นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ส่วนที่ 1.1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่างๆ โดยองค์กรต้องจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวทางปฏิบัติดังนี้

1.1.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Management Directions for Information Security)

1) นโยบายสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Policy for Information Security)
   1.1) องค์กรต้องจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากประธานกรรมการบริษัท หรือผู้บริหารระดับสูงที่ประธานกรรมการบริษัทมอบหมายให้เป็นผู้อนุมัติ
   1.2) องค์กรต้องเผยแพร่นโยบายดังกล่าวให้ผู้ใช้งานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบและถือปฏิบัติเป็นไปตามที่นโยบายกำหนด โดยการเผยแพร่ต้องดำเนินการในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย

2) การทบทวนนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Review of the Policies for Information Security)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องดำเนินการตรวจสอบ และทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามเงื่อนไขที่กำหนดไว้

ส่วนที่ 1.2 การจัดโครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่างๆ ภายในองค์กร และเพื่อเป็นแนวทางควบคุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1.2.1 การจัดโครงสร้างภายในองค์กร (Internal Organization)

1) การกำหนดบทบาทและหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities)
   1.1) ผู้บริหารระดับหน่วยงานต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศสำหรับบุคลากรในหน่วยงานอย่างเป็นลายลักษณ์อักษร และให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำหนดไว้

2) การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)
   2.1) ผู้บริหารระดับหน่วยงานต้องกำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ ในการปฏิบัติงานด้านต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจน เพื่อให้มีการสอบทานระหว่างกันได้

3) การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องด้านความมั่นคงปลอดภัย (Contact with authorities)
   3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อและช่องทางการติดต่อของหน่วยงานที่จำเป็น เช่น หน่วยงานด้านกฎหมาย หรือหน่วยงานที่เกี่ยวข้อง เป็นต้น สำหรับติดต่อเมื่อเกิดเหตุฉุกเฉิน พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

4) การประสานงานกับกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Contact with special interest groups)
   4.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และเพิ่มช่องทางการรับข่าวสารจากกลุ่มผู้เชี่ยวชาญ เพื่อให้สามารถติดต่อประสานงาน หรือรับข้อมูลข่าวสาร หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศได้ทันท่วงที พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

5) การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ (Information Security in Project Management)
   5.1) ผู้บริหารระดับหน่วยงานต้องกำหนดให้มีการควบคุมความเสี่ยง การติดตามการดำเนินงานโครงการ รวมถึงการประเมินภาพรวมในการดำเนินงานโครงการ ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก

1.2.2 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile Computing and Teleworking)

1) การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communication)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีมาตรการที่เหมาะสมเพื่อรับรองความปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ขององค์กร และเมื่อนำอุปกรณ์ออกไปใช้งานนอกสถานที่
   1.2) ผู้ใช้งานที่มีการใช้งานอุปกรณ์สื่อสารประเภทพกพาเพื่อเชื่อมต่อกับระบบสารสนเทศขององค์กรทั้งหมดต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และตระหนักถึงการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด
2) การปฏิบัติงานภายนอกสำนักงาน (Teleworking)
   2.1) ผู้ใช้งานที่มีการทำงานจากภายนอกสำนักงานทั้งหมด จะต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรเช่นเดียวกันกับการทำงานภายในสำนักงาน
   2.2) ผู้ใช้งานที่มีการใช้ข้อมูลสารสนเทศขององค์กรในการทำงานนอกสำนักงาน หรือการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากเจ้าของข้อมูลสารสนเทศ และหน่วยงานต้นสังกัดโดยต้องมีเหตุผลอันควร
   2.3) ผู้ใช้งานที่ต้องการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งาน

ส่วนที่ 1.3 การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม การกำกับ และติดตามการสรรหาบุคลากรเข้ามาปฏิบัติงานภายในองค์กร การบริหารจัดการบุคลากรระหว่างการจ้างงาน และการบริหารจัดการบุคลากรเมื่อพ้นสภาพการเป็นลูกจ้างหรือเมื่อมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงาน

1.3.1 การบริหารจัดการบุคลากรก่อนการจ้างงาน (Prior to Employment)

1) การตรวจสอบประวัติ (Screening)
   1.1) องค์กรต้องกำหนดให้มีการตรวจสอบประวัติของผู้สมัครงานและหน่วยงานภายนอกที่ต้องเข้ามาให้บริการภายในหน่วยงาน
2) ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)
   2.1) หน่วยงานบริหารทรัพยากรบุคคล ต้องกำกับให้มีการลงนามในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของบุคลากร หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ซึ่งได้มีการระบุหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญาหรือข้อตกลงการปฏิบัติงาน ซึ่งผู้ใช้งานต้องรับทราบและยอมรับระเบียบปฏิบัติขององค์กร โดยจะต้องอ่านทำความเข้าใจและปฏิบัติตามนโยบาย กฎ ระเบียบที่องค์กรได้กำหนดไว้

1.3.2 การบริหารจัดการบุคลากรระหว่างการจ้างงาน (During employment)

