การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Management)

นโยบายการบริหารจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber Security Management Policy)

เอกสารโดย

ส่วนสารสนเทศและพัฒนาระบบ
โรงงานไพ่ กรมสรรพสามิต

รหัสเอกสาร IT-DOC-NCSA-001
ปรับปรุงล่าสุด 30 กรกฎาคม 2567

บทนำ

บทนำ

ในยุคที่การเชื่อมต่อดิจิทัลและเทคโนโลยีสารสนเทศได้กลายเป็นส่วนสำคัญในทุกด้านของชีวิตประจำวัน การรักษาความมั่นคงปลอดภัยไซเบอร์จึงกลายเป็นปัจจัยที่ไม่อาจมองข้ามได้ การดำเนินการเพื่อป้องกันและรักษาความปลอดภัยของข้อมูลและระบบทางดิจิทัลเป็นสิ่งที่มีความสำคัญอย่างยิ่ง เพื่อให้สังคมและเศรษฐกิจสามารถดำเนินต่อไปได้อย่างมีประสิทธิภาพและปลอดภัย

เพื่อให้บรรลุเป้าหมายนี้ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ถูกประกาศใช้เพื่อเป็นกรอบในการบริหารจัดการและควบคุมความปลอดภัยทางไซเบอร์ในประเทศ โดยมีวัตถุประสงค์ในการปกป้องข้อมูลและระบบที่สำคัญจากภัยคุกคามต่างๆ และกำหนดบทบาทและหน้าที่ของหน่วยงานที่เกี่ยวข้องในการรับมือและจัดการกับเหตุการณ์ที่อาจเกิดขึ้น

เอกสารนี้ได้รวบรวม "นโยบายบริหารจัดการรักษาความมั่นคงปลอดภัยไซเบอร์" ที่พัฒนาขึ้นตามกรอบของพระราชบัญญัติและกฎหมายลำดับรองที่เกี่ยวข้อง โดยมีวัตถุประสงค์เพื่อสร้างแนวทางและมาตรการที่ชัดเจนในการจัดการและป้องกันภัยคุกคามในโลกไซเบอร์ เพื่อให้การปฏิบัติงานและความปลอดภัยของข้อมูลมีความเข้มแข็งและเป็นระบบ

เอกสารนี้จะเป็นแนวทางที่มีประโยชน์ในการเสริมสร้างระบบรักษาความปลอดภัยไซเบอร์ให้มีความยั่งยืนและมีประสิทธิภาพ พร้อมทั้งส่งเสริมการทำงานร่วมกันของทุกภาคส่วนในการสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยและเชื่อถือได้สำหรับประชาชนและองค์กรต่างๆ

วัตถุประสงค์

เพื่อกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

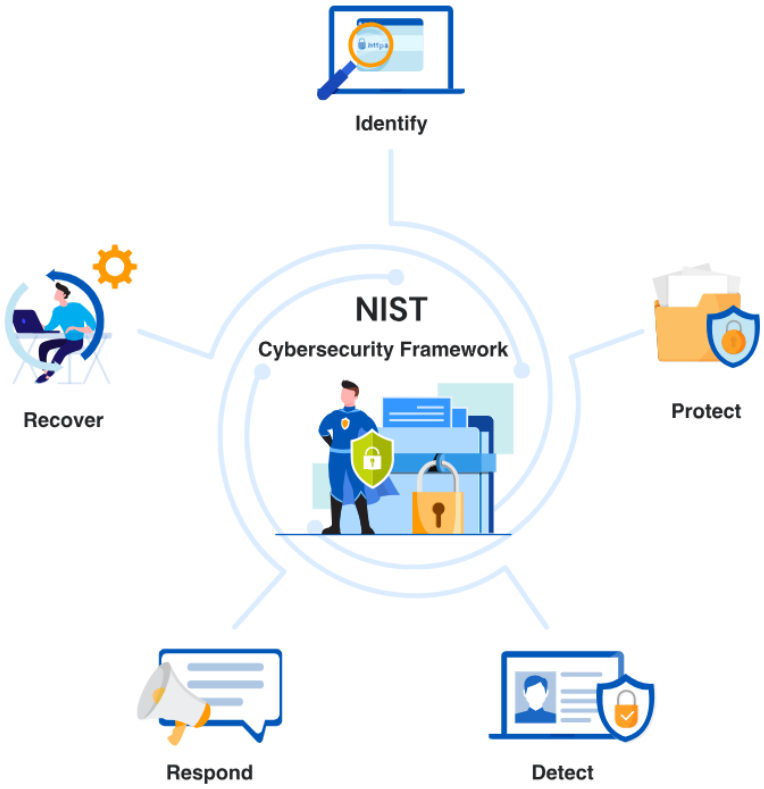
สารบัญ

สารบัญ

บทที่ 1
การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์

ในยุคดิจิทัลที่การเชื่อมต่อผ่านอินเทอร์เน็ตมีบทบาทสำคัญต่อการดำเนินธุรกิจ การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องที่ไม่สามารถมองข้ามได้ โดยเฉพาะองค์กรที่มีทรัพยากรจำกัด การมีกลยุทธ์และนโยบายที่ชัดเจนในการจัดการความเสี่ยงและการรักษาความปลอดภัยไซเบอร์จะช่วยให้องค์กรสามารถป้องกันและตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างมีประสิทธิภาพ

โรงงานไพ่ฯ ได้กำหนดทิศทางการทำงานให้มีความชัดเจนและโปร่งใสในการบริหารงาน โดยดำเนินงานตามแนวทางตามมาตรฐาน ISO/IEC 27001:2022, ISO/IEC 27701:2019 และกรอบความมั่นคงปลอดภัยด้านไซเบอร์ NIST Cyber Security Framework ที่ครอบคลุมการดำเนินงานทั้ง 5 ด้านอัน ได้แก่ การ Identify การ Protect การ Detect การ Respond และการ Recover



โดยสามารถแบ่งลำดับขั้นการบริหารได้ทั้งหมด 3 ขั้น อันประกอบด้วย (1) ระดับกำกับดูแล (2) ระดับบริหารจัดการ และ (3) ระดับปฏิบัติการ

1. บทบาทความรับผิดชอบ

ระดับ	บทบาท	คณะกรรมการ/หน่วยงาน
ระดับกำกับดูแล	กำกับ ดูแล บริหารการดำเนินงาน และกำหนดทิศทางกลยุทธ์และเป้าหมาย	คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล
ระดับบริหารจัดการ	จัดการข้อมูลสารสนเทศตามมาตรฐาน และติดตามตรวจสอบความถูกต้องและแม่นยำ	- ผู้บริหารโรงงานไพ่ - ส่วนสารสนเทศและพัฒนาระบบ - คณะทำงานบริหารจัดการความเสี่ยงและควบคุมภายใน
ระดับปฏิบัติการ	กำหนดระบบ วิธีปฏิบัติ และบริการ ให้แก่ผู้ใช้งานปฏิบัติตาม และ ประเมินการติดตามผลงานและรายงานความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงระดับองค์กร	ส่วนสารสนเทศและพัฒนาระบบ

2. การกำหนดนโยบายด้านความปลอดภัยไซเบอร์

- จัดทำนโยบายความปลอดภัยไซเบอร์ที่ชัดเจนและครอบคลุมทุกด้านของการดำเนินงาน
- นโยบายควรระบุถึงการป้องกัน การตรวจจับ การตอบสนอง และการกู้คืนจากเหตุการณ์ความปลอดภัยไซเบอร์
- ดำเนินการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) เป็นประจำอย่างน้อยปีละ 1 ครั้ง

3. การบริหารจัดการความเสี่ยงด้านความปลอดภัยไซเบอร์

โครงสร้างการบริหารความเสี่ยง

- ส่วนงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ มีหน้าที่ ประเมินความเสี่ยงและควบคุมความเสี่ยงด้านความปลอดภัยไซเบอร์
- ส่วนงานที่ทำหน้าที่ด้านความปลอดภัย ต้องจัดให้มีแนวทางการควบคุม ติดตาม และรายงานการปฏิบัติงาน รวมทั้งติดตาม จัดทำรายงาน เฝ้าระวังภัยคุกคาม และศึกษาแนวโน้มภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นและส่งผลกระทบต่อโรงงานไพ่ และนำเสนอรายงานต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้อง
- ส่วนงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งครอบคลุมถึงความเสี่ยงด้านไซเบอร์ มีหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จัดให้มีการประเมินความเสี่ยงตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยงและทบทวนการควบคุม ความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงาน และขององค์กรในภาพรวมให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ และนำเสนอผลการประเมินและการบริหารความเสี่ยงองค์กรต่อคณะทำงานที่ทำหน้าที่กำกับดูแลความเสี่ยง
- หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมการตรวจสอบด้านการรับมือกับภัยคุกคามทางไซเบอร์ มีหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงของหน่วยงาน รวมถึงงานอื่นๆ ที่เกี่ยวข้อง เช่น การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ เป็นต้น เพื่อสอบทานให้มั่นใจว่ามีการปฏิบัติที่เป็นไปตามนโยบายมาตรฐาน และระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ

4. การจัดการความเสี่ยง

- มีกระบวนการบริหารจัดการความเสี่ยงด้านไซเบอร์ที่ครอบคลุม ดังนี้
    - การประเมินความเสี่ยง (Risk Assessment) โดยครอบคลุม การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินค่าความเสี่ยง (Risk Evaluation)
    - การปิดและการจัดการความเสี่ยง (Risk Treatment)
    - การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)
    - การรายงานความเสี่ยง (Risk Reporting)
- การประเมินความเสี่ยงด้านไซเบอร์ครอบคลุมผลกระทบที่อาจเกิดขึ้นในด้านอื่น ๆ ด้วย เช่นผลกระทบต่อกลยุทธ์ การดำเนินธุรกิจหรือต่อชื่อเสียง เป็นต้น

5. การใช้เทคโนโลยีและเครื่องมือที่เหมาะสม

- เลือกใช้เทคโนโลยีและเครื่องมือที่เหมาะสมในการป้องกันความเสี่ยง เช่น โปรแกรมป้องกันไวรัส ระบบตรวจจับการบุกรุก (IPS) และไฟร์วอลล์ (Nextgen firewall)
- อัปเดตระบบและซอฟต์แวร์อย่างสม่ำเสมอเพื่อป้องกันการถูกโจมตีจากช่องโหว่
- ตรวจสอบและบำรุงรักษาอุปกรณ์และระบบอย่างสม่ำเสมอ

