศาสตร์ชาติ พ.ศ. 2561-2580, แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. 2561-2580), แผนการปฏิรูปประเทศ (ฉบับปรับปรุง) ด้านสื่อมวลชน เทคโนโลยีสารสนเทศ, แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13, แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566-2570, แผนยุทธศาสตร์รัฐวิสาหกิจ พ.ศ. 2566-2570, ยุทธศาสตร์กรมสรรพสามิต ปี 2566, แผนยุทธศาสตร์ของโรงงานไพ่ฯ ประจำปี 2567-2571, พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ,พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ , พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล , พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ , พระราชบัญญัติลิขสิทธิ์ , พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกฎหมายอื่นๆที่เกี่ยวข้อง
- เทรน แนวโน้ม ทางด้านเทคโนโลยีดิจิทัล ISO/IEC 27001:2018 และปัจจัยอื่นๆ ที่เกี่ยวข้อง

ปัจจัยภายใน

- แผนวิสาหกิจ แผนการบริหารนวัตกรรม แผนด้านการตลาด แผนยุทธศาสตร์องค์กร , แผนบริหารทรัพยากรบุคคล แผนอื่นๆที่เกี่ยวข้อง และ ระเบียบ นโยบาย ที่เกี่ยวข้อง
- แบบสัมภาษณ์ และแบบสำรวจผู้บริหาร และพนักงาน

2. แผนระดับส่วนสารสนเทศและพัฒนาระบบ

มีการทบทวน ปรับปรุง อย่างต่อเนื่องเป็นรายไตรมาศ โดยนำคะแนนผลการประเมินจากผู้ใช้งานมาวิเคราะห์และทบทวน ร่วมกับผลการประเมินผ่านการเฝ้าติดตามจากผู้ดูแลระบบสารสนเทศ

3. แนวทางในการทบทวนเพื่อจัดทำแผนงานขององค์กรในระยะยาว

1) นำผลคะแนนประเมินความพึงพอใจในแต่ละหมวดหมู่มาทำการวิเคราะห์ หากเรื่องใด ได้รับคะแนนประเมินต่ำกว่ามาตรฐาน ให้ถือเป็นเรื่องที่ควรดำเนินการจัดทำแผนปรับปรุงเป็นกรณีเร่งด่วน

2) นำตัวเลขปัญหาหรือคำร้องเรียนมาวิเคราะห์ หากเรื่องใด มีแนวโน้มเพิ่มขึ้นในแต่ละไตรมาศ ให้ถือเป็นเรื่องที่ควรดำเนินการจัดทำแผนปรับปรุงเป็นกรณีเร่งด่วน

KPI 5 การบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)

KPI 5.2 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management)

เอกสารโดย

ส่วนสารสนเทศและพัฒนาระบบ
โรงงานไพ่ กรมสรรพสามิต

รหัสเอกสาร IT-DOC-KPI5-002
ปรับปรุงล่าสุด 3 กรกฎาคม 2566

บทนำ

1. หลักการและเหตุผล

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อดำเนินงานบริหารความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงาน การตัดสินใจด้านต่างๆ การวางแผนงาน การกำหนดกลยุทธ์ การติดตามควบคุมและการวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น อีกทั้งช่วยลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กรในด้านการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และสามารถปฏิบัติงานได้ทุกๆ สถานการณ์

ดังนั้นการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุถึงปัจจัยความเสี่ยงใดที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น การจัดลำดับความสำคัญของปัจจัยเสี่ยง เพื่อกำหนดแนวทางในการจัดการความเสี่ยงโดยคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

2. วัตถุประสงค์

1) กำหนดกรอบการปฏิบัติงานในกระบวนการบริหารความเสี่ยงทางด้านสารสนเทศที่มีความสอดคล้องกัน เพื่อให้ผู้บริหารและผู้ปฏิบัติงานทุกระดับมีความรู้ ความเข้าใจในหลักการ แนวคิด วิธีการ กระบวนการและขั้นตอนการบริหารความเสี่ยง เพื่อนำไปปฏิบัติทั่วทั้งองค์กรในช่องทางที่เกี่ยวข้องอย่างมีประสิทธิภาพ

2) เพื่อให้มั่นใจว่ามีการกำหนดหน้าที่ความรับผิดชอบในการควบคุมความเสี่ยงที่ได้ระบุไว้อย่างเหมาะสม

3) เพื่อเป็นเครื่องมือให้ปฏิบัติงานตามนโยบายการบริหารความเสี่ยง อย่างเป็นระบบ มีการทำซ้ำและต่อเนื่อง รวมถึงตอบสนองต่อการเปลี่ยนแปลง เพื่อให้มั่นใจว่า สอดคล้องกับวัตถุประสงค์ เป้าหมาย กลยุทธ์ หรือวิสัยทัศน์ขององค์กร

4) เพื่อเป็นแนวทางในการติดตามและประเมินผลการดำเนินงานให้มีประสิทธิภาพ และประสิทธิผล สามารถรับมือกับความเสี่ยงที่เกิดขึ้นในอนาคต

5) เพื่อเป็นเครื่องมือช่วยในการปลูกฝังวัฒนธรรมองค์กรที่มุ่งเน้นการสร้างองค์ความรู้ ด้านการบริหารความเสี่ยงไปยังผู้บริหารและบุคลากรทุกระดับ

สารบัญ

สารบัญ

บทที่ 1
แนวทางในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

แนวทางในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจัดทำขึ้นเพื่อเป็นกรอบ แนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง ตอบสนองความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้ยอมรับได้ โดยมุ่งหวังให้โรงงานไพ่ฯ สามารถบรรลุตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม จึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite) ฝ่ายเทคโนโลยีสารสนเทศและพัฒนาระบบหวังเป็นอย่างยิ่งว่า คู่มือและการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศฉบับนี้จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของโรงงานไพ่ฯ ต่อไป

ทั้งนี้คู่มือฉบับนี้จัดทำขึ้นภายใต้กรอบหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM โดยมีองค์ประกอบดังนี้

1. กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ของรัฐวิสาหกิจ

2. รัฐวิสาหกิจมีการกำหนดปัจจัยภายในและภายนอกที่สอดคล้องกับวัตถุประสงค์และบริบทขององค์กร ซึ่งส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

3. รัฐวิสาหกิจมีนโยบายหรือแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศโดยอย่างน้อยประกอบด้วย

3.1 โครงสร้างองค์กรและบทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้มีหน้าที่และความรับผิดชอบดังนี้

1) คณะกรรมการโรงงานไพ่

มีบทบาทหน้าที่และความรับผิดชอบหลักในการกำกับดูแลและติดตามการบริหารความเสี่ยงและควบคุมภายในกำกับดูแลและติดตามผลการดำเนินการ ดังนี้

- เป็นผู้แต่งตั้งคณะอนุกรรมการที่ประกอบด้วย 1.ประธานอนุกรรมการ ซึ่งมาจากคณะกรรมการโรงงานไพ่ 2. อนุกรรมการ 3. อนุกรรมการและเลขานุการ
- กำกับดูแลและสนับสนุนการดำเนินงานด้านการบริหารความเสี่ยงและการควบคุมภายในผ่านคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน รวมทั้งผู้บริหารระดับสูง
- ติดตามผลการปฏิบัติงานตามนโยบาย รวมทั้งแผนงานต่าง ๆ ของการบริหารความเสี่ยงและควบคุมภายใน
- มีความเข้าใจและตระหนักเกี่ยวกับความเสี่ยงที่อาจส่งผลกระทบต่อโรงงานไพ่ และทำให้มั่นใจว่าโรงงานไพ่ จะดำเนินการอย่างเหมาะสมเพื่อจัดการความเสี่ยงนั้น
- มีให้ข้อเสนอแนะเรื่องการบริหารความเสี่ยงและการควบคุมภายในของโรงงานไพ่
- ติดตามผลการดำเนินงานจากคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน โรงงานไพ่ เพื่อให้มั่นใจว่ามีการดำเนินการที่เหมาะสมในการจัดการความเสี่ยงของโรงงานไพ่โดยรวม

และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้และมีระบบการควบคุมภายในที่เพียงพอ

2). คณะกรรมการตรวจสอบ

มีบทบาทหน้าที่และความรับผิดชอบหลักในการกำกับดูแลและติดตามการบริหารความเสี่ยงและควบคุมภายในอย่างเป็นอิสระ ดังนี้

- สอบทานกรอบการบริหารความเสี่ยงและการควบคุมภายใน และเสนอแนะวิธีการปรับปรุงในกรณีที่จำเป็น เพื่อให้มั่นใจว่ากรอบการบริหารความเสี่ยงและการควบคุมภายในได้รับการปฏิบัติอย่างมีประสิทธิภาพและประสิทธิผล
- มีความเข้าใจในความเสี่ยงที่สำคัญของโรงงานไพ่ และสอบทานเพื่อให้มั่นใจว่าผู้บริหารมีกระบวนการจัดการความเสี่ยงและการควบคุมภายในอย่างมีประสิทธิภาพและประสิทธิผล และทำให้เกิดความมั่นใจว่าโรงงานไพ่มีการควบคุมภายในที่เหมาะสมเพื่อจัดการความเสี่ยงทั่วทั้งองค์กร
- ทำให้มั่นใจว่ามีการควบคุมภายในที่เหมาะสมเพื่อจัดการความเสี่ยงทั่วทั้งองค์กร
- กำกับดูแลและติดตามการบริหารความเสี่ยงและควบคุมภายในอย่างเป็นอิสระและจัดทำรายงานเสนอต่อคณะกรรมการโรงงานไพ่ เกี่ยวกับประสิทธิภาพและประสิทธิผลของ
- การควบคุมภายใน
- ให้คำปรึกษาการบริหารความเสี่ยงและการควบคุมภายในต่อคณะอนุกรรมการบริหาร
- ความเสี่ยงและควบคุมภายใน โรงงานไพ่
- สอบทานและสื่อสารกับคณะกรรมการบริหารความเสี่ยงและควบคุมภายในโรงงานไพ่ เพื่อให้เข้าใจความเสี่ยงที่สำคัญ ได้รับการจัดหาและเชื่อมโยงกับระบบการควบคุมภายในอย่างเหมาะสม
- ติดตามประสิทธิภาพการทำงานของหน่วยตรวจสอบภายใน

3) คณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน โรงงานไพ่ (RMC)

มีบทบาทหน้าที่และความรับผิดชอบเกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ดังนี้

- อนุมัตินโยบาย/มาตราการหรือแผนปฏิบัติการบริหารความเสี่ยงและการควบคุมภายใน ปัจจัยเสี่ยง แผนบริหารความเสี่ยง คู่มือการปฏิบัติงานความเสี่ยงและการควบคุมภายใน และกระบวนการบริหารความเสี่ยงและการควบคุมภายใน
- พัฒนากรอบการบริหารความเสี่ยงและการควบคุมภายใน
- กำกับดูแลให้มีการบูรณาการระหว่างการกำกับดูแลกิจการที่ดี (Governance) การบริหารความเสี่ยง (Risk Management) และการปฏิบัติตามข้อกฎหมาย ระเบียบ ข้อบังคับ ประกาศ และหลักเกณฑ์ (Compliance) เพื่อให้บรรลุถึงผลการดำเนินงานที่เกิดจาก
- การมีส่วนร่วมของทุกส่วนงาน
- ติดตามและกำกับดูแล การดำเนินงานตามกระบวนการบ่งชี้ปัจจัยเสี่ยงและการประเมิน ความเสี่ยง รวมทั้งคัดเลือกปัจจัยเสี่ยงที่มีนัยสำคัญต่อองค์กรมาจัดทำแผนตอบสนอง
- ความเสี่ยงที่เหมาะสมร่วมกับผู้บริหารหรือเจ้าหน้าที่ที่เกี่ยวข้อง

- รายงานผลการบริหารจัดการความเสี่ยงและการควบคุมภายในระดับองค์กรเป็นรายไตรมาส ต่อคณะกรรมการโรงงานไพ่ และคณะกรรมการตรวจสอบ
- เชิญผู้บริหารหรือเจ้าหน้าที่ และบุคคลภายนอกเพื่อเข้าร่วมประชุมหรือให้ข้อมูลในเรื่อง
- ที่เกี่ยวข้อง
- มีอำนาจเป็นไปตามกฎบัตรคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในโรงงานไพ่

4) คณะทำงานบริหารจัดการความเสี่ยงและควบคุมภายใน โรงงานไพ่

บทบาทหน้าที่และความรับผิดชอบเกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ดังนี้

- จัดทำร่างนโยบายความเสี่ยงและควบคุมภายใน และร่างกรอบการบริหารความเสี่ยง
- และควบคุมภายใน เสนอคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในโรงงานไพ่ เพื่อพิจารณาอนุมัติ
- ประสานงานกับผู้เกี่ยวข้องเพื่อรวบรวมข้อมูลในการจัดทำแผนบริหารจัดการความเสี่ยงและ แผนการควบคุมภายใน
- จัดทำแผนปฏิบัติการ และแผนอื่น ๆ สำหรับการบริหารจัดการความเสี่ยงและการควบคุม ภายใน
- รวบรวมข้อมูลหลักฐานและสรุปผลการดำเนินงานของการบริหารจัดการความเสี่ยงและ
- การควบคุมภายใน
- พัฒนา/ทบทวนกระบวนการบริหารความเสี่ยงและควบคุมภายใน ของหน่วยงาน
- อย่างสม่ำเสมอ
- ติดตาม แนะนำ และให้คำปรึกษาการปฏิบัติงานตามกระบวนการบริหารความเสี่ยงและ ควบคุมภายใน เพื่อลดผลกระทบและป้องกันความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- ทบทวนประเมินผลรายงานผลการดำเนินงานมาตรการหรือแผนปฏิบัติการ เพื่อกำหนด แนว ทางการปรับปรุงระบบบริหารความเสี่ยงของโรงงานไพ่
- ดำเนินการประชาสัมพันธ์ต่อผู้มีส่วนได้ส่วนเสียกรณีที่มีเหตุการณ์วิกฤติ ซึ่งมีผลกระทบ
- ที่จะสร้างความเสียหาย รั่วไหล หรือสูญเปล่า อันจะทำให้การบริหารงานของโรงงานไพ่
- ไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้
- สื่อสาร/ทำความเข้าใจให้พนักงานรับทราบและทำความเข้าใจกับการบริหารความเสี่ยงและ ควบคุมภายใน
- รวบรวมกลั่นกรองข้อมูลจากแหล่งข้อมูลต่าง ๆ จัดทำเป็นฐานข้อมูลเพื่อการตัดสินใจ
- อย่างมีประสิทธิภาพ ตามลำดับความสำคัญของการบริหารความเสี่ยงและควบคุมภายใน
- รายงานผลการดำเนินงานของการบริหารจัดการความเสี่ยงและการควบคุมภายใน
- ต่อคณะอนุกรรมการบริหารความเสี่ยงฯ เป็นประจำทุกเดือน
- รายงานผลการดำเนินงานของการบริหารจัดการความเสี่ยงและการควบคุมภายใน
- ต่อคณะกรรมการโรงงานไพ่ คณะกรรมการตรวจสอบ คณะอนุกรรมการบริหารความเสี่ยง และควบคุมภายใน (รายไตรมาส)
- ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

5) ผู้อำนวยการโรงงานไพ่

มีบทบาทหน้าที่และความรับผิดชอบเกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ดังนี้

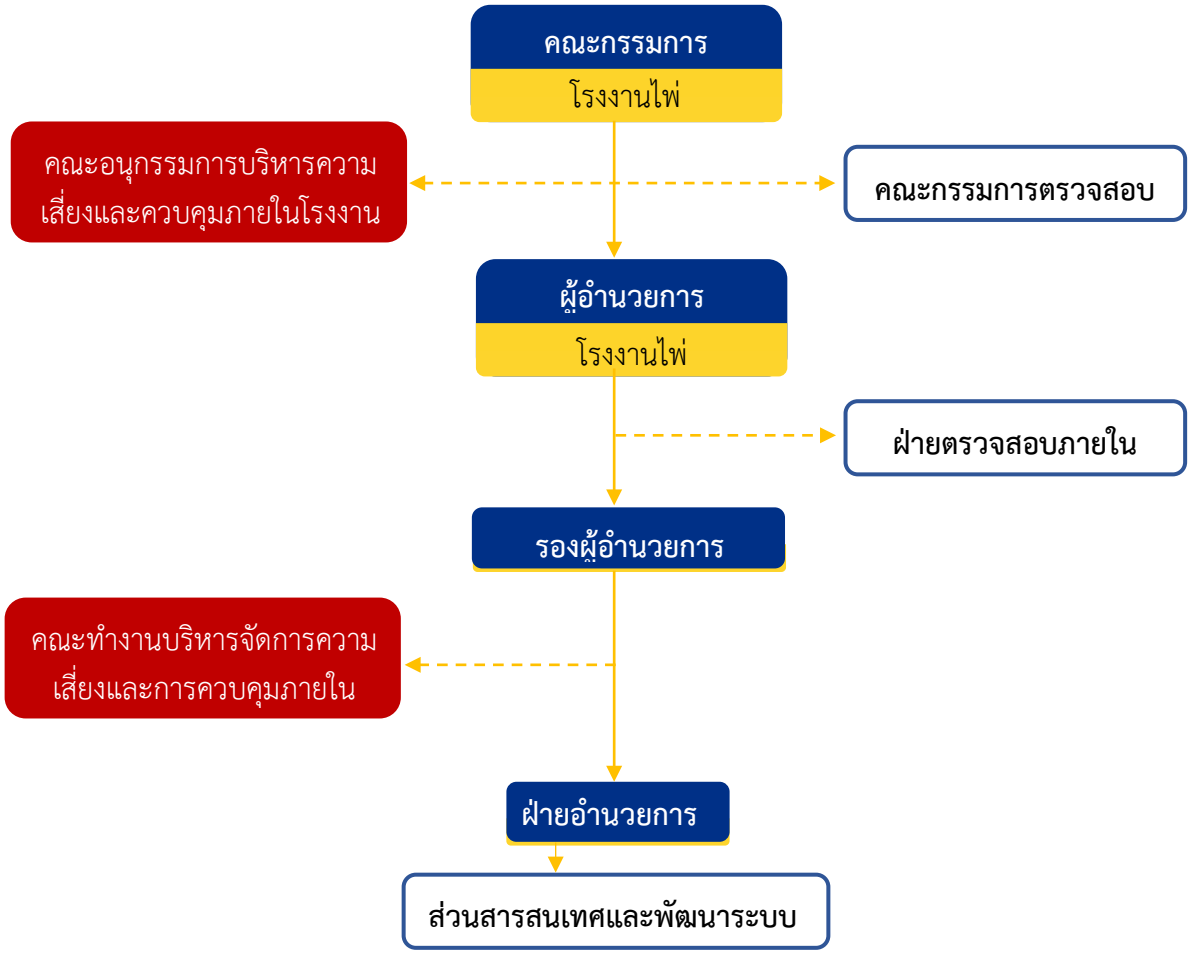
- การวางแผนและดำเนินการตามนโยบาย และแผนงานการบริหารความเสี่ยงร่วมกับคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน โรงงานไพ่
- สั่งการและติดตามให้ทุกหน่วยงานปฏิบัติงานตามกระบวนการบริหารความเสี่ยง
- แต่งตั้งเจ้าหน้าที่หรือผู้รับผิดชอบ เพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผล
- สนับสนุนและส่งเสริมให้การบริหารความเสี่ยงเป็นการปฏิบัติงานตามปกติและ
- เป็นวัฒนธรรมของหน่วยงาน
- อื่น ๆ ตามหน้าที่ที่ได้รับมอบหมายจากคณะกรรมการโรงงานไพ่

6) ส่วนสารสนเทศและพัฒนาระบบ

มีบทบาทหน้าที่และความรับผิดชอบเกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ดังนี้

- รวบรวมและวิเคราะห์เหตุการณ์และประเมินผลความเสี่ยงเบื้องต้นเพื่อรายงานต่อคณะทำงานบริหารจัดการความเสี่ยงและควบคุมภายในโรงงานไพ่
- มีส่วนร่วมในการประชุมสัมมนาเชิงปฏิบัติการ เพื่อจัดทำแผนบริหารความเสี่ยงและ
- การควบคุมภายใน
- ส่งเสริมให้พนักงานในหน่วยงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงและควบคุมภายใน
- ประสานงานกับเลขาฯ คณะทำงานบริหารจัดการความเสี่ยงและควบคุมภายใน โรงงานไพ่ เพื่อรายงานความก้าวหน้าของแผนบริหารความเสี่ยงฯ ที่ได้รับมอบหมาย
- อื่น ๆ ตามที่ได้รับมอบหมาย

โครงสร้างองค์กรการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศ



3.2 หลักเกณฑ์ ระเบียบวิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้แก่

3.2.1 การประเมินความเสี่ยง (Risk assessment) ประกอบด้วย

- การระบุความเสี่ยง (Risk identification)
- การวิเคราะห์ความเสี่ยง (Risk analysis)
- การประเมินค่าความเสี่ยง (Risk evaluation)

3.2.2 การจัดการความเสี่ยง (Risk treatment) เป็นแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

3.2.3 การติดตามและทบทวนความเสี่ยง (Risk monitoring and review) ควรมีการกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามตัวชี้วัดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ตามที่กำหนดและทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับที่ยอมรับได้

3.2.4 การรายงานความเสี่ยง (Risk reporting) มีการนำเสนอผลการบริหารแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมกับการรายงานผลการประเมินและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร

4. รัฐวิสาหกิจมีการสื่อสารนโยบายหรือแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์กร

5. รัฐวิสาหกิจมีการกำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์กร

นิยามและความหมายของการบริหารความเสี่ยง

1) ความเสี่ยง (Risk) หมายถึง ผลรวม หรือผลสืบเนื่องของเหตุการณ์ที่มีความไม่แน่นอนที่มีผลต่อวัตถุประสงค์ ซึ่งมีโอกาสที่จะเกิดขึ้นในอนาคต และมีผลกระทบ ทั้งทางบวก และ ทางลบ หากเป็นทางลบจะก่อให้เกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ทำให้การดำเนินงานขององค์กรไม่ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้ จึงจำเป็นต้องพิจารณาโอกาสที่จะเกิดของเหตุการณ์ (Likelihood) และผลกระทบที่จะได้รับ (Impact)

2) การบริหารความเสี่ยง (Risk Management) คือกระบวนการในการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ โดยลดสาเหตุของแต่ละโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินการที่ไม่เป็นไปตามแผน และเพื่อให้ระดับของความเสียหายและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคต อยู่ในระดับที่บริษัทยอมรับได้ ประเมิน หรือ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายองบริษัทเป็นสำคัญ

3) กรอบการบริหารความเสี่ยง (Risk Management Framework) คือหลักการและแนวทางที่ใช้ในการบริหารความเสี่ยง การกำหนดองค์ประกอบ นโยบาย หรือวัตถุประสงค์รวมถึงการออกแบบจัดการบริหารความเสี่ยงเพื่อการนำไปปฏิบัติ ติดตามตรวจสอบ หรือปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่องของทุกหน่วยงานในองค์กร เพื่อลดสาเหตุของโอกาสที่องค์กรจะเกิดความเสียหาย และรักษาระดับของความเสี่ยงและผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

4) การประเมินความเสี่ยง (Risk Assessment) คือกระบวนการระบุรายการหรือประเด็นความเสี่ยง การวิเคราะห์สาเหตุ หรือปัจจัยที่อาจจะเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กร กำหนดระดับของผลกระทบหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง และกำหนดค่าความเสี่ยงของเหตุการณ์ความเสี่ยงนั้น การจัดลำดับความเสี่ยงโดยจะประเมินจากโอกาสที่จะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) หรือขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดความเสี่ยงนั้น ๆ

จากนิยามและความหมายของการบริหารความเสี่ยง รวมถึงกรอบแนวทางในการบริหารจัดการความเสี่ยงข้างต้นตามหลักเกณฑ์ระบบประเมินผลรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM ที่กล่าวมาแล้วนั้น ทางโรงงานไพ่ฯ จะใช้เป็นแนวทางในการกำหนดกระบวนการและองค์ประกอบเพิ่มเติมต่างๆ ของกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยจะกล่าวถึง ในบทถัดไป

บทที่ 2
กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และแนวปฏิบัติ

ในการจัดทำกระบวนการ และแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ มีหลากหลายองค์ประกอบที่จำเป็นต้องศึกษาและวิเคราะห์ โดยมีองค์ประกอบดังนี้

1. การวิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

1) ระบบเครือข่าย (Network)

- ซอฟต์แวร์สำหรับบริหารจัดการเครือข่าย (Network Management Software)
- ซอฟต์แวร์สำหรับตรวจสอบการโจมตีจากเครือข่ายภายนอกและภายใน (Security Management Software)
- ซอฟต์แวร์สำหรับใช้การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Traffic Software)