1) หน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Management Responsibilities)
   1.1) ผู้บริหารระดับหน่วยงานต้องกำหนดให้มีการควบคุม และกำกับให้บุคลากร หรือหน่วยงานภายนอกที่ได้รับการว่าจ้างเพื่อปฏิบัติงานหรือให้บริการกับองค์กร ปฏิบัติงานตามนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่องค์กรได้ประกาศใช้
2) การอบรม การสร้างความตระหนัก การให้ความรู้ในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information security awareness, education and training)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดช่องทางให้บุคลากรสามารถทำการศึกษาและทำความเข้าใจในนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ บทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของตนเองก่อนที่จะอนุญาตให้เริ่มต้นปฏิบัติงานกับองค์กร
   2.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไปโดยหน่วยงานผู้รับผิดชอบ เพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เช่น วิธีการใช้ระบบงาน วิธีการใช้งานซอฟต์แวร์สำเร็จรูป การแก้ปัญหาการใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง เป็นต้น
   2.3) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดการอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยเพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เพื่อช่วยให้ผู้รับการว่าจ้างสามารถปฏิบัติงานที่ตนเองรับผิดชอบได้เป็นอย่างดีและอย่างมั่นคงปลอดภัย
3) กระบวนการลงโทษทางวินัย (Disciplinary Process)
   3.1) องค์กรต้องจัดให้มีกระบวนการลงโทษทางวินัย เพื่อลงโทษผู้ใช้งานที่ฝ่าฝืนหรือละเมิดนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

1.3.3 การสิ้นสุดการจ้างงานหรือโยกย้ายตำแหน่งงาน (Termination or Change of Employment)

1) การบริหารจัดการบุคลากรพ้นสภาพหรือเปลี่ยนหน้าที่ความรับผิดชอบในการปฏิบัติงาน (Termination or Change of Employment Responsibilities)
   1.1) หน่วยงานบริหารทรัพยากรบุคคล ต้องกำหนดกฎระเบียบและความรับผิดชอบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรและหน่วยงานภายนอกภายหลังจากที่พ้นสภาพการจ้างงาน หรือมีการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน อย่างเป็นลายลักษณ์อักษร
   1.2) หน่วยงานบริหารทรัพยากรบุคคล ต้องควบคุมดูแลให้บุคลากร และหน่วยงานภายนอก ปฏิบัติตามกฎระเบียบที่กำหนดไว้อย่างเคร่งครัด

ส่วนที่ 1.4 การบริหารจัดการทรัพย์สิน (Asset Management)

วัตถุประสงค์

เพื่อให้สินทรัพย์และระบบสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม เพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลขององค์กรโดยไม่ได้รับอนุญาต รวมถึงป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์ และเกิดความเสียหายกับทรัพย์สินสารสนเทศขององค์กร

1.4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)

1) การจัดทำบัญชีทรัพย์สิน (Inventory of Assets)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมให้หน่วยงานภายในหน่วยงานจัดทำบัญชีทรัพย์สินสารสนเทศเพื่อบริหารจัดการและควบคุมทรัพย์สินสารสนเทศอย่างเหมาะสม และให้มีการปรับปรุงบัญชีทรัพย์สินให้เป็นปัจจุบันอยู่เสมอ
2) การระบุผู้ถือครองทรัพย์สิน (Ownership of Assets)
   2.1) ผู้บังคับบัญชา หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการระบุผู้ถือครองทรัพย์สิน ผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม
3) การใช้ทรัพย์สินสารสนเทศ (Acceptable Use of Assets)
   3.1) หน่วยงานเทคโนโลยีสารสนเทศต้องจัดทำข้อกำหนดในการใช้ทรัพย์สิน เพื่อการบริหารจัดการอุปกรณ์คอมพิวเตอร์ให้เหมาะสมก่อให้เกิดประสิทธิภาพสูงสุด รวมทั้งมีความปลอดภัยจากความเสียหายที่อาจเกิดขึ้นได้ โดยต้องสื่อสารให้บุคลากรขององค์กรรับทราบและปฏิบัติตาม
4) การคืนทรัพย์สิน (Return of Assets)
   4.1) หน่วยงานบริหารทรัพยากรบุคคล หัวหน้างาน หรือผู้บังคับบัญชาต้องกำกับและติดตามให้บุคลากรในหน่วยงานหรือหน่วยงานภายนอกที่เข้ามาให้บริการดำเนินการคืนทรัพย์สิน (Return of Assets) อาทิ เครื่องคอมพิวเตอร์พกพา เอกสาร กุญแจ บัตรพนักงาน ที่เป็นทรัพย์สินขององค์กรให้กับหน่วยงานที่เกี่ยวข้อง

1.4.2 การจัดลำดับชั้นความลับของสารสนเทศ (Information Classification)

1) การจัดลำดับชั้นความลับของสารสนเทศ (Classification of Information)
   1.1) องค์กรต้องกำหนดให้มีการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับโดยให้นำกฎหมายและข้อกำหนดที่เกี่ยวข้องกับองค์กรมาร่วมพิจารณาการกำหนดชั้นความลับที่เหมาะสม
   1.2) หน่วยงานภายในองค์กร ต้องจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศที่ใช้ในการดำเนินงานขององค์กร และกำหนดลำดับชั้นความลับของข้อมูลและทรัพย์สินสารสนเทศ
   1.3) หน่วยงานภายในองค์กร ต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้ใน<u>ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ</u>

2) การบ่งชี้สารสนเทศ (Labeling of Information)
   2.1) องค์กร ต้องควบคุมให้ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นมีการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้บุคลากรและผู้ที่เกี่ยวข้องต้องปฏิบัติตาม เพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม
   2.2) หน่วยงานเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง ต้องทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สิน และขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

3) การบริหารจัดการทรัพย์สิน (Handling of Assets)
   3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการบริหารจัดการทรัพย์สินสารสนเทศ ไม่ให้นำไปใช้ผิดประเภท