6. การตรวจสอบ

ขอบเขตการตรวจสอบ

- ขอบเขตการตรวจสอบครอบคลุมนโยบาย มาตรฐาน ระเบียบวิธีปฏิบัติ และการควบคุมการปฏิบัติงานสำคัญที่เกี่ยวข้องกับความเสี่ยงด้านไซเบอร์ ซึ่งรวมถึงความเสี่ยงด้านไซเบอร์จากการออกผลิตภัณฑ์ใหม่ การใช้ระบบและเทคโนโลยีใหม่
- มีการตรวจสอบการประเมินการรักษาความมั่นคงปลอดภัยการจัดเก็บและรับส่งข้อมูลที่มีความสำคัญขององค์กร
- มีการตรวจสอบการประเมินความเพียงพอของการบริหารจัดการและการควบคุมความเสี่ยงด้านไซเบอร์กับระดับความเสี่ยงด้านไซเบอร์ขององค์กร
- มีการตรวจสอบการประเมินการรับมือและความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่องต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cybersecurity Incident) เพื่อให้มั่นใจว่ามีการเตรียมการที่สอดคล้องกับระดับความเสี่ยงด้านไซเบอร์ขององค์กร

กระบวนการตรวจสอบ

- มีทบทวนและปรับปรุงกระบวนการตรวจสอบ โดยคำนึงถึงการเปลี่ยนแปลงระดับความเสี่ยงด้านไซเบอร์ขององค์กร

การบริหารจัดการบุคลากรและการฝึกอบรม

- มีการกำหนดบทบาทหน้าที่และความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ชัดเจน
- มีการอบรมและพัฒนาทักษะความรู้ความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเสริมสร้างศักยภาพ ให้บุคลากรที่รับผิดชอบงานด้านนี้อย่างเพียงพอและต่อเนื่อง

- จัดฝึกอบรมและให้ความรู้แก่พนักงานเกี่ยวกับความปลอดภัยไซเบอร์เป็นประจำอย่างน้อยปีละ 1 ครั้ง
- ส่งเสริมการตระหนักรู้เกี่ยวกับภัยคุกคามและการปฏิบัติที่ปลอดภัย เช่น การจัดการรหัสผ่าน การระวัง Phishing

บทสรุป การรักษาความมั่นคงปลอดภัยไซเบอร์อาจเป็นเรื่องที่ท้าทาย แต่ด้วยการกำกับดูแลที่ดีและการปฏิบัติตามแนวทางที่ถูกต้อง องค์กรจะสามารถป้องกันและตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ การสร้างวัฒนธรรมการตระหนักรู้ การบริหารจัดการความเสี่ยง การใช้เทคโนโลยีที่เหมาะสม การจัดการข้อมูลอย่างปลอดภัย และการตรวจสอบและประเมินผลอย่างสม่ำเสมอ จะเป็นกุญแจสำคัญในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ขององค์กร

บทที่ 2
การบริหารความเสี่ยง

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

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 เพื่อให้มั่นใจว่ามีการดำเนินการที่เหมาะสมในการจัดการความเสี่ยงของโรงงานไพ่โดยรวมและสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้และมีระบบการควบคุมภายในที่เพียงพอ

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
- รายงานผลการบริหารจัดการความเสี่ยงและการควบคุมภายในระดับองค์กรเป็นรายไตรมาสต่อคณะกรรมการโรงงานไพ่ และคณะกรรมการตรวจสอบ
- เชิญผู้บริหารหรือเจ้าหน้าที่ และบุคคลภายนอกเพื่อเข้าร่วมประชุมหรือให้ข้อมูลในเรื่องที่เกี่ยวข้อง

- มีอำนาจเป็นไปตามกฎบัตรคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในโรงงานไพ่

4) คณะทำงานบริหารจัดการความเสี่ยงและควบคุมภายใน โรงงานไพ่
บทบาทหน้าที่และความรับผิดชอบเกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ดังนี้

- จัดทำร่างนโยบายความเสี่ยงและควบคุมภายใน และร่างกรอบการบริหารความเสี่ยง
- และควบคุมภายใน เสนอคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในโรงงานไพ่ เพื่อพิจารณาอนุมัติ
- ประสานงานกับผู้เกี่ยวข้องเพื่อรวบรวมข้อมูลในการจัดทำแผนบริหารจัดการความเสี่ยงและแผนการควบคุมภายใน
- จัดทำแผนปฏิบัติการ และแผนอื่น ๆ สำหรับการบริหารจัดการความเสี่ยงและการควบคุมภายใน
- รวบรวมข้อมูลหลักฐานและสรุปผลการดำเนินงานของการบริหารจัดการความเสี่ยงและ
- การควบคุมภายใน
- พัฒนา/ทบทวนกระบวนการบริหารความเสี่ยงและควบคุมภายใน ของหน่วยงาน
- อย่างสม่ำเสมอ
- ติดตาม แนะนำ และให้คำปรึกษาการปฏิบัติงานตามกระบวนการบริหารความเสี่ยงและควบคุมภายใน เพื่อลดผลกระทบและป้องกันความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- ทบทวนประเมินผลรายงานผลการดำเนินงานมาตรการหรือแผนปฏิบัติการ เพื่อกำหนด แนวทางการปรับปรุงระบบบริหารความเสี่ยงของโรงงานไพ่
- ดำเนินการประชาสัมพันธ์ต่อผู้มีส่วนได้ส่วนเสียกรณีที่มีเหตุการณ์วิกฤติ ซึ่งมีผลกระทบที่จะสร้างความเสียหาย รั่วไหล หรือสูญเปล่า อันจะทำให้การบริหารงานของโรงงานไพ่
- ไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้
- สื่อสาร/ทำความเข้าใจให้พนักงานรับทราบและทำความเข้าใจกับการบริหารความเสี่ยงและควบคุมภายใน
- รวบรวมกลั่นกรองข้อมูลจากแหล่งข้อมูลต่าง ๆ จัดทำเป็นฐานข้อมูลเพื่อการตัดสินใจ
- อย่างมีประสิทธิภาพ ตามลำดับความสำคัญของการบริหารความเสี่ยงและควบคุมภายใน
- รายงานผลการดำเนินงานของการบริหารจัดการความเสี่ยงและการควบคุมภายใน
- ต่อคณะอนุกรรมการบริหารความเสี่ยงฯ เป็นประจำทุกเดือน
- รายงานผลการดำเนินงานของการบริหารจัดการความเสี่ยงและการควบคุมภายใน
- ต่อคณะกรรมการโรงงานไพ่ คณะกรรมการตรวจสอบ คณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน (รายไตรมาส)
- ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

5) ผู้อำนวยการโรงงานไพ่
มีบทบาทหน้าที่และความรับผิดชอบเกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ดังนี้

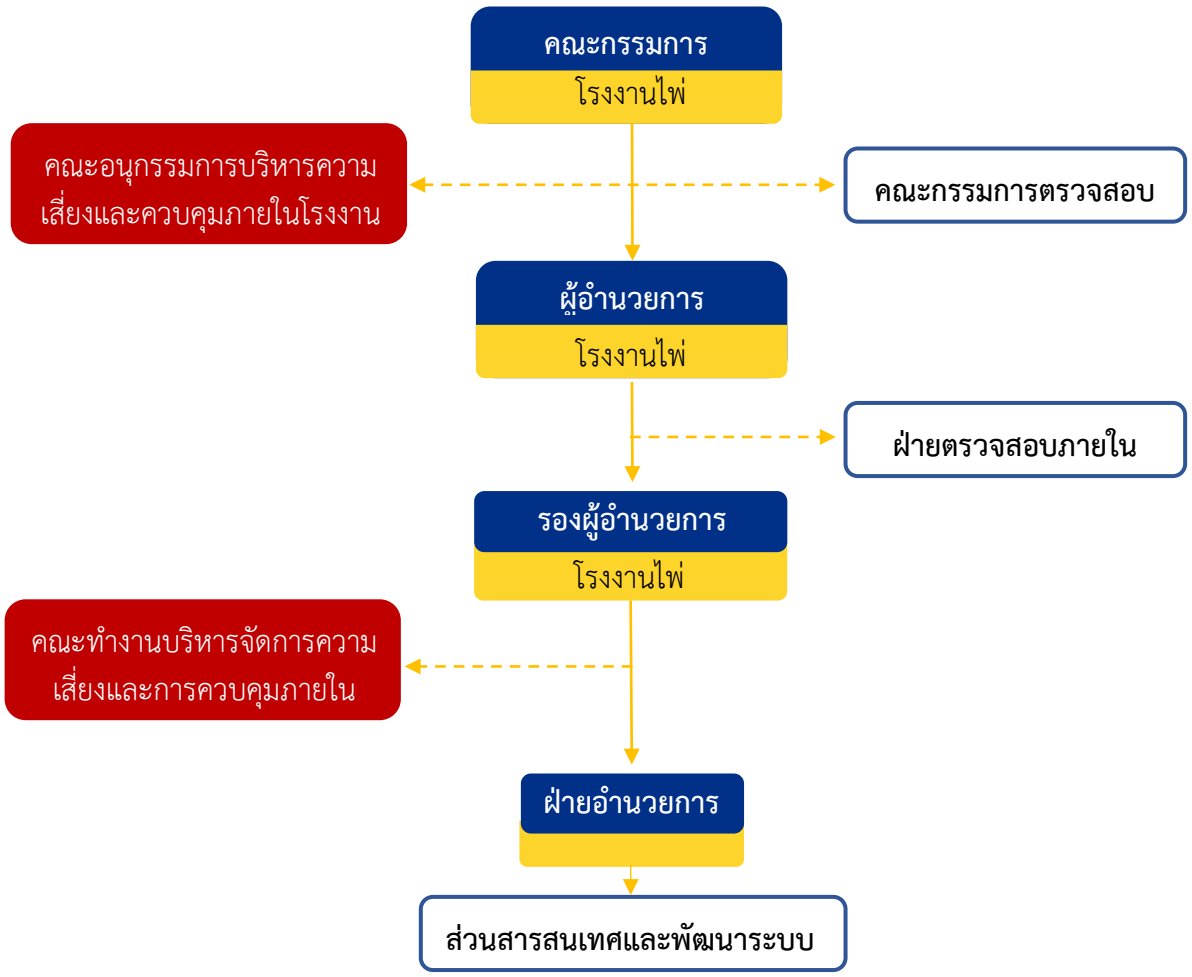
- การวางแผนและดำเนินการตามนโยบาย และแผนงานการบริหารความเสี่ยงร่วมกับคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน โรงงานไพ่

- สั่งการและติดตามให้ทุกหน่วยงานปฏิบัติงานตามกระบวนการบริหารความเสี่ยง
- แต่งตั้งเจ้าหน้าที่หรือผู้รับผิดชอบ เพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผล
- สนับสนุนและส่งเสริมให้การบริหารความเสี่ยงเป็นการปฏิบัติงานตามปกติและ
- เป็นวัฒนธรรมของหน่วยงาน
- อื่น ๆ ตามหน้าที่ที่ได้รับมอบหมายจากคณะกรรมการโรงงานไพ่