2) เครื่องแม่ข่าย (Server)

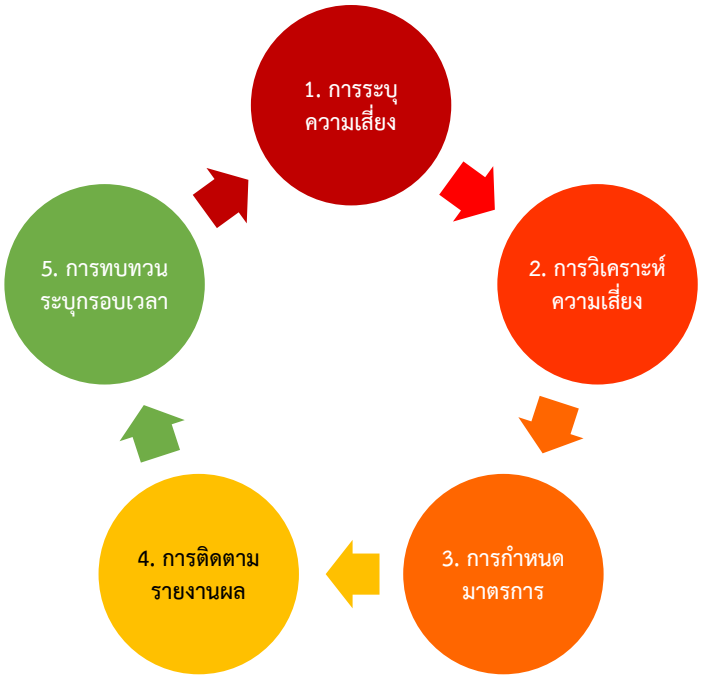
- ซอฟต์แวร์ระบบปฏิบัติการเครื่องแม่ข่าย (Server Operating System)
- ระบบฐานข้อมูล (Database Server)
- เว็บแอปพลิเคชั่น (Web Application Software)

3) อุปกรณ์คอมพิวเตอร์ (Hardware)

- เครื่องคอมพิวเตอร์แม่ข่าย (Server)
- อุปกรณ์เครือข่าย (Network Device)
- อุปกรณ์ตรวจสอบการบุกรุกของเครือข่าย (IPS Device)
- อุปกรณ์ป้องกันการโจมตีของเครือข่าย (Firewall Device)
- เครื่องคอมพิวเตอร์สำหรับผู้ใช้งานแบบตั้งบนโต๊ะ (Desktop)
- เครื่องคอมพิวเตอร์สำหรับพกพา (Laptop)

2. กรอบกระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอนดังนี้



1) การระบุความเสี่ยงหรือปัจจัยความเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในระบุความเสี่ยงมีหลายวิธี เช่น

1.1) การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

1.2) การใช้ Checklist

1.3) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

1.4) การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

1.5) การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จและปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในดำเนินการต่อไป

2) การวิเคราะห์ความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยงประกอบด้วย 4 ขั้นตอนคือ

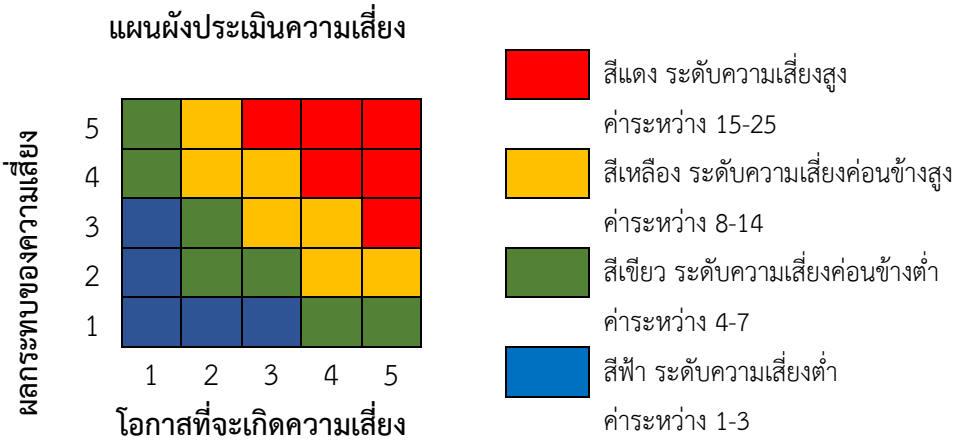
2.1) การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยนงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ 4 ระดับ (สูงมาก สูง ปานกลางและน้อย)

2.2) การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจาก

ความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมิน ผลกระทบ		เกณฑ์การประเมิน โอกาสของการเกิดความเสี่ยง	
ระดับ	การประเมิน	ระดับ	การประเมิน
5	สูงมาก	5	เกิดขึ้นสูงมาก
4	สูง	4	เกิดขึ้นสูง
3	ปานกลาง	3	เกิดขึ้นปานกลาง
2	น้อย	2	เกิดขึ้นน้อย
1	น้อยมาก	1	เกิดขึ้นน้อยมาก

2.3) การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่เกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดความระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน



2.4) การจัดลำดับความเสี่ยง เป็นการจัดลำดับรุนแรงของความเสี่ยงที่มีต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

3) การกำหนดมาตรการจัดการความเสี่ยงอย่างรุดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภทคือ

3.1) ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึง เอกสาร เป็นต้น

3.2) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

3.3) การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

3.4) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยจำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

3.4.1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมากหรือสูงมากำหนดวิธีควบคุมที่ควรจะมีเพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

3.4.2) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

3.4.3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

4) การติดตามรายงานผลและการประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยงหรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงเมื่อองค์กรทราบความเสี่ยงที่เหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือกเพื่อตัดสินใจมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

4.1) พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

4.2) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่ได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

5) การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยงว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือติดตามผลในระหว่างการปฏิบัติงาน

3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนสารสนเทศได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) เป็น 8 ประเภทดังนี้

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตะภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการทำงาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น มัลแวร์คอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Network) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Harddisk Drive เป็นต้น

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Park) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดตให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจากข้อผิดพลาด (Bug) ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบหรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศ อันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้นการรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติหรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศ

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาลและผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศ ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์ที่เปลี่ยนแปลงไป

ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงต่อการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

ความเสี่ยงในด้านการบริหารจัดการ (Management Risk) หมายถึง ความเสี่ยงเนื่องจากมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินงานที่ดี

4. การตอบสนองความเสี่ยง

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรม ความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิด ความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงานองค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

5. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของโรงงานไพ่ กรมสรรพสามิต ได้แก่

1) ปัจจัยภายนอก ได้แก่

1.1) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

1.2) การชำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server)

1.3) ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

1.4) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

1.5) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2) ปัจจัยภายใน ได้แก่

2.1) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.2) การถูกมัลแวร์ (Virus) ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

2.3) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดทำงาน

6. การประเมินความเสียหาย

1) ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากมัลแวร์

2) ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วคราว ได้แก่ การถูกเจาะระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

7. การติดตามและรายงานผล

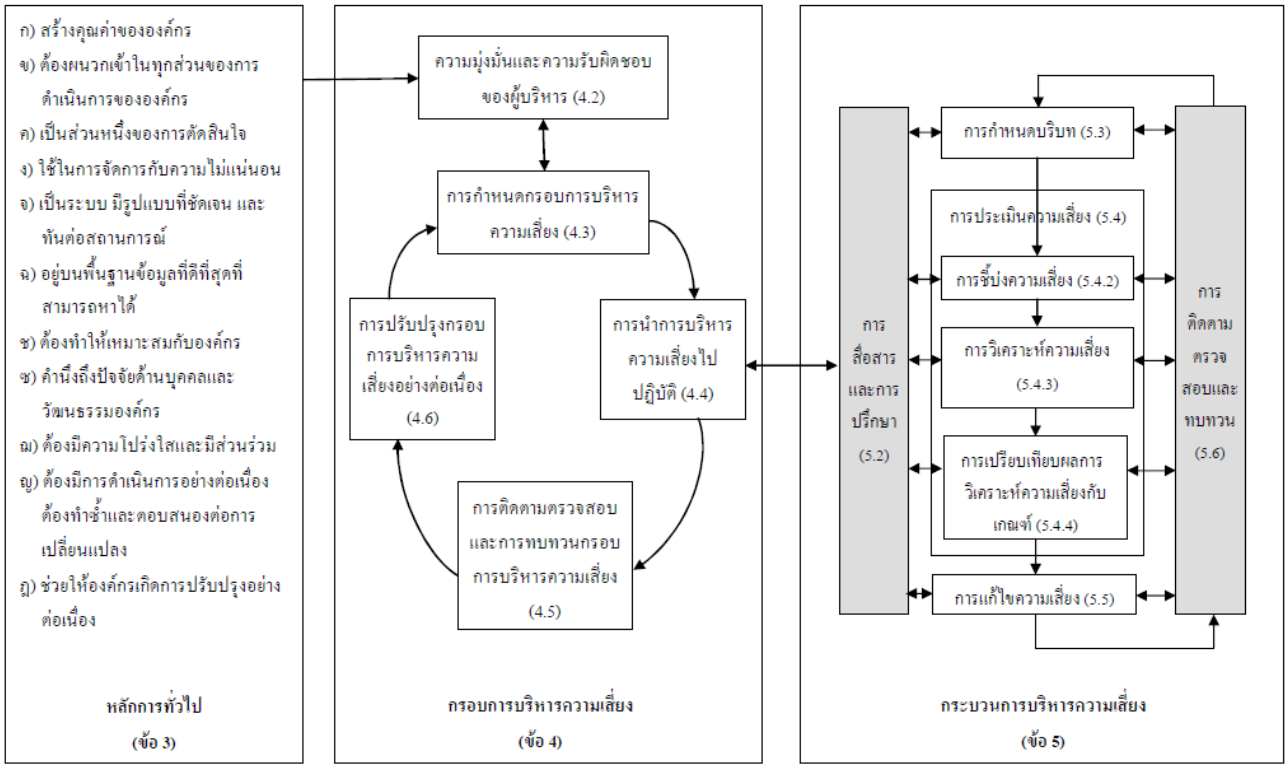
กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

ส่วนสารสนเทศและพัฒนาระบบ ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนบริหารความเสี่ยงของโรงงานไพ่ กรมสรรพสามิต โดยเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนการงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล แลกเปลี่ยนความคิดเห็นร่วมกันกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

8. ตารางการบริหารจัดการความเสี่ยง (Risk Management Framework)

8.1 กรอบการบริหารจัดการความเสี่ยง (Risk Management Framework)

โดยหลักการและแนวทางในการบริหารความเสี่ยง เป็นไปตามมาตรฐาน ISO 31000:2009 ซึ่งเป็นดังแผนภาพดังต่อไปนี้



ตามแผนภาพความสัมพันธ์ระหว่างองค์ประกอบของการบริหารความเสี่ยงตามมาตรฐาน ISO 31000:2009 ซึ่งแบ่งส่วนประกอบเป็น 3 ส่วนหลักๆ คือ 1) หลักการทั่วไปพื้นฐานในการบริหารความเสี่ยง (Principle) 2) กรอบการบริหารความเสี่ยง (Framework) และ 3) กระบวนการบริหารความเสี่ยง (Process)

1) หลักการทั่วไปพื้นฐานในการบริหารความเสี่ยง (Principle)

ทั้งนี้ องค์กรได้นำหลักการทั่วไปพื้นฐานในการบริหารความเสี่ยงมาใช้ ซึ่งประกอบไปด้วย

- สร้างคุณค่าขององค์กร
- ต้องผนวกเข้าใจทุกส่วนของการดำเนินการขององค์กร
- เป็นส่วนหนึ่งของการตัดสินใจ
- ใช้ในการจัดการกับความไม่แน่นอน
- เป็นระบบ มีรูปแบบที่ชัดเจน และทันต่อสถานการณ์
- อยู่บนพื้นฐานข้อมูลที่ดีที่สุดที่สามารถหาได้
- ต้องทำให้เหมาะสมกับองค์กร
- คำนึงถึงปัจจัยด้านบุคคลและวัฒนธรรมองค์กร
- ต้องมีความโปร่งใสและมีส่วนร่วม
- ต้องมีการดำเนินการอย่างต่อเนื่อง และทำซ้ำ และตอบสนองต่อการเปลี่ยนแปลง
- ช่วยให้องค์กรเกิดการปรับปรุงอย่างต่อเนื่อง

2) กำหนดกรอบการบริหารความเสี่ยง

ตามมาตรฐานการบริหาความเสี่ยงสากล ISO 31000:2009 ซึ่งแบ่งออกเป็น 4 ส่วนคือ

2.1) การกำหนดกรอบการบริหารความเสี่ยง

2.2) การนำการบริหารความเสี่ยงไปปฏิบัติ

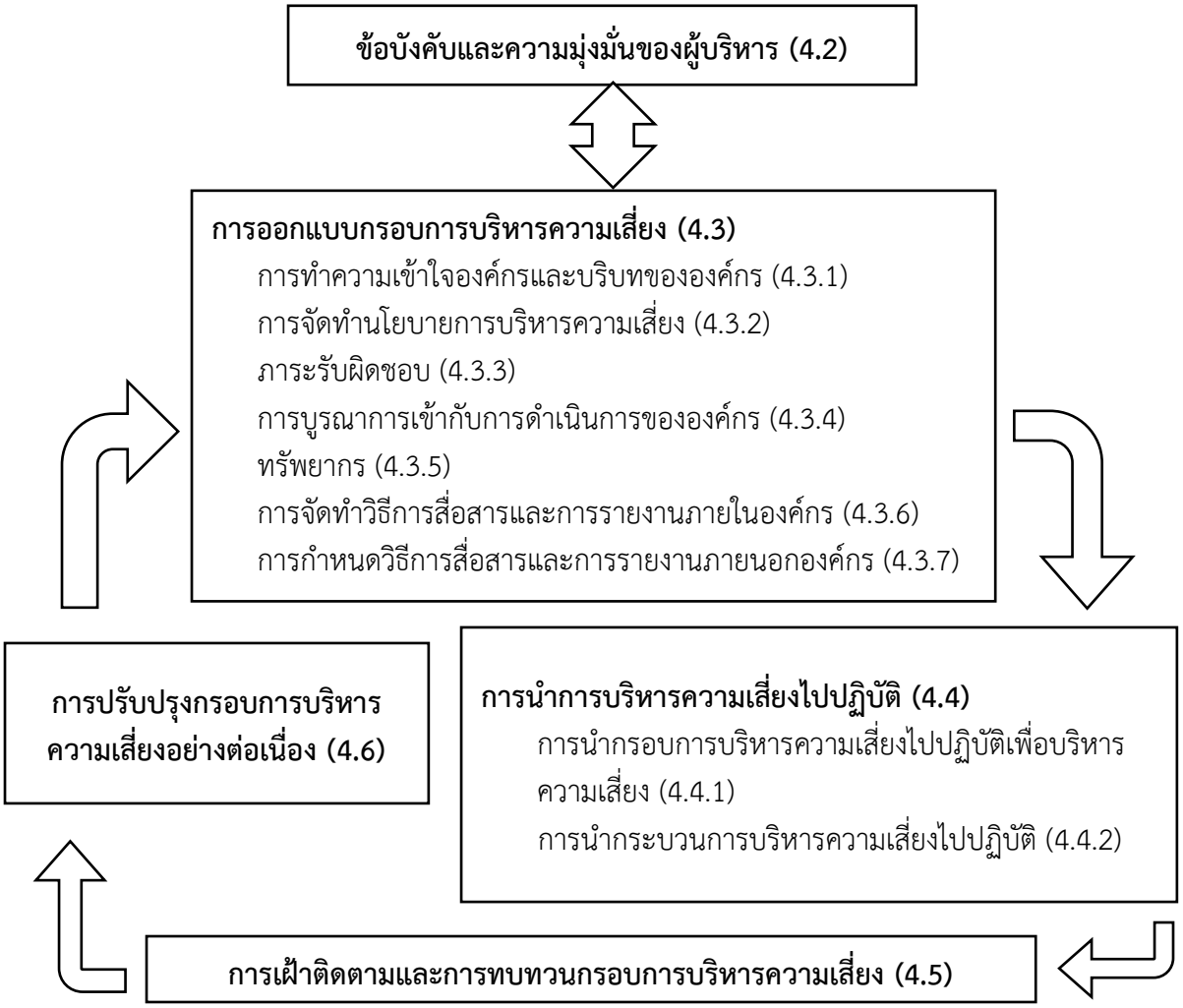
2.3) การติดตามตรวจสอบและการทบทวนกรอบการบริหารความเสี่ยง

2.4) การปรับปรุงกรอบการบริหารความเสี่ยงอย่างต่อเนื่อง

3) กระบวนการบริหารความเสี่ยง ประกอบด้วย

- การสื่อสารและปรึกษา
- การกำหนดบริบท
- การประเมินความเสี่ยง
- การวิเคราะห์ความเสี่ยง
- การเปรียบเทียบผลการวิเคราะห์ความเสี่ยง
- การแก้ไขความเสี่ยง
- การติดตามตรวจสอบ ทบทวนความเสี่ยง

8.2 การกำหนดกรอบบริหารความเสี่ยง



จากตารางการกำหนดกรอบความเสี่ยงสามารถอธิบายได้ดังนี้

การกำหนดข้อบังคับและความมุ่งมั่นของผู้บริหาร

คือ “การเป็นผู้ให้บริการรับจัดทำเงินเดือนระดับมืออาชีพที่ผู้ใช้บริการสามารถเชื่อถือและไว้วางใจได้ โดยองค์กรจะมีการนำปัจจัยต่างๆ เข้ามาใช้ในการประเมินความเสี่ยงเพื่อการปรับปรุง เปลี่ยนแปลง บริการเพื่อให้บริษัทก้าวขึ้นเป็นผู้นำในการให้บริการ”

ทั้งนี้ ในการบริหารความเสี่ยงได้รับการสนับสนุนจากผู้บริหารระดับสูงขององค์กร โดยสิ่งที่ผู้บริหารจะต้องให้ความสำคัญประกอบด้วย

- การประกาศ และให้การรับรองต่อนโยบายการบริหารความเสี่ยง (Risk Management Policy)
- กำหนดบทบาทและหน้าที่ความรับผิดชอบที่เหมาะสม
- กำหนดวัตถุประสงค์การบริหาความเสี่ยงให้สอดคล้องกับวัตถุประสงค์และกลยุทธ์ขององค์กร
- สื่อสารถึงประโยชน์ที่จะได้รับจากการบริหารความเสี่ยง
- ดูแลให้มีการจัดสรรทรัพยากรที่จำเป็นเพื่อการบริหารความเสี่ยงอย่างเพียงพอ
- ดูแลความเหมาะสมของกรองการบริหารความเสี่ยงอย่างต่อเนื่อง
- ติดตามการดำเนินงานตามแผนการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง

การออกแบบกรอบบริหารความเสี่ยง

ขั้นตอนในการออกแบบการบริหารความเสี่ยงขององค์กรจะเริ่มจากการทำความเข้าใจในสภาพแวดล้อมทั้งภายใน และภายนอกขององค์กร การทำความเข้าใจในสภาพแวดล้อมทั้งภายในและภายนอกขององค์กรมีประเด็นต่างๆ ที่เกี่ยวข้องตามมาตรฐาน ISO 31000:2009 ดังต่อไปนี้

1) การประเมินบริบทภายนอกองค์กร

บริบทภายนอกองค์กรที่อาจจะมีผลต่อวัตถุประสงค์หลักของโรงงานไพ่ อาจประกอบไปด้วย

- ด้านการเมือง เนื่องด้วยประเทศไทย มีการเปลี่ยนแปลงและมีเหตุการณ์ทางด้านการเมืองอยู่เป็นระยะ ในรอบ 3-5 ปีที่ผ่านมา
- การเงิน เศรษฐกิจ สภาพแวดล้อมในการแข่งขันทั้งระดับในประเทศและระดับภูมิภาค
- เทคโนโลยี
- สังคม วัฒนธรรม
- การเปลี่ยนแปลงของในอุตสาหกรรม
- ความเสี่ยงจากการเปลี่ยนแปลงของความต้องการของลูกค้า

2) การประเมินบริบทภายในองค์กร

บริบทภายในองค์กร หมายรวมถึง

- การกำกับดูแล กระบวนการ โครงสร้างองค์กร บทบาทและภาระรับผิดชอบ
- ระบบสารสนเทศ การรับส่งสารสนเทศและกระบวนการตัดสินใจ
- ความเชื่อมั่นและชื่อเสียงขององค์กร
- ขีดความสามารถ ความเข้าใจในรูปแบบของทรัพยากร ความรู้ เช่น บุคลากร ความสามารถ

การนำการบริหารความเสี่ยงไปปฏิบัติ

องค์กรจะต้อง

- กำหนดช่วงเวลาและกลยุทธ์ที่เหมาะสมสำหรับการดำเนินการตามกรอบการบริหารความเสี่ยง
- กำหนดนโยบายและนำกระบวนการบริหารความเสี่ยงมาใช้กับกระบวนการต่าง ๆ ขององค์กร
- ดำเนินการให้สอดคล้องกับข้อกฎหมายและระเบียบข้อบังคับต่างๆ
- จัดทำเอกสารอธิบายถึงการตัดสินใจ รวมถึงการจัดทำวัตถุประสงค์
- จัดให้มีข้อมูลสารสนเทศและการฝึกอบรม
- สื่อสารและให้คำปรึกษากับผู้มีส่วนได้ส่วนเสีย เพื่อให้มั่นใจว่ากระบวนการบริหารความเสี่ยงต่างๆ ได้มีการนำไปปฏิบัติในทุกระดับและหน้าที่งานที่เกี่ยงข้องในองค์กร โดยเป็นส่วนหนึ่งของการปฏิบัติงานขององค์กรและกระบวนการทางธุรกิจ

การเฝ้าติดตามและการทบกวนกรอบการบริหารความเสี่ยง

เพื่อให้มั่นใจว่าการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิผลและสนับสนุนการดำเนินงานขององค์กรอย่างต่อเนื่อง ควรจะต้อง

- มีการกำหนดการวัดผลการดำเนินงาน ตามช่วงเวลาที่กำหนดอย่างเหมาะสม
- มีการทบทวนกรอบบริหารความเสี่ยง นโยบาย และแผนงานอย่างสม่ำเสมอ

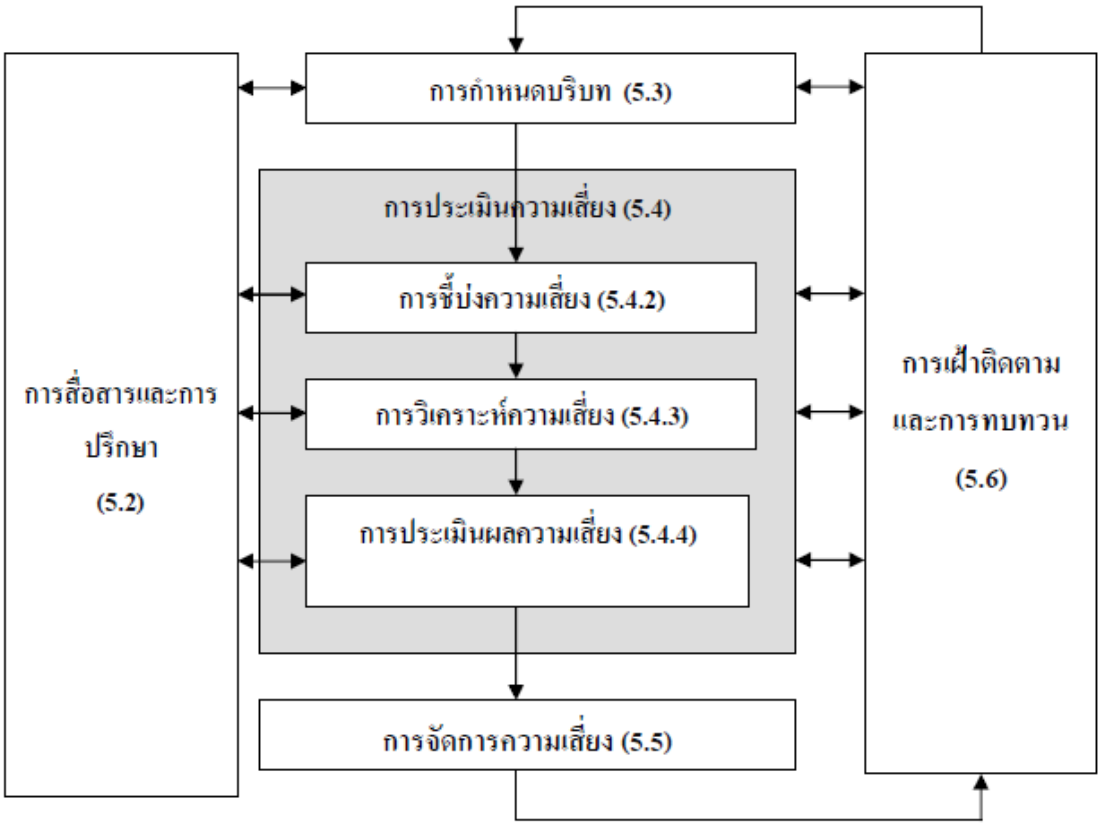
- จัดทำรายงานความเสี่ยง ความก้าวหน้าของแผนการบริหารความเสี่ยงและการดำเนินการกับนโยบายการบริหารความเสี่ยง
- ทบทวนถึงความมีประสิทธิผลของกระบวนการบริหารความเสี่ยง

