นโยบายการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เนื่องจากองค์กร ได้นำระบบสารสนเทศมาใช้ในการดำเนินงานและให้บริการผู้ใช้งานทั้งภายในและภายนอกองค์กร ดังนั้นเพื่อให้การใช้สารสนเทศและระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่เหมาะสม หรือถูกคุกคามจากภัยต่างๆ ซึ่งจะช่วยลดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน และบุคลากร

โดยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การรักษาความมั่นคงปลอดภัยในการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศขององค์กร โดยไม่เปิดเผยข้อมูลต่อบุคคล หรือระบบงานที่ไม่ได้รับสิทธิ์ (Confidentiality) การรักษาไว้ซึ่งความถูกต้องและครบถ้วนของข้อมูล (Integrity) และการสามารถให้เข้าถึงและใช้งานได้ตามความต้องการของผู้ที่ได้รับสิทธิ์ (Availability)

ทางองค์กรจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีนโยบาย แนวทางปฏิบัติ หรือขั้นตอนปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย มาตรฐานและแนวปฏิบัติสากลของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทั้งนี้

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

1. ความลับ (Confidentiality) การป้องกันความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
2. ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดยทำลายโดยผู้ที่ไม่ได้รับอนุญาต
3. ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้
4. ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของการกระทำตามบทบาทหน้าที่นั้นๆ
5. การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
6. การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต
7. การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (Parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

<u>คำนิยาม</u>

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน ดังนี้

1. “บริษัท (Company)” หมายถึง บริษัท ลอนดรี้ ยู จำกัด (มหาชน)
2. “ฝ่ายทรัพยากรบุคคล” หมายถึง ฝ่ายทรัพยากรบุคคล ของ บริษัท ลอนดรี้ ยู จำกัด (มหาชน)
3. “ฝ่ายเทคโนโลยีสารสนเทศ” หมายถึง หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศของบริษัท
4. “พนักงาน (Employee)” หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท
5. “ผู้ใช้งาน (User)” หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท
6. “ผู้บังคับบัญชา” หมายถึง พนักงานซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท
7. “ข้อมูลสารสนเทศ (Information Technology)” หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ รูปภาพ เสียง เครื่องหมาย และสัญญาลักษณ์ต่างๆ ไม่ว่าจะเก็บในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใดๆ

8. “ระบบคอมพิวเตอร์ (Computer System)” หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่างๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่างๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของ
9. “ข้อมูลสำคัญ” หรือ “ข้อมูลที่เป็นความลับ (Sensitive Information)” หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผู้พันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์สนการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสีย
10. “ระบบที่มีความสำคัญ (Important System)” หมายถึง ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์ เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัทให้เป็นปกติ และระบบที่ได้การกำหนดโดยหน่วยงานด้านความปลอดภัยข้อมูลและระบบสารสนเทศของบริษัท ทั้งนี้หากระบบมีความสำคัญดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงักหรือด้อยประสิทธิภาพ
11. “Remote Access” หมายถึง การเข้าถึงระบบสารสนเทศของบริษัทจากภายนอก
12. “เจ้าของระบบ (System Owner)” หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์
13. “ผู้ดูแลข้อมูล (Custodian)” หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศในการสนับสนุนงานการดูแล จัดการ และควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศกำหนด
14. “ผู้ดูแลระบบ (Administrator)” หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไขให้ระบบคอมพิวเตอร์ของบริษัท ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องความต้องการทางธุรกิจและมีความปลอดภัย
15. “การรักษาความมั่นคงปลอดภัย” หรือ “ความมั่นคงปลอดภัย (Security) หมายถึง กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน กระระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบรัษัทได้รับความเสียหาย

16. “บุคคลภายนอก (External Party)” หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัท เช่น
    - บริษัทคู่ค้า (Business Partner)
    - ผู้รับจ้างปฏิบัติงานให้กับบริษัท (Outsource)
    - ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier)
    - ผู้ให้บริการต่างๆ (Service Provider)
    - ที่ปรึกษา(Consultant)

<u>วัตถุประสงค์</u>

1. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวข้องกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อให้พนักงาน และผู้ที่ต้องใช้ หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ใช้สามารถใช้ระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลายแทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

<u>แนวทาง</u>

1. จัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีนโยบาย แนวทางปฏิบัติ หรือขั้นตอนปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการมาตรฐานสากลของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยอ้างอิงมาตรฐาน ISO/IEC 27001:2013 Information Security Management System
2. จัดให้ข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับสารสนทศ การพัฒนาและบำรุงรักษาระบบสารสนเทศ และสิ่งใดๆที่เกี่ยวข้องกับสารสนเทศมีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมและเพียงพอ และมีการควบคุมการเข้าถึงที่กำหนดอย่างชัดเจนตามหลักการของความต้องการในการใช้งานที่เหมาะสมและมั่นคงปลอดภัย
3. จัดให้มีระบบสำรองข้อมูล ระบบกู้คืนข้อมูล และระบบสำรองที่ใช้ทดแทนระบบเทคโนโลยีสารสนเทศหลักในกรณีฉุกเฉิน โดยระบบสำรองต้องอยู่ในสภาพพร้อมใช้ และมีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน
4. จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยมีแนวทางที่สอดคล้องกับการบริหารความเสี่ยงขององค์กร
5. จัดให้มีการตรวจสอบและดำเนินการแก้ไข เมื่อมีเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยเกิดขึ้น พร้อมทั้งดำเนินการป้องกันไม่ให้เกิดซ้ำ และให้รายงานและทำบันทึกไว้อย่างชัดเจน

6. จัดให้ผู้ใช้บริการได้รับความรู้เรื่องนโยบาย แนวทางปฏิบัติ มาตรฐาน และระเบียบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผู้ใช้บริการจะต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

<u>บทบาทและหน้าที่</u>

1. หน้าที่กรรมการผู้จัดการและประธานเจ้าหน้าที่บริหาร
    - กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท
2. หน้าที่ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
    - ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค้า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท
    - ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ
    - กำหนดเป้าหมาย นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท
    - จัดการพัฒนานโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ Policy, Standard, Procedure และ Guideline เพื่อให้บริษัทได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และความเสถียรภาพความมั่งคงระบบ (Availability)
    - จัดการบริหารเฝ้าระวังโจมตีระบบและภัยต่างๆ ที่อาจจะเกิดขึ้นกับระบบรวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน
    - มีการบริหารความเสี่ยงและการวิเคราะห์ความเสี่ยงที่อาจจะทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุระกิจของบริษัท
    - นำเสนอผู้บริหารระดับสูง เช่น กรรมการผู้จัดการและประธานเจ้าหน้าที่บริหาร เรื่องแผนการปฏิบัติ นโยบายงบประมาณ อัตรากำลัง
    - เตรียมพร้อมรับสถานการณ์ และเรียนรู้เทคนิคใหม่ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ
3. หน้าที่ผู้บังคับบัญชา
    - ชี้แจง และส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม
4. หน้าที่ผู้ใช้งาน
    - ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งคัด
    - ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทให้มีความปลอดภัย