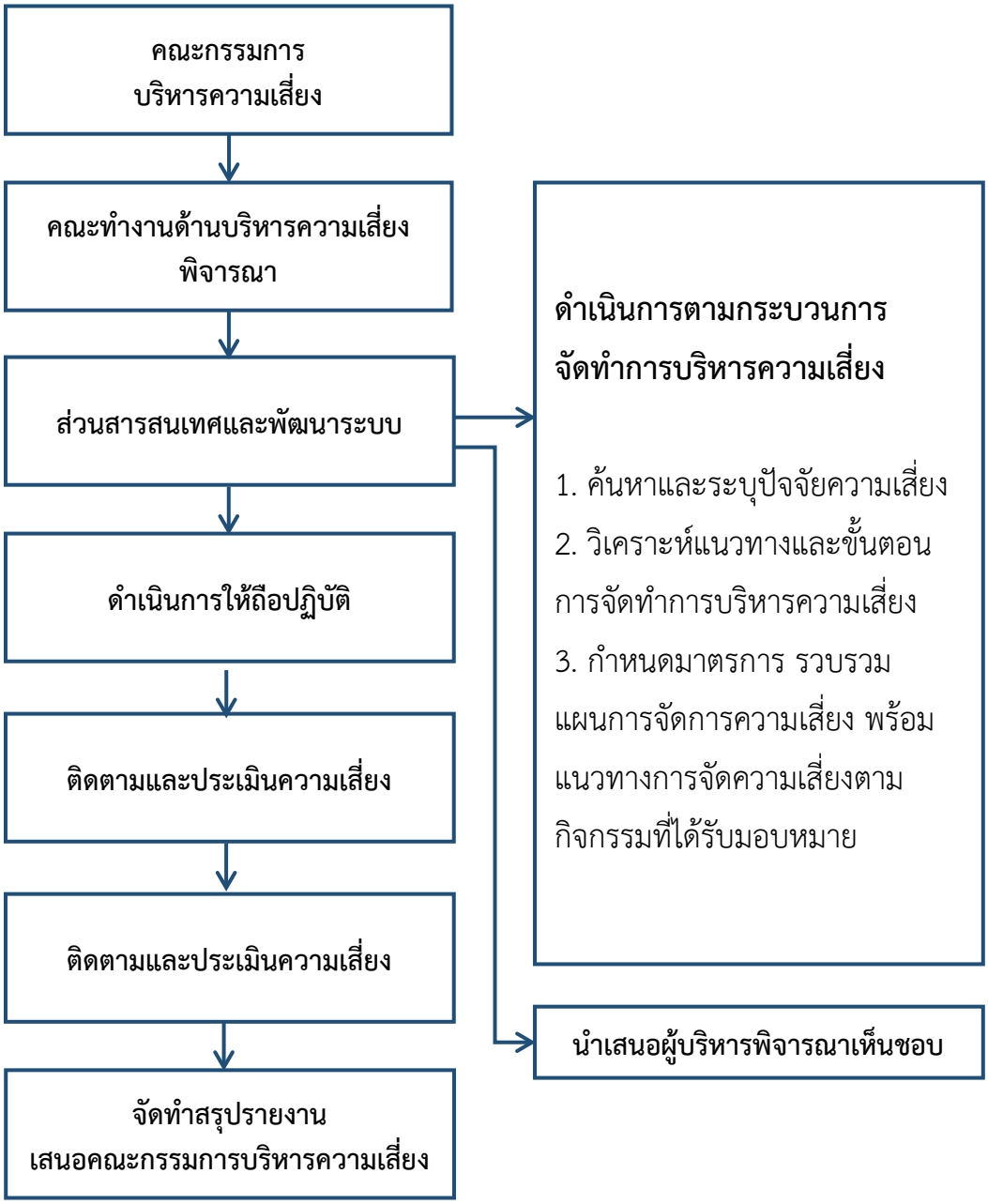
6) ส่วนสารสนเทศและพัฒนาระบบ
มีบทบาทหน้าที่และความรับผิดชอบเกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ดังนี้

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

โครงสร้างองค์กรการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์



ขั้นตอนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ



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 การจัดลำดับความเสี่ยงโดย

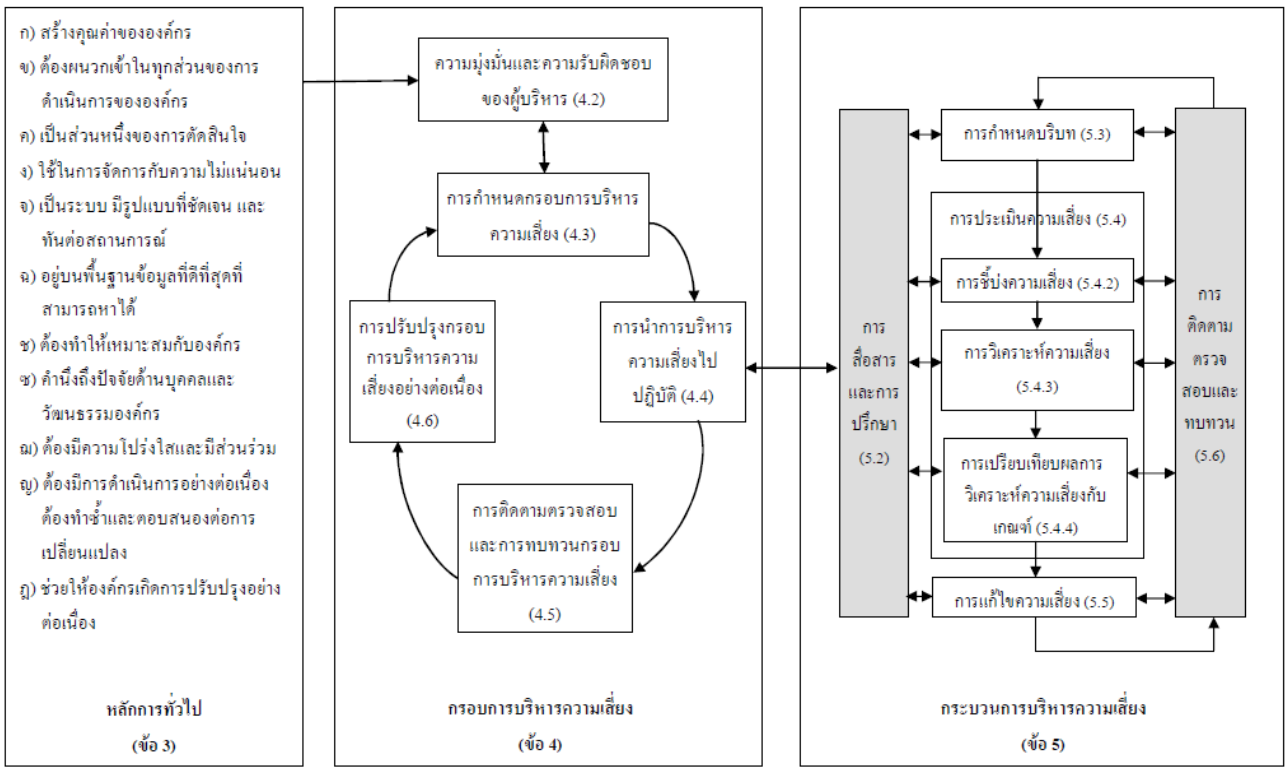
จะประเมินจากโอกาสที่จะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) หรือขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดความเสี่ยงนั้น ๆ

จากนิยามและความหมายของการบริหารความเสี่ยง รวมถึงกรอบแนวทางในการบริหารจัดการความเสี่ยงข้างต้น ทางโรงงานไพ่ฯ จะใช้เป็นแนวทางในการกำหนดกระบวนการและองค์ประกอบเพิ่มเติมต่างๆ ของกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยจะกล่าวถึง ในบทถัดไป

ตารางการบริหารจัดการความเสี่ยง (Risk Management Framework)

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

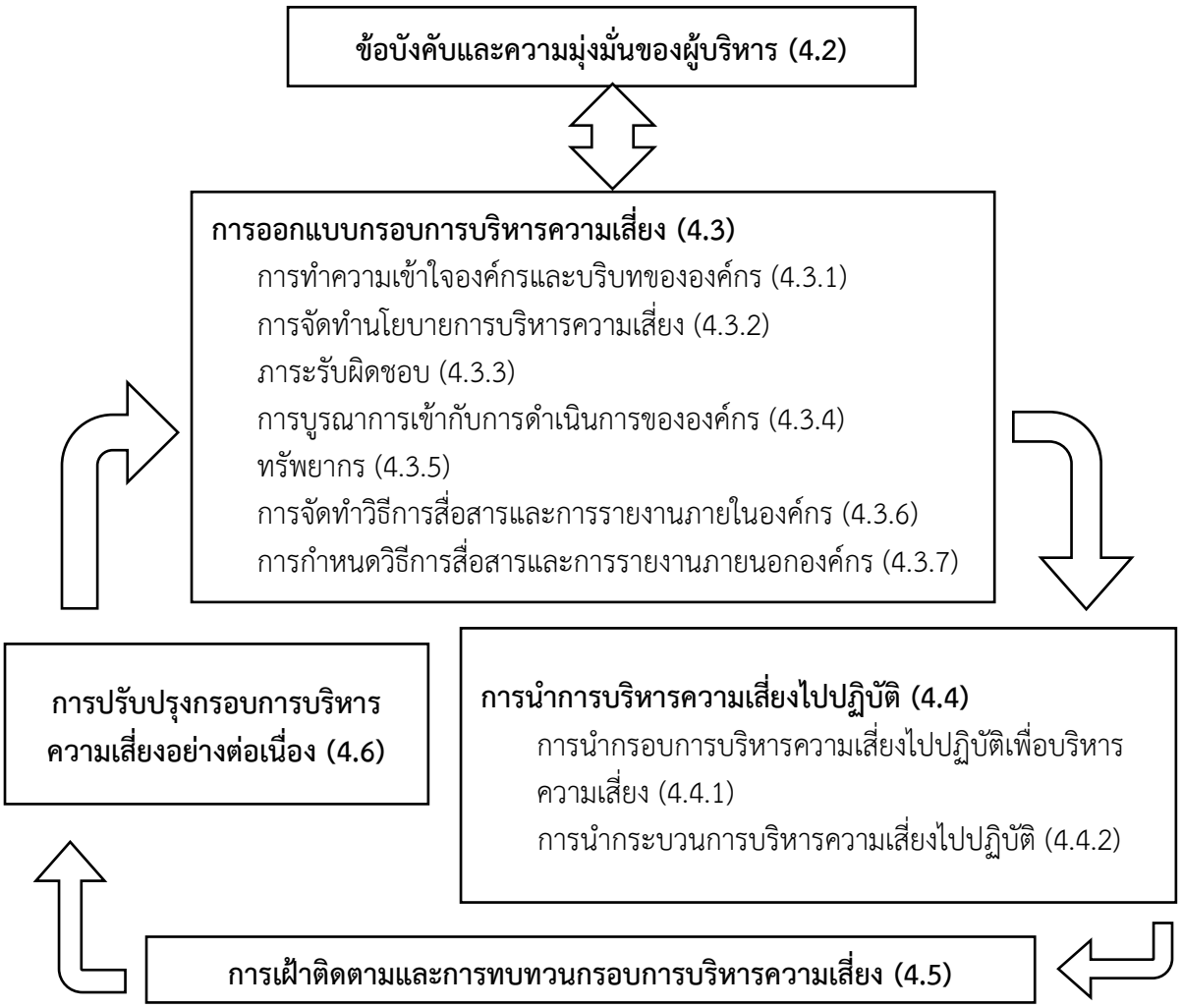
2.3) การติดตามตรวจสอบและการทบทวนกรอบการบริหารความเสี่ยง