การปรับปรุงกรอบการบริหารความเสี่ยงอย่างต่อเนื่อง

เมื่อองค์กรได้มีการเฝ้าติดตามและทบทวนกรอบการบริหารความเสี่ยงแล้ว ผลของการทบทวนจะนำไปสู่การตัดสินใจในการปรับปรุงกรอบการบริหารความเสี่ยง นโยบาย และแผนการบริหารความเสี่ยง และวัฒนธรรมการบริหารงานขององค์กร รวมถึงช่วยปรับปรุงความคล่องตัว การควบคุม และความรับผิดชอบที่มีต่อเป้าหมายขององค์กรด้วย

8.3 กระบวนการบริหารความเสี่ยง (Process)

สำหรับกระบวนการบริหารความเสี่ยงตามมาตรฐาน ISO31000:2009 ที่ทุกหน่วยงานยึดถือเป็นหลักในการดำเนินการ และถือเป็นส่วนหนึ่งของการบริหาร โดยมีกิจกรรมต่างๆ ซึ่งแสดงขั้นตอนดังรูป



การสื่อสารและการปรึกษา

เป็นกิจกรรมที่ควรมีอยู่ในทุกขั้นตอนของกระบวนการบริหารความเสี่ยง เป็นการชี้แจง บอกกล่าวให้กับผู้ที่มีส่วนเกี่ยวข้องทั้งภายใน และภายนอกองค์กร และยังให้คำปรึกษา ถึงประเด็นต่างๆ ที่เกี่ยวข้อง ขั้นตอนขอบเขตการดำเนินงาน เพื่อให้เกิดความเข้าใจในมาตรการในการจัดการความเสี่ยงต่างๆ มีหลักการและวิธีปฏิบัติที่ตรงกัน รวมถึงควรมีการชี้บ่งและบันทึกการรับรู้ของผู้มีส่วนได้เสียไว้ และนำไปพิจารณาในกระบวนการตัดสินใจ

การกำหนดบริบทขององค์กร

คือการกำหนดสภาพแวดล้อมขององค์กร ทั้งภายในและภายนอกที่มีความสัมพันธ์เกี่ยวข้องกับองค์กร โดยเชื่อมโยงเกี่ยวข้องกับวัตถุประสงค์ ขอบเขตที่ชัดเจน ที่ทำให้เกิดผลกระทบต่อองค์กร และนำไปสู่กระบวนการบริหารความเสี่ยง

การกำหนดสภาพแวดล้อมภายนอก หมายถึง องค์ประกอบต่างๆ ภายนอกที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร ซึ่งการทำความเข้าใจในสภาพแวดล้อมภายนอกองค์กรและนำมากำหนดเกณฑ์ความเสี่ยง จะช่วยสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียขององค์กรได้ สภาพแวดล้อมภายนอกองค์กร อาจจะประกอบด้วย เศรษฐกิจ การเมือง วัฒนธรรม กฎหมาย หรือสภาพการเงิน การแข่งขันภายในประเทศและต่างประเทศ

การกำหนดสภาพแวดล้อมภายใน หมายถึง องค์ประกอบต่างๆ ภายในซึ่งมีอิทธิพลต่อความสำเร็จของวัตถุประสงค์ขององค์กร และวิถีทางของการบริหารความเสี่ยง ซึ่งสภาพแวดล้อมภายในองค์กร อาจรวมถึง โครงสร้างองค์กร บทบาทและภาระหน้าที่ ความสามารถของบุคลากร จำนวนคน นโยบาย วัตถุประสงค์ หรือกลยุทธ์ ระบบสารสนเทศ

การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงประกอบด้วยกระบวนการหลัก 3 กระบวนการคือ

1) การระบุความเสี่ยง (Risk Identification)

องค์กรจะต้องทำการระบุความเสี่ยงที่ครอบคลุมเหตุการณ์ต่างๆ ที่อาจส่งเสริม ขัดขวาง ลดเร่ง หรือชะลอการบรรลุวัตถุประสงค์ โดยอาจรวมถึงแหล่งที่มาของความเสี่ยง ปัจจัยเสี่ยง พื้นที่ที่ได้รับผลกระทบ เหตุการณ์ และสาเหตุ แม้ว่า ความเสี่ยงนั้น ไม่ได้อยู่ภายใต้การควบคุมขององค์กร หรือสาเหตุยังไม่ปรากฏชัด เช่น เกิดความล้มเหลวบางอย่างของระบบที่ทำให้วัตถุประสงค์เกิดการคลาดเคลื่อน

2) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เมื่อองค์กรมีการวิเคราะห์ความเสี่ยง จะต้องพิจารณาถึงสาเหตุและแหล่งที่มาของความเสี่ยง รวมถึงโอกาสที่ผลสืบเนื่องจะเกิดขึ้นจากความเสี่ยงนั้นที่สามารถส่งผลต่อการบรรลุของวัตถุประสงค์ ข้อมูลเหล่านี้จะใช้ในการประเมินและการตัดสินใจในการจัดการกับความเสี่ยง โดยพิจารณาจากผลกระทบที่อาจเกิดขึ้น (Impact) และโอกาสในการเกิด (Likelihood) ความเสี่ยงอาจวิเคราะห์ออกมาในเชิงคุณภาพ หรือ ปริมาณ หรือผสมผสานกันได้ขึ้นอยู่กับสภาพการณ์

3) การประเมินผลความเสี่ยง (Risk Evaluation)

จุดมุ่งหมายของการประเมินผลความเสี่ยง เพื่อจะบอกถึงระดับความสำคัญของความเสี่ยง เพื่อช่วยในการตัดสินใจว่าต้องมีการจัดการและจัดลำดับความสำคัญเพื่อดำเนินการจัดการความเสี่ยงนั้นอย่างไร ซึ่งลำดับความสำคัญของความเสี่ยง พิจารณาจากการวิเคราะห์ความเสี่ยง ซึ่งเป็นระดับ เช่น สูงมาก สูง ปานกลาง และต่ำ องค์กรจะเป็นผู้พิจารณาระดับความสำคัญของความเสี่ยงเพื่อนำมาดำเนินจัดการความเสี่ยงต่อไป

การจัดการความเสี่ยง (Risk Treatment)

แนวทางในการจัดการความเสี่ยง ประกอบไปด้วย

1) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหลีกเลี่ยงความเสี่ยงเป็นการเลี่ยงกิจกรรมที่เป็นสาเหตุนำมาซึ่งความเสี่ยง โดยการตัดสินใจไม่ดำเนินการต่อในกิจกรรมที่เกิดความเสี่ยงขึ้นแล้วจะมีผลกระทบต่อวัตถุประสงค์ขององค์กร เช่น การหยุดการดำเนินงาน หรือการยกเลิกโครงการ

2) การลดความเสี่ยง (Risk Reduction) การลดความเสี่ยง โดยการลดโอกาสหรือความถี่ที่อาจจะเกิดความเสี่ยงนั้น ลดผลกระทบหรือลดความเสียหาย หรือลดทั้งสองอย่าง ที่มีผลให้ความเสี่ยงนั้นมีค่าลดลง

หรือปรับระดับลงจนถึงระดับที่ยอมรับได้ เช่น การฝึกอบรมพนักงานให้มีความรู้ในเรื่องของความปลอดภัยของข้อมูล จัดคู่มือปฏิบัติงาน ทำแผนสำรองหากเกิดเหตุการณ์ฉุกเฉิน

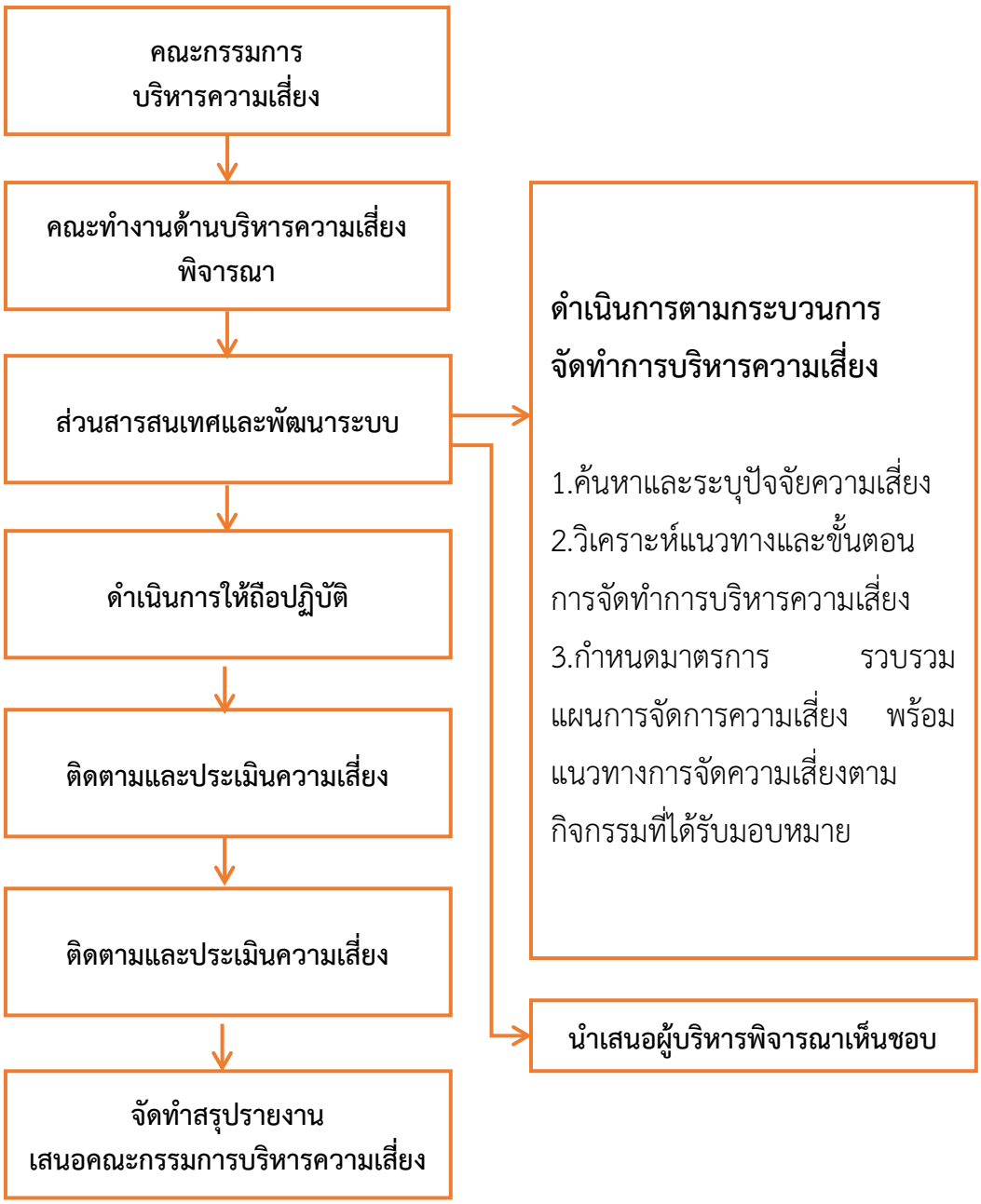
3) การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับความเสี่ยง โดยทั่วไป เมื่อองค์กรมีการปรับลดความเสี่ยงจำถึงระดับที่องค์กรยอมรับได้ แปลว่า ความเสี่ยงนั้น มีโอกาสที่จะเกิดขึ้นน้อย หรือผลกระทบของความเสี่ยงนั้น ก่อให้เกิดผลเสียหายไม่มาก

4) การส่งต่อความเสี่ยง (Transfer Risk) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้กับหน่วยงานอื่นทั้งภายใน และภายนอกองค์กร เพื่อช่วยลดโอกาสที่จะเกิดความเสี่ยง หรือระดับความรุนแรงของผลกระทบจากความเสี่ยงนั้น เช่น การทำประกันภัยจากบริษัทประกันภัยต่างๆ หรือการมอบการจัดการให้ผู้เชี่ยวชาญภายนอกที่มีความชำนาญมาดำเนินการแทน

การติดตามตรวจสอบและการทบทวนความเสี่ยง (Monitor and Review)

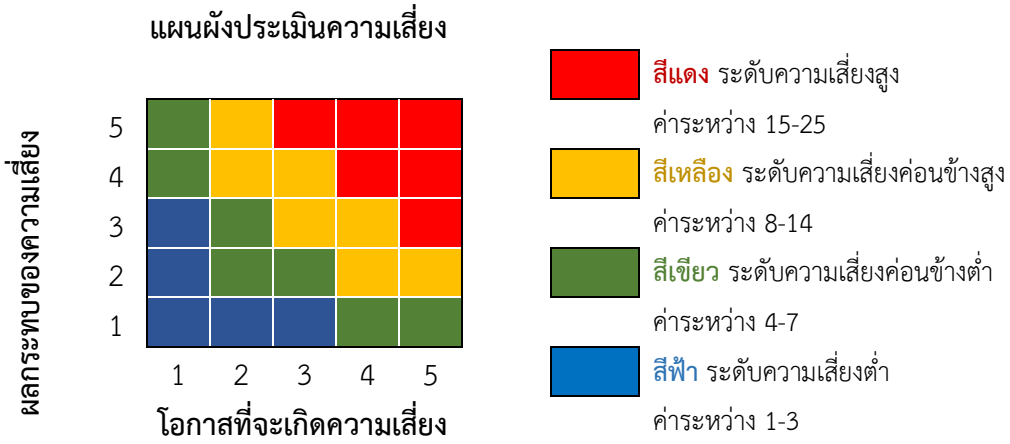
การติดตามและตรวจสอบเป็นส่วนหนึ่งของแผนกระบวนการบริหารความเสี่ยง โดยองค์กรจัดให้มีผู้รับผิดชอบและกรอบเวลาในการดำเนินการให้ชัดเจน ทั้งนี้ให้นำบทเรียนจากเหตุการณ์ต่างๆ ในอดีต การเปลี่ยนแปลงต่างๆ มาร่วมวิเคราะห์เพื่อปรับปรุง ทบทวน เปลี่ยนแปลงทั้งบริบทภายนอก ภายใน และเกณฑ์ความเสี่ยง รวมถึงความเสี่ยงต่างๆ ด้วยผลของการตรวจสอบและทบทวน องค์กรต้องจัดให้มีการบันทึกและรายงานผลด้วย

9. สรุปขั้นตอนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ



10. การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเชิญอยู่ การกำหนดความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้และมีผลกระทบมีดังนี้



ความเสี่ยงเรื่อง

1. การเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจ และเทคโนโลยีอย่างรวดเร็ว
2. ภัยคุกคามไซเบอร์ (Cyber Risk)
3. การปฏิบัติการดานไอที (Operation risk)
4. การบริหารจัดการโครงการด้านไอที

ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน
1	ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดต	3	5	15
2	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	2	5	10
3	ความเสี่ยงจากข้อมูลรั่วไหลจากสื่อบันทึกภายนอก	2	3	6
4	ความเสี่ยงจากการโจรกรรมฐานข้อมูล	1	5	5
5	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	3	3	9
6	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	3	5	15
7	ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์	2	4	8
8	ความเสี่ยงจากไฟกระชากจากสายพ่วง	2	4	8
9	ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์หรือสายไฟฟ้า/สายสัญญาณ	3	4	12
10	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่าย อินเทอร์เน็ต และอินทราเน็ตขัดข้อง	3	3	9
11	ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	3	4	12
12	ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	3	4	12
13	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์	2	5	10

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน
14	ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	2	3	6
15	ความเสี่ยงจากการนำอุปกรณ์ภายนอกเข้ามาใช้งานภายในเครือข่ายองค์กร	2	3	6
16	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายนอก	3	5	15
17	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	3	5	15
18	ความเสี่ยงจากการถูกโจมตีเว็บไซต์	3	4	12
19	ความเสี่ยงจากการเกิดอัคคีภัย	3	5	15
20	ความเสี่ยงจากอุทกภัย	2	3	6
21	ความเสี่ยงจากโรคระบาด	2	3	6
22	ความเสี่ยงจากวินาศภัย/การก่อการร้าย	2	5	10
23	ความเสี่ยงจากแผ่นดินไหว	2	4	8

11. สรุปแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและข้อเสนอแนะ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
O	ความเสี่ยงจากการสำรองข้อมูลการทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดต	1. เสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานได้ตามปกติ 2. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	1. ระบบงานอาจไม่สามารถกู้คืนได้ 2. ข้อมูลขาดความครบถ้วนตามหลัก CIA	15	1. มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำ อย่างสม่ำเสมอ 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	8		ส่วนสารสนเทศและพัฒนาระบบ
C	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	1. การสูญหายของข้อมูล 2. การถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือขององค์กร	1. ถูกโจมตีจาก Hacker ทำให้ข้อมูลสูญหาย 2. ผิดกฎหมายตามพรบ. คอมพิวเตอร์ พ.ศ. 2560	10	1. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย 2. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น	5		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากข้อมูลรั่วไหลจากสื่อบันทึกภายนอก	ผู้ใช้งานมีการนำข้อมูลอุปกรณ์ภายนอกไปใช้บนเครื่องที่ไม่ใช่เครื่องสำนักงาน เช่น External	1. ข้อมูลอาจถูกส่งต่อให้กับบุคคลที่ 3 2. ข้อมูลส่วนบุคคลอาจรั่วไหล 3. ทำให้องค์กรขาดความน่าเชื่อถือ	6	มีการบริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Harddisk, CD/DVD ให้แน่ใจ	3		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
		HDD, CD/DVD, USB Drive, SD Card			ว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้น ๆ ทิ้งแล้ว หากทำได้			
O	ความเสี่ยงจากการโจรกรรมฐานข้อมูล	ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	1. ข้อมูลส่วนบุคคลอาจรั่วไหล 2. ทำให้องค์กรขาดความน่าเชื่อถือ	5	1. มีการบริหารจัดการด้านการป้องกันข้อมูล 2. มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) 3. มีการบริหารสื่อจัดเก็บข้อมูล เช่น Harddisk 4. Disk ม้วนเทป (Cartridge Tape) แผ่น CD/DVD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์หรือสื่อเก็บข้อมูลนั้น ๆ ทิ้งแล้ว หากทำได้	4		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
O	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	ขาดการวางแผนการพัฒนาระบบเทคโนโลยีสารสนเทศ	ทำให้ธุรกิจหยุดชะงักหรือเกิดความล่าช้า หากระบบมีปัญหา	9	1. ติดตามข้อมูลข่าวสารที่สำคัญต่างๆ เพื่อคาดการณ์แนวโน้มการเกิดเหตุการณ์เพื่อปรับตัว 2. จัดทำแผนการบริหารจัดการพัฒนาโปรแกรมตามมาตรฐาน ISO/IEC27001 และ ITIL 5	6		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1. ไม่สามารถใช้งานระบบงานได้เต็มประสิทธิภาพ 2. เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	อาจทำให้ธุรกิจหยุดชะงักหรือเกิดความล่าช้า หากระบบมีปัญหา	15	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล 2. จัดตั้งศูนย์สำรองข้อมูล (Backup Site)	8		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	1. ข้อมูลอาจถูกส่งต่อให้กับบุคคลที่ 3 2. ข้อมูลส่วนบุคคลอาจรั่วไหล 3. เจ้าของเครื่องมีความผิด	8	1. ตรวจสอบผู้เข้ามาติดต่อ 2. ติดตั้งกล้องวงจรปิดให้ครอบคลุม	4		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
O	ความเสี่ยงจากไฟกระชากจากสายพ่วง	เสี่ยงต่อไฟไหม้ ไฟดูด ไฟย้อนกลับ ทำให้อุปกรณ์คอมพิวเตอร์เสียหายทั้งหมดได้	ทำให้เกิดอัคคีภัยและธุรกิจเกิดความเสียหาย	8	1. งดใช้สายไฟพ่วงหรืองดใช้สายพ่วงที่ไม่ได้มาตรฐาน ม.อ.ก. และไม่มีสายดิน 2. ไม่ใช้อุปกรณ์ที่ไม่มีสายดิน (ปลั๊ก 2 ขาหรือ 3 ขาแต่หักสายดินออก) ต่อเข้ากับสายพ่วงหรือเต้าไฟฟ้า (Receptacle)	6		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์อุปกรณ์หรือสายไฟฟ้า/สายสัญญาณ	เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเกิดความเสียหาย	12	1. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในที่มีความเสี่ยง 2. มีท่อห่อหุ้มสายไฟฟ้าหรือสายสัญญาณ	8		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	1. ไม่สามารถใช้งานระบบงานภายในขององค์กรได้ 2. ไม่สามารถเชื่อมต่อเครือข่ายภายนอกผ่านอินเทอร์เน็ตได้	1. องค์กรขาดความน่าเชื่อถือ 2. ทำให้ขาดโอกาสและสูญเสียรายได้ ณ ช่วงเวลาดังกล่าว	9	1. ตรวจสอบระบบเครือข่ายสื่อสารหลัก	6		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
O	ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1. ข้อมูลส่วนบุคคลอาจรั่วไหล 2. ทำให้องค์กรขาดความน่าเชื่อถือ	12	1. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย 2. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ 3. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	8		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	1. อุปกรณ์เครื่องแม่ข่ายและเครือข่ายอาจเสียหายได้ 2. ไม่สามารถใช้งานเครื่องแม่ข่าย และเครือข่ายได้ 3. ความเสี่ยงต่อความเสียหายของระบบปฏิบัติการและระบบฐานข้อมูลระหว่างทำงานอันเนื่องมาจากการปิดเครื่องที่ไม่ถูกต้อง	อาจทำให้ธุรกิจหยุดชะงักหรือเกิดความล่าช้า หากระบบมีปัญหา	12	1. ตรวจสอบระบบสำรองไฟฟ้า (UPS)	8		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
O	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์	1. โปรแกรมหรือข้อมูลถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูล	1. อาจทำให้ธุรกิจหยุดชะงักหรือเกิดความล่าช้า หากระบบมีปัญหา 2. ข้อมูลส่วนบุคคลอาจรั่วไหล 3. ถูกโจมตีจาก Hacker ทำให้ข้อมูลสูญหาย	10	1. ติดตั้งโปรแกรมป้องกันไวรัสกับเครื่องแม่ข่ายและเครื่องลูกข่าย 2. อัพเดตข้อมูลไวรัสอย่างสม่ำเสมอ	5		ส่วนสารสนเทศและพัฒนาระบบ
C	ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1. เสี่ยงต่อการใช้งานในทางที่ผิดหรือเปล่าประโยชน์ เช่น การดู Live Streaming, Video Content ขนาดใหญ่, เว็บไซต์ดูหนังผิดกฎหมาย, เล่นเกม เป็นต้น 2. การดาวน์โหลดไฟล์ผิดกฎหมาย เช่น วิดีโอ, ภาพยนตร์, เพลงที่มีลิขสิทธิ์ เป็นต้น	1. เกิดการละเมิดแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยของสารสนเทศ 2. ทำให้ทรัพยากรอินเทอร์เน็ตไม่เพียงพอต่อการใช้งาน	6	1. การกำหนด Policy ของอุปกรณ์ความมั่นคงปลอดภัย เปิด Port เท่าที่จำเป็น 2. การมีข้อตกลงระหว่างผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ ไปใช้ในทางที่ผิด รวมถึงบันทึกการใช้งานและรายงานการใช้งานของ	3		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					ผู้ใช้งานที่ฝ่าฝืนต่อผู้บังคับบัญชา			
O	ความเสี่ยงจากการนำอุปกรณ์ภายนอกเข้ามาใช้งานภายในเครือข่ายองค์กร	เสี่ยงต่อการนำไวรัสคอมพิวเตอร์เข้ามาแพร่กระจายภายในองค์กร	1. เครื่องคอมพิวเตอร์ลูกข่ายและคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย 2. อาจทำให้ธุรกิจหยุดชะงักหรือเกิดความล่าช้า หากระบบมีปัญหา	6	1. มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่าง ๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายภายใน	3		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอก โดยโจมตีทั้งเครื่องแม่ข่ายและเครือข่ายในทุกรูปแบบ	1. เครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย 2. อาจทำให้ธุรกิจหยุดชะงักหรือเกิดความล่าช้า หากระบบมีปัญหา	15	1. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย 2. ตรวจสอบ Policy และ Log ของ Firewall และ IPS อย่างสม่ำเสมอ	10		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงจากเครื่องลูกข่ายโดยผู้ใช้งานอาจตั้งใจและไม่ได้ตั้งใจผ่านทางโปรแกรมต่างๆ ที่ได้ติดตั้งบนเครื่องลูกข่าย	1. เครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย	15	1. มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่าง ๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายภายใน	5		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
O	ความเสี่ยงจากการถูกโจมตีเว็บไซต์	เสี่ยงต่อการถูกโจมตีอาจเกิดจาก ภาษาที่ใช้เขียน (Source code) ไม่มีการอัพเดท , ใช้ username password ง่ายต่อการถูกเจาะเว็บไซต์	1. เว็บไซต์ไม่สามารถให้บริการกับผู้มาติดต่อได้ 2. ข้อมูลส่วนบุคคลอาจรั่วไหล 3. ทำให้องค์กรขาดความน่าเชื่อถือ	12	1. ดำเนินการ backup ข้อมูลเพื่อเตรียมพร้อมในการกู้ระบบกลับคืน	8		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากการเกิดอัคคีภัย	1. คอมพิวเตอร์และเครือข่ายถูกทำลาย 2. ข้อมูลถูกทำลาย 3. การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	1. เครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย 2. ข้อมูลอาจสูญหายจากอัคคีภัย	15	1. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง 2. วางแผนจัดหาและติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง 3. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	10		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากอุทกภัย	ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	1. เครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย 2. ข้อมูลอาจสูญหายจากนำเข้าเครื่องทำให้ Harddisk เสียหาย	6	1. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	3		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากโรคระบาด	พนักงานไม่สามารถปฏิบัติงานได้	1. ทำให้ไม่สามารถเข้าใช้งานระบบงานภายในได้	6	ติดตามข้อมูลข่าวสารที่สำคัญ	3		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ระดับความเสี่ยงหลังการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
			2. ไม่สามารถประสานงานกับผู้ปฏิบัติงานอื่นได้		ต่างๆ เพื่อคาดการณ์แนวโน้มการเกิดเหตุการณ์เพื่อระวังภัย			
O	ความเสี่ยงจากวินาศภัย/การก่อการร้าย	การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	1. พนักงานเสียชีวิตจากการปฏิบัติหน้าที่ 2. อุปกรณ์อาจถูกทำลายหรือลักทรัพย์	10	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2. จัดทำแผนสำรองฉุกเฉิน 3. จัดทำศูนย์สำรอง (Backup Site)	4		ส่วนสารสนเทศและพัฒนาระบบ
O	ความเสี่ยงจากแผ่นดินไหว	ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	1. เครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย 2. ข้อมูลอาจสูญหายจากการสั่นสะเทือน ทำให้ Harddisk เสียหาย	8	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไร และจะใช้เครื่องทดแทนได้อย่างต่อเนื่อง 3. จัดทำศูนย์สำรอง (Backup Site)	4		ส่วนสารสนเทศและพัฒนาระบบ