- รายงานต่อบริษัททันที เมื่อพบว่าอุปกรณ์ หรือข้อมูลสารสนเทศสำคัญสูญหายหรือพบเห็นเป็นการบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อบริษัท

5. หน้าที่ของเจ้าของข้อมูลและสารสนเทศ
    - จัดให้มีการจัดทำเอกสร มาตรการ และขั้นตอนควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท
    - ดูแลให้พนักงานปฏิบัติตามนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศของบริษัท
    - ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ
    - รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ
    - แจ้งหน่วยงานเทคโนโลยีสารสนเทศที่รับผิดชอบด้านการบริหารบัญชีผู้ใช้งานและสิทธิ์ในการใช้ระบบสารสนเทศเพื่อลบ / เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงาน / อำนาจหน้าที่ / โอนย้าย
6. หน้าที่ของหน่วยงานตรวจสอบภายใน (Internal Audit)
    - ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศตามความจำเป็น

<u>ระยะเวลาทบทวน</u>

เพื่อให้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งแนวทางปฏิบัติ หรือ ขั้นตอนปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง ทางองค์กรจึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ หรือขั้นตอนการปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยที่มีผลกระทบกับองค์กร

<u>ขอบเขต</u>

บังคับใช้กับทุกหน่วยงานในบริษัท ลอนดรี้ ยู จำกัด (มหาชน)

<u>บทลงโทษ</u>

ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามข้อปฏิบัติต่างๆ ถือเป็นความผิดตามระเบียบปฏิบัติที่ นโยบายหลักบริษัทฯ ได้กำหนดไว้แล้ว

1. ตักเตือนด้วยวาจา
2. ตักเตือนเป็นลายลักษณ์อักษร
3. พักงานชั่วคราวโดยไม่ได้รับค่าจ้าง
4. ปลดออก
5. ไล่ออก
6. การดำเนินทางกฎหมายอาญาหรือแพ่ง

กรณีการลงโทษพนักงาน บริษัทไม่จำเป็นต้องปฏิบัติตามลำดับดังกล่าวข้างต้น บริษัทอาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (IT Security)

1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์ เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

- ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น
- ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
- ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก
- ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นจ้าของข้อมูลนั้นๆ
- ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
- ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
- ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

2. ความปลอดภัยเกี่ยวกับบุคลากร

วัตถุประสงค์ เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัท

แนวทางปฏิบัติ

- ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของบริษัท
- ต้องมีการลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงาน ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ปฏิบัติงานนั้นๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

- เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศทราบทันที เมื่อมีเหตุดังนี้
    - การว่าจ้างงาน
    - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
    - การลาออกจากงาน หรือการสิ้นสุดการเป็นกรรมการและผู้ปฏิบัติงานของบริษัท
    - การโยกย้ายหน่วยงาน
- ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ผู้ปฏิบัติงานใหม่ของบริษัทต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ
- จัดอบรมให้ความรู้แก่ผู้ใช้งานทุกคนเกี่ยวข้องกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติบุคลากร ถ้ามีการเปลี่ยนแปลงทางด้านความมั่นคงปลอดภัยต้องแจ้งให้พนักงานทราบ
- ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎและแนวปฏิบัติของบริษัท หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำ และเป็นไปตามระเบียบบริษัท
- หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องคืนทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศ

3. ความปลอดภัยเกี่ยวกับทรัพย์สินสารสนเทศ

<u>วัตถุประสงค์</u> เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

<u>แนวทางปฏิบัติ</u>

- ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
- ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
- ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
- ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม

- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย
- ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
- การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 30 นาที
- ระมัดระวังและดูแลทรัพย์สินของบริษัท ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

4. ความปลอดภัยเกี่ยวกับการใช้งานโปรแกรมคอมพิวเตอร์

<u>วัตถุประสงค์</u> เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ตลอดจนเข้าใจการใช้โปรแกรมที่ถูกต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายบริษัท

<u>แนวทางปฏิบัติ</u>

- ข้อกำหนดสำหรับผู้ดูแลระบบ
    - มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทตามสิทธิ์การใช้งานที่กำหนด
    - มีหน้าที่รับผิดชอบในการติดตั้ง และอัพเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย
    - ทำการถอดและยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัท และ/หรือหน่วยงานแจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์

- ข้อกำหนดสำหรับผู้ใช้งาน
    - โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน

- ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย
- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

5. ความปลอดภัยเกี่ยวกับข้อมูลสารสนเทศ

<u>วัตถุประสงค์</u> เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานข้อมูลสารสนเทศของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

<u>แนวทางปฏิบัติ</u>

- บริษัทต้องกำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม เอกสารหรือสิ่งตีพิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับของข้อมูลนั้น
- มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
- ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย การจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบดังนี้
    - ในฐานข้อมูลของระบบ Application นั้นๆ ที่จัดเก็บภายใน Data Center/Cloud Provider Server
    - สามารถจัดเก็บใน Shared File (Drive กลาง) ใน Folder ตามสิทธิ์ที่ได้รับ

6. ความปลอดภัยเกี่ยวกับการเข้าถึงระบบสารสนเทศ และการใช้งานระบบเครือข่ายของบริษัท

<u>วัตถุประสงค์</u> เพื่อกำหนดมาตรการในการใช้งานระบบสารสนเทศและระบบเครือข่ายของบริษัท เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย และอนุญาติให้เข้าใช้งานได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น

<u>แนวทางปฏิบัติ</u>

- ต้องกำหนดให้มีขึ้นตอนสำหรับลงทะเบียนต่าง เพื่อให้มีสิทธิ์และควบคุมสิทธิ์ในการเข้าถึงสารสนเทศของบริษัทตามความจำเป็น รวมถึงการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น รวมถึงต้องมีกระบวนการจัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานตามความเหมาะสมหรือที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย
- ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษาบัญชีผู้ใช้งาน และรหัสผ่านของตนให้มีความมั่นคงปลอดภัย
- การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทจะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงาน และสามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องจำกัดการเข้าถึงให้เฉพาะผู้ที่ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น
- ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
    1. ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric)
    2. ควรใช้อักขระพิเศษประกอบ เช่น : ; < > $ @ # เป็นต้น
    3. สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน ส่วนผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ (System Administrator) และผู้ใช้งานที่ติดมากับระบบ (Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน
    4. ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 3 ครั้งหลังสุด
    5. ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น “ abcdef ” “ aaaaaa ” “123456” “password” “P@ssw0rd” เป็นต้น
    6. ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด (Logon Attempt -Retires) ซึ่งในทางปฏิบัติโดยทั่วไปให้อยู่ที่ 5 ครั้ง หากการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนดไว้ ระบบงานหรือโปรแกรมจะไม่อนุญาตหรือระงับการใช้งาน
    7. ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย
    8. ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

9. ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
10. สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses เช่นระบบ BC เป็นต้น ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด

- ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ปฏิบัติงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน รหัสผ่าน เป็นต้น
- จัดให้มีการทบทวนสิทธิ์การใช้งานระบบสารสนเทศต่างๆ ทุกๆ ไตรมาส
- ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท
- ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น
- ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด
- การเข้าถึงแอพพลิเคชั่นใดๆ ต้องถูกควบคุมและจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตหรือได้รับมอบหมายสิทธิ์ เช่น ผู้ดูแลระบบ เป็นต้น รวมถึงการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ ต้องอนุญาติเฉพาะผู้ที่มีสิทธิ์ตามจำนวนที่ซื้อเท่านั้น

7. ความปลอดภัยเกี่ยวกับการดูและรักษาระบบสารสนเทศ

<u>วัตถุประสงค์</u> เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการสูญหายของข้อมูล และได้รับการปกป้องจากโปรแกรมไม่ประสงค์ดี

<u>แนวทางปฏิบัติ</u>

- จัดทำคู่มือหรือขั้นตอนปฏิบัติงาน เช่นขั้นตอนการกู้คืนระบบ ขั้นตอนการบำรุงรักษาและดูแลระบบ เป็นต้น และต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบคอมพิวเตอร์ ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์
- ต้องมีการแบ่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต
- ต้องมีระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบสารสนเทศที่สำคัญของบริษัท เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต
- ต้องสำรวจข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล
- ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกบริษัท
- ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

8. ความปลอดภัยเกี่ยวกับระบบเครือข่ายของบริษัท

<u>วัตถุประสงค์</u> เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศ

<u>แนวทางปฏิบัติ</u>

- ต้องมีการจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้งานภายนอก
- เครือข่ายภายในอนุญาติให้สามารถเชื่อมต่อและใช้งานในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทได้เฉพาะอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์พกพาของบริษัทเท่านั้น
- จัดให้มีการเข้าถึงข้อมูลหรือสารสนเทศของบริษัทจากระยะไกลได้ โดยผู้ใช้งานสามารถเชื่อมต่อผ่านระบบ VPN ของบริษัท และต้องมีสิทธิ์การเข้าใช้งาน
- ผู้ใช้งานที่ใช้อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์พกพาส่วนตัว ในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท ต้องได้รับการอนุมัติจากหน้างานหน่วยงาน หรือเลขานุการบริษัทกรณีเป็นกรรมการ และหน่วยงานเทคโนโลยีสารสนเทศก่อนการใช้งาน
- อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทจะต้องเป็นอุปกรณ์ที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย เช่น “Jail breaking” หรือ “Rooting” ไม่ติดตั้งซอฟแวร์ที่ละเมิดลิขสิทธิ์ รวมทั้งต้องกำหนดรหัสผ่าน ตามนโนบายที่หน่วยงานเทคโนโลยีสารสนเทศกำหนด

- บริษัทขอสงวนสิทธิ์สนการตรวจสอบ ระงับ เพิกถอนการใช้งาน และลบข้อมูลทั้งหมด (Wipe) บนอุปกรณ์พกพาทั้งที่เป็นของบริษัท และของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บและสารสนเทศของบริษัท หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐาน หรือข้อมูลและสารสนเทศของบริษัท

9. ความปลอดภัยเกี่ยวกับการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

<u>วัตถุประสงค์</u> การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

<u>แนวทางปฏิบัติ</u>

- ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน
- ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง
- ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม
- การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน มีการดำเนินการดังนี้
    - การร้องขอ
        1. การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร โดยอาจเป็น Electronic Transaction เช่น อีเมล เป็นต้น และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือผู้รับผิดชอบระบบสารสนเทศ เป็นต้น
        2. ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
        3. ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ
    - การปฏิบัติงานพัฒนาระบบงาน
        1. ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่

เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

2. ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
3. ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

- การทดสอบ

  ผู้ที่ร้องขอและส่วนเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

- การโอนย้ายระบบงานเพื่อใช้งานจริง

  ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

- การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

  1. ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
  2. ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิ์ใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
  3. ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

- การทดสอบหลังการใช้งาน (Post-Implementation Test)

  ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

- การสื่อสารการเปลี่ยนแปลง

  ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

10. ความปลอดภัยเกี่ยวกับการใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (IT Outsourcing)

วัตถุประสงค์ เพื่อเป็นการป้องกันสินทรัพย์ของบริษัทที่มีการเข้าถึงโดย IT Outsourcing และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

แนวทางปฏิบัติ

- ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัท
- ต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
- ในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ
- หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

11. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

แนวทางปฏิบัติ

- ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท
- ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน
- หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ
- กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว
- ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน

12. การใช้งานจดหมายอิเล็กทรอนิกส์

<u>วัตถุประสงค์</u> เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัท ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

<u>แนวทางปฏิบัติ</u>

- ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด
- หน่วยงานหรือผู้ปฏิบัติงานผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์เพื่อผลประโยชน์ของบริษัท
- ผู้ปฏิบัติงานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล
- ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ เว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
- การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
- การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
- การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท
- ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัท

- ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีการกระทำดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ หรือเจ้าของผู้ใช้บริการ เป็นผู้รับผิดชอบการกระทำดังกล่าว
- ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น
- ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัท
- การส่งข้อมูลข่าวสารที่เป็นความลับบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น และไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ปฏิบัติงานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ
- หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด เกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท
- การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัทไม่มีส่วนเกี่ยวข้องใดๆ

การบริหารความสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

ความเสี่ยงเกิดขึ้นได้จากหลายปัจจัยหลายรูปแบบ และการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการดำเนินงานก็อาจก่อให้เกิดความเสี่ยงต่อองค์กร โดยความเสี่ยงที่ให้ความสำคัญ ได้แก่ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (access risk) ความเสี่ยงด้านการบริหารจัดการระบบคอมพิวเตอร์ บุคลากรด้านคอมพิวเตอร์ ที่ไม่เหมาะสมเพียงพอ (infrastructure risk) ซึ่งความเสี่ยงดังกล่าว อาจก่อให้เกิดผลกระทบต่อองค์กรและภาคีได้ จึงต้องมีการประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อให้เกิดการจัดการความเสี่ยงอย่างเหมาะสม ทำให้เกิดความมั่นคงของระบบสารสนเทศอันเป็นหลักประกันว่าองค์กรจะมีระบบสารสนเทศให้ใช้งานได้อย่างต่อเนื่องไม่หยุดชะงักและมีความมั่นคงปลอดภัย

<u>วัตถุประสงค์</u>

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
2. เพื่อพิจารณาแนวทางป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ
3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอัตรายต่อระบบสารสนเทศ
4. เพื่อรับรองว่าการจัดเก็บสารสนเทศขององค์กรเป็นไปตามนโยบายและกฎหมายด้านความมั่นคงปลอดภัยและความลับส่วนบุคคล
5. เพื่อให้สอดคล้องกับแนวทางการบริหารความเสี่ยงขององค์กร

<u>แนวทาง</u>

1. องค์กรต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ(Information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง
    - มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ
    - มีการตรวจสอบประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
    - ให้มีการตรวจสอบประเมินความเสี่ยง โดยผู้ตรวจสอบภายในขององค์กร (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง
2. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
    - กำหนดให้มีการดำเนินการทบทวนปรับปรุงนโยบายระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศรวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศว่าสอดคล้องกับนโยบายหรือไม่
    - อย่างน้อยปีละ 1 ครั้ง ให้ประธานเจ้าหน้าที่บริหารทราบพร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง

- ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความมั่นคงปลอดภัย
- ควรมีเครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ระบบงานและเอกสารที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

3. กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ประมวลผลสารสนเทศจากบุคคลหรือหน่วยงานภายนอก
4. มีมาตรการสำหรับการตรวจประเมินระบบสารสนเทศ ดังนี้
   - มีการกำหนดข้อตกลงร่วมกันระหว่างผู้ตรวจสอบกับผู้ดูแลระบบและ/หรือเจ้าของระบบ
   - มีการทำสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบสามารถตรวจสอบได้จากข้อมูลสำเนา และมีการทำลายสำเนาทิ้งทันทีที่การตรวจสอบเสร็จสิ้น หรือหากมิได้ทำลายต้องมีการจัดเก็บไว้อย่างปลอดภัยและมีมาตรการป้องกันที่เหมาะสม
   - มีการจำกัดสิทธิ์ให้ผู้ที่ทำการตรวจสอบให้สามารถเข้าถึงข้อมูลได้โดยการอ่านเพียงอย่างเดียว
   - มีการกำหนดวิธีการจัดเก็บหลักฐานการตรวจสอบข้อมูลที่ปลอดภัย
   - มีการกำหนดขั้นตอนการปฏิบัติและหน้าที่ความรับผิดชอบของผู้ตรวจสอบอย่างชัดเจน
5. บุคลากรที่ทำหน้าที่เป็นผู้ตรวจสอบต้องมีการกำหนดให้เป็นอิสระแยกจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ
6. ให้มีการแปลผลการประเมินความเสี่ยงให้อยู่ในรูปแบบ risk map ตามแนวทางบริหารความเสี่ยงขององค์กร

แนวทางปฏิบัติในการประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวปฏิบัติในการประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ อันจะเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

<u>แนวทางปฏิบัติ</u>

1. จัดให้มีการตรวจสอบและประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง
   - มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
   - มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
   - มีการกำหนดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายใน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง
2. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้องค์กรได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศขององค์กร

- กำหนดให้มีการดำเนินการทบทวนปรับปรุงนโยบายระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศรวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศว่าสอดคล้องกับนโยบายหรือไม่อย่างน้อยปีละ 1 ครั้ง และรายงานให้คณะกรรมการบริหารความเสี่ยงทราบพร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยสารสนเทศมีจุดบกพร่อง
- ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความมั่นคงปลอดภัย
- ควรมีเครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ระบบงานและเอกสารที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

3. กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ประมวลผลสารสนเทศจากบุคคลหรือหน่วยงานภายนอก
4. มีมาตรการสำหรับการตรวจประเมินระบบสารสนเทศ ดังนี้
   - มีการกำหนดข้อตกลงร่วมกันระหว่างผู้ตรวจสอบกับผู้ดูแลระบบและ/หรือเจ้าของระบบ
   - มีการกำหนดขอบเขตในการตรวจสอบประเมิน
   - มีการกำหนดวิธีการในการตรวจสอบประเมินที่เหมาะสมกับขอบเขตที่ได้กำหนด
   - มีการทำสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบสามารถตรวจสอบได้จากข้อมูลสำเนา และมีการทำลายสำเนาทิ้งทันทีที่การตรวจสอบเสร็จสิ้น หรือหากมิได้ทำลาย ต้องมีการจัดเก็บไว้อย่างปลอดภัยและมีมาตรการป้องกันที่เหมาะสม
   - มีการจำกัดสิทธิ์ให้ผู้ที่ทำการตรวจสอบให้สามารถเข้าถึงข้อมูลได้โดยการอ่านเพียงอย่างเดียว
   - มีการกำหนดวิธีการจัดเก็บหลักฐานการตรวจสอบข้อมูลที่ปลอดภัย
   - มีการกำหนดขั้นตอนการปฏิบัติและหน้าที่ความรับผิดชอบของผู้ตรวจสอบอย่างชัดเจน
5. บุคลากรที่ทำหน้าที่เป็นผู้ตรวจสอบต้องมีการกำหนดให้เป็นอิสระแยกจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ และต้องเป็นผู้ที่มีความเชี่ยวชาญในการตรวจสอบประเมินเรื่องความมั่นคงปลอดภัยของระบบสารสนเทศ
6. ให้มีการแปลผลการประเมินความเสี่ยงให้อยู่ในรูปแบบ risk map ตามแนวทางบริหารความเสี่ยงขององค์กร

การบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

เนื่องจากองค์กรได้กำหนดแนวทางการป้องกันและเตรียมความพร้อมในการจัดการเมื่ออยู่ในภาวะวิกฤติ โดยต้องดำเนินการให้องค์กรดำเนินภารกิจได้อย่างต่อเนื่อง จึงได้กำหนดให้มีนโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ เพื่อการตอบสนองและบรรเทาผลกระทบต่อกระบวนการทำงานสำคัญที่มีการพึ่งพาระบบเทคโนโลยีสารสนเทศ ให้สามารถทำงานได้อย่างต่อเนื่องในระดับที่ได้มีการตกลงกันไว้กับผู้มีส่วนได้ส่วนเสีย

<u>วัตถุประสงค์</u>

- เพื่อให้มีการวิเคราะห์ วางแผน เตรียมการ ทบทวนและซักซ้อมกระบวนการต่างๆ ที่จำเป็น
- เพื่อให้สามารถใช้งานระบบสารสนเทศได้อย่างต่อเนื่องในระดับที่ได้มีการตกลงกันไว้ในภาวะฉุกเฉิน
- เพื่อให้ผู้มีส่วนได้ส่วนเสียได้เกิดความเข้าใจร่วมกัน และทราบถึงบทบาทหน้าที่ในการมีส่วนร่วมเมื่อเกิดเหตุฉุกเฉินหรืออุบัติการณ์

<u>แนวทางปฏิบัติในการบริหารจัดการความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ</u>

การบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ หมายถึง การจัดเตรียมกระบวนการหรือระบบสำรองเพื่อให้สามารถใช้งานทดแทนเมื่อระบบหลักเกิดการหยุดชะงักในภาวะฉุกเฉินในระดับที่ได้มีการตกลงกันไว้ ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด(MTPD : Maximum Tolerable Period of Disruption) ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO : Recovery Time Objective) เป้าหมายของการฟื้นคืนสภาพ (RPO : Recovery Point Objective) และทำการฟื้นฟูระบบหลักให้กลับคืนสู่สภาวะปกติให้ได้

ทางองค์กรจึงกำหนดนโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ให้มีนโยบายแนวทางปฏิบัติ หรือขั้นตอนปฏิบัติของการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย แนวปฏิบัติและมาตรฐานสากลของการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ดังนี้