2.4) การปรับปรุงกรอบการบริหารความเสี่ยงอย่างต่อเนื่อง

3) กระบวนการบริหารความเสี่ยง ประกอบด้วย

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

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

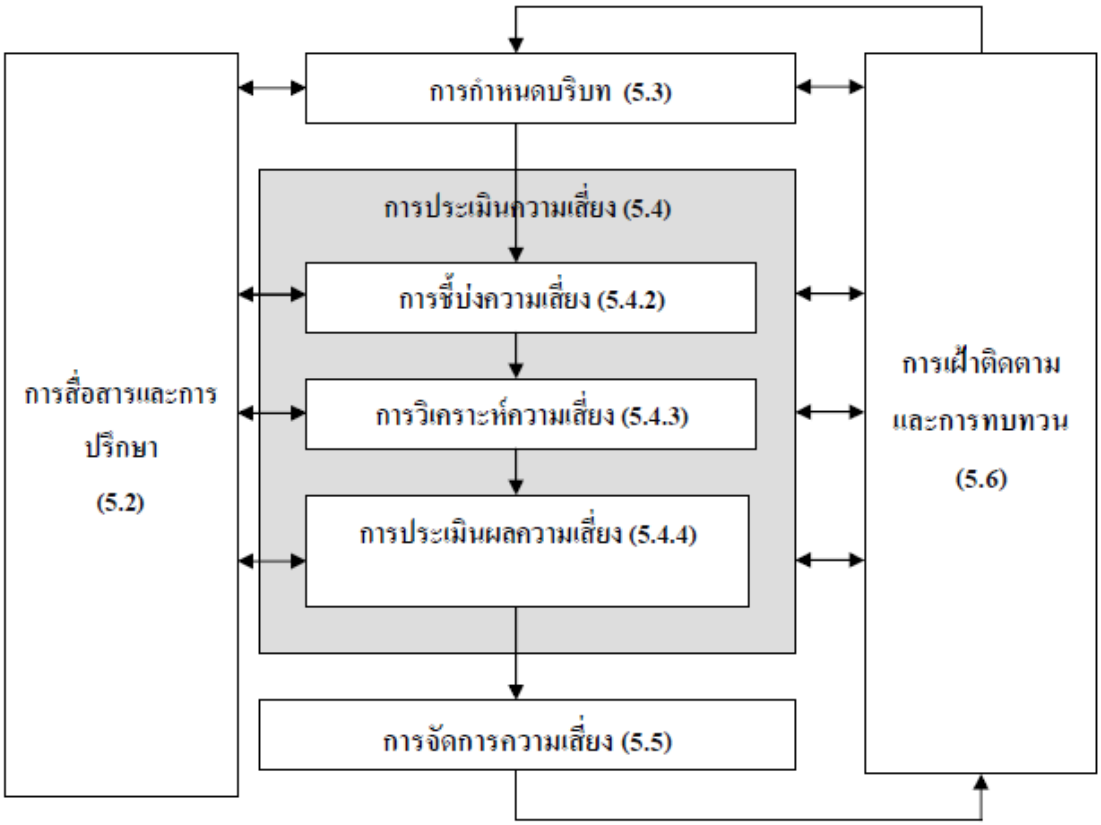
- ทบทวนถึงความมีประสิทธิผลของกระบวนการบริหารความเสี่ยง

การปรับปรุงกรอบการบริหารความเสี่ยงอย่างต่อเนื่อง

เมื่อองค์กรได้มีการเฝ้าติดตามและทบทวนกรอบการบริหารความเสี่ยงแล้ว ผลของการทบทวนจะนำไปสู่การตัดสินใจในการปรับปรุงกรอบการบริหารความเสี่ยง นโยบาย และแผนการบริหารความเสี่ยง และวัฒนธรรมการบริหารงานขององค์กร รวมถึงช่วยปรับปรุงความคล่องตัว การควบคุม และความรับผิดชอบที่มีต่อเป้าหมายขององค์กรด้วย

กระบวนการบริหารความเสี่ยง (Process)

สำหรับกระบวนการบริหารความเสี่ยงตามมาตรฐาน ISO31000:2009 ที่ทุกหน่วยงานยึดถือเป็นหลักในการดำเนินการ และถือเป็นส่วนหนึ่งของการบริหาร โดยมีกิจกรรมต่างๆ ซึ่งแสดงขั้นตอนดังรูป



การสื่อสารและการปรึกษา

เป็นกิจกรรมที่ควรมีอยู่ในทุกขั้นตอนของกระบวนการบริหารความเสี่ยง เป็นการชี้แจง บอกกล่าวให้กับผู้ที่มีส่วนเกี่ยวข้องทั้งภายใน และภายนอกองค์กร และยังให้คำปรึกษา ถึงประเด็นต่างๆ ที่เกี่ยวข้อง ขั้นตอน ขอบเขตการดำเนินงาน 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

บทที่ 3
นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

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 บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือและอุปกรณ์ต่าง ๆ

- 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)

วัตถุประสงค์

เพื่อปกป้องข้อมูลสำคัญขององค์กรและลดความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นจากการใช้สื่อบันทึกข้อมูลภายนอก

ขอบเขต

นโยบายนี้ครอบคลุมผู้ใช้งานด้านเทคโนโลยีสารสนเทศฯ ที่มีการใช้สื่อบันทึกข้อมูลภายนอกกับระบบขององค์กร

นิยาม

สื่อบันทึกข้อมูลภายนอก อุปกรณ์ที่มีพื้นที่การจัดเก็บข้อมูลในรูปแบบอ่านเดียว และทั้งเขียนและอ่านข้อมูลได้

นโยบาย

1. การกำหนดแนวทางการจำกัดการใช้สื่อบันทึกข้อมูลภายนอก
2. การกำหนดผู้รับผิดชอบ
   - แต่งตั้งผู้รับผิดชอบควบคุมการใช้อุปกรณ์ที่ได้รับอนุญาตในแต่ละหน่วยงาน
3. การตรวจสอบความปลอดภัย
   - กำหนดวิธีการตรวจสอบความปลอดภัย

แนวปฏิบัติ

1. จำกัดการใช้งานสื่อบันทึกข้อมูลภายนอกกับผู้ใช้งานระบบสารสนเทศฯ เว้นแต่มีความจำเป็นในการใช้งานสื่อบันทึกข้อมูลภายนอก โดยมีข้อพิจารณาการอนุญาตตามความจำเป็นดังต่อไปนี้

ข้อกำหนด	การอนุญาต	การดำเนินการ
1. การใช้งานที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์แม่ข่าย/ระบบ IoT (Internet of Thing)/เครื่องจักรทุกประเภท/อุปกรณ์ด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยระดับประเทศ	ไม่อนุญาต	-
2. หน่วยงานที่มีหน้าที่หรือมีความเกี่ยวข้องกับการจัดเก็บข้อมูลส่วนบุคคลหรือมีข้อมูลอ่อนไหว ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ไม่อนุญาต	-
3. หน่วยงานที่มีหน้าที่หรือมีความเกี่ยวข้องกับการเก็บข้อมูลที่อยู่ในระดับชั้นความลับ	ไม่อนุญาต	-

ข้อกำหนด	การอนุญาต	การดำเนินการ
4. หน่วยงานที่มีการติดต่อประสานงานกับบุคคลภายนอกและใช้สื่อบันทึกข้อมูลภายนอกเป็นภารกิจหลัก	อนุญาต	เฉพาะไฟล์นามสกุลที่เกี่ยวข้องกับงาน
5. การโอนถ่ายข้อมูลระหว่างระบบที่ไม่เชื่อมต่อกัน	อนุญาต	โดยมีเจ้าหน้าที่ควบคุมการถ่ายโอนข้อมูลระหว่างระบบ
6. ผู้พัฒนาซอฟต์แวร์ที่ต้องการทดสอบหรือปรับปรุงระบบที่ไม่ได้เชื่อมต่อกับเครือข่ายหลัก	อนุญาต	ต้องใช้งานบนระบบเครือข่ายแบบปิดหรือไม่เชื่อมต่อระบบเครือข่าย
7. การติดตั้งระบบปฏิบัติการบนเครื่องคอมพิวเตอร์หรืออุปกรณ์เป็นครั้งแรก	อนุญาต	เฉพาะอุปกรณ์ที่ผ่านการตรวจสอบความปลอดภัยแล้ว
8. การใช้ในกรณีฉุกเฉินที่เกี่ยวข้องกับการกู้คืนระบบ	อนุญาต	เฉพาะกรณีฉุกเฉินเท่านั้น
9. งานสำรองข้อมูลเครื่องแม่ข่ายอย่างน้อย 3 ชุด ได้แก่ • ข้อมูลหลักต้นฉบับบนคอมพิวเตอร์ 1 ชุด และข้อมูลสำรองบนระบบสำรองอีก 2 ชุด • ใช้ 2 เทคโนโลยีในการสำรองข้อมูลเป็นอย่างน้อย • มีการสำรองข้อมูล 1 ชุดไปยังที่อื่น หรือสำรองเอาไว้แบบออฟไลน์	อนุญาต	ต้องสำรองข้อมูลด้วยเครื่องคอมพิวเตอร์ส่วนกลางที่ผ่านการตรวจสอบความปลอดภัยแล้ว

2. ผู้รับผิดชอบ

ผู้รับผิดชอบ	ขอบเขตความรับผิดชอบ
ส่วนสารสนเทศและพัฒนาระบบ	สำหรับเครื่องคอมพิวเตอร์ คอมพิวเตอร์แม่ข่าย อุปกรณ์ด้านเทคโนโลยีสารสนเทศพื้นฐานและซอฟต์แวร์ที่อยู่ภายใต้ความดูแลของหน่วยงาน
ส่วนเตรียมการพิมพ์	สำหรับเครื่องคอมพิวเตอร์ คอมพิวเตอร์แม่ข่าย อุปกรณ์ด้านเทคโนโลยีสารสนเทศพื้นฐานและซอฟต์แวร์จำเฉพาะสำหรับใช้ในงานผลิตสิ่งพิมพ์
ส่วนทรัพยากรบุคคล	สำหรับเครื่องคอมพิวเตอร์ คอมพิวเตอร์แม่ข่าย อุปกรณ์ด้านเทคโนโลยีสารสนเทศพื้นฐานและซอฟต์แวร์จำเฉพาะสำหรับใช้ในการบริหารงานบุคคล

3. การตรวจสอบความปลอดภัย

1) การกำหนดสิทธิ์การใช้งาน

ผู้รับผิดชอบ ส่วนสารสนเทศและพัฒนาระบบ

<u>มาตรการ</u>

กำหนดสิทธิ์การใช้งานสื่อบันทึกข้อมูลภายนอกให้เฉพาะพนักงานที่มีความจำเป็นผ่านระบบ Windows Active Directory หรือซอฟต์แวร์อื่น ๆ ในการควบคุมการจำกัดสิทธิ์