ประเภทความเสี่ยงแบ่งออกเป็น 4 ส่วน คือ

1. S = Strategic Risk
2. O = Operational Risk
3. F = Financial Risk และ
4. C = Compliance Risk

บทที่ 3
การถ่ายทอดกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

การนำนโยบายไปปฏิบัติเป็นสิ่งสำคัญในการผลักดันให้นโยบายได้รับการรับรู้เข้าใจ ยอมรับและสร้างทัศนคติที่ดีต่อผู้ปฏิบัติตามนโยบาย เพื่อให้เกิดการปฏิบัติอย่างมีประสิทธิภาพ จึงต้องมีการสื่อสารถ่ายทอดนโยบาย และกระบวนการอย่างชัดเจนเป็นลายลักษณ์อักษรให้ครอบคลุมในทุกๆ ช่องทาง

1. วัตถุประสงค์

1) เพื่อให้ผู้เกี่ยวข้องและผู้มีส่วนได้เสีย ทั้งภายในและภายนอกองค์กร ยึดถือเป็นกรอบแนวทางปฏิบัติอย่างสอดคล้องกัน

2) เพื่อให้นโยบายหรือแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรทุกข้อกำหนด ถูกนำไปใช้ในทุกภาคส่วนอย่างมีระบบ

3) เพื่อให้การดำเนินการตามแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรมีประสิทธิภาพสูงสุด

2. ช่องทางการสื่อสาร

ส่วนสารสนเทศฯ ถ่ายทอดกระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ การกำกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) โดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ

1) ผู้ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการวิเคราะห์และจัดทำการกำกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้ผู้อำนวยการพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

2) ข้อมูลข่าวสาร (Message)

ข้อมูลข่าวสาร ได้แก่ กระบวนการวิเคราะห์และจัดทำการกำกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ที่ผ่านการพิจารณาจากผู้อำนวยการโดยได้รับการรับรองความถูกต้องเป็นที่เรีย

3) ช่องทางการสื่อสาร (Channel)

ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้ สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารระบบอินทราเน็ต และจดหมายอิเล็กทรอนิกส์

พร้อมมีการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ของโรงงานไพ่ฯ โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ จัดทำการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่ง ในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องจำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ

และเพื่อให้สอดคล้องกับการดำเนินการด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ การใช้โซเชียลมีเดีย เช่น เฟซบุ๊ก จึงเป็นอีกหนึ่งช่องทางที่สามารถเผยแพร่ข่าวสารในเรื่องดังกล่าวนี้ได้ โดยเลือกเฉพาะข้อมูลที่มีสาระสำคัญต้องการสื่อสารในเชิงสร้างภาพลักษณ์ให้กับโรงงานไพ่ กรมสรรพสามิต

3. การถ่ายทอดกระบวนการและการวิเคราะห์การดำเนินการด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของสารสนเทศ

การถ่ายทอดกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ มีกระบวนการดำเนินงานดังนี้

3.1 กำหนดวัตถุประสงค์ของการถ่ายทอดกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

1) เพื่อสร้างการรับรู้ในกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ

2) เพื่อสร้างความเข้าใจในกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

3) เพื่อนำข้อมูลที่ได้รับ (Feedback) จากผู้มีส่วนได้ส่วนเสียต่าง ๆ มาปรับปรุงและพัฒนากระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพมากยิ่งขึ้น

3.2 วิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

1) กำหนดมีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders) ที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

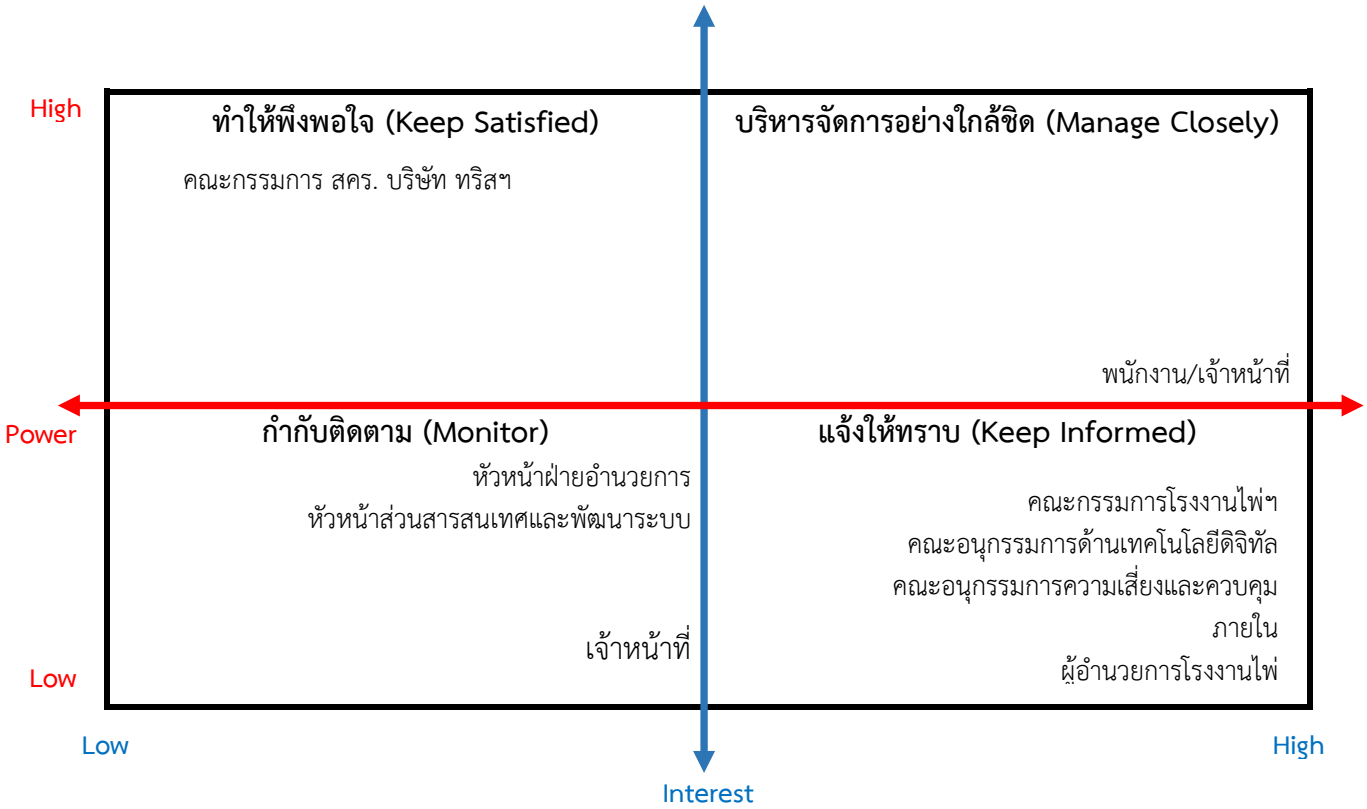
ผู้มีส่วนได้ส่วนเสียที่สำคัญต่อกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ ประกอบด้วย คณะกรรมการ คณะทำงาน ผู้บริหารและเจ้าหน้าที่ ซึ่งในแต่ละกลุ่มนั้นมีบทบาทหน้าที่ที่ส่งผลกระทบต่อกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ ที่เหมือนและแตกต่างกันออกไป โดยสามารถสรุปได้ ดังนี้

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
1. คณะกรรมการโรงงานไพ่ กรมสรรพสามิต	● กำกับดูแล (Governance) การดำเนินการด้านการแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
2. คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	● กำกับดูแล (Governance) การดำเนินการด้านแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
3. ผู้อำนวยการโรงงานไพ่ฯ	● พิจารณาเห็นชอบแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อสนับสนุนการดำเนินงานด้านสารสนเทศ ● กำกับดูแล (Governance) การดำเนินการด้านการแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ● การดำเนินการด้านการบังคับใช้แนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ● กำหนดและถ่ายทอดนโยบายการประยุกต์ใช้แนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
4. รองผู้อำนวยการโรงงานไพ่ฯ	● กำกับดูแล (Governance) การดำเนินการด้านการแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ● การดำเนินการด้านการบังคับใช้แนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ● กำหนดและถ่ายทอดนโยบายการประยุกต์ใช้แนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
5. หัวหน้าฝ่าย/ส่วนงานต่าง ๆ	● บริหารจัดการการดำเนินงานในส่วนงานที่รับผิดชอบให้มีความสอดคล้องกับนโยบายองค์กรของโรงงานไพ่ฯ ที่กำหนด ● ให้ความคิดเห็น ข้อเสนอแนะ และข้อวิพากษ์ต่าง ๆ ที่เกี่ยวข้องกับสถาปัตยกรรมองค์กร เพื่อนำไปปรับปรุงกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ● สื่อสารและถ่ายทอดข้อมูลข่าวสารต่าง ๆ ที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรไปยังพนักงานในฝ่าย/ส่วน

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
6. พนักงาน/เจ้าหน้าที่	● ดำเนินงานตามนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ ● ให้ความคิดเห็น ข้อเสนอแนะ และข้อวิพากษ์ต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อนำไปปรับปรุงกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

3.3 กำหนดเครื่องมือในการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่สำคัญ

โรงงานไพ่ฯ ได้กำหนดตำแหน่งของผู้มีส่วนได้ส่วนเสียที่สำคัญกับกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ ในรูปแบบของตารางเส้น (Grid) ได้แบ่งออกเป็นแกน X หมายถึง ผู้ที่มีอำนาจ (Power) และแกน Y หมายถึง ผู้ที่ได้รับผลประโยชน์ (Interest) จำแนกออกเป็น 4 กลุ่ม ได้แก่ กลุ่มที่ควรทำให้พึงพอใจ กลุ่มที่ควรบริหารจัดการอย่างใกล้ชิด กลุ่มที่ต้องกำกับติดตาม และกลุ่มที่ต้องแจ้งข้อมูลข่าวสารให้ทราบ โดยสามารถสรุปได้ ดังนี้



ภาพตำแหน่งของผู้มีส่วนได้ส่วนเสียที่สำคัญ จำแนกตามกลุ่มต่าง ๆ

3.4 กำหนดบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญ

โรงงานไพ่ฯ ได้กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ ในรูปแบบตาราง RACI (RACI Matrix) โดยในแต่ละกระบวนการผู้มีส่วนได้ส่วนเสียหลักจะมีบทบาทหน้าที่ที่เหมือน และแตกต่างกันออกไป

ประกอบด้วย ผู้รับผิดชอบงาน (A) ผู้ที่ทำงานนั้น ๆ (R) ผู้ที่มีหน้าที่ให้คำปรึกษา (C) และผู้ที่โรงงานไพ่ฯ จะต้องแจ้งข้อมูลข่าวสารที่เกี่ยวข้องกับการดำเนินงานให้ทราบเป็นระยะ ๆ (I) โดยสามารถสรุปได้ ดังนี้

ตารางบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญกับกระบวนการการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ

การจัดทำกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	R = Responsible A = Accountable C = Consulted I = Informed							
กิจกรรม	คณะกรรมการโรงงานไพ่	คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	คณะอนุกรรมการด้านความเสี่ยงและควบคุมภายใน	ผู้อำนวยการโรงงานไพ่	รองผู้อำนวยการโรงงานไพ่	หัวหน้าฝ่ายอำนวยการ	หัวหน้าส่วน/เจ้าหน้าที่สารสนเทศและพัฒนาระบบ	พนักงาน
กำหนดเป้าหมายการจัดทำกระบวนการฯ	I	I	I	C	I	R	A	I
ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง	I	I	I	C	I	R	A	I
สำรวจปัญหา อุปสรรค และความต้องการ	I	I	I	C	I	R	A	R
วิเคราะห์ข้อมูล	I	I	I	C	I	R	A	I
ออกแบบกระบวนการ	I	I	I	C	I	R	A	I
กำหนดแนวทางการใช้แนวนโยบายและแนวปฏิบัติฯ	I	I	I	C	I	R	A	I
วิเคราะห์ผู้มีส่วนได้ส่วนเสีย	I	I	I	C	I	R	A	I
ถ่ายทอดกระบวนการวิเคราะห์และจัดทำ	I	I	I	C	I	I	A	I
กำกับดูแลแนวนโยบายและแนวปฏิบัติฯ	I	I	I	C	I	R	A	I
บริหารจัดการแนวนโยบายและแนวปฏิบัติฯ	I	I	I	C	I	R	A	I

3.5 จัดทำกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ

กระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯใช้วิธีการวิเคราะห์กระบวนการทำงานด้วยแบบจำลอง SIPOC หรือ “SIPOC Model” ประกอบด้วยองค์ประกอบต่าง ๆ ได้แก่ ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier) ปัจจัยนำเข้า (Input) กระบวนการ (Processes) ผลผลิต (Outputs) และผู้ที่นำผลผลิตไปใช้งาน (Customers) ซึ่งสามารถแสดงให้เห็นโดยภาพรวม ดังนี้

ชื่อกระบวนการ : กระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ	**วันที่จัดทำ/ปรับปรุงกระบวนการ :** 3 กรกฎาคม 2566
ผู้รับผิดชอบ : ส่วนสารสนเทศและพัฒนาระบบ	**จัดทำครั้งที่ :** 2

ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	ปัจจัยนำเข้า (Input)	กระบวนการ (Process)	ผลผลิต (Outputs)	ผู้ที่นำผลผลิตไปใช้งาน (Customers)
S1: หัวหน้าส่วนสารสนเทศฯ	I1: งบประมาณในการดำเนินงาน I2: บุคลากร ประกอบด้วย ● ผู้อำนวยการ ● รองผู้อำนวยการ ● หัวหน้าฝ่ายอำนวยการ ● หัวหน้าส่วนสารสนเทศฯ ● เจ้าหน้าที่สารสนเทศ I3: เทคโนโลยี ได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ของระบบคอมพิวเตอร์ I4: วัสดุอุปกรณ์ ได้แก่ เครื่องใช้สำนักงาน I5: เครื่องมือที่ใช้ในการวิเคราะห์ ได้แก่ ● แผนภูมิก้างปลา ● SWOT Analysis ● TOWS Matrix ● Gap Analysis	**P1: กำหนดแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** ↓ **P2: ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง** ↓ **P3: สำรวจปัญหา อุปสรรค ความต้องการ** ↓ **P4: วิเคราะห์ข้อมูล** ↓ **P5: จัดทำแนวโยบายและแนวปฏิบัติ** ↓ **P6: ประกาศใช้** ↓	แนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	C1: ภายในองค์กร ● ฝ่ายอำนวยการ ● ฝ่ายโรงพิมพ์ ● ฝ่ายผลิตไพ่

ชื่อกระบวนการ : กระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ	**วันที่จัดทำ/ปรับปรุงกระบวนการ :** 3 กรกฎาคม 2566
ผู้รับผิดชอบ : ส่วนสารสนเทศและพัฒนาระบบ	**จัดทำครั้งที่ :** 2

ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	**ปัจจัยนำเข้า (Input)**	**กระบวนการ (Process)**	**ผลผลิต (Outputs)**	**ผู้ที่นำผลผลิตไปใช้งาน (Customers)**
		P7: ติดตามผลการดำเนินงาน		
S2: เจ้าหน้าที่สารสนเทศ				C2: ภายในองค์กร ● ผู้ติดต่อ ● บริษัท
S6: คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล				
S7: คณะอนุกรรมการด้านความเสี่ยงและควบคุมภายใน				

3.6 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการกำหนดกระบวนการ และแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

เป็นกระบวนการกำหนดเป้าหมาย หรือสิ่งที่โรงงานไพ่ฯ ต้องการจะเป็นในอนาคต ซึ่งได้แก่ การเป็นผู้นำด้านสิ่งพิมพ์ปลอดการปลอมแปลง และดิจิทัลปริ้นติ้งโซลูชั่นภาครัฐ ทั้งนี้ ในการจะบรรลุวัตถุประสงค์และเป้าหมายดังที่กำหนดได้นั้น แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO:IEC/27001 : 2018 จึงมีบทบาทสำคัญอย่างยิ่งในการช่วยสนับสนุนการดำเนินงานในด้านต่าง ๆ ขององค์กร ให้มีมาตรฐานการดำเนินงานที่น่าเชื่อถือ ปลอดภัย โดยจะสังเหตุเห็นได้ว่า ISO:IEC/27001 : 2018 เป็นเรื่องที่ว่าด้วยมาตรฐานความมั่นคงปลอดภัย ของสารสนเทศทั้งหมด ทั้งในส่วนของข้อมูล การปฏิบัติที่มีมาตรฐานมีการควบคุมภายในที่ดี สอดรับวิสัยทัศน์และพันธกิจของโรงงานไพ่ ที่จะมุ่งสู่การเป็นผู้นำด้านสิ่งพิมพ์ปลอดการปลอม และการดำเนินงานทางด้านโซลูชั่น และสอดคล้องตาม พรบ. ไซเบอร์ และ พรบ. คุ้มครองข้อมูลส่วนบุคคล ดังนั้น การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO:IEC/27001 : 2018 จึงมีความสัมพันธ์อย่างยิ่งกับเป้าหมายขององค์กรในอนาคต ดังนั้นผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการนี้ จึงประกอบด้วยทั้งบุคลากรภายในตั้งแต่ระดับการบริหาร ถึงระดับปฏิบัติงาน และผู้เกี่ยวข้องที่มีการใช้บริการ ติดต่อสื่อสาร กับโรงงานไพ่ เพื่อช่วยกันให้ข้อเสนอแนะ ข้อสังเกต และช่วยกันกำหนดเป้าหมาย และทิศทางการดำเนินงานขององค์กรในอนาคต เพื่อที่จะสามารถออกการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO:IEC/27001 : 2018 ที่มีความสอดคล้องกับเป้าหมายตามที่กำหนดได้ หรืออาจกล่าวได้ว่า หากเป้าหมายหรือวิสัยทัศน์ขององค์กรเปลี่ยน ก็จะส่งผลต่อการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ต้องปรับเปลี่ยนไปเพื่อรองรับเป้าหมายใหม่ตามที่กำหนด ดังนั้น การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจึงได้ถูกกำหนดให้มีการทบทวนเป็นประจำทุกปี

3.7 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการศึกษาทบทวนเอกสารที่เกี่ยวข้อง

การศึกษาทบทวนเอกสารที่เกี่ยวข้องจะแบ่งออกเป็น 2 ส่วน ได้แก่ เอกสารสำคัญที่เกี่ยวข้องกับการดำเนินงานของโรงงานไพ่ฯ ประกอบด้วย

1) วิสัยทัศน์ ยุทธศาสตร์ พันธกิจ และเป้าหมายขององค์กร

2) แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีความเหมาะสมกับบริบทของโรงงานไพ่ ในกระบวนการนี้เนื่องจากการกำหนดวิสัยทัศน์ ยุทธศาสตร์ พันธกิจ และเป้าหมายขององค์กร ได้ผ่านการพิจารณาในกระบวนการกำหนดเป้าหมายในอนาคตขององค์กรแล้ว การกำหนดการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีความเหมาะสมกับบริบทของโรงงานไพ่ฯ จึงเป็นหน้าที่ของผู้เชี่ยวชาญที่จะต้องทำการศึกษาการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เป็นมาตรฐานสากล โดยการวิเคราะห์เชิงเปรียบเทียบ พิจารณาถึงข้อดี – ข้อจำกัดขององค์ประกอบต่างๆ เพื่อคัดเลือกและกำหนดการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีความเหมาะสมกับโรงงานไพ่ฯ โดยในการกำหนดผู้เชี่ยวชาญนั้น จะต้องกำหนดผู้เชี่ยวชาญที่เกี่ยวข้องและครอบคลุมการดำเนินงานในด้านต่าง ๆ ขององค์กร ไม่เพียงแต่เฉพาะด้านเทคโนโลยีดิจิทัลเท่านั้น แต่จะต้องครอบคลุมการดำเนินงานในด้านต่าง ๆ ขององค์กรด้วย เพื่อให้การศึกษา วิเคราะห์ และออกแบบการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสามารถช่วยสนับสนุนการดำเนินงานในด้านต่าง ๆ ขององค์ได้อย่างเหมาะสม

3.8 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการสำรวจข้อมูล

การสำรวจข้อมูลเป็นการเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการดำเนินงานขององค์กรได้เข้ามามีส่วนร่วมในการแสดงความคิดเห็น ให้ข้อเสนอแนะ และวิพากษ์กในประเด็นที่เกี่ยวข้องกับการดำเนินงานของ

องค์กรที่ผ่านมา ในกระบวนการนี้จึงทำให้ทราบถึงบริบทการดำเนินงานของโรงงานไพ่ฯ ในปัจจุบัน ช่วยสะท้อนให้เห็นถึงปัญหา อุปสรรค และข้อจำกัดต่าง ๆ ทั้งด้านเทคโนโลยีดิจิทัล และการดำเนินงานขององค์กร ซึ่งจะมีผลต่อการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสมกับโรงงานไพ่ฯ ทั้งนี้เพราะในการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีความเหมาะสมกับโรงงานไพ่ฯ นั้น ไม่เพียงแต่จะพิจารณาเฉพาะกรอบการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรที่เป็นมาตรฐานเท่านั้น แต่จะต้องพิจารณาบริบทการดำเนินงานขององค์กรในปัจจุบันร่วมด้วย เพื่อให้ได้รับแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่เป็นมาตรฐานและสามารถประยุกต์ใช้กับการดำเนินงานได้อย่างเหมาะสม ดังนั้น ในกระบวนการนี้นอกจากจะมีผู้มีผู้เชี่ยวชาญเข้ามาร่วมดำเนินการแล้ว ยังมีบุคลการของโรงงานไพ่ฯ ที่เป็นผู้รับผิดชอบในส่วนงานต่าง ๆ ซึ่งเป็นผู้ที่มีความรู้ความเข้าใจในส่วนงานที่ตนเป็นผู้รับผิดชอบเป็นอย่างดี โดยใช้วิธีการสัมภาษณ์เชิงลึก หรือการประชุมกลุ่มย่อย