- จัดให้มีคณะทำงานบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศที่สอดคล้องตามแนวทางการบริหารความต่อเนื่องในการดำเนินงานขององค์กร โดยมีการวางแผน การนำไปปฏิบัติ การฝึกซ้อม และการปรับปรุงแก้ไขอย่างต่อเนื่อง
- จัดให้มีการทำงานร่วมกับคณะกรรมการบริหารความเสี่ยง และคณะอนุกรรมการควบคุมภายใน ที่มีหน้าที่กำกับดูแลการพัฒนาระบบการบริหารความต่อเนื่องดำเนินงานขององค์กรในภาพรวม
- จัดให้มีการทำงานร่วมกับส่วนงานที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัย โดยประสานความเชื่อมโยงกันของแต่ละขอบข่ายที่พึ่งพาระบบสารสนเทศในการจัดทำแผนป้องกัน / ระงับเหตุฉุกเฉิน รวมทั้งร่วมเป็นคณะทำงานในโครงสร้างศูนย์อำนวยการเหตุฉุกเฉิน และภาวะวิกฤต
- จัดให้มีการพัฒนาระบบการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศตามขอบข่ายที่รับผิดชอบ โดยมีการวางแผน การนำไปปฏิบัติ การฝึกซ้อม และปรับปรุงแก้ไขอย่างต่อเนื่อง รวมทั้งจัดทำและกำหนดผู้รับผิดชอบในการจัดทำแผนเพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญต่อการดำเนินงานของระบบเทคโนโลยีสารสนเทศ และรายงานผลการดำเนินงานต่อคณะกรรมการบริหารความเสี่ยงและควบคุมภายในทราบเป็นระยะๆ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

- จัดให้ผู้บริหาร/ผู้บังคับบัญชามีหน้าที่รับผิดชอบ ผลักดัน และสนับสนุนการดำเนินงานด้านต่างๆ ตามกระบวนการการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ รวมทั้งเสริมสร้างและพัฒนาความรู้ความสามารถของบุคลากรที่เกี่ยวข้องเพื่อให้มั่นใจว่าบุคลากรสามารถปฏิบัติงานได้อย่างมีประสิทธิผล
- จัดให้ผู้บริหาร เจ้าหน้าที่ บุคลากร ลูกจ้าง และผู้เกี่ยวข้อง ได้รับความรู้และความตระหนักถึงการมีส่วนร่วมที่จะทำให้ การบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศบรรลุวัตถุประสงค์ของการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

<u>ขอบเขตของนโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ</u>

ขอบเขตของกระบวนการ การให้บริการ สถานที่ปฏิบัติงาน ความต้องการด้านความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ตลอดจนการให้บริการสารสนเทศที่ใช้สนับสนุนกระบวนการที่สำคัญที่จะถูกรวมอยู่ในขอบเขตของนโยบายนี้ สามารถพิจารณาได้จากปัจจัยที่มีความสำคัญ มีกระบวนการทำงานที่มีการพึ่งพาระบบสารสนเทศ

- กระบวนการทำงานที่มีการพึ่งพาระบบสารสนเทศที่สำคัญ ได้แก่ กระบวนงานในระบบบริหารโครงการ, ระบบบัญชีการเงินเบิกจ่าย, ระบบจัดเก็บเอกสารและระบบสารบรรณอิเล็กทรอนิกส์, เว็บไซต์หลักของสำนักงานฯ
- ระดับความสำคัญของการกู้คืนระบบเทคโนโลยีสารสนเทศ
- ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (MTPD) และระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO)
- เกี่ยวกับระยะเวลาในขั้นตอนการทำสัญญา, การเบิกจ่ายทางการเงินและบัญชี กับการทำโครงการต่างๆ
- ฝ่ายเทคโนโลยีสารสนเทศในด้านที่เป็นผู้ทำหน้าที่เป็นผู้ให้บริการสารสนเทศพื้นฐานให้กับสำนักงานฯ ได้แก่ การเป็นผู้ให้บริการระบบสารสนเทศ คอมพิวเตอร์ และอุปกรณ์เครือข่าย
- ความเสี่ยงสำคัญในสถานที่ปฏิบัติงานหลัก ซึ่งอาจก่อให้เกิดผลกระทบต่อการให้บริการระบบงานที่สำคัญ ได้แก่ ห้องปฏิบัติการเครื่องแม่ข่ายและอุปกรณ์เครือข่ายในสำนักงานฯ
- ความเสี่ยงสำคัญในการพึ่งพาการบริการด้านเทคโนโลยีจากผู้ให้บริการรายหนึ่งรายใด

แนวทางปฏิบัติในการฟื้นคืนสภาพจากภัยพิบัติ (Disaster Recovery Plan Guideline)

องค์กรมีการสำรองข้อมูลที่สำคัญ โดยกำหนดรูปแบบและแนวทางปฏิบัติ รวมทั้งแผนสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของสารสนเทศ เพื่อป้องกันการสูญหายอันอาจเกิดขึ้นจากภาวะคุกคาม หรือจากการเกิดภัยพิบัติ โดยมอบหมายผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบ แผนการ และแนวทางปฏิบัติที่กำหนดไว้ เพื่อกำหนดเป็นมาตรฐานในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย หรือเครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย การเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืน หรือฟื้นฟูสภาพ ได้ภายในระยะเวลาที่เหมาะสม

วัตถุประสงค์

แนวทางปฏิบัติในการฟื้นคืนสภาพจากภัยพิบัตินี้ ใช้เพื่อเป็นแนวทางในการดำเนินงานของการฟื้นคืนสภาพด้วยวิธีการทางอิเล็กทรอนิกส์อย่างมีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปตามมาตรฐาน และระเบียบปฏิบัติที่เกี่ยวข้อง รวมถึงสอดคล้องกับนโยบายการบริหารความต่อเนื่องในการดำเนินงานขององค์กร โดยให้บุคลากรที่เกี่ยวข้องได้รับทราบและปฏิบัติตามอย่างเคร่งครัด

แนวทางปฏิบัติ

แนวทางปฏิบัติการฟื้นคืนสภาพจากภัยพิบัติ ในเอกสารฉบับนี้ ประกอบไปด้วย

1. แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment)
2. แนวทางในการสำรองข้อมูล
3. แนวทางในการกู้คืนระบบ
4. แนวทางในการซ้อมแผนการบริหารความต่อเนื่องของระบบสารสนเทศ