2) การเข้ารหัสข้อมูล

ผู้รับผิดชอบ ส่วนสารสนเทศและพัฒนาระบบ

<u>มาตรการ</u>

ข้อมูลทุกประเภทที่จัดเก็บในสื่อบันทึกข้อมูลภายนอกต้องมีการเข้ารหัส

3) การสแกนไวรัส

ผู้รับผิดชอบ ส่วนสารสนเทศและพัฒนาระบบ

มาตรการ

กำหนดการตั้งค่าให้ทำการสแกนไวรัสทุกครั้งก่อนนำข้อมูลเข้า/ออกจาก USB และใช้โปรแกรมสแกนไวรัสที่มีฐานข้อมูลไวรัสล่าสุดและได้รับการรับรองจากองค์กร

4) การจัดเก็บสื่อบันทึกข้อมูลภายนอกอย่างปลอดภัย

ผู้รับผิดชอบ ผู้ใช้งาน

มาตรการ

จัดเก็บสื่อบันทึกข้อมูลภายนอกในที่ปลอดภัย เช่น ตู้ล็อคเก็บเอกสาร หรือพื้นที่ที่ได้รับการควบคุมการเข้าถึง ห้ามทิ้งสื่อบันทึกข้อมูลภายนอกไว้ในที่ที่ไม่ปลอดภัย เช่น โต๊ะทำงานที่ไม่มีการล็อคเก็บ เป็นต้น

5) การรายงานเหตุการณ์ผิดปกติ

ผู้รับผิดชอบ ผู้ใช้งาน

มาตรการ

รายงานเหตุการณ์ที่ไม่ปกติ เช่น การสูญหายของสื่อบันทึกข้อมูลภายนอกหรือการตรวจพบไวรัสต่อส่วนสารสนเทศและพัฒนาระบบทันที

ส่วนสารสนเทศและพัฒนาระบบ จะตรวจสอบและแก้ไขปัญหา พร้อมรายงานผลการดำเนินการให้ผู้บริหารทราบต่อไป

6) การฝึกอบรมและความตระหนักรู้

ผู้รับผิดชอบ ส่วนทรัพยากรบุคคลและส่วนสารสนเทศและพัฒนาระบบ

มาตรการ

จัดการฝึกอบรมพนักงานเกี่ยวกับการใช้งานสื่อบันทึกข้อมูลภายนอกอย่างปลอดภัยและให้ความรู้เกี่ยวกับความเสี่ยงและวิธีการป้องกันภัยทางไซเบอร์อย่างน้อยปีละ 1 ครั้งและมีการติดตามผลหลังจบการฝึกอบรม

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 โดยมีการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

5) มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในบริษัทและกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของบริษัท ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

6) รายงานการเปลี่ยนแปลงของทรัพย์สินในความรับผิดชอบของตนต่อผู้อำนวยการอาวุโสฝ่ายดิจิทัล เพื่อรับทราบ

7) กำหนดหน้าที่ความรับผิดชอบและควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control) ดังนี้

7.1) ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัทต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน

- ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้าหรือบริการใด ๆ 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 หรือโยน ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่

– หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบ หมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

– ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน

– การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติ ตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท

– ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางอุปกรณ์ทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

8) มีการควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License) ให้ถูกต้องลิขสิทธิ์ และปฏิบัติ ตามแนวทางปฏิบัติอย่างเคร่งครัด 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 สำนักงานตำรวจแห่งชาติ โครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (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 เขียน อ่าน 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 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ 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 สำหรับการเข้าสู่ระบบสารสนเทศของโรงงานไพ่กรมสรรพสามิตอย่างน้อย 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 เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น 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) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เข้า มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง หรือ ผู้ใช้งานเข้าถึงข้อมูลหรือกระทำการไม่เหมาะสม 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 โดยสามารถเข้าใช้งานระบบในช่วงวันทำงานตั้งแต่เวลา 6.00น.–21.00น. 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

– ผู้รับจ้างมีหน้าที่ในการคัดสรรพนักงานที่เข้ามาดำเนินโครงการของการพัฒนาระบบสารสนเทศของโรงงานไพ่กรมสรรพสามิตจะต้องไม่เคยเป็นผู้มีความผิดเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ระหว่างการจ้างผู้รับจ้างมีหน้าที่และความรับผิดชอบในการควบคุมดูแลพนักงานของผู้รับจ้างให้รักษาข้อมูลที่เป็นความลับเช่นเดียวกับที่ผู้รับจ้างต้องปฏิบัติ

– ผู้รับจ้างจะต้องใช้ความระมัดระวังอย่างที่สุดตามที่ผู้ประกอบวิชาชีพจะพึงมีในการรักษาข้อมูลที่เป็นความลับอย่างเคร่งครัด โดยไม่บอกหรือเปิดเผยข้อมูลทีเป็นความลับแก่บุคคลภายนอกรู้ไม่ว่ากรณีใดๆ ทั้งสิ้น เว้นแต่เพื่อความจำเป็นในการปฏิบัติงานตามหน้าที่ของผู้รับจ้างตามสัญญาหลักเท่านั้นต้องเสริมสร้างความเข้าใจอันดีต่อพนักงานทุกคน 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 Clear Screen policy)

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

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญอันหนึ่งของระบบรักษาความมั่นคงปลอดภัย ความมั่นคงทางกายภาพรวมถึงการป้องกันสถานที่และอุปกรณ์ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติเช่น แผ่นดินไหว น้ำท่วมเป็นต้น การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจรอุณหภูมิ หรือความชื้น ในห้องควบคุมที่สูงเกินขีดจำกัด หรือการกระทำโดยประมาท เช่น การทำน้ำกรดโดนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ 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 ในพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงต้องมีอุปกรณ์ควบคุมฝุ่น 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
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) วัตถุประสงค์เพื่อให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

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

- การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ ที่ไม่ได้ลงทะเบียนเข้ามาใช้งานโดยไม่ได้รับอนุญาตหรือผ่านการตรวจสอบจากเจ้าหน้าที่ส่วนสารสนเทศและพัฒนาระบบ

– 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 ดำเนินการยื่นคำร้อง

ต่อผู้บริหารดิจิทัล 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 วีดีโอ 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 รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ที่บรรจุรายชื่อบัญชีผู้ใช้ที่ขึ้นทะเบียนในเครือข่ายของ

องค์กร 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 โดยสามารถเพิ่มหรือลดค่าแต่ละบัญชีจดหมายอิเล็กทรอนิกส์ตามความเหมาะสมเพื่อให้การใช้งาน และการบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ

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 โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัดพร้อมแนบเหตุผลความจำเป็นส่งถึงส่วน

สารสนเทศและพัฒนาระบบ 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 หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความ

มั่นคงปลอดภัยด้านสารสนเทศ “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 เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา 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 เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหายถูกทำลายจากมัลแวร์ หรือผู้บุกรุก 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 จัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้า ระวังในเครือข่าย (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 เพื่อพัฒนาทักษะ ความรู้ 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 ผู้บริหารด้านดิจิทัลสำหรับการเข้าถึงระบบงานขององค์กร 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 ให้เจ้าหน้าที่ผู้ดูแลระบบของหน่วยงาน รับผิดชอบการปฏิบัติงาน 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

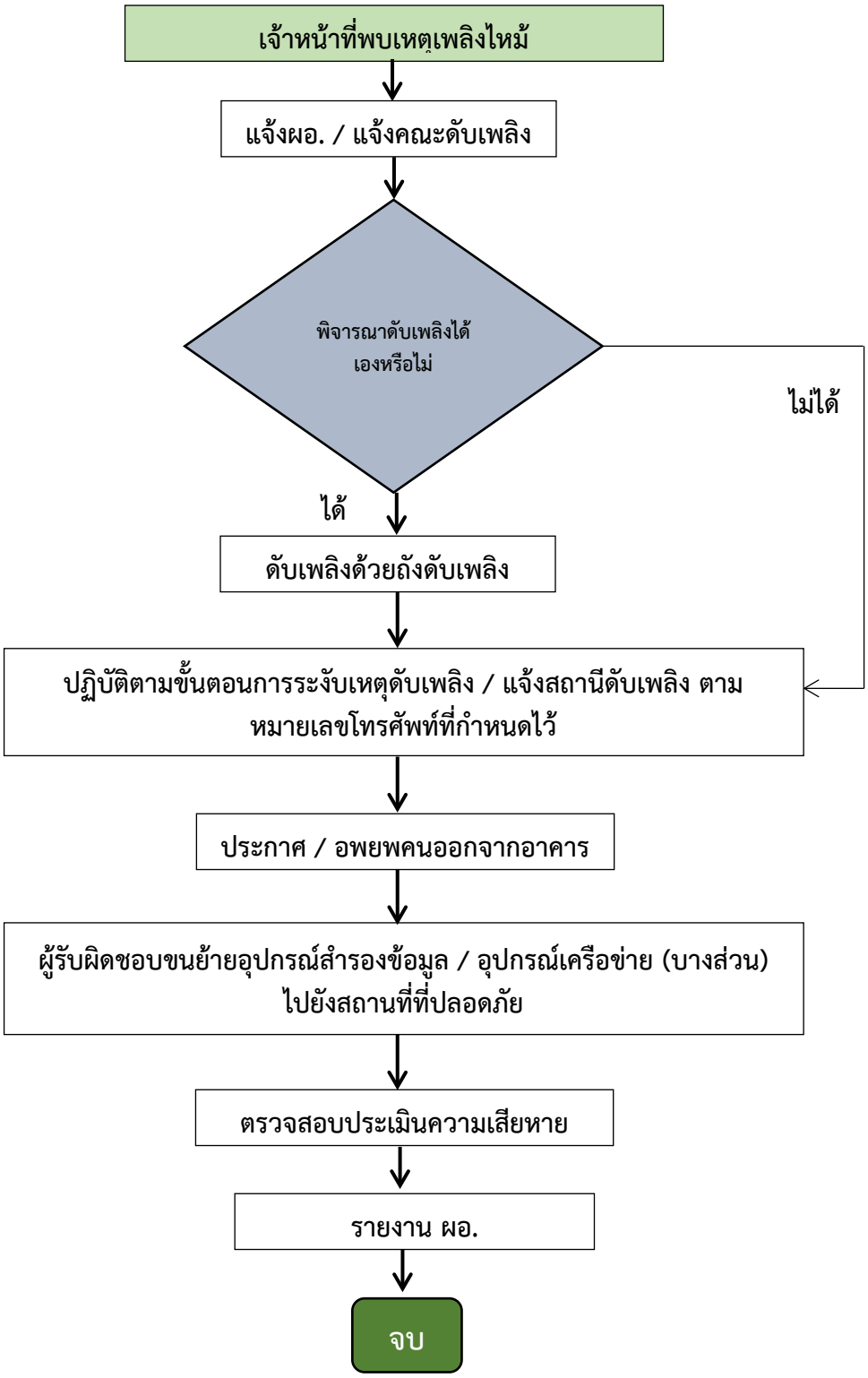
ค. ทีมแก้ไขกรณีแผ่นดินไหว ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