3.9 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลจะประกอบไปด้วยการนำข้อมูลมาเปรียบเทียบกับแม่แบบของแนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตราฐานสากล ISO:IEC 27001:2018 พร้อมนำผลการดำเนินงานที่ผ่านมาร่วมกันวิเคราะห์ข้อมูลเพื่อหา ช่องว่าง (Gap) ต้องปรับปรุงแก้ไขเพื่อให้บรรลุเป้าหมายขององค์กรได้ในอนาคต จนนำไปสู่การสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัย ให้กับองค์กร คู่ค้า บุคคล หรือองค์กรภายนอกอื่นๆ และสร้างความยั่งยืนในการพัฒนาองค์กรให้สำเร็จตามวิสัยทัศน์ และกลยุทธ์ ขององค์กร

3.10 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการจัดทำแนวโยบายและแนวปฏิบัติ

แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ มีการจัดทำตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO:IEC/27001:2018 ซึ่งมาตราฐานดังกล่าวจะมีแม่แบบในการดำเนินงานแต่ละขั้นตอนที่ชัดเจน ทั้งสิ้น 14 Domain โดยสามารถกำหนดเป็นกรอบนโยบายการบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร (IT Management) ดังนี้

1) นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)
3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)
4) การจัดหมวดหมู่และควบคุมทรัพย์สินองค์กร (Asset Management)
5) การควบคุมการเข้าถึง (Access Control)
6) การเข้ารหัสข้อมูล (Cryptography)
7) ความมั่นคงทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)
8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)
9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
10) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
11) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

13) การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อสร้างความต่อเนื่องขององค์กร (Information security aspects of business continuity management)

14) ความสอดคล้อง (Compliance)

นอกจากนั้นแล้ว ยังต้องพิจารณาถึงหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสากิจ ตามระบบประเมินผลรัฐวิสาหกิจ (SE-AM) หัวข้อการพัฒนาเทคโนโลยีดิจิทัล ประเด็นด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ได้กำหนดหลักเกณฑ์การการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ในด้านต่าง ๆ ทั้งในด้านของแนวทาง กระบวนการ การถ่ายทอดกระบวนการ การกำหนดตัววัด ติดตาม วิเคราะห์ และประเมินตัววัดผลลัพธ์ รวมทั้งการนำผลลัพธ์ที่ได้เข้าสู่กระบวนการการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ดังนั้น ในกระบวนการนี้จึงมีความเกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียต่าง ๆ หลายส่วน โดยเฉพาะอย่างยิ่ง ผู้เชี่ยวชาญด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่ต้องเป็นผู้รับผิดชอบหลักในการกำหนดรูปแบบ และออกแบบการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในอนาคตที่มีความเหมาะสมกับโรงงานไพ่ฯ

3.11 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศองค์กรอย่างเป็นรูปธรรม

กระบวนการกำหนดกรอบแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นรูปธรรม เป็นกระบวนการกำหนดการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ ไปปรับใช้กับการดำเนินงานในด้านต่าง ๆ เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องดำเนินงานภายใต้การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดขึ้น โดยมีการกำหนดแนวทางที่ชัดเจน ภายใต้หลักการกำกับดูแลด้านดิจิทัล (Digital Governance) ประกอบด้วยแนวทางต่าง ๆ ได้แก่ กำหนดผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ประกาศนโยบาย กำหนดเป้าหมายในการดำเนินงาน และตัวชี้วัดผลการดำเนินงานการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดความสอดคล้องในการดำเนินงาน และสื่อสารให้ผู้มีส่วนได้ส่วนเสียในองค์กรได้รับทราบ ในกระบวนการนี้ผู้ที่ได้เข้ามามีบทบาทสำคัญ นอกจากนั้นแล้ว โรงงานไพ่ฯ ยังได้เปิดโอกาสให้ผู้บริหาร และพนักงานทุกคนในองค์กรได้เข้ามามีส่วนร่วมกับกระบวนการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นรูปธรรม ผ่านช่องทางการสื่อสารต่าง ๆ ได้แก่ ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ เว็บไซต์ของโรงงานไพ่ฯ ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ จดหมายอิเล็กทรอนิกส์ และแอพลิเคชั่นไลน์ (LINE) ทั้งนี้เพราะสถาปัตยกรรมองค์กรของโรงงานไพ่ฯ จะต้องถูกนำไปใช้กับทุกคนในองค์กร ดังนั้น จึงได้เปิดโอกาสให้ทุกคนในองค์กรได้เข้ามามีส่วนร่วมในการกำหนดแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อให้มีความเหมาะสมกับบริบทการดำเนินงานของบุคลากรในโรงงานไพ่ฯ

3.12 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการถ่ายทอดกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

การถ่ายทอดแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้เข้ามามีส่วนร่วมในการพิจารณาให้ข้อเสนอแนะ วิพากษ์ และร่วมแสดงความคิดเห็นเพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับมาปรับปรุงและพัฒนากระบวนการฯ ให้มีประสิทธิภาพมากยิ่งขึ้นต่อไป จนเกิดการพัฒนาที่มีแนวทางการปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) โดยโรงงานไพ่ฯ ได้กำหนดให้มีการทบทวนปรับปรุงกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเป็นประจำทุกปี ทั้งนี้ ผู้มีส่วนได้ส่วนเสียที่มีความเกี่ยวข้องกับกระบวนการนี้

จะประกอบด้วย ผู้อำนวยการโรงงานไพ่ฯ และผู้แทนในระดับหัวหน้าฝ่ายและหัวหน้าส่วนงานต่าง ๆ ของโรงงานไพ่ฯ ได้แก่ ฝ่ายอำนวยการ ฝ่ายโรงพิมพ์ ฝ่ายผลิตไพ่ ฝ่ายตรวจสอบภายใน ส่วนพัฒนาธุรกิจและการตลาด รวมทั้งส่วนสารสนเทศและพัฒนาระบบ จึงทำให้ได้รับมุมมองที่มีความหลากหลายครอบคลุมในมิติต่าง ๆ ในการดำเนินงานขององค์กร ผ่านช่องทางการสื่อสาร คือ การประชุมแบบเผชิญหน้า (Face to Face) หรือการประชุมออนไลน์ผ่านระบบการประชุมทางไกล (Video Conference)

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
1. กำหนดเป้าหมาย	1.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1.1.1 ผู้อำนวยการโรงงานไพ่ฯ 1.1.2 รองผู้อำนวยการโรงงานไพ่ฯ หัวหน้าฝ่ายอำนวยการ 1.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 1.2.2 เจ้าหน้าที่สารสนเทศฯ	การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ สารสนเทศ (Information Security Management)	ส่วนสารสนเทศและพัฒนาระบบ
2. ศึกษาทบทวนเอกสารที่เกี่ยวข้อง	2.1 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 2.1.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2.1.2 เจ้าหน้าที่สารสนเทศ	ข้อมูลพื้นฐานที่สามารถนำมาช่วยในการออกแบบกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศของสารสนเทศที่เหมาะสมกับโรงงานไพ่ฯ ประกอบด้วย ● แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศ	ส่วนสารสนเทศและพัฒนาระบบ
3. สำรวจปัญหา อุปสรรค และความต้องการ	3.1 หัวหน้าฝ่ายงาน และส่วนงานต่าง ๆ หรือผู้แทนในแต่ละฝ่ายงาน ผู้ใช้ติดต่อ กับโรงงานไพ่	ผลการสำรวจข้อมูลของโรงงานไพ่ฯ ที่ทำให้ทราบถึง ● ปัญหา อุปสรรค การใช้งานระบบสารสนเทศ	ส่วนสารสนเทศและพัฒนาระบบ

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
		● ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศ	
4. วิเคราะห์ข้อมูล	4.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 4.1.1 ผู้อำนวยการโรงงานไพ่ฯ 4.1.2 รองผู้อำนวยการโรงงานไพ่ฯ 4.1.3 หัวหน้าฝ่ายอำนวยการ 4.1.4 หัวหน้าฝ่ายโรงพิมพ์ 4.1.5 .หัวหน้าส่วนแผนงานและกลยุทธ์ 4.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 4.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 4.2.2 เจ้าหน้าที่สารสนเทศ	ข้อเสนอแนะ คำแนะนำ และแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ
5. จัดทำแนวโยบายและแนวปฏิบัติฯ	5.1 การจัดทำแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วย 5.1.1 หัวหน้าฝ่าย / หัวหน้าส่วน 5.1.2 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 5.1.3 เจ้าหน้าที่สารสนเทศ	ร่างแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
6. พิจารณาแนวนโยบายและแนวปฏิบัติฯ	6.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 6.1.1 ผู้อำนวยการโรงงานไพ่ฯ 6.1.2 รองผู้อำนวยการโรงงานไพ่ฯ 6.1.3 หัวหน้าฝ่ายอำนวยการ 6.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 6.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 6.2.2 เจ้าหน้าที่สารสนเทศฯ	แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศ	ผู้บริหารและพนักงานของโรงงานไพ่ฯ ทุกคน
7. ประกาศใช้แนวนโยบายและแนวปฏิบัติฯ	7.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 7.1.1 ผู้อำนวยการโรงงานไพ่ 7.1.2 รองผู้อำนวยการโรงงานไพ่ 7.1.3 หัวหน้าฝ่ายอำนวยการ	แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศ	ผู้บริหารและพนักงานของโรงงานไพ่ฯ ทุกคน
8. ติดตามผลการดำเนินงาน	8.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 8.1.1 ผู้อำนวยการโรงงานไพ่ 8.1.2 รองผู้อำนวยการโรงงานไพ่ 8.1.3 หัวหน้าฝ่ายอำนวยการ 8.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 8.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 8.2.2 เจ้าหน้าที่สารสนเทศฯ	ผลการประเมิน ความคิดเห็น และข้อเสนอแนะต่าง ๆ	ส่วนสารสนเทศและพัฒนาระบบนำข้อมูลที่ได้มาปรับปรุงกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศ

4. ถ่ายทอดกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

โรงงานไพ่ฯ ได้กำหนดวิธีการถ่ายทอดกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ ทั้งนี้ โรงงานไพ่ฯ ได้ประยุกต์ใช้แบบจำลองการสื่อสารดังกล่าว สำหรับการถ่ายทอดกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ดังนี้

4.1 ผู้ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล และคณะทำงานกำกับดูแลและการบริหารจัดการสถาปัตยกรรมองค์กรพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

4.2 ข้อมูลข่าวสาร (Message)

ข้อมูลข่าวสาร ได้แก่ กระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่ผ่านการพิจารณาจากคณะอนุกรรมการฯ และคณะทำงานฯ โดยได้รับการรับรองความถูกต้องเป็นที่เรียบร้อยแล้ว

4.3 ช่องทางการสื่อสาร (Channel)

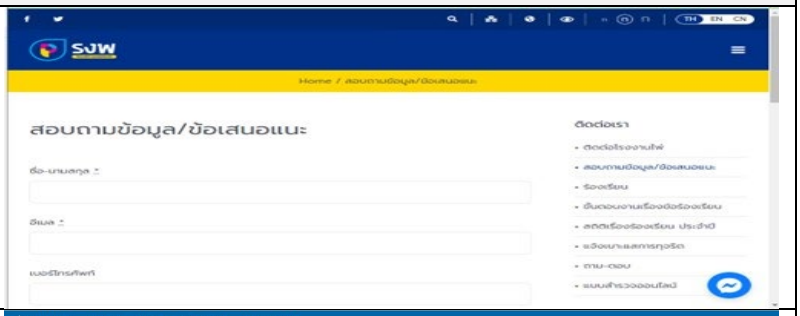
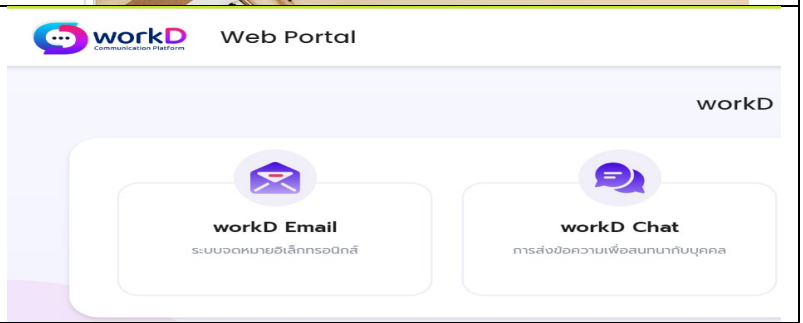
ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้

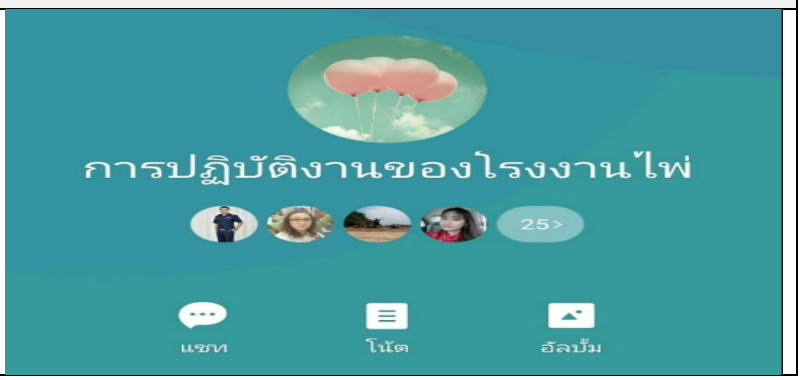
1) สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการ และหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารผ่านที่ประชุมคณะอนุกรรมการด้านเทคโนโลยีดิจิทัล

ตำแหน่ง	ภาพประกอบ
หน้าทางเข้าโรงงานไพ่ฯ	
ห้องสันทนาการ	

ตำแหน่ง	ภาพประกอบ
หน้าห้องส่วนบริหารงานกลาง	

2) สื่อสมัยใหม่ ประกอบด้วย เว็บไซต์ของโรงงานไพ่ฯ ได้แก่(https://www.playingcard.or.th/) ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)และแอพลิเคชั่นไลน์ (LINE) โดยในช่องทางดังกล่าว ได้เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถให้ความคิดเห็น และข้อเสนอแนะต่าง ๆ ที่เกี่ยวข้องกับกระบวนการวิเคราะห์และการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อมที่สามารถเข้าถึงได้จากอุปกรณ์การอิเล็กทรอนิกส์ต่าง ๆ ทั้งสมาร์ทโฟน และคอมพิวเตอร์ เพื่อที่จะสามารถนำข้อมูลต่าง ๆ เหล่านั้นมาปรับปรุงและพัฒนากระบวนการฯ ให้มีประสิทธิภาพมากขึ้นต่อไป

สื่อที่ใช้	ภาพประกอบ
เว็บไซต์ของโรงงานไพ่ฯ (https://www.playingcard.or.th/)	
ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ	
ระบบการสื่อสารแบบรวมศูนย์ (workD Platform) -workD Mail ระบบจดหมายอิเล็กทรอนิกส์ (saraban@playingcard.mail.go.th) -workD Chat การส่งข้อความเพื่อสนทนา	

สื่อที่ใช้	ภาพประกอบ
แอพลิเคชั่นไลน์ (LINE)	

4.4 ผู้รับสาร (Receiver)

ผู้รับสาร หรือผู้ที่มีความเกี่ยวข้องกับข้อมูลข่าวสารในกระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่ บุคลากรของโรงงานไพ่ฯ ทั้งในระดับผู้บริหาร พนักงาน และผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้อง

5. ประเมินการรับรู้จากผู้ที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ในขั้นตอนนี้เป็นกระบวนการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และการดำเนินการด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ ที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่ง ในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการวิเคราะห์และการดำเนินการด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ ให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องกับกระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ จำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ ได้ดังนี้

วิธีการประเมินการรับรู้

กระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
1. กำหนดเป้าหมาย	1.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ 1.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	ผู้บริหารในระดับต่างๆ ได้เข้ามามีส่วนร่วมกับการกำหนดเป้าหมายของกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของสารสนเทศผ่านการประชุม	● รายงานการประชุม
2. ศึกษาทบทวนเอกสารที่เกี่ยวข้อง	2.1 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ และเจ้าหน้าที่สารสนเทศได้ศึกษา ทบทวนทั้งปัจจัยภายนอก และปัจจัยภายในเพื่อพิจารณาทบทวนเอกสารต่าง ๆ ที่เกี่ยวข้อง	● ผลการศึกษาทบทวนเอกสารที่เกี่ยวข้อง
3. สำรวจปัญหา อุปสรรค และความต้องการ	3.1 หัวหน้าฝ่าย/ส่วนงานต่าง ๆ หรือผู้แทนในแต่ละฝ่ายงาน	นัดสัมภาษณ์เชิงลึกกับหัวหน้าฝ่าย/ส่วนงานต่าง ๆ	● รายงานสรุปผลการสำรวจข้อมูล ● แบบสัมภาษณ์
4. วิเคราะห์ข้อมูล	4.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ	● ทำหนังสือเวียนถึงผู้บริหาร เพื่อพิจารณาผลการวิเคราะห์ข้อมูล	● รายงานผลการวิเคราะห์ข้อมูล ● เอกสารสรุปรายงานประชุม

กระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
	4) หัวหน้าฝ่ายโรงพิมพ์ 5) หัวหน้าส่วนแผนงานและกลยุทธ์ 4.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศ		● หนังสือเวียน
5. จัดทำแนวโยบายและแนวปฏิบัติฯ	5.1 การจัดทำแผนการดำเนินการด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ประกอบด้วย 1) หัวหน้าฝ่าย/ส่วนงานต่าง ๆ ของโรงงานไพ่ฯ 2) หัวหน้าส่วนสารสนเทศ 3) เจ้าหน้าที่ส่วนสารสนเทศ	ผู้มีส่วนเกี่ยวข้องร่วมกันเพื่อพิจารณาออกแบบกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของสารสนเทศของโรงงานไพ่ฯ	● กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของสารสนเทศของโรงงานไพ่ฯ ● เอกสารสรุปรายงานประชุม
6. พิจารณาแนวนโยบายและแนวปฏิบัติฯ	6.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ 6.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	ทำบันทึกข้อความถึงผู้อำนวยการ เพื่อพิจารณาเห็นชอบผลการทบทวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management)	● การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ● บันทึกข้อความ

กระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
7. ประกาศใช้แนวนโยบายและแนวปฏิบัติฯ	7.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 1) ผู้อำนวยการโรงงานไพ่ 2) รองผู้อำนวยการโรงงานไพ่ 3) หัวหน้าฝ่ายอำนวยการ 7.2 หัวหน้าฝ่าย/ส่วนต่างๆ 7.3 พนักงานโรงงานไพ่ 7.4 ผู้ติดต่อประสานงานกับโรงงานไพ่	● นำกระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเข้าสู่ที่ประชุมคณะอนุกรรมการด้านเทคโนโลยีดิจิทัลเพื่อพิจารณา ● ใช้แบบสอบถามประเมินการรับรู้ด้านกระบวนการวิเคราะห์และการดำเนินการด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโรงงานไพ่ฯ	● หนังสือเวียน ● การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management)
8. ติดตามผลการดำเนินงาน	8.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 1) ผู้อำนวยการโรงงานไพ่ 2) รองผู้อำนวยการโรงงานไพ่ 3) หัวหน้าฝ่ายอำนวยการ 8.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	● ติดตามผลการประเมินจาก ตัวชี้วัดการดำเนินกิจกรรม โครงการต่างๆ ทางด้านเทคโนโลยีดิจิทัล ว่าสอดคล้อง เป็นไปตามแผนทางการบริหารจัดการใช้ทรัพยากรอย่างเหมาะสมหรือไม่	● การดำเนินกิจกรรมโครงการต่าง ๆ ทางด้านเทคโนโลยีดิจิทัลสอดคล้อง เป็นไปตามแผนทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสารสนเทศขององค์กร

สรุปโรงงานไพ่ฯ ได้กำหนดวิธีการประเมินผลการรับรู้กระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศด้วยรูปแบบที่แตกต่างกัน จำแนกตามผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการต่าง ๆ ซึ่งได้ผ่านการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการมาเป็นที่เรียบร้อยแล้ว ทั้งนี้เพราะผู้มีส่วนได้ส่วนเสียต่าง ๆ เหล่านั้น ล้วนเป็นส่วนหนึ่งของการจัดทำ พัฒนา และยกระดับกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของสารสนเทศของโรงงานไพ่ฯ ให้ดียิ่งขึ้น ดังนั้น การจัดทำสถาปัตยกรรมองค์ในครั้งนี้ จึงเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้เข้ามามีส่วนร่วมในการแสดงความคิดเห็น และให้ข้อเสนอแนะสำหรับการปรับปรุงกระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งสอดคล้องกับหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยโรงงานไพ่ฯ ได้กำหนดให้การประเมินการรับรู้ดำเนินการควบคู่กับการจัดทำกระบวนการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเป็นประจำทุกปี เพื่อให้กระบวนการมีแนวทางปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice)

หมายเหตุ : บันทึกข้อความที่ 180/2566 วันที่ 4 กรกฎาคม 2566

บทที่ 4
การกำหนดตัววัดผลลัพธ์ ของกระบวนการบริหารจัดการความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้มั่นใจได้ว่ากระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ได้ถูกดำเนินการอย่างมีระบบแบบแผน และมีประสิทธิผล จึงมีการกำหนดหลักเกณฑ์การประเมินผลไว้ดังนี้

1. เป้าหมายและหลักเกณฑ์การประเมินผล

1. ต้องมีการสื่อสาร โดยประกาศแจ้งแผนการบริหารความเสี่ยงให้คลอบคลุมไปยังผู้มีส่วนได้เสีย ให้ได้รับทราบไม่ต่ำกว่าร้อยละ 90 ของบุคลากรทั้งหมด
2. ต้องมีการสื่อสารแผนบริหารความเสี่ยงไม่ต่ำกว่าร้อยละ 80 จากจำนวนแผนทั้งหมด 23 แผน หรือคิดเป็นจำนวนที่ต้องสื่อสารไม่ต่ำกว่า 19 แผน
3. เมื่อเกิดเหตุการณ์ หรือสภาวะการณ์ความเสี่ยง ต้องสามารถดำเนินการตามแนวทาง “วิธีการจัดการความเสี่ยง” ที่กำหนดไว้อย่างเป็นระบบตามขั้นตอนได้ครอบคลุมไม่ต่ำกว่าร้อยละ 90
4. จากการวิเคราะห์ตัวเลขเคสที่รับแจ้งผ่านระบบ ezSUPPORT ทั้งสามหมวด ประกอบด้วย
    - [OSC] แจ้งปัญหาการใช้งาน
    - [REQ] ยื่นคำร้อง/คำขอ
    - [ASK] สอบถามข้อมูลทั่วไป

ซึ่งพิจารณาวัดผลในภาพรวมทุกหัวข้อเนื่องจากเป็นเรื่องที่เกี่ยวโยงกับมาตรการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรทั้งสิ้น ภายใต้หลักการที่ว่าหากปริมาณตัวเลขเคสเป็นไปในทิศทางที่ลดลง โอกาสที่จะเกิดผลกระทบจากความเสี่ยงในทุกๆ มิติยิ่งมีน้อยลงเท่านั้น โดยมีเป้าหมายคือปริมาณเคสในภาพรวมต้องลดไม่ต่ำกว่าร้อยละ 10 ในแต่ละไตรมาส

บทที่ 5
การทบทวน ติดตามประสิทธิผลของการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management)

ผู้บริหารความเสี่ยงต้องกำหนดแผนการบริหารความเสี่ยงที่แต่ละหน่วยงานจะต้องร่วมปฏิบัติ หลังจากที่ได้มีการวางแนวทางในการบริหารความเสี่ยงที่เหมาะสม ซึ่งความเสี่ยงบางอย่างอาจเป็นความเสี่ยงเฉพาะที่เกิดจากหน่วยงานใดหน่วยงานหึ่งในองค์กรเท่านั้น แต่ความเสี่ยงหลายอย่างเป็นความเสี่ยงที่ทุกฝ่ายมีส่วนก่อให้เกิดการนำแผนกลยุทธ์การการบิหารความเสี่ยงไปสู่การปฏิบัติ จึงต้องอาศัยความเข้าใจและความร่วมมือจากทุกฝ่ายที่เกี่ยวข้อง ปัญหาที่ทีมบริหารความเสี่ยงต้องเผชิญคือ การขาดความร่วมมือจากหน่วยงานในองค์กร ที่ทุกคนต้องปฏิบัติตามแผนกลยุทธ์การบริหารความเสี่ยง จะเห็นได้ว่าการบริหารความเสี่ยงเป็นงานที่ต้องทำอย่างต่อเนื่อง ความเสี่ยงแต่ละประเภทเปลี่ยนไปตามการเปลี่ยนแปลงของโลกเทคโนโลยีที่ทันสมัยมากกขึ้น ทำหมีความเสี่ยงเพิ่มมากขึ้นเช่นกัน การบิหารความเสี่ยงจึงต้องได้รับการประเมินผลและปรับปรุงให้สอดคล้องกับสถานการณ์ปัจจุบัน การติดตามประเมินผลจึงไม่ใช่ขั้นตอนสุดท้ายในการบริหารความเสี่ยง แต่เป็นขั้นตอนที่นำไปสู่ระบบการบริหารความเสี่ยงที่มีความต่อเนื่องและทันต่อเหตุการณ์ เพื่อสร้างความมั่นใจว่า กลยุทธ์ที่กำหนดในการบริหารความเสี่ยงได้ถูกดำเนินการตามแนวทางที่ได้วางแผนไว้จริง และติดตามว่าความเสี่ยงนั้นลดลงอยู่ในระดับที่องค์กรยอมรับได้หรือไม่ ประเด็นสำคัญสำหรับการติดตามกลยุทธ์ในการบริหารความเสี่ยงคือ การกำหนดผู้รับผิดชอบความเสี่ยงเพื่อการติดตามแผนการนั้นจะได้เป็นไปอย่างมีประสิทธิภาพ