<u>แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment)</u>

- จัดให้มีการระบุภัยคุกคามที่สำคัญที่เกิดขึ้นในปัจจุบัน และอาจจะเกิดขึ้นในอนาคต โดยภัยคุกคามที่ถูกระบุจะขึ้นอยู่กับลักษณะของกระบวนงานหลัก อาจคำนึงถึงความเสี่ยงโดยทั่วไปด้านความต่อเนื่องในการดำเนินงานที่รวบรวมโดยสถาบันอันเป็นที่ยอมรับในระดับสากล เช่น Business Continuity Institute (BCI) เป็นต้น
- จัดให้มีคณะทำงานบริหารความเสี่ยง ทำหน้าที่ร่วมกันระบุภัยคุกคาม โดยพิจารณาปัจจัยจากภายในองค์กร เช่น บุคลากร ระบบโครงสร้างพื้นฐานของอาคาร ปัจจัยจากภายนอกองค์กร เช่น การสื่อสารและการโทรคมนาคม ภัยธรรมชาติการโจมตีระบบโดยผู้ไม่ประสงค์ดี เป็นต้น
- จัดให้มีการประเมินและวัดระดับความเสี่ยงเป็นขั้นตอนที่ช่วยในการจัดลำดับความเสี่ยง โดยเรียงลำดับความเสี่ยงสูงสุดไปจนถึงความเสี่ยงต่ำสุด การประเมินระดับความเสี่ยงจะอาศัยพื้นฐานในการพิจารณาความสัมพันธ์ของผลกระทบ (Impact) และโอกาสที่จะเกิด (Probability) ตามหลักเกณฑ์การประเมินความเสี่ยงที่ได้ตกลงร่วมกัน และสามารถคำนวณได้จาก ระดับความเสี่ยง = โอกาสที่จะเกิด x ผลกระทบ
- จัดให้มีการกำหนดเงื่อนไขที่ใช้ในการจัดลำดับความเสี่ยง และจัดลำดับความสี่ยงจากมากไปหาน้อย เพื่อใช้ประโยชน์ในการพิจารณาเลือกภัยคุกคามที่สำคัญ และจัดทำแผนตอบสนองอุบัติการณ์
- จัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และอาจส่งผลกระทบต่อองค์กร เช่น ระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย หรือการเกิดความเสียหายจากภัยธรรมชาติต่างๆ เป็นต้น
- จัดให้มีการจัดทำแผนตอบสนองอุบัติการณ์ โดยพิจารณาเลือกจากภัยคุกคามที่มีผลการประเมินความเสี่ยงอยู่ในขอบเขตการเฝ้าระวัง (Amber Zone) ได้แก่ ภัยคุกคามที่มีผลกระทบอยู่ในระดับสูง แต่มีโอกาสที่จะเกิดภัยคุกคามอยู่ในระดับต่ำ ซึ่งอ้างอิงตามแนวทางอันเป็นที่ยอมรับในระดับสากลคือ Good Practice Guideline 2008 ของสถาบัน Business Continuity Institute (BC)
- จัดให้มีการจัดทำรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ และข้อเสนอแนะ เพื่อนำเสนอต่อคณะทำงานบริหารความเสี่ยง

<u>แนวทางในการสำรองข้อมูล</u>

จัดให้มีการกำหนดระบบเทคโนโลยีสารสนเทศในการสำรองข้อมูลที่สอดคล้องกับความเสี่ยงต่างๆ ที่จะเกิดขึ้นกับระบบสารสนเทศ อาจได้แก่ การโจมตีระบบโดยผู้ไม่ประสงค์ดี การเกิดอัคคีภัย อุทกภัย และอุบัติภัยต่างๆ โดยคำนึงถึงผลกระทบของความเสี่ยงการยอมรับได้ของการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ และงบประมาณของฝ่ายเทคโนโลยีสารสนเทศให้ได้ข้อสรุปว่าจะทำการสำรองและการกู้คืนระบบในรูปแบบเทคโนโลยีใด โดยทางองค์กรจะจัดการเช่าสถานที่สำรองไว้ที่ Data center ที่มีมาตรฐานสำหรับการทำ Disaster Recovery Site และจัดซื้อหรือเช่าอุปกรณ์ที่จำเป็นในการปฏิบัติการของการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายและอินเตอร์เน็ต และมี Private Link เชื่อมโยงจากสถานที่หลักไปยังสถานที่สำรองดังกล่าว ตามแนวทางที่ได้ตกลงกันไว้และให้ใช้งานระบบสำรองได้ภายในระยะเวลาที่ยอมรับได้การทำ Disaster Recovery Site มี 5 รูปแบบ ดังต่อไปนี้

1. Hot Site คือ สามารถทำงานได้ทันทีโดยที่อุปกรณ์ในสถานที่หลักและสถานที่สำรองทำงานควบคู่กันไป เมื่อเกิดเหตุอุบัติภัยขึ้นสามารถที่จะดำเนินงานตามปกติได้ทันที
2. Warm Site คือ สามารถทำงานได้ต่อเมื่อ เมื่อเกิดเหตุอุบัติภัยขึ้นจะต้องทำการติดตั้งอุปกรณ์ต่างๆ ก่อนจึงจะสามารถดำเนินงานได้ตามปกติ
3. Cold Site คือ เมื่อเกิดเหตุอุบัติภัยขึ้น จึงทำการซื้อหรือเช่าอุปกรณ์ต่างๆ ใหม่ เช่น เครื่องคอมพิวเตอร์แม่ข่าย และจะต้องทำการติดตั้งระบบสารสนเทศใหม่ทั้งหมด ใช้เวลานานพอสมควรในการขึ้นระบบเทคโนโลยีสารสนเทศ
4. Standby site คือ จัดการสรรหาสถานที่ ยังมิได้ดำเนินการใด ๆ ทั้งสิ้น
5. Nothing คือ ไม่มีการดำเนินการทำระบบสำรองใดๆทั้งสิ้น

รูปแบบเทคโนโลยีที่ใช้การสำรองและกู้คืนระบบแบ่งออกได้เป็น 3 แบบ ดังต่อไปนี้

1. Automation ใช้เวลาในการกู้คืนระบบเป็นระยะเวลาวินาที สามารถทำการสำรองข้อมูลทันที
2. Replication ใช้เวลาในการกู้คืนระบบเป็นระยะเวลาชั่วโมง จะทำการคัดลอกสำเนาข้อมูลไปเก็บไว้ที่ปลายทางและทำการขึ้นระบบแบบ Manual
3. Restore ใช้เวลาในการกู้คืนระบบเป็นระยะเวลา เป็นวันหรือสัปดาห์ เป็นการกู้ข้อมูลจากสื่อบันทึกประเภทต่างๆ เช่น เทป หรือ ดิสก์

เครื่องมือหรือโปรแกรมในการสำรองและกู้คืนระบบสารสนเทศ

ผู้ดูแลระบบและพัฒนาแผนกู้คืนระบบเทคโนโลยีสารสนเทศ มีหน้าที่จัดหาเครื่องมือในการใช้สำรองและกู้คืนระบบสารสนเทศตามงบประมาณที่ได้รับการจัดสรรในการทำการสำรองข้อมูลในองค์กรที่สำคัญ รวมถึงซอฟต์แวร์ที่ใช้ประกอบในการสำรองข้อมูลสำคัญในองค์กร มีขั้นตอนการปฏิบัติการดังนี้

<u>การสำรองข้อมูล</u>

1. ต้องสำรองข้อมูลสำคัญในการดำเนินกิจการ รวมถึงซอฟต์แวร์ระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ชุดคำสั่งที่ใช้ทำงาน และข้อมูลสำคัญให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง
2. มีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยควรมีรายละเอียด ดังนี้
   - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง

- ประเภทสื่อบันทึก
- จำนวนและความถี่ที่ต้องสำรอง
- ขั้นตอนและวิธีการสำรองข้อมูลโดยละเอียด
- สถานที่และวิธีการเก็บรักษาสื่อบันทึก