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

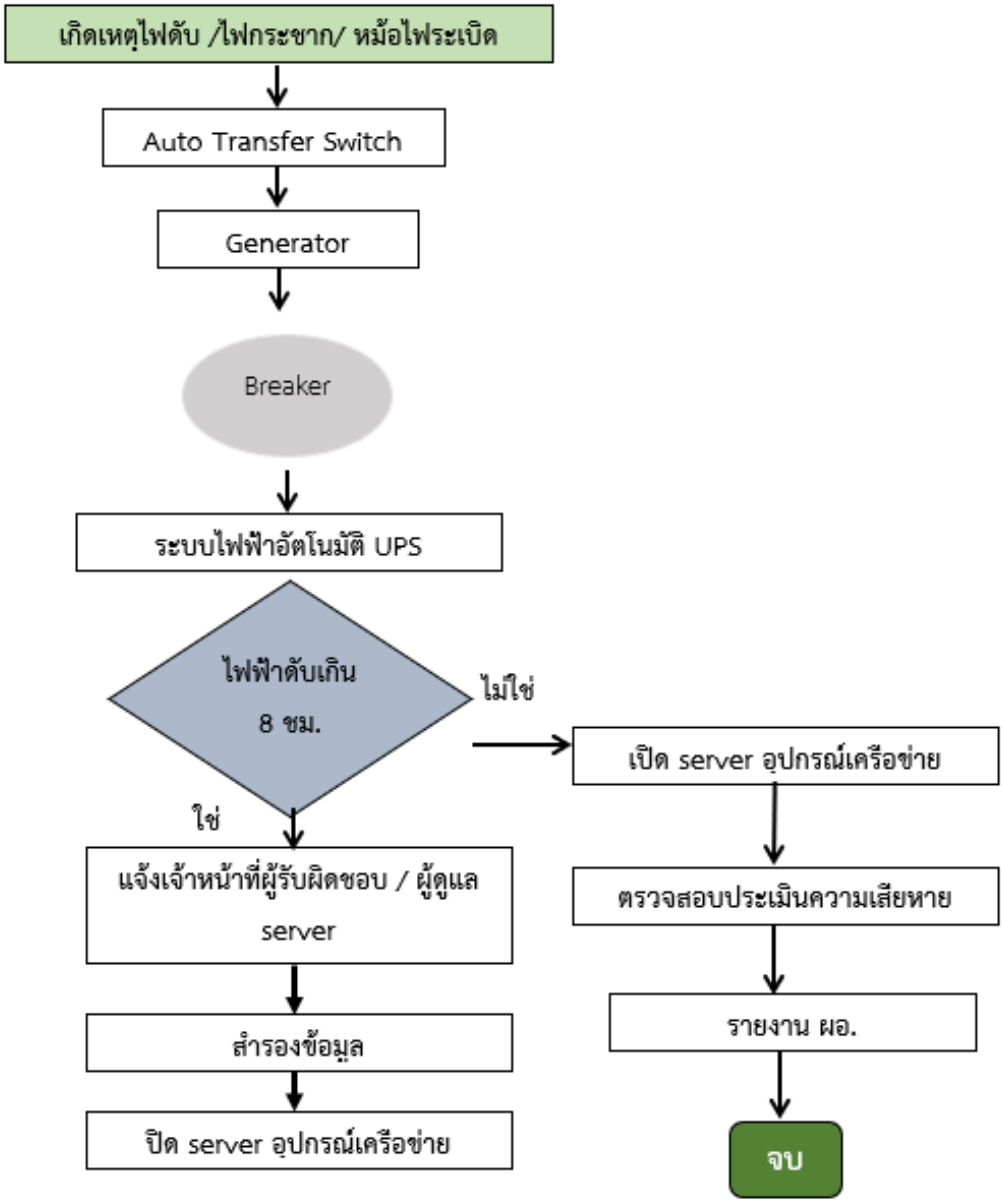
ง. ทีมแก้ไขกรณีเกิดการจลาจล ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

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

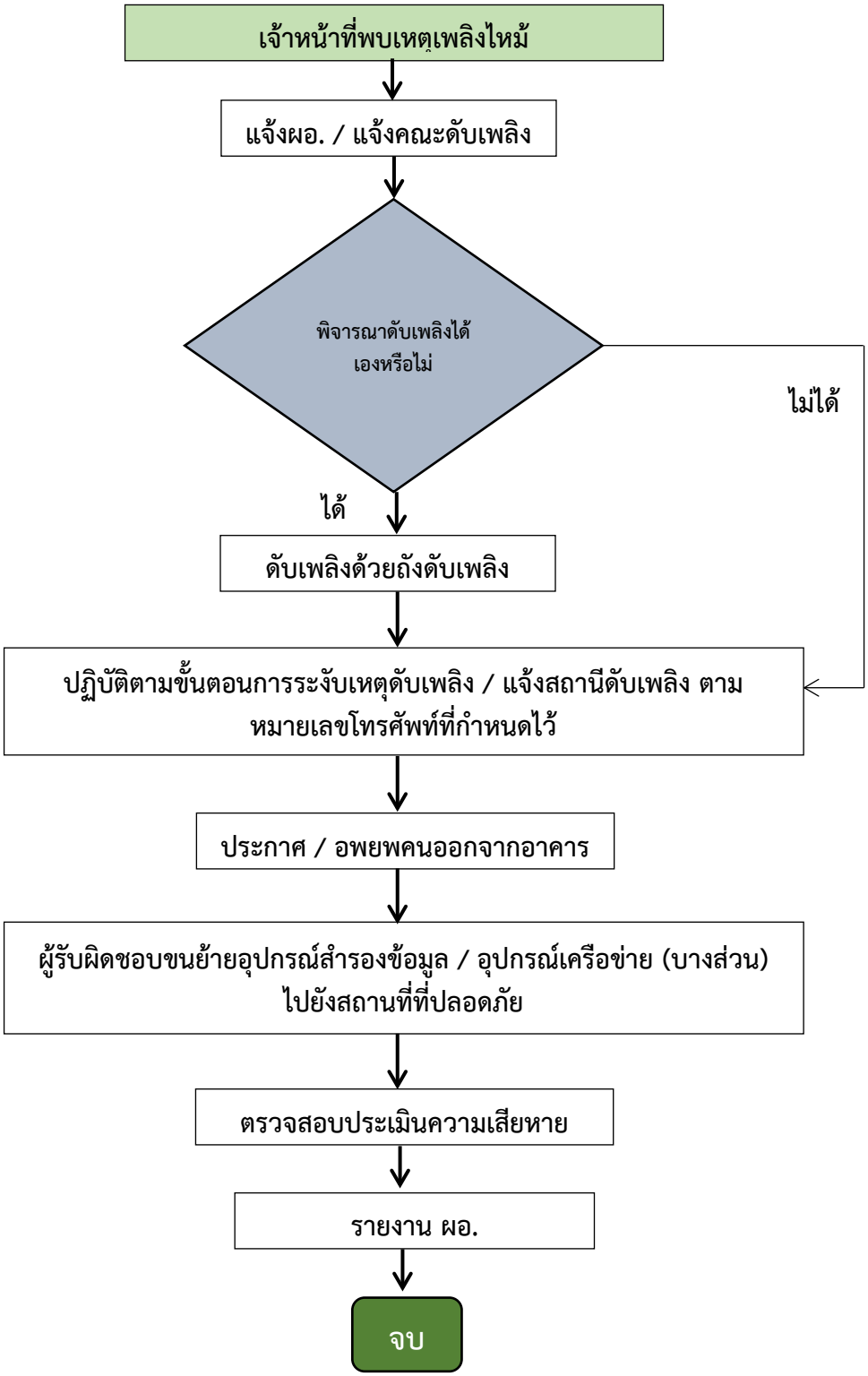
10) ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ
– ขั้นตอนการปฏิบัติงานกรณีไฟไหม้ (ห้องควบคุมระบบ)


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

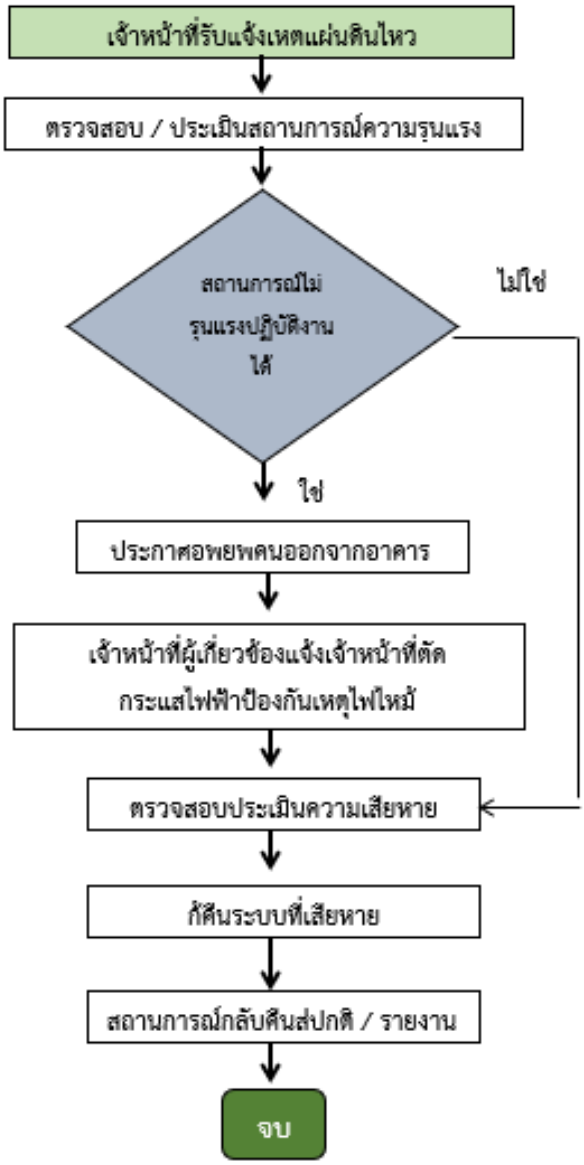
– ขั้นตอนการปฏิบัติงานกรณีเกิดเหตุไฟดับ ไฟกระชาก หม้อไฟระเบิด