1. วัตถุประสงค์

1) เพื่อให้การดำเนินการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ได้รับการกำกับดูแลอย่างต่อเนื่องตลอดทั้งกระบวนการ และสามารถนำแผนไปปฏิบัติได้จริงอย่างเป็นรูปธรรม

2) เพื่อลดข้อผิดพลาด ผลกระทบ หรือความเสี่ยงร้ายแรงที่อาจเกิดขึ้นจากการเกิดปัญหาในสภาวะฉุกเฉิน

2. เป้าหมายและหลักเกณฑ์การประเมินผล

1) ต้องมีการสื่อสาร โดยประกาศแจ้งแผนการบริหารความเสี่ยงให้คลอบคลุมไปยังผู้มีส่วนได้เสีย ให้ได้รับทราบไม่ต่ำกว่าร้อยละ 90 ของบุคลากรทั้งหมด

2) ต้องมีการสื่อสารแผนบริหารความเสี่ยงไม่ต่ำกว่าร้อยละ 80 จากจำนวนแผนทั้งหมด 23 แผน หรือคิดเป็นจำนวนที่ต้องสื่อสารไม่ต่ำกว่า 19 แผน

3) เมื่อเกิดเหตุการณ์ หรือสภาวะการณ์ความเสี่ยง ต้องสามารถดำเนินการตามแนวทาง “วิธีการจัดการความเสี่ยง” ที่กำหนดไว้อย่างเป็นระบบตามขั้นตอนได้ครอบคลุมไม่ต่ำกว่าร้อยละ 90

4) จากการวิเคราะห์ตัวเลขเคสที่รับแจ้งผ่านระบบ ezSUPPORT ทั้งสามหมวด ประกอบด้วย [OSC] แจ้งปัญหาการใช้งาน, [REQ] ยื่นคำร้อง/คำขอ และ “[ASK] สอบถามข้อมูลทั่วไป” ซึ่งพิจารณาวัดผลในภาพรวมทุกหัวข้อ เนื่องจากเป็นเรื่องที่เกี่ยวโยงกับมาตรการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรทั้งสิ้น ภายใต้หลักการที่ว่าหากปริมาณตัวเลขเคสเป็นไปในทิศทางที่ลดลง โอกาสที่จะเกิดผลกระทบจากความเสี่ยงในทุกๆ มิติยิ่งมีน้อยลงเท่านั้น โดยมีเป้าหมายคือปริมาณเคสในภาพรวมต้องลดไม่ต่ำกว่าร้อยละ 10 ในแต่ละไตรมาส

3. ผลการประเมินประจำปีงบประมาณ 2566

1) มีการสื่อสารแผนการบริหารจัดการความเสี่ยงได้ครอบคลุมไปยังผู้มีส่วนได้เสียแล้วทั้งสิ้นร้อยละ 100 ของจำนวนบุคลากรทั้งหมด

2) มีการสื่อสารแผนการบริหารจัดการความเสี่ยงไปแล้วทั้งสิ้น 23 แผน หรือคิดเป็นร้อยละ 100 จากจำนวนแผนทั้งหมด 23 แผน

3) ในปีงบประมาณ 2566 เกิดเหตุการณ์ความเสี่ยงขึ้นทั้งสิ้น 5 เหตุการณ์ และสามารถดำเนินการตาม “วิธีการจัดการความเสี่ยง” ที่กำหนดไว้ได้ครอบคลุม 5 เหตุการณ์ หรือคิดเป็นร้อยละ 100

4) ผลการวิเคราะห์เคสจากตัวเลขรายงาน ezSUPPORT พบว่าปริมาณเคสในภาพรวมไตรมาสที่ 2/2566 เพิ่มขึ้นร้อยละ 17.65, ปริมาณเคสไตรมาสที่ 3/2566 ลดลงร้อยละ 41.67 และปริมาณเคสไตรมาสที่ 4/2566 เพิ่มขึ้นร้อยละ 7.69 จึงสรุปได้ว่าในภาพรวมปริมาณเคสที่ลดลงตามเป้าหมาย(ไม่ต่ำกว่าร้อยละ 10) สัมฤทธิ์ผลเพียงไตรมาส 3/2566 เท่านั้น จึงเห็นควรพิจารณาหาแนวทางปรับปรุงพัฒนาในรายละเอียดต่อไป

สรุปข้อมูลรายไตรมาสแยกตามหมวดหมู่การแจ้งเคส

หัวข้อปัญหา	**ปริมาณปัญหา**			
	ไตรมาส 1 ต.ค.-ธ.ค.65	**ไตรมาส 2 ม.ค.-มี.ค.66**	**ไตรมาส 3 เม.ย.-มิ.ย.66**	**ไตรมาส 4 ก.ค.-ก.ย.66**
[ASK] สอบถามข้อมูลทั่วไป	0	0	0	0
[OSC] แจ้งปัญหาการใช้งาน	9	15	7	8
[REQ] ยื่นคำขอ/คำร้อง	5	2	5	5
รวม	14	17	12	13
เพิ่ม/ลด (%)		**17.65**	**-41.67**	**7.69**

KPI 5 การบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)

KPI 5.3 การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management System (ISMS) Audit)

เอกสารโดย

ส่วนสารสนเทศและพัฒนาระบบ
โรงงานไพ่ กรมสรรพสามิต

รหัสเอกสาร IT-DOC-KPI5-003
ปรับปรุงล่าสุด 3 กรกฎาคม 2566

บทนำ

บทนำ

เดิมโรงงานไพ่ กรมสรรพสามิต ได้เคยมีการตรวจสอบความมั่นคงด้านสารสนเทศและการสื่อสาร และจากที่ส่วนสารสนเทศและพัฒนาระบบ โรงงานไพ่ กรมสรรพสามิต (ซึ่งต่อไปขอเรียกว่า “โรงงานไพ่”) ได้ตระหนักถึงความสำคัญของการควบคุมและตรวจสอบทางด้านเทคโนโลยีสารสนเทศ จึงได้จัดทำแผนการตรวจสอบด้านเทคโนโลยีสารสนเทศ ขึ้นอย่างเป็นทางการ โดยอ้างอิงกรอบการดำเนินงานตามมาตรฐาน ISO/IEC 27001:2018 เพื่อให้ส่วนสารสนเทศและพัฒนาระบบสามารถดำเนินการให้เป็นไปตามแผนกลยุทธ์ ด้านเทคโนโลยีสารสนเทศที่ได้กำหนดไว้

ดังนั้น โรงงานไพ่ จึงได้ดำเนินโครงการเพื่อตรวจสอบการควบคุมทั่วไปทางด้านเทคโนโลยี สารสนเทศ เพื่อเสริมสร้างศักยภาพของเจ้าหน้าที่ส่วนสารสนเทศและพัฒนาระบบให้สามารถปฏิบัติงาน ให้ได้อย่างมีประสิทธิผลและมีประสิทธิภาพ และมีการควบคุมที่ดีเป็นไปตามมาตรฐานสากลและสอดคล้องกับสภาวะในปัจจุบัน

วัตถุประสงค์

1) เพื่อดำเนินการตรวจสอบการควบคุมทั่วไปทางด้านเทคโนโลยีสารสนเทศของ โรงงานไพ่ ให้เป็นไปตามมาตรฐานสากลโดยจะต้องครอบคลุมวัตถุประสงค์ ดังนี้

2) เพื่อพัฒนาศักยภาพการควบคุมทั่วไปทางด้านเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยและน่าเชื่อถือ

3) เพื่อพัฒนาศักยภาพของบุคลากร เพิ่มพูนความรู้ ทักษะ และวิธีการปฏิบัติงานให้เป็นไปตามมาตรฐานสากลและให้คำปรึกษาแก่ผู้บริหาร โดยใช้ผลที่ได้จากการตรวจสอบการควบคุมทั่วไป ทางด้านเทคโนโลยีสารสนเทศ

สารบัญ

บทที่ 1
แนวทางการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management System (ISMS) Audit)

ในบทนี้จะกล่าวถึงแนวทางในการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ซึ่งโรงงานไพ่ฯ ดำเนินการตามกรอบแนวทางตามระบบประเมินผลรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM ภายใต้การกำกับดูแลของ สคร. โดยระบุให้มีองค์ประกอบดังนี้

- กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (ISMS Audit)
- รัฐวิสาหกิจมีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Audit) โดยมีแนวทางดังนี้

1. วางแผน จัดตั้ง นำไปปฏิบัติ และรักษาให้คงไว้ตามแผนการตรวจประเมิน รวมถึงความถี่ วิธีการหน้าที่ความรับผิดชอบ ข้อกำหนดของการวางแผนและการรายงานผล รวมทั้งให้ความสำคัญกับกระบวนการที่เกี่ยวข้องและผลการประเมินครั้งก่อน
2. กำหนดเกณฑ์การตรวจประเมิน และขอบเขตการประเมินแต่ละครั้ง
3. คัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินที่มีความเป็นกลางและความเป็นธรรม
4. รายงานผลการตรวจประเมินเสนอต่อผู้บริหารที่เกี่ยวข้องและเก็บรักษาเอกสารสนเทศ เพื่อใช้เป็นหลักฐานแสดงแผนการตรวจประเมินและผลการตรวจประเมิน

- รัฐวิสาหกิจกำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ขององค์กร

และได้กำหนดหลักเกณฑ์การประเมินเป็น 5 ระดับ ในลักษณะของระดับวุฒิภาวะ (Mutuality level) ดังนี้

ระดับ	วิธีการดำเนินการ
ระดับ 1	เริ่มมีแนวทางในการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร
ระดับ 2	รัฐวิสาหกิจมีกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย • การวางแผน จัดตั้ง นำไปปฏิบัติ และรักษาให้คงไว้ตามแผนการตรวจประเมิน • การกำหนดเกณฑ์การตรวจประเมิน และขอบเขตการประเมินแต่ละครั้ง • การคัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินที่มีความเป็นกลาง และความเป็นธรรม • การรายงานผลการตรวจประเมินเสนอต่อผู้บริหาร
ระดับ 3	รัฐวิสาหกิจมีการถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรแก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจนและมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
ระดับ 4	รัฐวิสาหกิจมีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

ระดับ	วิธีการดำเนินการ
ระดับ 5	รัฐวิสาหกิจมีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

ทั้งนี้จะมีการกล่าวถึงรายละเอียดและขั้นตอนการดำเนินการในบทถัดไป

บทที่ 2
แนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1. ขอบเขตการดำเนินการตรวจสอบ

1.1 การตรวจสอบจากผู้ตรวจสอบภายนอก

โดยองค์กรได้ทำการว่าจ้างที่ปรึกษาจากภายนอก ซึ่งจะต้องส่งทีมงานผู้เชี่ยวชาญที่มีความรู้ ความชำนาญและมีประสบการณ์การตรวจสอบการควบคุมทั่วไปทางด้านเทคโนโลยีสารสนเทศมาดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศของ โรงงานไพ่ ดังนี้

1) ดำเนินการจัดทำแผนการบริหารงานโครงการ (Project Management Plan) โดยแสดงรายละเอียดขั้นตอนและวิธีการปฏิบัติงาน แผนการดำเนินงาน พร้อมทั้งบุคลากร และระยะเวลาในการดำเนินงานของทีมที่ปรึกษา

2) ดำเนินการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ

3) ติดตามผลการดำเนินงานปรับปรุง แก้ไข ของโรงงานไพ่ กรมสรรพสามิต ตามข้อเสนอแนะผลการดำเนินงานโครงการตรวจสอบความมั่นคงด้านสารสนเทศและการสื่อสาร (Computer Audits) ISO 27001 ในรอบการประเมินครั้งก่อน

4) ดำเนินการวิเคราะห์ พร้อมข้อเสนอแนะในการปรับปรุงแก้ไข ตามมาตรฐาน ISO/IEC 27001:2018 พร้อมส่งมอบผลการวิเคราะห์ ให้กับโรงงานไพ่ กรมสรรพสามิต ตามโดเมน ดังนี้

โดเมนที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policies)

โดเมนที่ 2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

โดเมนที่ 3 ความมั่นคงปลอดภัยสาหรับบุคลากร (Human Resource Security)

โดเมนที่ 4 การบริหารจัดการทรัพย์สิน (Asset Management)

โดเมนที่ 5 การควบคุมการเข้าถึง (Access Control) ในส่วนระบบบริหารงานบุคคล (HR) ระบบ บริหาร ความเสี่ยงและควบคุมภายใน และระบบบริหารทรัพยากรองค์การ (ERP)

โดเมนที่ 6 การเข้ารหัสข้อมูล (Cryptography)

โดเมนที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)

โดเมนที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

โดเมนที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

โดเมนที่ 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

โดเมนที่ 11 ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)

โดเมนที่ 12 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

โดเมนที่ 13 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

โดเมนที่ 14 ความสอดคล้อง (Compliance)

1.2 การตรวจสอบจากผู้ตรวจสอบภายใน

1) แนวทางการตรวจสอบ

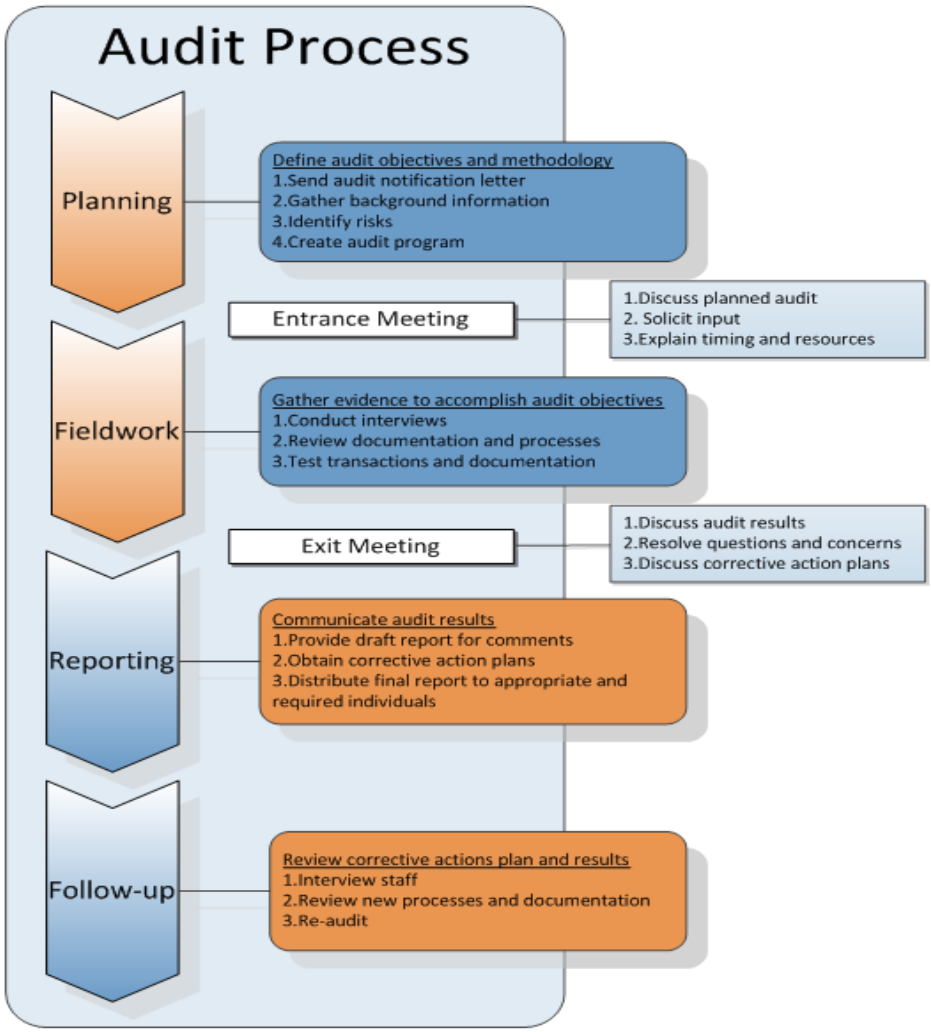
โดยการตรวจสอบระบบสารสนเทศ ใช้หลักการ “GRC” หรือ “Governance , Risk Management and Compliance” มาประยุกต์ใช้ และมีลักษณะการตรวจสอบในแบบ “Risk-Based Approach” โดยทำการคัดเลือกผู้ตรวจสอบจากภายในองค์กร และจำเป็นต้องมีองค์ความรู้เรื่อง “Information System Audit Process” เป็นองค์ความรู้หลัก ซึ่งองค์ความรู้ที่จำเป็นต้องศึกษามีทั้งหมด 6 องค์ความรู้ได้แก่

- IS Audit Process
- IT Governance
- Systems and Infrastructure Lifecycle Management
- IT Service Delivery and Support
- Protection of Information Assets
- Business Continuity and Disaster Recovery

2) กระบวนการตรวจสอบ

- ความถี่ในการตรวจสอบตามความเหมาะสม โดยทั่วไปองค์กรควรได้รับการตรวจประเมินปีละ 1 ครั้ง
- เกณฑ์การประเมินใช้รูปแบบเดียวกับการตรวจสอบจากนอก
- หัวข้อการประเมินในแต่ละวาระต้องได้รับการกำหนดร่วมกันจากคณะทำงาน
- คัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินที่มีความเป็นกลางและความเป็นธรรม
- วิเคราะห์ผลการประเมิน และส่งบันทึกรายงานแก่ผู้บริหาร เพื่อปรับปรุงพัฒนาต่อไป

1.2 กระบวนการตรวจสอบ



โดยการตรวจสอบอ้างอิงกระบวนการตามมาตรฐาน ISO/IEC 27001:2018 ดังนี้

1.2.1 หัวข้อนโยบายการตรวจสอบ ISO/IEC 27001:2018

1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policies)
2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of information technology)
3) ความมั่นคงปลอดภัยสำหรับบุคลากร (Human resource security)
4) การบริหารจัดการทรัพย์สิน (Asset management)
5) การควบคุมการเข้าถึง (Access Control)
6) การเข้ารหัสข้อมูล (Cryptography)
7) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)
8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation security)
9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communication security)
10) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
11) ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationship)

12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)

13) ประเด็นด้านความมั่นคงปลอดภัยของสารสนเทศของการบริหารจัดการเพื่อสร้างความมั่นคงต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

14) ความสอดคล้อง (Compliance)

1.2.2 เกณฑ์กำหนดระดับความเสี่ยงที่ใช้ในรายการตรวจสอบ

เกณฑ์ในการกำหนดระดับความเสี่ยงที่ใช้ในรายงานการตรวจสอบนี้ คือ

สูง	เป็นประเด็นซึ่งควรได้รับการพิจารณาแก้ไขจากผู้บริหารทันที เพราะหากไม่ได้รับการแก้ไขอาจเกิดเหตุการณ์ทั้งโดยเจตนาและมิได้เจตนาซึ่งก่อให้เกิดผลกระทบที่ร้ายแรงต่อความครบถ้วนสมบูรณ์(Completeness) ความถูกต้อง (Accuracy) ความสมเหตุผลของข้อมูล(Validation) และการจำกัดสิทธิการเข้าถึงระบบงาน(Restricted Access) ตลอดจนความน่าเชื่อถือ(Reliability) ของระบบสารสนเทศของโรงงานไพ่
ปานกลาง	เป็นประเด็นที่มีความเสี่ยงอยู่ในระดับปานกลาง ซึ่งอาจมีผลกระทบต่อความครบถ้วนสมบูรณ์ (Completeness) ความถูกต้อง (Accuracy) ความสมเหตุผลของข้อมูล(Validation) และการจำกัดสิทธิการเข้าถึงระบบงาน (Restricted Access) ตลอดจนความน่าเชื่อถือ(Reliability) ของระบบสารสนเทศของโรงงานไพ่ โดยประเด็นดังกล่าวนี้ควรได้รับการพิจารณาแก้ไขหลังจากการแก้ไขประเด็นที่มีความเสี่ยงสูงแล้ว
ต่ำ	เป็นประเด็นที่มีความเสี่ยงอยู่ในระดับต่ำ ซึ่งอาจมีผลกระทบต่อความครบถ้วนสมบูรณ์ (Completeness) ความถูกต้อง (Accuracy) ความสมเหตุผลของข้อมูล (Validation) และการจำกัดสิทธิการเข้าถึงระบบงาน (Restricted Access) ตลอดจนความน่าเชื่อถือ (Reliability) ของระบบสารสนเทศของโรงงานไพ่ ซึ่งประเด็นดังกล่าวสามารถแก้ไขปรับปรุงเพื่อเพิ่มประสิทธิภาพของการควบคุม และทำให้สภาพแวดล้อมของการควบคุมระบบสารสนเทศโดยรวมดีขึ้นในระยะยาว

1.2.3 เกณฑ์การควบคุม

โดยระดับความมีประสิทธิผลในภาพรวมของแต่ละหัวข้อการควบคุมแบ่งออกเป็น 3 ระดับ ได้แก่ “ดี” “พอใช้” และ “ควรปรับปรุง” ตามนิยาม ดังต่อไปนี้

ระดับความมีประสิทธิผล	นิยาม
ดี	มีการกำหนดให้มีการควบคุมอย่างเพียงพอ และมีการปฏิบัติตามการควบคุมที่กำหนดไว้
พอใช้	มีการกำหนดให้มีการควบคุม และมีการปฏิบัติตามการควบคุมที่กำหนดไว้ อย่างไรก็ตามการควบคุมที่กำหนดไว้ ยังคงสามารถปรับปรุงเพิ่มเติมให้มีคุณภาพที่ดียิ่งขึ้นได้อีก
ควรปรับปรุง	กากำหนดให้มีการควบคุมยังไม่เพียงพอ หรือยังไม่มีการปฏิบัติตามการควบคุมที่กำหนดไว้อย่างเพียงพอ

1.2.4 ผลการการวิเคราะห์ความเสี่ยง

รูปแบบตารางผลการวิเคราะห์ความเสี่ยง โดยผู้ตรวจสอบทำการประเมินตามเกณฑ์ เพื่อจัดทำรายงานเสนอผู้บริหาร และหาแนวทางปรับปรุงแก้ไข (ตามหัวข้อที่ได้รับตรวจสอบในแต่ละวาระ)

ลำดับ	หัวข้อการตรวจสอบ	ระดับการมีประสิทธิผล	รายละเอียดการควบคุม
1	โดเมนที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policies)	ดี	
2	โดเมนที่ 2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)	ดี	
3	โดเมนที่ 3 ความมั่นคงปลอดภัยสาหรับบุคลากร (Human Resource Security)	ดี	
4	โดเมนที่ 4 การบริหารจัดการทรัพย์สิน (Asset Management)	ดี	
5	โดเมนที่ 5 การควบคุมการเข้าถึง (Access Control) ในส่วนระบบบริหารงานบุคคล (HR) ระบบบริหารความเสี่ยงและควบคุมภายใน และระบบบริหารทรัพยากรองค์การ (ERP)	ดี	
6	โดเมนที่ 6 การเข้ารหัสข้อมูล (Cryptography)	ดี	
7	โดเมนที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)	พอใช้	ควรต้องมีการปรับปรุงการควบคุมเพื่อให้มีความรัดกุมทางกายภาพและสภาพแวดล้อมมากยิ่งขึ้น ตามรายงานผลการตรวจสอบความมั่นคงด้านสารสนเทศและการสื่อสาร (Computer Audits) ISO/IEC 27001:2018 ปีงบประมาณ 2566
8	โดเมนที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)	ดี	
9	โดเมนที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)	ดี	
10	โดเมนที่ 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)	ดี	
11	โดเมนที่ 11 ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)	พอใช้	ควรต้องมีการปรับปรุงการควบคุมเพื่อให้มีความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอกรัดกุมมากยิ่งขึ้น ตามรายงานผลการตรวจสอบความมั่นคงด้านสารสนเทศและการสื่อสาร (Computer Audits) ISO/IEC 27001:2018 ปีงบประมาณ 2566