1.4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

1) การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Management of Removable Media)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
   1.2) การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ ต้องมีความสอดคล้องกับการกำหนดลำดับชั้นความลับข้อมูล
2) การทำลายสื่อบันทึกข้อมูล (Disposal of Media)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล ที่เป็นความลับหรือมีความสำคัญ
   2.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการทำลายสื่อบันทึกข้อมูล โดยอ้างอิงมาตรฐานซึ่งเป็นที่ยอมรับในสากล
3) การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)
   3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติงานหรือข้อกำหนดในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ติดตั้งหรือพื้นที่ปฏิบัติงาน

ส่วนที่ 1.5 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลขององค์กร

1.5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement for Access Control)

1) นโยบายควบคุมการเข้าถึง (Access Control Policy)
   1.1) องค์กรต้องกำหนดให้มีนโยบายควบคุมการเข้าถึง (Access Control Policy) อย่างเป็นลายลักษณ์อักษร และปรับปรุงนโยบายให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

2) การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Service)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการขอเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งาน โดยต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น
   2.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้ เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตให้เข้าถึงเท่านั้น โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

1.5.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

1) การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องร่วมกันกำหนดวิธีการบริหารจัดการการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
2) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดให้มีการมอบหมายหรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ
   2.2) หน่วยงานเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องจัดทำเอกสารการมอบหมายสิทธิ์การเข้าถึงข้อมูลหรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน
   2.3) หน่วยงานเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดกระบวนการในการบริหารจัดการสิทธิ์การเข้าถึง ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องใช้งานข้อมูลหรือระบบสารสนเทศเกินสิทธิ์ที่ได้รับมอบหมาย

3) การบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง (Management of Privileged Access Right)
   3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดเก็บรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง เช่น Administrator/ root บนเครื่องแม่ข่าย หรือ Administrator ของระบบ Application และให้มีการเบิกใช้งานตามความจำเป็นเท่านั้น
   3.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม
4) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้ (Management of Secret Authentication Information of Users)
   4.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
5) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)
   5.1) หน่วยงานเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องจัดทำขั้นตอนปฏิบัติการทบทวนสิทธิ์การเข้าถึงข้อมูล ระบบสารสนเทศ และโปรแกรมประยุกต์ (Application) อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
   5.2) หน่วยงานเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดรอบในการทบทวนสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศอย่างชัดเจนและแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ
   5.3) การทบทวนสิทธิ์การเข้าถึง ต้องพิจารณาประเด็นดังต่อไปนี้
      1. รอบการทบทวนสิทธิ์ที่กำหนดไว้
      2. การพ้นสภาพการเป็นบุคลากรขององค์กร
      3. การเปลี่ยนแปลงโยกย้ายหน้าที่การปฏิบัติงาน
      4. การขอใช้สิทธิ์นอกเหนือจากหน้าที่ความรับผิดชอบที่กำหนดไว้
   5.4) เมื่อดำเนินการทบทวนสิทธิ์เรียบร้อยแล้ว ให้เจ้าของข้อมูล หรือผู้ดูแลระบบจัดเก็บหลักฐานการทบทวนสิทธิ์ โดยให้แยกหลักฐานตามช่วงเวลาการทบทวนสิทธิ์
6) การถอดถอนสิทธิ์ในการเข้าถึง (Removal of Access Rights)
   6.1) เจ้าของข้อมูล และผู้ดูแลระบบ ต้องกำหนดเกณฑ์การพิจารณาการถอดถอนสิทธิ์การเข้าถึงและวิธีการถอดถอนสิทธิ์ในการเข้าถึงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

1.5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1) การใช้งานข้อมูลการพิสูจน์ตัวตน (Use of Secret Authentication Information)
   1.1) ผู้ใช้งานจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการเดา อาทิ คำศัพท์ในพจนานุกรม หรือคัดลอกหรือผสมจากชื่อผู้ใช้ หรืออักขระเรียงลำดับ หรือข้อมูลส่วนบุคคล หรือประโยควลีใดๆ ที่สามารถคาดเดาได้ง่าย
   1.2) ผู้ใช้งานจะต้องไม่เขียนหรือบันทึกรหัสผ่านที่ใช้ และเก็บหรือแสดงให้เห็นไว้ใกล้กับระบบหรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น
   1.3) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานของตน หรือกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ์
   1.4) ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการบริหารจัดการรหัสผ่านอื่นๆ ที่องค์กรกำหนดไว้

1.5.4 การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)
   1.1) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการเข้าถึงข้อมูล ระบบสารสนเทศและฟังก์ชั่นในระบบงาน โดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง
   1.2) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นข้อมูล ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานงานนั้นๆ เป็นลายลักษณ์อักษร
2) การเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย อย่างเป็นลายลักษณ์อักษร โดยอ้างอิงวิธีการที่เป็นมาตรฐานสากลและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
3) ระบบสำหรับบริหารจัดการรหัสผ่าน (Password Management System)

3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีระบบสำหรับบริหารจัดการบัญชีผู้ใช้และรหัสผ่านสำหรับการเข้าถึงระบบสารสนเทศของผู้ใช้งานภายในองค์กร เพื่อให้เกิดการบริหารจัดการที่เป็นมาตรฐานเดียวกัน

4) การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

4.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ และจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบสารสนเทศหรือโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

5) การเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

5.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม และการนำซอร์สโค้ดของโปรแกรมไปใช้ในการพัฒนา เพื่อป้องกันการเกิดข้อผิดพลาดในการพัฒนาระบบสารสนเทศ และระบบงานขององค์กร

ส่วนที่ 1.6 การเข้ารหัสลับข้อมูล (Cryptographic)