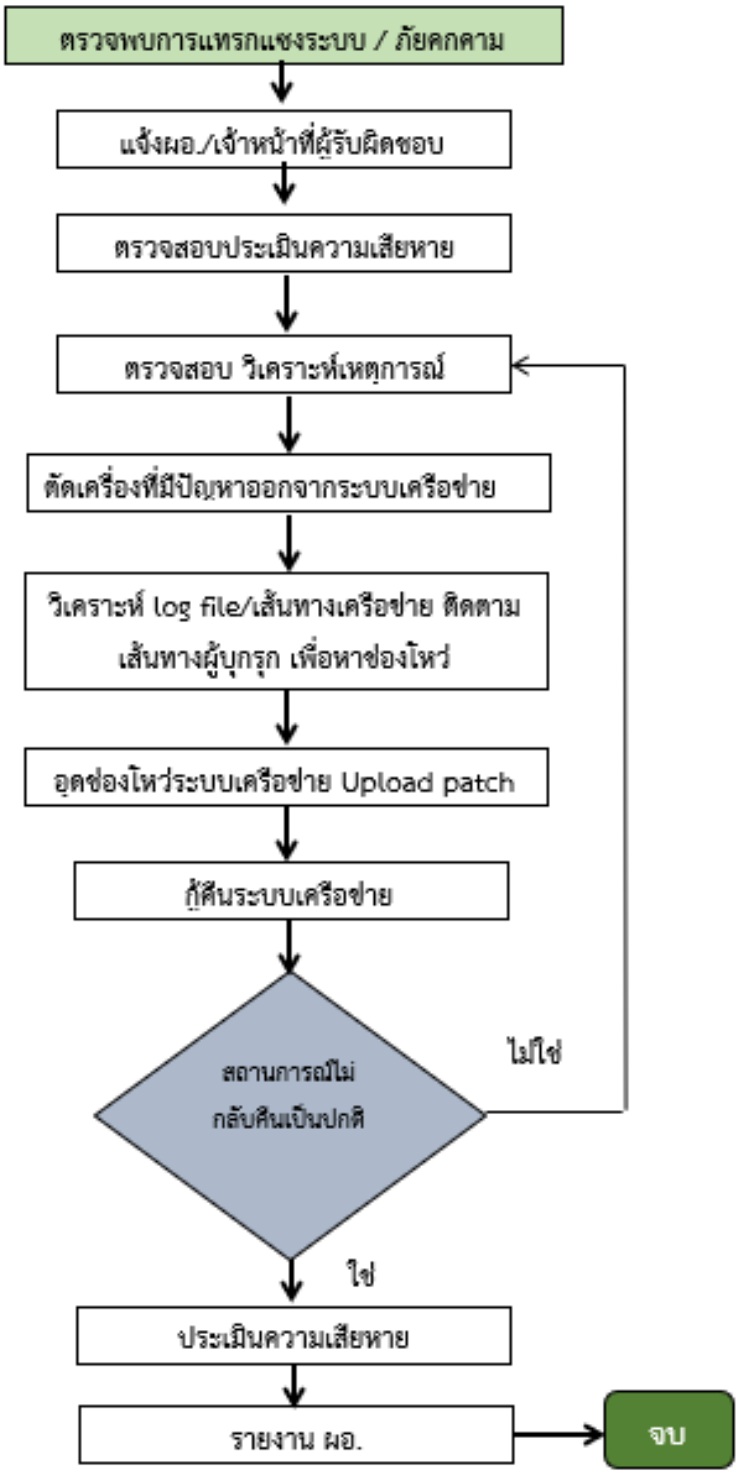
– ขั้นตอนการปฏิบัติงานกรณีเกิดเหตุจราจล



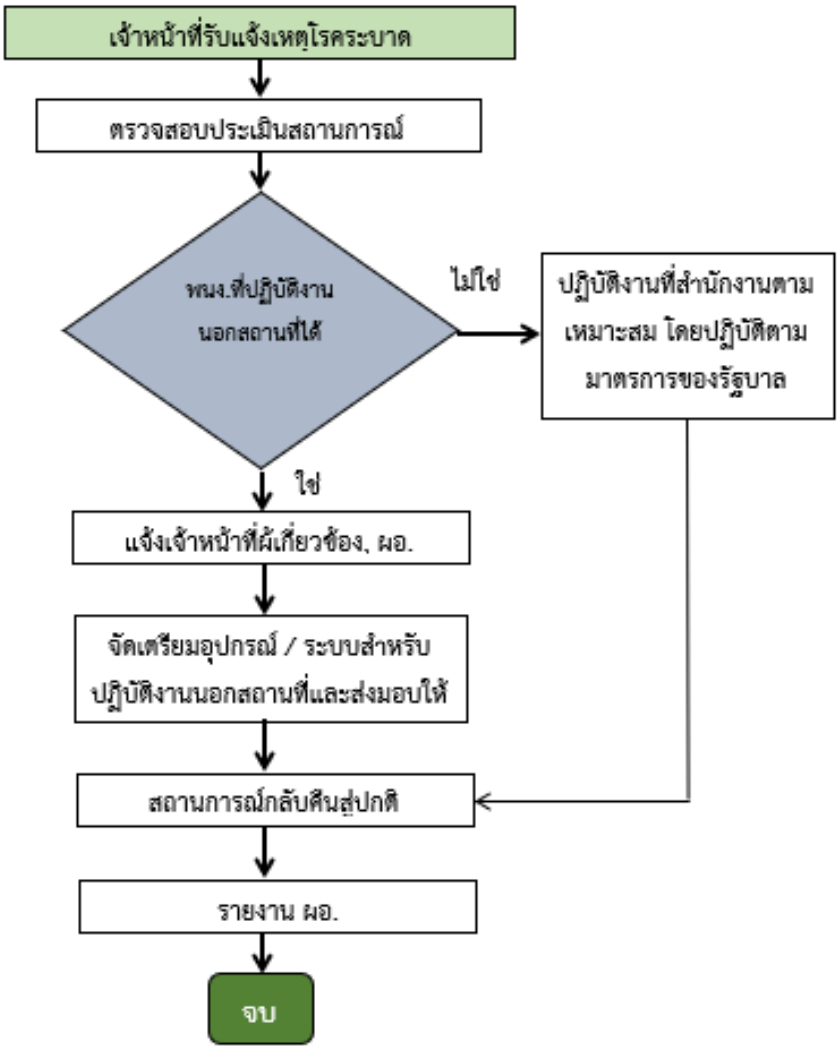
– ขั้นตอนการปฏิบัติงานกรณีเกิดแผ่นดินไหว



– 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

การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง 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 ให้ปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

5) ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่ส่วนสารสนเทศและพัฒนาระบบจัดสรรไว้ตามสิทธิ์ที่ได้รับ

6) ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเทอร์เน็ต

1) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ส่วนสารสนเทศและพัฒนาระบบจัดสรรไว้ ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจาก หัวหน้าส่วนสารสนเทศ 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 Security)

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)

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

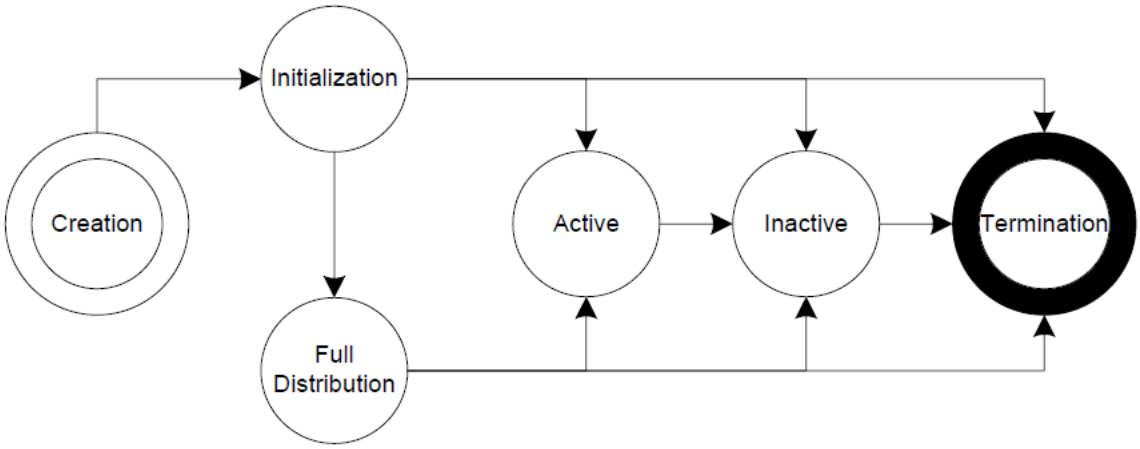
14.2 โรงงานไพ่ต้องจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูล ตลอดช่วงเวลาการใช้งาน (key management whole life cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าวอ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

แนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ และการบริหารจัดการกุญแจ

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

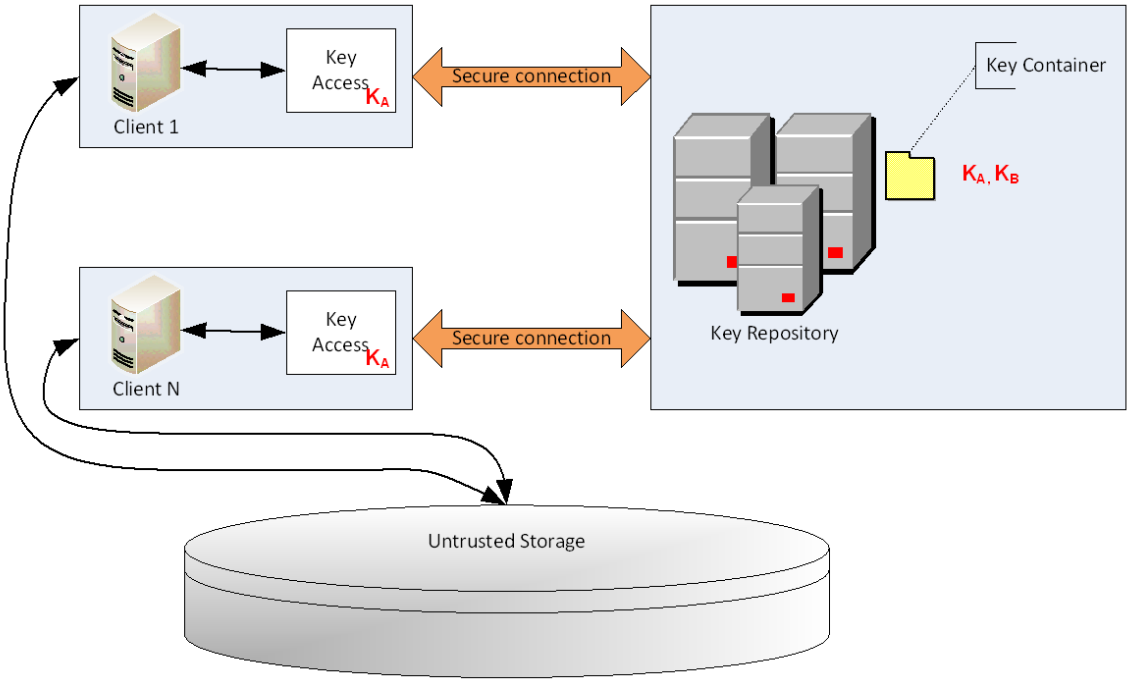
บทความนี้พิจารณาถึงวงจรชีวิตที่สำคัญตามอายุ กระบวนทัศน์อีกประการหนึ่งคือการกำหนดวงจรชีวิตตามจำนวนการใช้คีย์ (หรือตัวนับที่เพิ่มขึ้นแบบจำเจ) อย่างไรก็ตาม การรักษาตัวนับที่เพิ่มขึ้นแบบโมโนโทนเป็นเรื่องยากในระบบแบบกระจาย สิ่งนี้จะยิ่งท้าทายมากขึ้นไปอีก หากเราต้องการใช้ประโยชน์จากที่เก็บแบบกระจายที่มีอยู่ในขณะที่ทำการเปลี่ยนแปลงน้อยที่สุด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