ลำดับ	หัวข้อการตรวจสอบ	ระดับการมีประสิทธิผล	รายละเอียดการควบคุม
12	โดเมนที่ 12 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)	ดี	
13	โดเมนที่ 13 ประเด็นด้านความมั่นคงปลอดภัยของสารสนเทศของการบริหารจัดการเพื่อสร้างความมั่นคงต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)	ดี	
14	โดเมนที่ 14 ความสอดคล้อง (Compliance)	พอใช้	ควรต้องมีการปรับปรุงการควบคุมเพื่อให้มีความรัดกุมด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความมั่นคงต่อเนื่องทางธุรกิจให้มากขึ้น ตามรายงานผลการตรวจสอบความมั่นคงด้านสารสนเทศและการสื่อสาร (Computer Audits) ISO/IEC 27001:2018 ปีงบประมาณ 2566

บทที่ 3
การสื่อสาร ถ่ายทอด กระบวนการตรวจสอบ การบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

ส่วนสารสนเทศฯ ถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ

1) ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการวิเคราะห์และจัดทำการกำกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้ผู้อำนวยการพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

2) ข้อมูลข่าวสาร (Message)

ข้อมูลข่าวสาร ได้แก่ กระบวนการวิเคราะห์และจัดทำการกำกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management) ที่ผ่านการพิจารณาจากผู้อำนวยการ โดยได้รับการรับรองความถูกต้องเป็นที่เรียบร้อยแล้ว

3) ช่องทางการสื่อสาร (Channel)

ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้ สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารระบบอินทราเน็ต และจดหมายอิเล็กทรอนิกส์

พร้อมมีการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับกระบวนการวิเคราะห์และจัดทำกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management System (ISMS) Audit) โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management System (ISMS) Audit) ที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเพื่อเป็นแนวทางปรับปรุงให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องจำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ

1. วัตถุประสงค์

1) เพื่อให้ผู้เกี่ยวข้องและผู้มีส่วนได้เสีย ทั้งภายในและภายนอกองค์กร ยึดถือเป็นกรอบแนวทางปฏิบัติอย่างสอดคล้องกัน

2) เพื่อให้นโยบายการบริหารความมั่นคงปลอดภัยของสารสนเทศทุกข้อกำหนด ถูกนำไปใช้ในทุกภาคส่วนอย่างมีระบบ

3) เพื่อให้การบริหารความมั่นคงปลอดภัยของสารสนเทศ มีประสิทธิภาพสูงสุด
4) เพื่อรักษามาตรฐานการบริหารความมั่นคงปลอดภัยของสารสนเทศ ตามกรอบ ISO27001:2018

2. ช่องทางการสื่อสาร

ส่วนสารสนเทศฯ ถ่ายทอดกระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ การกำกับตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) โดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ

1) ผู้ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการวิเคราะห์และจัดทำการกำกับตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้ผู้อำนวยการพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

2) ข้อมูลข่าวสาร (Message)

ข้อมูลข่าวสาร ได้แก่ กระบวนการวิเคราะห์และจัดทำการกำกับตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) ที่ผ่านการพิจารณาจากผู้อำนวยการ โดยได้รับการรับรองความถูกต้องเป็นที่เรีย

3) ช่องทางการสื่อสาร (Channel)

ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้ สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารระบบอินทราเน็ต และจดหมายอิเล็กทรอนิกส์

พร้อมมีการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) ของโรงงานไพ่ฯ โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ จัดทำตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) ที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่ง ในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) ให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องจำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ

และเพื่อให้สอดคล้องกับการดำเนินการด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร การใช้โซเชียลมีเดีย เช่น เฟซบุ๊ก จึงเป็นอีกหนึ่งช่องทางที่สามารถเผยแพร่ข่าวสารในเรื่องดังกล่าวนี้ได้ โดยเลือกเฉพาะข้อมูลที่มีสาระสำคัญต้องการสื่อสารในเชิงสร้างภาพลักษณ์ให้กับโรงงานไพ่ กรมสรรพสามิต

3. การถ่ายทอดกระบวนการและการวิเคราะห์การดำเนินการด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของสารสนเทศ

การถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ มีกระบวนการดำเนินงานดังนี้

3.1 กำหนดวัตถุประสงค์ของการถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

1) เพื่อสร้างการรับรู้ในกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ

2) เพื่อสร้างความเข้าใจในกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

3) เพื่อนำข้อมูลที่ได้รับ (Feedback) จากผู้มีส่วนได้ส่วนเสียต่าง ๆ มาปรับปรุงและพัฒนากระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรให้มีประสิทธิภาพมากยิ่งขึ้น

3.2 วิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

1) กำหนดมีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders) ที่เกี่ยวข้องกับกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

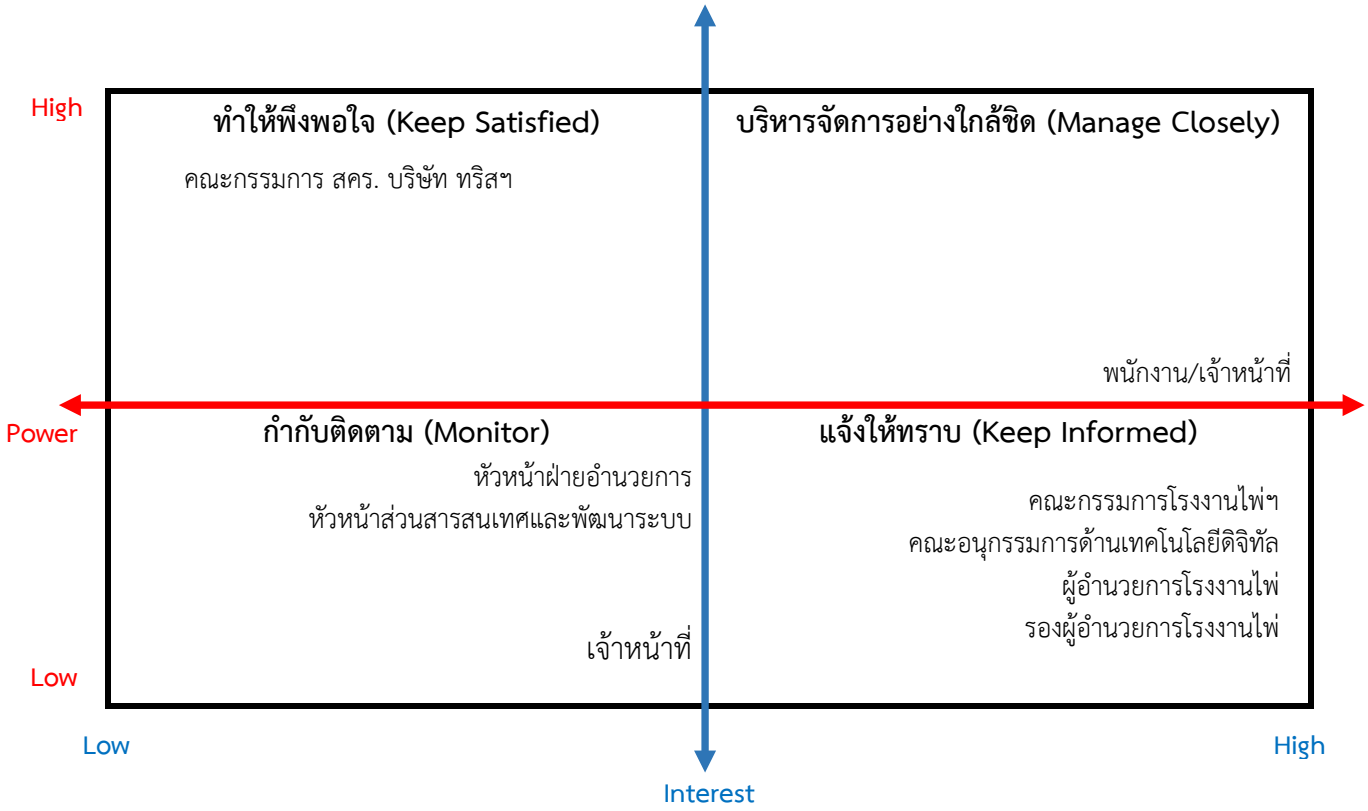
ผู้มีส่วนได้ส่วนเสียที่สำคัญต่อกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ประกอบด้วย คณะกรรมการ คณะทำงาน ผู้บริหารและเจ้าหน้าที่ ซึ่งในแต่ละกลุ่มนั้นมีบทบาทหน้าที่ที่ส่งผลกระทบต่อกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ที่เหมือนและแตกต่างกันออกไป โดยสามารถสรุปได้ ดังนี้

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
1. คณะกรรมการโรงงานไพ่ กรมสรรพสามิต	● กำกับดูแล (Governance) การดำเนินการด้านการแนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร
2. คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	● กำกับดูแล (Governance) การดำเนินการด้านแนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร
3. ผู้อำนวยการโรงงานไพ่ฯ	● พิจารณาเห็นชอบแนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรเพื่อสนับสนุนการดำเนินงานด้านสารสนเทศ ● กำกับดูแล (Governance) การดำเนินการด้านการแนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ● การดำเนินการด้านการบังคับใช้แนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
	● กำหนดและถ่ายทอดนโยบายการประยุกต์ใช้แนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร
4. รองผู้อำนวยการโรงงานไพ่ฯ	● กำกับดูแล (Governance) การดำเนินการด้านการแนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ● การดำเนินการด้านการบังคับใช้แนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ● กำหนดและถ่ายทอดนโยบายการประยุกต์ใช้แนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร
5. หัวหน้าฝ่าย/ส่วนงานต่าง ๆ	● บริหารจัดการการดำเนินงานในส่วนงานที่รับผิดชอบให้มีความสอดคล้องกับนโยบายองค์กรของโรงงานไพ่ฯ ที่กำหนด ● ให้ความคิดเห็น ข้อเสนอแนะ และข้อวิพากษ์ต่าง ๆ ที่เกี่ยวข้องกับสถาปัตยกรรมองค์กร เพื่อนำไปปรับปรุงกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ● สื่อสารและถ่ายทอดข้อมูลข่าวสารต่าง ๆ ที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรไปยังพนักงานในฝ่าย/ส่วน
6. พนักงาน/เจ้าหน้าที่	● ดำเนินงานตามนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ ● ให้ความคิดเห็น ข้อเสนอแนะ และข้อวิพากษ์ต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อนำไปปรับปรุงกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

3.3 กำหนดเครื่องมือในการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่สำคัญ

โรงงานไพ่ฯ ได้กำหนดตำแหน่งของผู้มีส่วนได้ส่วนเสียที่สำคัญกับกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ในรูปแบบของตารางเส้น (Grid) ได้แบ่งออกเป็น แกน X หมายถึง ผู้ที่มีอำนาจ (Power) และแกน Y หมายถึง ผู้ที่ได้รับผลประโยชน์ (Interest) จำแนกออกเป็น 4 กลุ่ม ได้แก่ กลุ่มที่ควรทำให้พึงพอใจ กลุ่มที่ควรบริหารจัดการอย่างใกล้ชิด กลุ่มที่ต้องกำกับติดตาม และกลุ่มที่ต้องแจ้งข้อมูลข่าวสารให้ทราบ โดยสามารถสรุปได้ ดังนี้



ภาพตำแหน่งของผู้มีส่วนได้ส่วนเสียที่สำคัญ จำแนกตามกลุ่มต่าง ๆ

3.4 กำหนดบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญ

โรงงานไพ่ฯ ได้กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ในรูปแบบตาราง RACI (RACI Matrix) โดยในแต่ละกระบวนการผู้มีส่วนได้ส่วนเสียหลักจะมีบทบาทหน้าที่ที่เหมือน และแตกต่างกันออกไป ประกอบด้วย ผู้รับผิดชอบงาน (A) ผู้ที่ทำงานนั้น ๆ (R) ผู้ที่มีหน้าที่ให้คำปรึกษา (C) และผู้ที่โรงงานไพ่ฯ จะต้องแจ้งข้อมูลข่าวสารที่เกี่ยวข้องกับการดำเนินงานให้ทราบเป็นระยะ ๆ (I) โดยสามารถสรุปได้ ดังนี้

ตารางบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญกับกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ

การจัดทำกระบวนตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร	R = Responsible A = Accountable C = Consulted I = Informed						
กิจกรรม	**คณะกรรมการโรงงานไพ่**	**คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล**	**ผู้อำนวยการโรงงานไพ่**	**รองผู้อำนวยการโรงงานไพ่**	**หัวหน้าฝ่ายอำนวยการ**	**หัวหน้าส่วน/เจ้าหน้าที่สารสนเทศและพัฒนาระบบ**	**พนักงาน**
กำหนดเป้าหมายการจัดทำกระบวนการฯ	I	I	C	I	R	A	I
ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง	I	I	C	I	R	A	I
สำรวจปัญหา อุปสรรค และความต้องการ	I	I	C	I	R	A	R
วิเคราะห์ข้อมูล	I	I	C	I	R	A	I
ออกแบบกระบวนการ	I	I	C	I	R	A	I
กำหนดแนวทางการใช้แนวปฏิบัติฯ	I	I	C	I	R	A	I
วิเคราะห์ผู้มีส่วนได้ส่วนเสีย	I	I	C	I	R	A	I
ถ่ายทอดกระบวนการวิเคราะห์และจัดทำ	I	I	C	I	I	A	I
กำกับดูแลแนวปฏิบัติฯ	I	I	C	I	R	A	I
บริหารจัดการแนวปฏิบัติฯ	I	I	C	I	R	A	I

3.5 จัดทำกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ

กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ใช้วิธีการวิเคราะห์กระบวนการทำงานด้วยแบบจำลอง SIPOC หรือ “SIPOC Model” ประกอบด้วยองค์ประกอบต่าง ๆ ได้แก่ ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier) ปัจจัยนำเข้า (Input) กระบวนการ (Processes) ผลผลิต (Outputs) และผู้ที่นำผลผลิตไปใช้งาน (Customers) ซึ่งสามารถแสดงให้เห็นโดยภาพรวม ดังนี้

ชื่อกระบวนการ : กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ	**วันที่จัดทำ/ปรับปรุงกระบวนการ :** 3 กรกฎาคม 2566
ผู้รับผิดชอบ : ส่วนสารสนเทศและพัฒนาระบบ	**จัดทำครั้งที่ :** 2

ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	ปัจจัยนำเข้า (Input)	กระบวนการ (Process)	ผลผลิต (Outputs)	ผู้ที่นำผลผลิตไปใช้งาน (Customers)
S1: หัวหน้าส่วนสารสนเทศฯ	I1: งบประมาณในการดำเนินงาน I2: บุคลากร ประกอบด้วย ● ผู้อำนวยการ ● รองผู้อำนวยการ ● หัวหน้าฝ่ายอำนวยการ ● หัวหน้าส่วนสารสนเทศฯ ● เจ้าหน้าที่สารสนเทศ I3: เทคโนโลยี ได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ของระบบคอมพิวเตอร์ I4: วัสดุอุปกรณ์ ได้แก่ เครื่องใช้สำนักงาน I5: เครื่องมือที่ใช้ในการวิเคราะห์ ได้แก่ ● แผนภูมิก้างปลา ● SWOT Analysis ● TOWS Matrix ● Gap Analysis	**P1: กำหนดแนวปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** ↓ **P2: ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง** ↓ **P3: สำรวจปัญหา อุปสรรค ความต้องการ** ↓ **P4: วิเคราะห์ข้อมูล** ↓ **P5: จัดทำแนวโยบายและแนวปฏิบัติ** ↓ **P6: ประกาศใช้** ↓	แนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร	C1: ภายในองค์กร ● ฝ่ายอำนวยการ ● ฝ่ายโรงพิมพ์ ● ฝ่ายผลิตไพ่

ชื่อกระบวนการ : กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ	**วันที่จัดทำ/ปรับปรุงกระบวนการ :** 3 กรกฎาคม 2566
ผู้รับผิดชอบ : ส่วนสารสนเทศและพัฒนาระบบ	**จัดทำครั้งที่ :** 2

ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	ปัจจัยนำเข้า (Input)	กระบวนการ (Process)	ผลผลิต (Outputs)	ผู้ที่นำผลผลิตไปใช้งาน (Customers)
		P7: ติดตามผลการดำเนินงาน		
S2: เจ้าหน้าที่สารสนเทศ				C2: ภายในองค์กร ● ผู้ติดต่อ ● บริษัท
S6: คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล				

3.6 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการกำหนดกระบวนการ และแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

เป็นกระบวนการกำหนดเป้าหมาย หรือสิ่งที่โรงงานไพ่ฯ ต้องการจะเป็นในอนาคต ซึ่งได้แก่ การเป็นผู้นำด้านสิ่งพิมพ์ปลอดการปลอมแปลง และดิจิทัลปริ้นติ้งโซลูชั่นภาครัฐ ทั้งนี้ ในการจะบรรลุวัตถุประสงค์และเป้าหมายดังที่กำหนดได้นั้น แนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ตามมาตรฐาน ISO:IEC/27001 : 2018 จึงมีบทบาทสำคัญอย่างยิ่งในการช่วยสนับสนุนการดำเนินงานในด้านต่าง ๆ ขององค์กร ให้มีมาตรฐานการดำเนินงานที่น่าเชื่อถือ ปลอดภัย โดยจะสังเหตุเห็นได้ว่า ISO:IEC/27001 : 2018 เป็นเรื่องที่ว่าด้วยมาตรฐานความมั่นคงปลอดภัย ของสารสนเทศทั้งหมด ทั้งในส่วนของข้อมูล การปฏิบัติที่มีมาตรฐานมีการควบคุมภายในที่ดี สอดรับวิสัยทัศน์และพันธกิจของโรงงานไพ่ ที่จะมุ่งสู่การเป็นผู้นำด้านสิ่งพิมพ์ปลอดการปลอมและการดำเนินงานทางด้านโซลูชั่น และสอดคล้องตาม พรบ. ไซเบอร์ และ พรบ. คุ้มครองข้อมูลส่วนบุคคล ดังนั้น ตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ตามมาตรฐาน ISO:IEC/27001 : 2018 จึงมีความสัมพันธ์อย่างยิ่งกับเป้าหมายขององค์กรในอนาคต ดังนั้นผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการนี้ จึงประกอบด้วยทั้งบุคลากรภายในตั้งแต่ระดับการบริหาร ถึงระดับปฏิบัติงาน และผู้เกี่ยวข้องที่มีการใช้บริการติดต่อสื่อสาร กับโรงงานไพ่ เพื่อช่วยกันให้ข้อเสนอแนะ ข้อสังเกต และช่วยกันกำหนดเป้าหมาย และทิศทางการดำเนินงานขององค์กรในอนาคต เพื่อที่จะสามารถออกตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ตามมาตรฐาน ISO:IEC/27001 : 2018 ที่มีความสอดคล้องกับเป้าหมายตามที่กำหนดได้ หรืออาจกล่าวได้ว่าหากเป้าหมายหรือวิสัยทัศน์ขององค์กรเปลี่ยน ก็จะส่งผลต่อตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่ต้องปรับเปลี่ยนไปเพื่อรองรับเป้าหมายใหม่ตามที่กำหนด ดังนั้น ตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรจึงได้ถูกกำหนดให้มีการทบทวนเป็นประจำทุกปี

3.7 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการศึกษาทบทวนเอกสารที่เกี่ยวข้อง

การศึกษาทบทวนเอกสารที่เกี่ยวข้องจะแบ่งออกเป็น 2 ส่วน ได้แก่ เอกสารสำคัญที่เกี่ยวข้องกับการดำเนินงานของโรงงานไพ่ฯ ประกอบด้วย

1) วิสัยทัศน์ ยุทธศาสตร์ พันธกิจ และเป้าหมายขององค์กร

2) แนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่มีความเหมาะสมกับบริบทของโรงงานไพ่ ในกระบวนการนี้เนื่องจากการกำหนดวิสัยทัศน์ ยุทธศาสตร์ พันธกิจ และเป้าหมายขององค์กร ได้ผ่านการพิจารณาในกระบวนการกำหนดเป้าหมายในอนาคตขององค์กรแล้ว การกำหนดตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่มีความเหมาะสมกับบริบทของโรงงานไพ่ฯ จึงเป็นหน้าที่ของผู้เชี่ยวชาญที่จะต้องทำการศึกษาตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่เป็นมาตรฐานสากล โดยการวิเคราะห์เชิงเปรียบเทียบ พิจารณาถึงข้อดี – ข้อจำกัดขององค์ประกอบต่างๆ เพื่อคัดเลือก และกำหนดตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่มีความเหมาะสมกับโรงงานไพ่ฯ โดยในการกำหนดผู้เชี่ยวชาญนั้น จะต้องกำหนดผู้เชี่ยวชาญที่เกี่ยวข้องและครอบคลุมการดำเนินงานในด้านต่าง ๆ ขององค์กร ไม่เพียงแต่เฉพาะด้านเทคโนโลยีดิจิทัลเท่านั้น แต่จะต้องครอบคลุมการดำเนินงานในด้านต่าง ๆ ขององค์กรด้วย เพื่อให้การศึกษา วิเคราะห์ และออกแบบตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสามารถช่วยสนับสนุนการดำเนินงานในด้านต่าง ๆ ขององค์ได้อย่างเหมาะสม

3.8 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการสำรวจข้อมูล

การสำรวจข้อมูลเป็นการเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการดำเนินงานขององค์กรได้เข้ามามีส่วนร่วมในการแสดงความคิดเห็น ให้ข้อเสนอแนะ และวิพากษ์กในประเด็นที่เกี่ยวข้องกับการดำเนินงานขององค์กรที่ผ่านมา ในกระบวนการนี้จึงทำให้ทราบถึงบริบทการดำเนินงานของโรงงานไพ่ฯ ในปัจจุบัน ช่วยสะท้อนให้เห็นถึงปัญหา อุปสรรค และข้อจำกัดต่าง ๆ ทั้งด้านเทคโนโลยีดิจิทัล และการดำเนินงานขององค์กร ซึ่งจะมีผลต่อตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่เหมาะสมกับโรงงานไพ่ฯ ทั้งนี้เพราะในการกำหนดแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่มีความเหมาะสมกับโรงงานไพ่ฯ นั้น ไม่เพียงแต่จะพิจารณาเฉพาะกรอบตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร องค์กรที่เป็นมาตรฐานเท่านั้น แต่จะต้องพิจารณาบริบทการดำเนินงานขององค์กรในปัจจุบันร่วมด้วย เพื่อให้ได้รับแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่เป็นมาตรฐานและสามารถประยุกต์ใช้กับการดำเนินงานได้อย่างเหมาะสม ดังนั้น ในกระบวนการนี้นอกจากจะมีผู้มีผู้เชี่ยวชาญเข้ามาร่วมดำเนินการแล้ว ยังมีบุคลการของโรงงานไพ่ฯ ที่เป็นผู้รับผิดชอบในส่วนงานต่าง ๆ ซึ่งเป็นผู้ที่มีความรู้ความเข้าใจในส่วนงานที่ตนเป็นผู้รับผิดชอบเป็นอย่างดี โดยใช้วิธีการสัมภาษณ์เชิงลึก หรือการประชุมกลุ่มย่อย

3.9 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลจะประกอบไปด้วยการนำข้อมูลมาเปรียบเทียบกับแม่แบบของแนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตราฐานสากล ISO:IEC 27001:2018 พร้อมนำผลการดำเนินงานที่ผ่านมาร่วมกันวิเคราะห์ข้อมูลเพื่อหา ช่องว่าง (Gap) ต้องปรับปรุงแก้ไขเพื่อให้บรรลุเป้าหมายขององค์กรได้ในอนาคต จนนำไปสู่การสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัย ให้กับองค์กร คู่ค้า บุคคล หรือองค์กรภายนอกอื่นๆ และสร้างความยั่งยืนในการพัฒนาองค์กรให้สำเร็จตามวิสัยทัศน์ และกลยุทธ์ ขององค์กร

3.10 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการจัดทำแนวโยบายและแนวปฏิบัติ

แนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร มีการจัดทำตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO:IEC/27001:2018 ซึ่งมาตราฐานดังกล่าวจะมีแม่แบบในการดำเนินงานแต่ละขั้นตอนที่ชัดเจน ทั้งสิ้น 14 Domain โดยสามารถกำหนดเป็นกรอบนโยบายการบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร (IT Management) ดังนี้

1) นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)
3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)
4) การจัดหมวดหมู่และควบคุมทรัพย์สินองค์กร (Asset Management)
5) การควบคุมการเข้าถึง (Access Control)
6) การเข้ารหัสข้อมูล (Cryptography)
7) ความมั่นคงทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)
8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)
9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
10) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

11) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

13) ตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรเพื่อสร้างความต่อเนื่องขององค์กร (Information security aspects of business continuity management)

14) ความสอดคล้อง (Compliance)