วัตถุประสงค์

เพื่อกำหนดแนวทางการเข้ารหัสลับข้อมูล และทำให้ระบบสารสนเทศธำรงไว้ซึ่งการรักษาความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และ/หรือ ป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีความเหมาะสม มีประสิทธิภาพ โดยมีข้อปฏิบัติดังนี้

1.6.1 มาตรการการเข้ารหัสลับข้อมูล (Cryptographic Controls)

1) นโยบายการใช้มาตรการการเข้ารหัสลับข้อมูล (Policy on the Use of Cryptographic Controls)

1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้

2) การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล (Key Management)

2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล โดยให้ครอบคลุมวงจรการบริหารจัดการกุญแจ (Key Management Life Cycle) รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

ส่วนที่ 1.7 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกัน ควบคุมการใช้งานและการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศขององค์กร ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

1.7.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Area)

1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

1.1) องค์กรต้องพิจารณาและจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัยโดยจะประกอบด้วยพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกหลัก และระบบรักษาความปลอดภัยอย่างเหมาะสม

2) การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)

2.1) องค์กร ต้องควบคุมการเข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ให้เข้าถึงได้เฉพาะบุคลากรผู้ได้รับอนุญาตเท่านั้น

2.2) รายชื่อผู้ได้รับอนุญาตให้เข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ต้องได้รับการตรวจสอบ ปรับปรุง และดูแลให้เหมาะสมอย่างสม่ำเสมอ

2.3) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความปลอดภัย (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ รวมถึงพื้นที่ปฏิบัติงานของผู้ดูแลระบบ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิ์ที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์ และบันทึกการเข้าออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก วัตถุประสงค์การผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices, Rooms, and Facilities)

3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบหรืออุปกรณ์สารสนเทศต่างๆ ที่ใช้ในการปฏิบัติงานอันเนื่องจากการได้รับความเสียหายและถูกเข้าถึงโดยไม่ได้รับอนุญาต

4) การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against External and Environmental Threats)

4.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยคุกคามจากภายนอก ทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล โรคระบาด เป็นต้น

5) การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

5.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำกับให้มีการกำหนดแนวปฏิบัติของการป้องกันทางกายภาพสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ พื้นที่ปฏิบัติงาน ห้อง Data Center และกำหนดให้มีการนำแนวปฏิบัติไปใช้งานอย่างเคร่งครัด

6) พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas)

6.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิ์เข้าถึงอาจสามารถเข้าถึงได้ โดยต้องกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์ ทั้งนี้ให้แยกเป็นสัดส่วนที่ชัดเจนเพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

1.7.2 อุปกรณ์ (Equipment)

1) การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดวางอุปกรณ์สารสนเทศไว้ในห้องหรือบริเวณที่ปลอดภัย อุปกรณ์ที่มีตู้ ประตูของตู้วางคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารเครือข่ายต้องถูกล็อคอยู่เสมอ โดยกำหนดให้มีเพียงเจ้าหน้าที่ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิ์ในการเปิดเพื่อซ่อมบำรุงหรือการปรับปรุงค่าคอนฟิกเกอเรชัน (Reconfiguration) เพื่อลดความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้มีการติดตั้งอุปกรณ์ป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ ภายในห้องคอมพิวเตอร์ ได้แก่ อุปกรณ์ดับเพลิง อุปกรณ์ดักจับควันไฟ อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิและความชื้น ระบบเตือนภัยน้ำรั่ว หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น และต้องบำรุงดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ

3) ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้การติดตั้งและการบำรุงรักษาสายสื่อสารในพื้นที่ปฏิบัติงานและห้องคอมพิวเตอร์เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรม เพื่อป้องกันไม่ให้มีการเข้าถึงหรือดักจับข้อมูล หรือเกิดความเสียหายทางด้านกายภาพ

4) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

4.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้อุปกรณ์ระบบสารสนเทศหลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนการทำงานได้รับการบำรุงดูแลรักษาตามช่วงเวลาและตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

4.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการบันทึกบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

5) การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets)

5.1) ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ ต้องไม่อนุญาตให้นำอุปกรณ์สารสนเทศออกจากองค์กร ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

5.2) ผู้ใช้งาน ต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกนอกองค์กร ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

5.3) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการนำทรัพย์สินออกนอกสำนักงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

6) ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of Equipment and Asset Off-Premises)

6.1) กำหนดให้ผู้บริหารระดับหน่วยงานขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์สารสนเทศขององค์กรไปใช้งานภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่างๆ ที่ใช้งานอยู่ภายนอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

6.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการความมั่นคงปลอดภัยในการควบคุมทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินขององค์กรออกไปใช้งาน

7) ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานซ้ำ (Secure Disposal or Re-Use of Equipment)
   7.1) ผู้ใช้งาน ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลายอย่างเหมาะสมตามลำดับชั้นความลับข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่
   7.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลหรือทรัพย์สินสารสนเทศ และมาตรการหรือเทคนิคสำหรับการทำลายข้อมูลเพื่อนำอุปกรณ์สารสนเทศกลับมาใช้งานซ้ำ โดยต้องมีความสอดคล้องกับการจัดลำดับชั้นความลับข้อมูล
   7.3) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดผู้รับผิดชอบในการทำหน้าที่ทำลายข้อมูลสารสนเทศที่ไม่จำเป็นต่อการดำเนินกิจการขององค์กรซึ่งจัดเก็บอยู่บนสื่อบันทึกข้อมูล
8) การป้องกันอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)
   8.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศที่ทิ้งไว้โดยไม่มีผู้ดูแล เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต
   8.2) ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์
   8.3) ผู้ใช้งานต้องออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน
   8.4) ผู้ใช้งาน ต้องล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์
9) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)
   9.1) ผู้ดูแลระบบ ต้องควบคุมให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน เช่น การตัดออกจากระบบ (Session Time Out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น
   9.2) ผู้ใช้งาน ต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ์
   9.3) ผู้ใช้งานต้องไม่จัดเก็บข้อมูลสำคัญไว้บนหน้าเดสท็อป (Desktop) ของเครื่องคอมพิวเตอร์ โดยผู้ใช้งานต้องจัดสรรพื้นที่ในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์และควบคุมการเข้าถึงอย่างเหมาะสม เพื่อป้องกันผู้อื่นเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