3. มีการบันทึกการปฏิบัติงานเกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วนและควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ (Operator logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก
4. มีการรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นรวมทั้งวิธีการที่ใช้แก้ไขด้วย
5. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของสำนักงานฯ จากจำเป็นมากไปหาน้อย
6. ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
7. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนทศได้ตามปกติอย่างต่อเนื่องโดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
8. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
9. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
10. ระบุความถี่ของการปฏิบัติในแต่ละข้อ ให้มีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้จากผู้เกี่ยวข้อง
11. จัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศขององค์กร
12. พิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ ตามลำดับความสำคัญ
13. จัดให้มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล
14. จัดให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้
15. มีขั้นตอนปฏิบัติในการสำรองข้อมูลและกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้องทั้งซอฟต์แวร์ โปรแกรมประยุกต์ และข้อมูลในระบบสารสนเทศ
16. มีขั้นตอนปฏิบัติในการตรวจสอบปัญหา ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหาและรายงานต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ
17. กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม และการสำรองข้อมูลแบบส่วนต่าง
18. จัดให้มีการเข้ารหัสข้อมูลในการสำรองข้อมูลที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

19. ต้องปฏิบัติตามขั้นตอนปฏิบัติ ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูลโดยเคร่งครัด

<u>การเก็บรักษาข้อมูลสำรอง</u>

1. ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง ในสถานที่จัดเก็บข้อมูลสำรองที่ได้มาตรฐาน ติดตั้งอยู่สถานที่อื่นหรือตามความจำเป็น
2. ดำเนินการสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหาย (Physical Security)
3. ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคต ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน เช่น เมื่อจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ต้องเก็บอุปกรณ์ ซอฟต์แวร์หรือโปรแกรมประยุกต์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น
4. จัดทำรายการหรือบัญชีที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองหรือบนระบบบันทึก เพื่อให้สามารถค้นหาได้โดยเร็วและป้องกันการใช้งานข้อมูลสำรองผิดพลาด
5. จัดทำทะเบียนคุมการรับและส่งมอบข้อมูลสำรอง โดยมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูลและเวลาการขอใช้งานข้อมูลสำรอง ต้องได้รับอนุมัติจากผู้มีอำนาจ
6. จัดทำขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว รวมถึงข้อมูลลับต่างๆ ที่อาจยังค้างอยู่ในสื่อบันทึก เช่น ใน Recycle bin ของระบบปฏิบัติการ เป็นต้น

<u>การทดสอบข้อมูลสำรอง</u>

1. กำหนดขั้นตอนการปฏิบัติของการทดสอบข้อมูลสำรอง ทั้งซอฟต์แวร์ระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ชุดคำสั่งที่ใช้ทำงาน และข้อมูลโดยปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
2. กำหนดแผนการทดสอบและปฏิบัติการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ โดยทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งซอฟต์แวร์และโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้
3. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องกู้คืนระบบ ผู้ดูแลระบบต้องดำเนินการแก้ไข พร้อมทั้งรายงานผลการแก้ไข บันทึกและสรุปผลการปฏิบัติงานต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

<u>แนวทางในการกู้คืนระบบ</u>

1. กำหนดให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม
2. แจ้งผู้ใช้ระบบทราบทันที เมื่อพบว่าความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย มีผลกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ และรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์
3. ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้คณะทำงานบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศแจ้งเหตุไปยังคณะทำงานบริหารความต่อเนื่องในการดำเนินงานขององค์กรเพื่อดำเนินการต่อไป

4. บันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหา
5. กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ 1 ครั้ง

แนวทางในการซ้อมแผนการบริหารความต่อเนื่องของระบบสารสนเทศ

การเตรียมพร้อมกรณีฉุกเฉิน

1. จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบ หรือฟื้นฟูสภาพระบบและข้อมูลมาได้ภายในระยะที่เหมาะสม หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว เพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้
   - จัดลำดับความสำคัญของระบบงาน ข้อมูล ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้คืนแต่ละระบบงาน
   - กำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
   - มีขั้นตอนการกู้คืนระบบและข้อมูลโดยละเอียดในแต่ละสถานการณ์
   - กำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
   - ระบุรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ค่ากำหนดการทำงาน (System configuration) ระบบเครือข่ายและอุปกรณ์เครือข่ายที่ต้องใช้งาน เป็นต้น
   - ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน ในกรณีที่มีศูนย์คอมพิวเตอร์สำรอง เช่น สถานที่ตั้ง แผนที่ การอนุญาตให้เข้าถึงสถานที่ เป็นต้น
   - ปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินสำเนาไว้นอกสถานที่
2. จัดให้มีการทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และบันทึกผลการทดสอบ หรือการรายงานผลด้วย
3. จัดให้มีมาตรการเพื่อการสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบ เฉพาะเท่าที่จำเป็น
4. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศเพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ
5. ทดสอบ ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง
6. บันทึกเหตุการณ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น โดยพิจารณาถึง ประเภท ปริมาณและหลักฐานสำหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย
7. ระบุรายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉินนี้ ควรมีสาระครอบคลุมภัยพิบัติหรือสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีหัวข้อสำคัญ ดังนี้
   - การเตรียมการเบื้องต้น
   - ผู้รับผิดชอบ
   - มาตรการความปลอดภัยและแผนดำเนินงานในการนำระบบคอมพิวเตอร์กลับสู่สภาพปกติ เมื่อเกิดความเสียหายหรือหยุดทำงาน

การจัดชั้นความลับของข้อมูล

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรฐานในการป้องกันสารสนเทศของบริษัทฯ โดยมีการจัดชั้นความลับจัดทำป้ายชื่อและบริหารจัดการสารสนเทศอย่างเหมาะสม การจัดชั้นความลับสารสนเทศที่ใช้ในการปฏิบัติงานภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ต้องทำบัญชีสารสนเทศของหน่วยงานและระบุชั้นความลับให้ชัดเจนเพื่อใช้ในการกำหนดระดับความสำคัญและวิธีการป้องกันที่เหมาะสม รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศแต่ละชนิด

<u>แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ</u>

1. ในหน่วยงานภายใน ต้องจัดให้มีวิธีการกำหนดประเภทข้อมูลและจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับตามแนวทางบริษัทฯ และระเบียบที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้
   1.1 ผู้ใช้งานต้องแบ่งประเภทของข้อมูลและชั้นความลับของข้อมูล ออกเป็น 3 ระดับ คือ
      - ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
      - ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
      - ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้
   1.2 ผู้ใช้งานต้องพิจารณาองค์ประกอบต่อไปนี้เพื่อเป็นแนวทางกำหนดชั้นความลับของข้อมูล
      - ความสำคัญของเนื้อหา เช่น เนื้อหาของข้อมูลนั้นมีความสำคัญต่อบริษัทฯ มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือ ข้อมูลลับ เป็นต้น
      - แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับจะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับจะเป็น ข้อมูลทั่วไป เปิดเผยได้ เป็นต้น
      - วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านการเงินของบริษัทฯ ดังนั้นข้อมูลนี้จะอยู่ในประเภท ข้อมูลลับที่สุด เป็นต้น
      - จำนวนบุคคลที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งาน ข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็น ข้อมูลทั่วไป เปิดเผยได้ เป็นต้น
      - ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการเงิน ด้านการปฏิบัติตามกฎระเบียบข้อยังคับที่องค์กรต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้น ข้อมูลสามารถจัดอยู่ในชั้นความลับประเภท ข้อมูลลับที่สุด เป็นต้น
      - หน่วยงานที่รับผิดชอบในฐานะเจ้าของเรื่อง เช่น ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใดจะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น
      - การดำเนินการกับข้อมูลลับ (ถ้ามี) เจ้าของข้อมูลลับต้องดำเนินการจัดทำทะเบียนข้อมูลลับที่ตนเองดูแลหรือรับผิดชอบ ซึ่งมีรายละเอียดประกอบด้วย
        - ชื่อของข้อมูล
        - ระดับชั้นความลับและระดับชั้นการเข้าถึง
        - ชื่อเจ้าของข้อมูลลับ
        - หน่วยงานภายในที่สามารถเข้าถึงได้