นอกจากนั้นแล้ว ยังต้องพิจารณาถึงหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสากิจ ตามระบบประเมินผลรัฐวิสาหกิจ (SE-AM) หัวข้อการพัฒนาเทคโนโลยีดิจิทัล ประเด็นด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ได้กำหนดหลักเกณฑ์การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ในด้านต่าง ๆ ทั้งในด้านของแนวทาง กระบวนการ การถ่ายทอดกระบวนการ การกำหนดตัววัด ติดตาม วิเคราะห์ และประเมินตัววัดผลลัพธ์ รวมทั้งการนำผลลัพธ์ที่ได้เข้าสู่กระบวนการการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ดังนั้น ในกระบวนการนี้จึงมีความเกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียต่าง ๆ หลายส่วน โดยเฉพาะอย่างยิ่ง ผู้เชี่ยวชาญด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่ต้องเป็นผู้รับผิดชอบหลักในการกำหนดรูปแบบ และออกแบบตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรในอนาคตที่มีความเหมาะสมกับโรงงานไพ่ฯ

3.11 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการกำหนดแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรองค์กรอย่างเป็นรูปธรรม

กระบวนการกำหนดกรอบแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างเป็นรูปธรรม เป็นกระบวนการกำหนดตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ไปปรับใช้กับการดำเนินงานในด้านต่าง ๆ เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องดำเนินงานภายใต้ตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่กำหนดขึ้น โดยมีการกำหนดแนวทางที่ชัดเจน ภายใต้หลักการกำกับดูแลด้านดิจิทัล (Digital Governance) ประกอบด้วยแนวทางต่าง ๆ ได้แก่ กำหนดผู้รับผิดชอบในตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ประกาศนโยบาย กำหนดเป้าหมายในการดำเนินงาน และตัวชี้วัดผลการดำเนินงานตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร กำหนดความสอดคล้องในการดำเนินงาน และสื่อสารให้ผู้มีส่วนได้ส่วนเสียในองค์กรได้รับทราบ ในกระบวนการนี้ผู้ที่ได้เข้ามามีบทบาทสำคัญ นอกจากนั้นแล้ว โรงงานไพ่ฯ ยังได้เปิดโอกาสให้ผู้บริหาร และพนักงานทุกคนในองค์กรได้เข้ามามีส่วนร่วมกับกระบวนการกำหนดแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างเป็นรูปธรรม ผ่านช่องทางการสื่อสารต่าง ๆ ได้แก่ ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ เว็บไซต์ของโรงงานไพ่ฯ ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ จดหมายอิเล็กทรอนิกส์ และแอพลิเคชั่นไลน์ (LINE) ทั้งนี้เพราะสถาปัตยกรรมองค์กรของโรงงานไพ่ฯ จะต้องถูกนำไปใช้กับทุกคนในองค์กร ดังนั้นจึงได้เปิดโอกาสให้ทุกคนในองค์กรได้เข้ามามีส่วนร่วมในการกำหนดแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรเพื่อให้มีความเหมาะสมกับบริบทการดำเนินงานของบุคลากรในโรงงานไพ่ฯ

3.12 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

การถ่ายทอดแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีวัตถุประสงค์เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรได้เข้ามามีส่วนร่วมในการพิจารณาให้ข้อเสนอแนะ วิพากษ์ และร่วมแสดง

ความคิดเห็น เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับมาปรับปรุงและพัฒนากระบวนการฯ ให้มีประสิทธิภาพมากยิ่งขึ้นต่อไป จนเกิดการพัฒนาที่มีแนวทางการปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) โดยโรงงานไพ่ฯ ได้กำหนดให้มีการทบทวนปรับปรุงกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรเป็นประจำทุกปี ทั้งนี้ ผู้มีส่วนได้ส่วนเสียที่มีความเกี่ยวข้องกับกระบวนการนี้ จะประกอบด้วย ผู้อำนวยการโรงงานไพ่ฯ และผู้แทนในระดับหัวหน้าฝ่ายและหัวหน้าส่วนงานต่าง ๆ ของโรงงานไพ่ฯ ได้แก่ ฝ่ายอำนวยการ ฝ่ายโรงพิมพ์ ฝ่ายผลิตไพ่ ฝ่ายตรวจสอบภายใน ส่วนพัฒนาธุรกิจและการตลาด รวมทั้งส่วนสารสนเทศและพัฒนาระบบ จึงทำให้ได้รับมุมมองที่มีความหลากหลายครอบคลุมในมิติต่าง ๆ ในการดำเนินงานขององค์กร ผ่านช่องทางการสื่อสาร คือ การประชุมแบบเผชิญหน้า (Face to Face) หรือการประชุมออนไลน์ผ่านระบบการประชุมทางไกล (Video Conference)

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
1. กำหนดเป้าหมาย	1.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1.1.1 ผู้อำนวยการโรงงานไพ่ฯ 1.1.2 รองผู้อำนวยการโรงงานไพ่ฯ หัวหน้าฝ่ายอำนวยการ 1.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 1.2.2 เจ้าหน้าที่สารสนเทศฯ	ตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ (Information Security Management)	ส่วนสารสนเทศและพัฒนาระบบ
2. ศึกษาทบทวนเอกสารที่เกี่ยวข้อง	2.1 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 2.1.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2.1.2 เจ้าหน้าที่สารสนเทศ	ข้อมูลพื้นฐานที่สามารถนำมาช่วยในการออกแบบกระบวนตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศของสารสนเทศที่เหมาะสมกับโรงงานไพ่ฯ ประกอบด้วย ● แนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ	ส่วนสารสนเทศและพัฒนาระบบ
3. สำรวจปัญหา อุปสรรค และความต้องการ	3.1 หัวหน้าฝ่ายงาน และส่วนงานต่าง ๆ หรือผู้แทนในแต่ละฝ่ายงาน ผู้ใช้ติดต่อ กับโรงงานไพ่	ผลการสำรวจข้อมูลของโรงงานไพ่ฯ ที่ทำให้ทราบถึง	ส่วนสารสนเทศและพัฒนาระบบ

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
		• ปัญหา อุปสรรค การใช้งานระบบสารสนเทศ • ความรู้ความเข้าใจเกี่ยวกับตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ	
4. วิเคราะห์ข้อมูล	4.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 4.1.1 ผู้อำนวยการโรงงานไพ่ฯ 4.1.2 รองผู้อำนวยการโรงงานไพ่ฯ 4.1.3 หัวหน้าฝ่ายอำนวยการ 4.1.4 หัวหน้าฝ่ายโรงพิมพ์ 4.1.5 .หัวหน้าส่วนแผนงานและกลยุทธ์ 4.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 4.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 4.2.2 เจ้าหน้าที่สารสนเทศ	ข้อเสนอแนะ คำแนะนำ และแนวทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ
5. จัดทำแนวโยบายและแนวปฏิบัติฯ	5.1 การจัดทำแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วย 5.1.1 หัวหน้าฝ่าย / หัวหน้าส่วน	ร่างแนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
	5.1.2 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 5.1.3 เจ้าหน้าที่สารสนเทศ		
6. พิจารณาแนวนโยบายและแนวปฏิบัติฯ	6.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 6.1.1 ผู้อำนวยการโรงงานไพ่ฯ 6.1.2 รองผู้อำนวยการโรงงานไพ่ฯ 6.1.3 หัวหน้าฝ่ายอำนวยการ 6.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 6.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 6.2.2 เจ้าหน้าที่สารสนเทศฯ	แนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ	ผู้บริหารและพนักงานของโรงงานไพ่ฯ ทุกคน
7. ประกาศใช้แนวนโยบายและแนวปฏิบัติฯ	7.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 7.1.1 ผู้อำนวยการโรงงานไพ่ 7.1.2 รองผู้อำนวยการโรงงานไพ่ 7.1.3 หัวหน้าฝ่ายอำนวยการ	แนวนโยบายและแนวปฏิบัติด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ	ผู้บริหารและพนักงานของโรงงานไพ่ฯ ทุกคน
8. ติดตามผลการดำเนินงาน	8.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 8.1.1 ผู้อำนวยการโรงงานไพ่ 8.1.2 รองผู้อำนวยการโรงงานไพ่ 8.1.3 หัวหน้าฝ่ายอำนวยการ 8.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย	ผลการประเมิน ความคิดเห็น และข้อเสนอแนะต่าง ๆ	ส่วนสารสนเทศและพัฒนาระบบนำข้อมูลที่ได้มาปรับปรุงกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรสารสนเทศ

กระบวนการวิเคราะห์และจัดทำกระบวนการ	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
	8.2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 8.2.2 เจ้าหน้าที่สารสนเทศฯ		

4. ถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

โรงงานไพ่ฯ ได้กำหนดวิธีการถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ ทั้งนี้ โรงงานไพ่ฯ ได้ประยุกต์ใช้แบบจำลองการสื่อสารดังกล่าว สำหรับการถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ดังนี้

4.1 ผู้ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล และคณะทำงานกำกับดูแลและการบริหารจัดการสถาปัตยกรรมองค์กรพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

4.2 ข้อมูลข่าวสาร (Message)

ข้อมูลข่าวสาร ได้แก่ กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่ผ่านการพิจารณาจากคณะอนุกรรมการฯ และคณะทำงานฯ โดยได้รับการรับรองความถูกต้องเป็นที่เรียบร้อยแล้ว

4.3 ช่องทางการสื่อสาร (Channel)

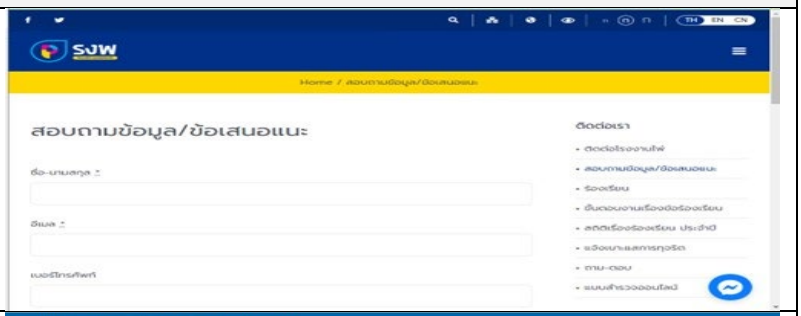
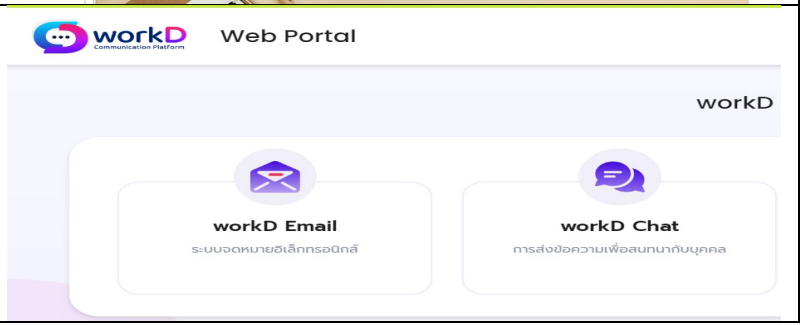
ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้

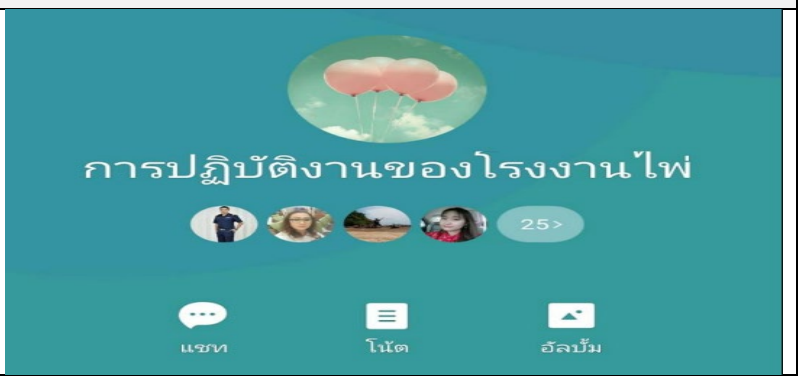
1) สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการ และหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารผ่านที่ประชุมคณะอนุกรรมการด้านเทคโนโลยีดิจิทัล

ตำแหน่ง	ภาพประกอบ
หน้าทางเข้าโรงงานไพ่ฯ	
ห้องสันทนาการ	

ตำแหน่ง	ภาพประกอบ
หน้าห้องส่วนบริหารงานกลาง	

2) สื่อสมัยใหม่ ประกอบด้วย เว็บไซต์ของโรงงานไพ่ฯ ได้แก่(https://www.playingcard.or.th/) ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)และแอพลิเคชั่นไลน์ (LINE) โดยในช่องทางดังกล่าว ได้เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถให้ความคิดเห็น และข้อเสนอแนะต่าง ๆ ที่เกี่ยวข้องกับกระบวนการวิเคราะห์และการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อมที่สามารถเข้าถึงได้จากอุปกรณ์การอิเล็กทรอนิกส์ต่าง ๆ ทั้งสมาร์ทโฟน และคอมพิวเตอร์ เพื่อที่จะสามารถนำข้อมูลต่าง ๆ เหล่านั้นมาปรับปรุงและพัฒนากระบวนการฯ ให้มีประสิทธิภาพมากขึ้นต่อไป

สื่อที่ใช้	ภาพประกอบ
เว็บไซต์ของโรงงานไพ่ฯ (https://www.playingcard.or.th/)	
ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ	
ระบบการสื่อสารแบบรวมศูนย์ (workD Platform) -workD Mail ระบบจดหมายอิเล็กทรอนิกส์ (saraban@playingcard.mail.go.th) -workD Chat การส่งข้อความเพื่อสนทนา	

สื่อที่ใช้	ภาพประกอบ
แอพลิเคชั่นไลน์ (LINE)	

4.4 ผู้รับสาร (Receiver)

ผู้รับสาร หรือผู้ที่มีความเกี่ยวข้องกับข้อมูลข่าวสารในกระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ได้แก่ บุคลากรของโรงงานไพ่ฯ ทั้งในระดับผู้บริหาร พนักงาน และผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้อง

5. ประเมินการรับรู้จากผู้ที่เกี่ยวข้องกับตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

ในขั้นตอนนี้เป็นกระบวนการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และการดำเนินการด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่ง ในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการวิเคราะห์และการดำเนินการด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ ให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องกับกระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร จำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ ได้ดังนี้

วิธีการประเมินการรับรู้

กระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
1. กำหนดเป้าหมาย	1.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ 1.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	ผู้บริหารในระดับต่างๆ ได้เข้ามามีส่วนร่วมกับการกำหนดเป้าหมายของกระบวนตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของสารสนเทศผ่านการประชุม	● รายงานการประชุม
2. ศึกษาทบทวนเอกสารที่เกี่ยวข้อง	2.1 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบ และเจ้าหน้าที่สารสนเทศได้ศึกษา ทบทวนทั้งปัจจัยภายนอก และปัจจัยภายในเพื่อพิจารณาทบทวนเอกสารต่าง ๆ ที่เกี่ยวข้อง	● ผลการศึกษาทบทวนเอกสารที่เกี่ยวข้อง
3. สำรวจปัญหา อุปสรรค และความต้องการ	3.1 หัวหน้าฝ่าย/ส่วนงานต่าง ๆ หรือผู้แทนในแต่ละฝ่ายงาน	นัดสัมภาษณ์เชิงลึกกับหัวหน้าฝ่าย/ส่วนงานต่าง ๆ	● รายงานสรุปผลการสำรวจข้อมูล ● แบบสัมภาษณ์
4. วิเคราะห์ข้อมูล	4.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ	● ทำหนังสือเวียนถึงผู้บริหาร เพื่อพิจารณาผลการวิเคราะห์ข้อมูล	● รายงานผลการวิเคราะห์ข้อมูล ● เอกสารสรุปรายงานประชุม

กระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
	4) หัวหน้าฝ่ายโรงพิมพ์ 5) หัวหน้าส่วนแผนงานและกลยุทธ์ 4.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศ		● หนังสือเวียน
5. จัดทำแนวโยบายและแนวปฏิบัติฯ	5.1 การจัดทำแผนการดำเนินการด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรขององค์กร ประกอบด้วย 1) หัวหน้าฝ่าย/ส่วนงานต่าง ๆ ของโรงงานไพ่ฯ 2) หัวหน้าส่วนสารสนเทศ 3) เจ้าหน้าที่ส่วนสารสนเทศ	ผู้มีส่วนเกี่ยวข้องร่วมกันเพื่อพิจารณาออกแบบกระบวนตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของสารสนเทศของโรงงานไพ่ฯ	● กระบวนตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของสารสนเทศของโรงงานไพ่ฯ ● เอกสารสรุปรายงานประชุม
6. พิจารณาแนวนโยบายและแนวปฏิบัติฯ	6.1 ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1) ผู้อำนวยการโรงงานไพ่ฯ 2) รองผู้อำนวยการโรงงานไพ่ฯ 3) หัวหน้าฝ่ายอำนวยการ 6.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	ทำบันทึกข้อความถึงผู้อำนวยการ เพื่อพิจารณาเห็นชอบผลการทบทวนตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management)	● ตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) ● บันทึกข้อความ

กระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
7. ประกาศใช้แนวนโยบายและแนวปฏิบัติฯ	7.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 1) ผู้อำนวยการโรงงานไพ่ 2) รองผู้อำนวยการโรงงานไพ่ 3) หัวหน้าฝ่ายอำนวยการ 7.2 หัวหน้าฝ่าย/ส่วนต่างๆ 7.3 พนักงานโรงงานไพ่ 7.4 ผู้ติดต่อประสานงานกับโรงงานไพ่	● นำกระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรเข้าสู่ที่ประชุมคณะอนุกรรมการด้านเทคโนโลยีดิจิทัลเพื่อพิจารณา ● ใช้แบบสอบถามประเมินการรับรู้ด้านกระบวนการวิเคราะห์และการดำเนินการด้านตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของโรงงานไพ่ฯ	● หนังสือเวียน ● ตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management)
8. ติดตามผลการดำเนินงาน	8.1 ผู้บริหารโรงงานไพ่ฯ ประกอบไปด้วย 1) ผู้อำนวยการโรงงานไพ่ 2) รองผู้อำนวยการโรงงานไพ่ 3) หัวหน้าฝ่ายอำนวยการ 8.2 ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 1) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2) เจ้าหน้าที่สารสนเทศฯ	● ติดตามผลการประเมินจาก ตัวชี้วัดการดำเนินกิจกรรม โครงการต่างๆ ทางด้านเทคโนโลยีดิจิทัล ว่าสอดคล้อง เป็นไปตามแผนทางการบริหารจัดการใช้ทรัพยากรอย่างเหมาะสมหรือไม่	● การดำเนินกิจกรรมโครงการต่าง ๆ ทางด้านเทคโนโลยีดิจิทัลสอดคล้อง เป็นไปตามแผนทางตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร สารสนเทศขององค์กร

สรุปโรงงานไพ่ฯ ได้กำหนดวิธีการประเมินผลการรับรู้กระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรด้วยรูปแบบที่แตกต่างกัน จำแนกตามผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการต่าง ๆ ซึ่งได้ผ่านการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการมาเป็นที่เรียบร้อยแล้ว ทั้งนี้เพราะผู้มีส่วนได้ส่วนเสียต่าง ๆ เหล่านั้น ล้วนเป็นส่วนหนึ่งของการจัดทำ พัฒนา และยกระดับกระบวนตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรของสารสนเทศของโรงงานไพ่ฯ ให้ดียิ่งขึ้น ดังนั้น การจัดทำสถาปัตยกรรมองค์ในครั้งนี้ จึงเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้เข้ามามีส่วนร่วมในการแสดงความคิดเห็น และให้ข้อเสนอแนะสำหรับการปรับปรุงกระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ซึ่งสอดคล้องกับหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยโรงงานไพ่ฯ ได้กำหนดให้การประเมินการรับรู้ดำเนินการควบคู่กับการจัดทำกระบวนการวิเคราะห์และตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรเป็นประจำทุกปี เพื่อให้กระบวนการมีแนวทางปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice)

หมายเหตุ : บันทึกข้อความที่ 180/2566 วันที่ 4 กรกฎาคม 2566

บทที่ 4
การวัดผล และประเมินผล การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

1. วัตถุประสงค์

1) เพื่อให้การบริหารความมั่นคงปลอดภัยของสารสนเทศได้รับการดูแล และติดตาม อย่างต่อเนื่อง

2) เพื่อวางแผนทบทวน ผลการดำเนินการบริหารความมั่นคงปลอดภัยของสารสนเทศ และหาแนวทางปรับปรุงพัฒนาให้มีประสิทธิภาพ

3) เพื่อวิเคราะห์และปรับปรุงพัฒนา ให้การบริหารความมั่นคงปลอดภัยของสารสนเทศ คงอยู่ตามกรอบมาตรฐาน ISO27001:2018

2. ขั้นตอนการวัดผล ติดตาม และประเมินผล

1) นำผลการประเมินที่ได้รับจากการตรวจสอบในแต่ละรอบมาวิเคราะห์

2) ปรับปรุงตามแนวทางที่ได้รับรายงานจากผลประเมิน ตามกรอบระยะเวลาที่กำหนดไว้

3) ทีมตรวจสอบติดตามผลผลความคืบหน้าในรอบก่อนประเมินถัดไป

3. เกณฑ์การประเมิน

จากหัวข้อตรวจสอบที่ถูกกำหนดขึ้นร่วมกันจากคณะกรรมการและผู้เกี่ยวข้องในแต่ละวาระภายใต้กรอบนโยบายการบริหารความมั่นคงปลอดภัยของสารสนเทศโดยระดับความมีประสิทธิผลในภาพรวมของแต่ละหัวข้อการควบคุม แบ่งออกเป็น 3 ระดับ ได้แก่ “ดี” “พอใช้” และ “ควรปรับปรุง” ตามนิยาม ดังต่อไปนี้

ระดับความมีประสิทธิผล	นิยาม
ดี	มีการกำหนดให้มีการควบคุมอย่างเพียงพอ และมีการปฏิบัติตามการควบคุมที่กำหนดไว้
พอใช้	มีการกำหนดให้มีการควบคุม และมีการปฏิบัติตามการควบคุมที่กำหนดไว้ อย่างไรก็ตามการควบคุมที่กำหนดไว้ยังคงสามารถปรับปรุงเพิ่มเติมให้มีคุณภาพที่ดียิ่งขึ้นได้อีก
ควรปรับปรุง	การกำหนดให้มีการควบคุมยังไม่เพียงพอ หรือยังไม่มีการปฏิบัติตามการควบคุมที่กำหนดไว้อย่างเพียงพอ

บทที่ 5
การทบทวน ปรับปรุง กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

1. แผนระดับองค์กร

มีการทบทวน ปรับปรุง และวางแผน เป็นประจำทุก 1 ปี โดยนำคะแนนผลการตรวจสอบทั้งจากผู้ตรวจสอบภายในและภายนอก มาวิเคราะห์และทบทวน ร่วมกับผลการประเมินผ่านการเฝ้าติดตามจากผู้ดูแลระบบสารสนเทศ และดำเนินการศึกษาทบทวนเอกสารที่เกี่ยวข้อง ตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ อันได้แก่

- ปัจจัยภายนอก

- แผนยุทธศาสตร์ชาติ, แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัล, แผนการพัฒนาเทคโนโลยีดิจิทัล กระทรวงการคลัง , แผนปฏิบัติการดิจิทัล กรมสรรพสามิต , พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์, พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล, พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์, พระราชบัญญัติลิขสิทธิ์, พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกฎหมายอื่นๆที่เกี่ยวข้อง

- เทรน แนวโน้ม ทางด้านเทคโนโลยีดิจิทัล ISO/IEC 27001:2018 และปัจจัยอื่นๆ ที่เกี่ยวข้อง

- ปัจจัยภายใน

- แผนวิสาหกิจ แผนการบริหารนวัตกรรม แผนด้านการตลาด แผนยุทธศาสตร์องค์กร , แผนบริหารทรัพยากรบุคคล แผนอื่นๆที่เกี่ยวข้อง และ ระเบียบ นโยบาย ที่เกี่ยวข้อง

- แบบสัมภาษณ์ และแบบสำรวจผู้บริหาร และพนักงาน

2. แผนระดับส่วนงานสารสนเทศและพัฒนาระบบ

มีการทบทวน ปรับปรุง อย่างต่อเนื่องเป็นรายไตรมาศ โดยนำคะแนนผลการตรวจสอบทั้งจากผู้ตรวจสอบภายในและภายนอก มาวิเคราะห์และทบทวน ร่วมกับผลการประเมินผ่านการเฝ้าติดตามจากผู้ดูแลระบบสารสนเทศ

3. แนวทางในการทบทวนเพื่อจัดทำแผนงานขององค์กรในระยะยาว

นำผลการตรวจสอบในแต่ละหมวดหมู่มาวิเคราะห์ หากเรื่องใด อยู่ในสถานะ “ควรปรับปรุง” ให้ถือเป็นเรื่องที่ควรดำเนินการจัดทำแผนปรับปรุงเป็นกรณีเร่งด่วน