ส่วนที่ 1.8 การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมให้การดำเนินงาน การจัดการด้านการสื่อสารความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร มีแนวทางปฏิบัติที่มีขั้นตอนชัดเจนและมีความมั่นคงปลอดภัย

1.8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operations Procedures and Responsibilities)

1) ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีขั้นตอนปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษร โดยต้องแบ่งแยกอำนาจหน้าที่ของบุคลากรตามโครงสร้างการปฏิบัติหน้าที่ที่ชัดเจนเพื่อให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร
   1.2) หน่วยงานในหน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงาน และกระบวนการทำงาน
   1.3) หน่วยงานในหน่วยงานเทคโนโลยีสารสนเทศ ต้องทบทวนวิธีปฏิบัติ คู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ดังกล่าวให้เป็นปัจจุบันอยู่เสมอรวมทั้งจัดให้ขั้นตอนปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้ และต้องสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม
2) การบริหารจัดการการเปลี่ยนแปลง (Change Management)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของการเปลี่ยนแปลงโครงสร้างองค์กร ขั้นตอนการปฏิบัติงาน ระบบสารสนเทศ เพื่อควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใดๆ ซึ่งส่งผลต่อการดำเนินงานของระบบงานต่างๆ ทั้งนี้ให้ปฏิบัติตามที่กำหนดไว้ใน**นโยบายส่วนที่ 5.1 การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)**
3) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)
   3.1) ผู้ดูแลระบบ ต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

3.2) ผู้ดูแลระบบ ต้องประเมินสมรรถภาพและความเพียงพอ (Capacity) ของทรัพยากรสารสนเทศ เช่น การใช้งานของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (Memory) หน่วยจัดเก็บข้อมูล (Disk) หรือปริมาณการใช้งานระบบเครือข่าย (Bandwidth) เป็นต้น และต้องวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมี ประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งานในอนาคต

4) การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)
   4.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) การทดสอบระบบงาน (Test Environment) และระบบที่ให้บริการจริง (Production Environment) ออกจากกัน
   4.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดสิทธิ์การเข้าถึงในแต่ละสภาพแวดล้อม และจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไข รวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

1.8.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

1.8.3 การสำรองข้อมูล (Back up)

1) การสำรองข้อมูล (Information Backup)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการสำรองข้อมูล และรอบการสำรองข้อมูลของระบบสารสนเทศที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล
   1.2) เจ้าของข้อมูลสารสนเทศ ต้องดำเนินการหรือกำหนดให้มีการสำรองข้อมูลสารสนเทศและการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ
   1.3) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น File Sharing หรือ Google Drive ที่ทางบริษัทจัดหาให้ เป็นต้น ให้เป็นปัจจุบันอย่างสม่ำเสมอ รวมถึงให้จัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

1.8.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

1) การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)
   1.1) ผู้ดูแลระบบ ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ
   1.2) ผู้ดูแลระบบ ต้องเฝ้าติดตาม (Monitoring) การใช้งานระบบสารสนเทศ โดยผลของการเฝ้าติดตามจะต้องถูกสอบทานอย่างสม่ำเสมอ เพื่อตรวจหาความผิดปกติ
   1.3) ผู้ดูแลระบบ ต้องควบคุมและกำกับให้มีการบันทึกเหตุการณ์ความผิดพลาด (Fault Logging) ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ รวมถึงวิเคราะห์ ดำเนินการแก้ไข ตลอดจนวางแนวทางป้องกันการเกิดปัญหาซ้ำอีกในอนาคต
2) การป้องกันข้อมูลล็อก (Protection of Log Information)
   2.1) ผู้ดูแลระบบ ต้องจัดให้มีการป้องกันข้อมูล และระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ถูกทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต
3) การบันทึกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs)
   3.1) ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบและผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ อาทิ เวลาเปิดและปิดระบบ การเปลี่ยนแปลงการตั้งค่าของระบบ ความผิดพลาดของระบบ และการดำเนินการแก้ไข และต้องมีการสอบทานบันทึกกิจกรรมอย่างสม่ำเสมอ
4) การตั้งเวลาระบบสารสนเทศ (Clock Synchronization)
   4.1) ผู้ดูแลระบบ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศขององค์กรได้รับการกำหนดเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องและตรงกับเวลาอ้างอิงสากล
   4.2) ผู้ดูแลระบบ ต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศและระบบสารสนเทศขององค์กร รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อป้องกันไม่ให้เกิดการบันทึกเวลาที่ไม่ถูกต้อง

1.8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)

1) การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems)

1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน

1.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ขององค์กรอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

1.8.6 การบริหารจัดการช่องโหว่ทางเทคนิคในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมให้ระบบสารสนเทศขององค์กร ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง

1.2) ผู้ดูแลระบบ ต้องดูแลและบำรุงรักษาระบบ เพื่อรักษาระดับความมั่นคงปลอดภัยด้านสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ที่ตรวจสอบพบ และการปรับปรุงแก้ไขช่องโหว่ของระบบสารสนเทศ

2) การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

2.1) ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ และไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ขององค์กร

1.8.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

1) มาตรการการตรวจประเมินระบบ (Information System Audit Controls)

1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ เช่น แผนการตรวจสอบช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) เป็นต้น

1.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบก่อนดำเนินการตรวจสอบระบบสารสนเทศทุกครั้ง

1.3) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ โดยกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (System Availability) ต้องจัดให้มีการทดสอบนอกเวลาทำการ

ส่วนที่ 1.9 การสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ (Communications Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการบริหารจัดการเครือข่าย และการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกองค์กรให้มีความมั่นคงปลอดภัย

1.9.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

a. การควบคุมเครือข่าย (Network Controls)การจัดหา การพัฒนา

1.1) ผู้ดูแลระบบ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

1) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

2.1) ผู้ดูแลระบบ ต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมด ลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก

2) การแบ่งแยกเครือข่าย (Segregation in Network)

3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

1.9.2 การแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer)

1) นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer Policies and Procedures)

1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล

2) ข้อตกลงสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Agreements on Information Transfer)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอกองค์กร
   2.2) การแลกเปลี่ยนข้อมูลสารสนเทศภายในองค์กรกับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อนทุกครั้ง และมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลสารสนเทศตามลำดับชั้นความลับข้อมูลอย่างเหมาะสม

3) การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)
   3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ์

4) ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements)
   4.1) ผู้บริหารระดับหน่วยงานต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้องค์กร มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลขององค์กรอย่างเป็นลายลักษณ์อักษร

ส่วนที่ 1.10 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

1.10.1 ความต้องการด้านความมั่นคงปลอดภัยระบบ (Security Requirements of Information Systems)

1) การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศและหน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศเพื่อนำมาใช้งานในองค์กร กำหนดคุณลักษณะความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือระบบที่จัดหามาใช้งาน
   1.2) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ 1, 2 และหน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศ ต้องติดตามการพัฒนาระบบสารสนเทศ เพื่อตรวจสอบว่าการพัฒนาระบบสารสนเทศตรงตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงความต้องการด้านการใช้งานที่กำหนดไว้

2) ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Service on Public Networks)
   2.1) ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกัน การกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission or Miss-Routing) หรือการเปิดเผยคัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูล โดยไม่ได้รับอนุญาต

3) การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting Application Services Transactions)
   3.1) ข้อมูลสารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง (Miss-Routing) การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการสำเนาข้อมูลโดยไม่ได้รับอนุญาต

1.10.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes)

1) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดกฎระเบียบสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย และครอบคลุมตลอดทั้งวงจรการพัฒนาระบบสารสนเทศ

2) ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร โดยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ

3) การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical Review of Applications after Operating Platform Changes)
   3.1) ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบทบที่อาจเกิดขึ้นเมื่อต้องการที่จะเปลี่ยนแปลงหรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชั่น และการแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัย เป็นต้น โดยจะต้องมีการทดสอบบนเครื่องทดสอบ (Test Environment) จนมั่นใจว่าระบบงานต่างๆ ที่ประมวลผลบนเครื่องดังกล่าว สามารถทำงานได้ตามปกติและมีความมั่นคงปลอดภัย จึงจะทำการเปลี่ยนแปลงหรือปรับปรุงบนเครื่องที่ใช้งานจริง (Production Environment)
   3.2) ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคภายหลังการเปลี่ยนแปลงระบบปฏิบัติการบนระบบจริง เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่มีผลกระทบต่อการทำงานของระบบ และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศ
4) การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)
   4.1) ซอฟต์แวร์สำเร็จรูปที่นำมาใช้งานในองค์กรควรใช้งานโดยปราศจากการแก้ไข หากในกรณีที่มีความจำเป็นต้องดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป หน่วยงานที่ได้รับมอบหมายให้ดำเนินการต้องพิจารณาการควบคุมการแก้ไขอย่างเข้มงวด
   4.2) การเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ต้องดำเนินการเปลี่ยนแปลงตามขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงที่หน่วยงานเทคโนโลยีสารสนเทศกำหนดไว้
5) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)
   5.1) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ 1, 2 และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้เป็นอย่างน้อย
      1. การให้สิทธิ์ต่ำที่สุด (Least Privilege) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
      2. การให้สิทธิ์เฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
      3. การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (Defense In-Depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
      4. การออกแบบในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกันและสามารถตรวจสอบการทำงานได้
6) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)
   6.1) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ 1, 2 และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ

7) การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)
   7.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดข้อตกลงในการพัฒนาระบบสำหรับหน่วยงานภายนอกที่ทำหน้าที่พัฒนาซอฟต์แวร์เพื่อใช้งานภายในองค์กรอย่างเป็นลายลักษณ์อักษร
   7.2) หน่วยงานที่ได้รับมอบหมายให้ดำเนินการจัดจ้างหน่วยงานภายนอกเข้ามาพัฒนาระบบสารสนเทศให้องค์กร ต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้เกิดความเสียหายใดๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ
8) การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)
   8.1) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ 1, 2 หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งาน ต้องร่วมกันทดสอบฟังก์ชันการทำงานของระบบสารสนเทศ และฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงทุกครั้ง
   8.2) การทดสอบการพัฒนาระบบสารสนเทศ ต้องดำเนินการทดสอบระหว่างการพัฒนา และก่อนนำระบบขึ้นใช้งานจริง โดยต้องจัดเก็บหลักฐานในการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงอย่างเป็นทางการ
9) การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)
   9.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ 1,2 พัฒนาขึ้น หรือที่มีการจัดหาจากหน่วยงานภายนอก และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง

1.10.3 ข้อมูลสำหรับการทดสอบ (Test Data)

1) การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)
   1.1) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ 1, 2 หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการ ควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง

ส่วนที่ 1.11 การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)

วัตถุประสงค์

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงานของหน่วยงานภายนอกในการให้บริการหรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย และได้รับผลประโยชน์สูงสุดแก่องค์กร

1.11.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับหน่วยงานภายนอก (Information Security in Supplier Relationships)

1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับหน่วยงานภายนอก (Information Security Policy for Supplier Relationships)
   - 1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน่วยงานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาหรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้หน่วยงานภายนอกหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศขององค์กร
   - 1.2) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมกำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้าง ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ
2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)
   - 2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศ เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร
   - 2.2) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมให้หน่วยงานภายนอกสามารถเข้าถึงสารสนเทศขององค์กรเฉพาะส่วนที่มีความจำเป็นต้องรู้ และต้องได้รับการยินยอมจากเจ้าของข้อมูลสารสนเทศ อย่างเป็นลายลักษณ์อักษรเท่านั้น
   - 2.3) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและหน่วยงานภายนอก
3) การบริหารจัดการและการสื่อสารต่อผู้รับจ้างช่วงของหน่วยงานภายนอก (Information and Communication Technology Supply Chain)
   - 3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมถึงผู้รับจ้างช่วงที่หน่วยงานภายนอกเป็นผู้จัดหา

1.11.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

1) การติดตามและทบทวนการให้บริการของหน่วยงานภายนอก (Monitoring and Review of Supplier Services)
   - 1.1) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องติดตามและตรวจทานการดำเนินงานของหน่วยงานภายนอกซึ่งมีหน้าที่ในการบริหารจัดการระบบประมวลผลข้อมูลสารสนเทศให้กับองค์กร ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการอย่างสม่ำเสมอ

2) การบริหารจัดการการเปลี่ยนแปลงบริการของหน่วยงานภายนอก (Managing Changes to Supplier Services)
   - 2.1) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหารและผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

ส่วนที่ 1.12 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ การเรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้นและการปรับปรุงแก้ไข ซึ่งเป็นการป้องกันไม่ให้เกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศซ้ำขึ้นอีก

1.12.1 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Management of Information Security Incidents and Improvements)

1) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดหน้าที่ในการบริหารจัดการสถานการด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และมอบหมายสิทธิการดำเนินงานอย่างชัดเจนให้บุคลากรภายในหน่วยงาน
   1.2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิดออกจากเหตุขัดข้องด้านการปฏิบัติงานทั่วไป เพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม
   1.3) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดช่องทางและเกณฑ์ในการรายงานเหตุการณ์ หรือจุดอ่อน หรือเหตุขัดข้องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และสื่อสารให้บุคลากรในองค์กรและหน่วยงานภายนอกรับทราบ
2) การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)
   2.1) ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้บังคับบัญชาและหน่วยงานเทคโนโลยีสารสนเทศ โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด
3) การรายงานจุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)
   3.1) ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้บังคับบัญชาและหน่วยงานเทคโนโลยีสารสนเทศ โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด
   3.2) ผู้ใช้งานและหน่วยงานภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศหรือจุดอ่อนใดๆ ของระบบสารสนเทศในองค์กร ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชาและหน่วยงานเทคโนโลยีสารสนเทศ และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศนั้นด้วยตนเอง
4) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events)
   4.1) ผู้ดูแลระบบ ต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทำการจัดแยกกลุ่มเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัยและจัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้ และแจ้งผู้ที่เกี่ยวข้องรับทราบเพื่อแก้ไขในกรณีที่พบว่าเหตุการณ์หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศ
5) การตอบสนองต่อเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents)
   5.1) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้
   5.2) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตอบสนองและแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หากไม่สามารถแก้ไขได้ตามเวลาที่กำหนดต้องแจ้งให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด
6) การเรียนรู้จากเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)
   6.1) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องจัดเตรียมรายงานผลการวิเคราะห์และการแก้ไขเหตุขัดข้อง จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และจัดเก็บไว้เป็นองค์ความรู้ เพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต
7) การเก็บรวบรวมหลักฐาน (Collection of Evidence)
   7.1) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องดำเนินการเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อรวบรวมหลักฐานให้เพียงพอต่อการนำเสนอผู้บริหารหน่วยงานที่เกี่ยวข้อง และใช้ในการดำเนินการด้านกฎหมายต่อไป

ส่วนที่ 1.13 ความมั่นคงปลอดภัยสำหรับการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อป้องกันการติดขัด หรือหยุดชะงักของการดำเนินธุรกิจขององค์กรและป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวของระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบสารสนเทศกลับคืนมาได้ในระยะเวลาอันเหมาะสม

1.13.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)