- หน่วยงานภายนอกที่อนุญาตให้เข้าถึงได้
- สถานที่จัดเก็บข้อมูล
- ช่องทางการเข้าถึง
- ระยะเวลาการเก็บรักษาข้อมูล
- ระยะเวลาที่ได้เข้าถึง

- พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ตามความจำเป็นปรับปรุงทะเบียนข้อมูลลับให้ถูกต้องและทันสมัย และต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูลหรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้ง เพื่อแก้ไขชั้นความลับให้ถูกต้อง
- ในการจัดทำหรือจัดเตรียมข้อมูลลับให้ผู้ใช้งาน ปฏิบัติดังนี้
    - จัดทำหรือจัดเตรียมข้อมูลในสถานที่ปลอดภัย เช่น จัดทำภายในส่วนสำนักงาน ไม่จัดทำในสถานที่สาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่จัดทำได้ และจำกัดบุคคลเฉพาะผู้ที่เกี่ยวข้องในการเข้าถึงข้อมูล
    - ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว เช่น กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์จะต้องทำการลบหรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้ (ดูวิธีการทำลายในตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูล) หากไม่ทำลาย ต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย
    - จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน เช่น มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้ามีจุดประสงค์ เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมด หากมีการสูญหายไปหน้าใดหน้าหนึ่งจะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้)
- ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติดังนี้
    - แสดงชั้นความลับของข้อมูล (ซึ่งประกอบด้วย "ลับ" "ลับมาก" หรือ "ลับที่สุด") ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Hard Disk, Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่นๆ
    - แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด
- ในการทำสำเนาหรือแจกจ่ายข้อมูลลับ ให้ปฏิบัติดังนี้
    - ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทางซึ่งเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น
    - แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตก่อน
- ในการเก็บรักษาเอกสารลับ ให้ปฏิบัติดังนี้

- จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับ และนำไปเก็บไว้ในตู้เก็บเอกสารลับโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ
- ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่นๆ เช่น ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลที่เปิดเผยได้
- จัดเก็บแฟ้มข้อมูลลับไว้ในตู้และปิดล็อคด้วยกุญแจที่แข็งแรงและมั่นคง

- ในการยืมหรือขอเข้าถึงข้อมูลลับ ให้ปฏิบัติดังนี้
  - เมื่อมีการขอยืมหรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้หัวหน้าของส่วนงานที่รับผิดชอบเป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อนว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย และแจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำการสำเนาเพิ่มเติม
  - เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าของส่วนงานที่รับผิดชอบกำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศ ให้ทำการยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที
- ในการส่งเอกสารลับทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้ปฏิบัติตามระเบียบการส่งเอกสารลับของ สบน. เพื่อตรวจสอบที่อยู่ E-Mail ของผู้รับปลายทางให้ถูกต้องก่อนจัดส่งไฟล์ข้อมูลนั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคล
- ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ ตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูล
- ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้
  - จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ (E-File) ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ เช่น การทำสัญลักษณ์ลายน้ำและแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
  - การสำเนา E-File ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล
  - ระมัดระวังการเผยแพร่ หรือแจกจ่าย E-File ที่เป็นความลับของบริษัทฯ ยังกลุ่มผู้รับ ต้องเฉพาะกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น
  - ผู้เป็นเจ้าของ E-File ต้องตรวจสอบความถูกต้องของ E-File ก่อนนำไปใช้งาน
  - ห้ามผู้เป็นเจ้าของ E-File ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นแต่จะได้ใช้วิธีเข้ารหัสที่บริษัทกำหนดไว้
  - ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัยและไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์

- ห้ามแบ่งปัน (Share) ไฟล์ข้อมูลลับบนเครือข่ายสาธารณะ (Internet) ของบริษัทฯ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)
- ตรวจสอบการทำงานของระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับอย่างสม่ำเสมอว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้ง โปรแกรมสำนักงานเพื่อแก้ไขช่องโหว่ของโปรแกรมในเครื่องตามปกติหรือไม่
- สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ หรือตามความจำเป็น
- ต้องทำลาย E-File บนหน่วยความจำหลัก (Hard disk) ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

-

การขอยกเว้นเกี่ยวกับนโยบายการรักษาความมั่งคงปลอดภัยด้านสารสนเทศ

<u>วัตถุประสงค์</u>

เพื่อกำหนดกระบวนการและแนวทางในการขออนุมัติยกเว้นการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในกรณีที่มีความจำเป็น โดยยังคงมุ่งเน้นการลดความเสี่ยงที่อาจเกิดขึ้นเพื่อให้ผู้ปฏิบัติงาน เจ้าของข้อมูล เจ้าของระบบ สามารถใช้ข้อมูลสารสนเทศ ระบบสารสนเทศ และเครือข่ายของบริษัท ในการดำเนินกิจกรรมของบริษัทได้อย่างเหมาะสม

<u>แนวทางปฏิบัติ</u>

1. เมื่อผู้ปฏิบัติงาน เจ้าของข้อมูล เจ้าของระบบ ที่ใช้ข้อมูลสารสนเทศ ระบบสารสนเทศ และเครือข่ายของบริษัท มีเหตุผลและความจำเป็นที่จะไม่ปฏิบัติตามนโยบายการรักษาความมั่งคงปลอดภัยด้านสารสนเทศให้จัดทำเอกสารเพื่อขอพิจารณายอมรับความสี่ยง
2. ต้องมีการระบุระยะเวลาที่ต้องการยกเว้น และระบุวันที่สิ้นสุดของการยกเว้นให้ชัดเจน
3. ต้องแสดงให้เห็นว่ามีมาตรการลดความเสี่ยงทดแทนในระหว่างที่ยกเว้น เช่น การตรวจสอบด้วยมือ, การใช้ซอฟต์แวร์สำรอง หรือการติดตามอย่างใกล้ชิด
4. ต้องระบุผลกระทบที่อาจเกิดขึ้นต่อระบบ, ข้อมูล, และองค์กรในกรณีที่อนุมัติการยกเว้น
5. นำเสนอและขอเห็นชอบจากหัวหน้าหน่วยงาน และหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ จากนั้นนำเสนอประธานเจ้าหน้าที่บริหารเพื่อขออนุมัติ

นโยบายเทคโนโลยีสารสนเทศฉบับนี้ได้รับอนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2568 และให้มีผลบังคับใช้ตั้งแต่วันที่ 25 กุมภาพันธ์ 2568 เป็นต้นไป