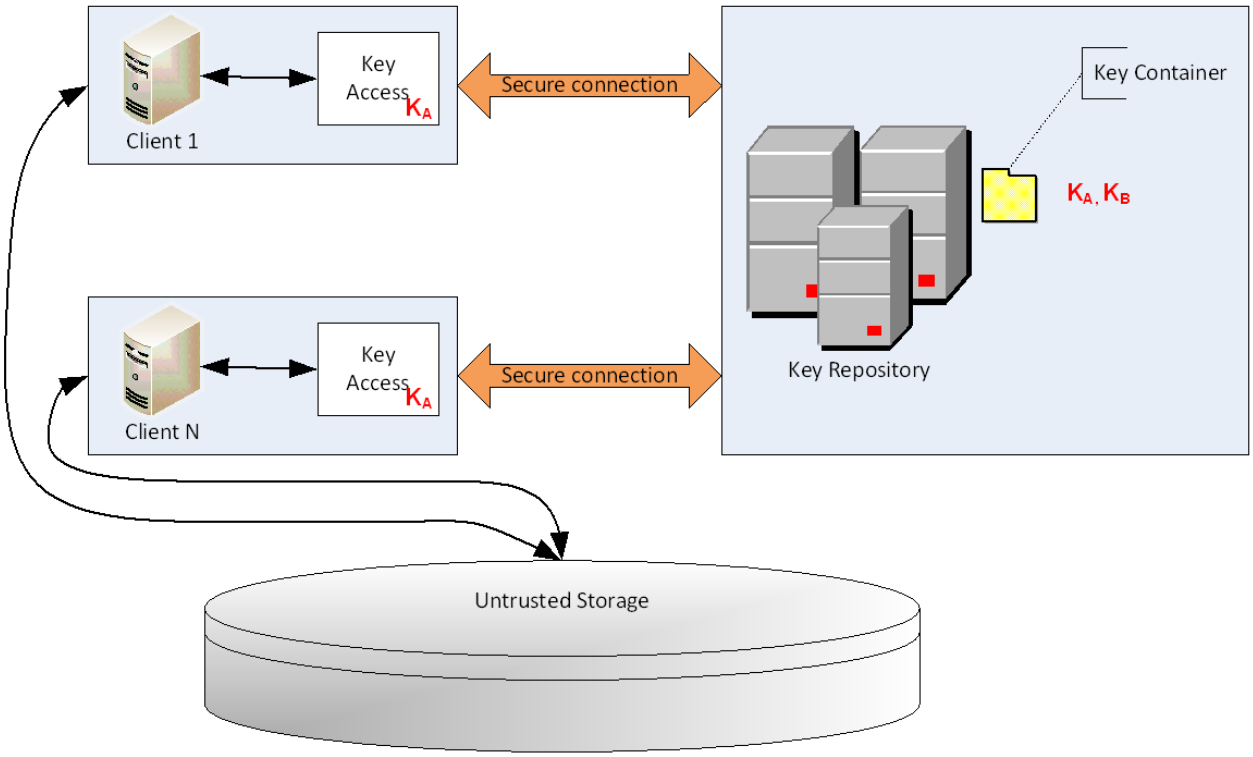
สถานะในวงจรชีวิตของคีย์การเข้ารหัส ผู้ที่คุ้นเคยกับขั้นตอนเหล่านี้อยู่แล้ว และมีความคล้ายคลึงกับขั้นตอนที่ระบุในระบบ Information Lifecycle Management (ILM) เราระบุสถานะที่มีรายละเอียดหลายอย่างในช่วงอายุของคีย์ที่ส่งผลต่อการทำงานภายในของระบบการจัดการคีย์แบบกระจาย ซึ่งการกำหนดมี 6 สถานะ ได้แก่

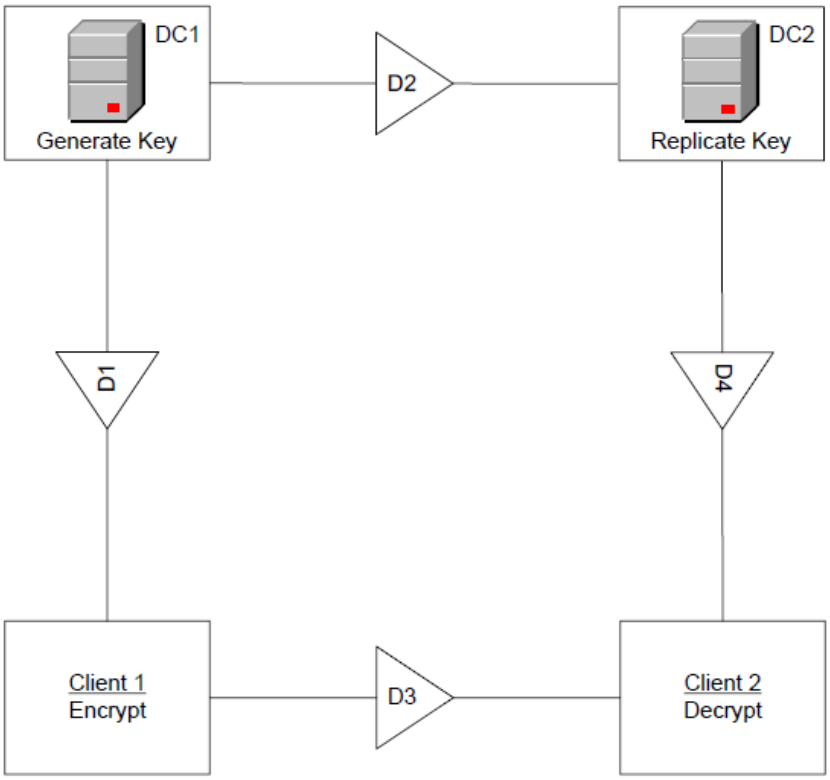


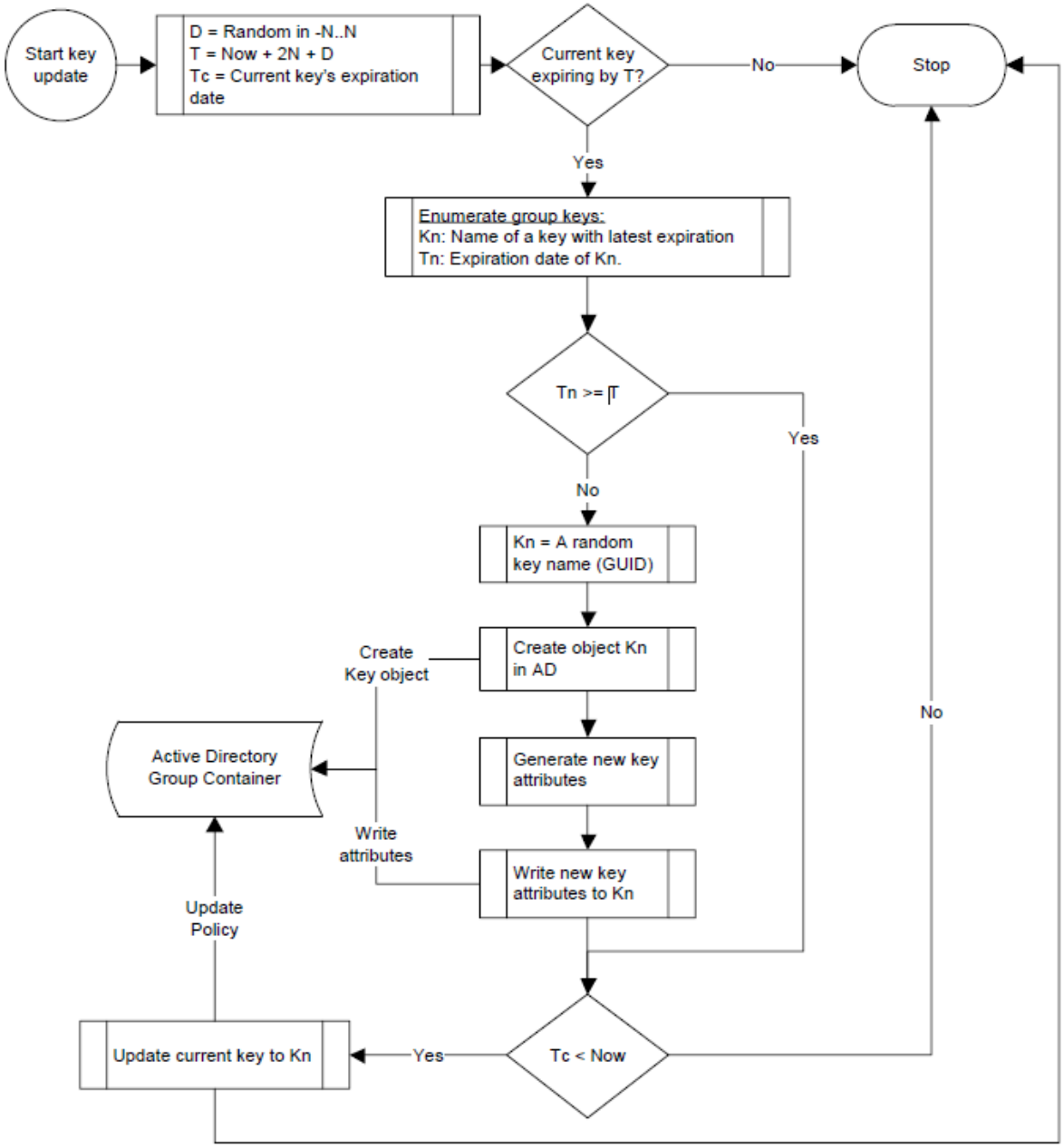
- Creation อ็อบเจ็กต์คีย์ถูกสร้างขึ้นบนตัวควบคุมโดเมนอย่างน้อยหนึ่งตัว แต่ไม่มีการตั้งค่าแอตทริบิวต์
- Initialization ออบเจ็กต์คีย์มีแอตทริบิวต์คีย์หลักทั้งหมดที่ตั้งค่าไว้บนตัวควบคุมโดเมนอย่างน้อยหนึ่งรายการ
- Full Distribution คีย์เริ่มต้นสามารถใช้ได้กับตัวควบคุมโดเมนทั้งหมด
- Active คีย์เริ่มต้นพร้อมใช้งานสำหรับการดำเนินการเข้ารหัสทั้งหมดบนตัวควบคุมโดเมนอย่างน้อยหนึ่งตัว
- 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