1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity)
   1.1) เจ้าของข้อมูลและหน่วยงานเทคโนโลยีสารสนเทศ ต้องร่วมกันระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ประเมินความเสี่ยงเหตุการณ์และระบบงานสำคัญ เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วน เพื่อใช้ในการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ
2) การสร้างกระบวนการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้เป็นส่วนหนึ่งของแผน และให้มีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจขององค์กร
3) การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)
   3.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ 1 ครั้ง และจัดให้มีการบันทึกผลการทดสอบ เพื่อให้มั่นใจว่าแผนงานที่จัดทำมีความถูกต้องและสามารถตอบสนองต่อการดำเนินงานได้เป็นอย่างดี
   3.2) บุคลากรผู้ซึ่งมีส่วนเกี่ยวข้องในการปฏิบัติงานกู้คืนระบบสารสนเทศ ต้องมีความรู้ด้านเทคนิคที่จำเป็นต่อการกู้คืนระบบและเข้าร่วมการซักซ้อมแผน
   3.3) เจ้าของข้อมูลและผู้ใช้งานระบบที่เกี่ยวข้องกับแผนรองรับการดำเนินการทางธุรกิจอย่างต่อเนื่องต้องเข้าร่วมการทดสอบแผน และดำเนินงานตามแผนที่กำหนดไว้

1.13.2 การจัดให้มีอุปกรณ์หรือระบบสารสนเทศสำรอง (Redundancies)

1) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)
   1.1) องค์กร ต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่มีความสำคัญสูง
   1.2) องค์กร ต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

ส่วนที่ 1.14 การปฏิบัติตามกฎระเบียบและข้อบังคับ (Compliance)

วัตถุประสงค์

เพื่อให้การดำเนินงานต่างๆ ขององค์กรเป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ ที่องค์กรและบุคลากรขององค์กรต้องปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

1.14.1 การปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง (Compliance with Legal and Contractual Requirements)

1) การระบุกฎหมายและข้อกำหนดในสัญญาจ้าง (Identification of Applicable Legislation and Contractual Requirements)
   1.1) หน่วยงานเทคโนโลยีสารสนเทศต้องร่วมกับหน่วยงานกฎหมาย และหน่วยงานบริหารทรัพยากรบุคคลในการรวบรวมกฎหมาย กฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ
   1.2) บุคลากรทั้งหมดต้องรับผิดชอบในการปฏิบัติตามข้อกำหนดที่ได้มีการระบุไว้อย่างเคร่งครัด
   1.3) ห้ามเจ้าหน้าที่ในองค์กรใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศขององค์กรกระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม
2) การป้องกันสิทธิ และทรัพย์สินทางปัญญา (Intellectual Property Rights)
   2.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดทำกระบวนการสำหรับการบริหารจัดการการใช้ซอฟต์แวร์ลิขสิทธิ์และทรัพย์สินทางปัญญา เพื่อให้มั่นใจว่าการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับ กฎหมายและข้อกำหนดตามสัญญาต่างๆ

2.2) ผู้ใช้งานต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

2.3) ห้ามผู้ใช้งานทำการใช้งานทำซ้ำ หรือ เผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กรโดยเด็ดขาด

2.4) ซอฟต์แวร์ที่พัฒนาเพื่อองค์กร ทั้งโดยหน่วยงานภายนอกหรือบุคลากรในหน่วยงานขององค์กรถือว่าเป็นทรัพย์สินขององค์กร องค์กรไม่อนุญาตให้หน่วยงานภายนอกหรือบุคลากรในหน่วยงานขององค์กรทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินขององค์กรโดยไม่ได้รับอนุญาต

2.5) ผู้ใช้งานที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรต้องยึดถือและปฏิบัติตามกฎหมาย ลิขสิทธิ์ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

2.6) ห้ามมิให้พนักงานเปิดเพลงที่ไม่มีใบอนุญาตและเพลงที่ทางบริษัทไม่ได้เป็นผู้จัดส่งให้เข้าในระบบกระจายเสียงของบริษัท ทั้งนี้รวมถึงการเปิดเพลงจากแผ่นเสียงที่มีลิขสิทธิ์ถูกต้อง หรือจากเครือข่ายสาธารณะ เช่น วิทยุ YouTube เป็นต้น เนื่องจากการกระทำดังกล่าวถือเป็นการละเมิดลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ในเรื่องของการเผยแพร่ผลงานต่อสาธารณชนโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

3) การป้องกันข้อมูลขององค์กร (Protection of Records)

3.1) เจ้าของข้อมูล ต้องปฏิบัติตามข้อบังคับทางกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศบางประเภท เช่น ด้านบัญชี ด้านลูกค้า และต้องจัดทำข้อกำหนดในการจัดการข้อมูลสารสนเทศ ระยะเวลาในการจัดเก็บ ให้สอดคล้องกับข้อบังคับดังกล่าว

3.2) เจ้าของข้อมูลต้องควบคุม ป้องกันมิให้ข้อมูลบันทึกหลักฐาน (Logs) ต่างๆ เกิดความเสียหาย สูญหาย ถูกเปลี่ยนแปลงแก้ไข ถูกเข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยการควบคุมต้องให้สอดคล้องกับกฎหมาย ข้อกำหนด และความต้องการทางธุรกิจ

4) ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)

4.1) องค์กรต้องจัดให้มีการควบคุมการใช้งานข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย, ประกาศ หลักเกณฑ์ของหน่วยงานที่ควบคุม โดยกำหนดเป็นนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร

4.2) ข้อมูลสารสนเทศรายละเอียดที่เกี่ยวกับลูกค้าถือว่ามีความสำคัญ หน่วยงานผู้รับผิดชอบในการดูแลข้อมูลต้องกำหนดให้บุคลากรและลูกจ้างที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศดังกล่าวได้

4.3) ข้อมูลสารสนเทศส่วนบุคคลของบุคลากร ลูกจ้าง และลูกค้า ถือว่าเป็นความลับ และ สามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ ตามที่องค์กรกำหนดเท่านั้น

5) ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสลับข้อมูล (Regulation of Cryptographic Controls)

5.1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมการเข้ารหัสลับข้อมูลให้มีความสอดคล้องกับกฎหมาย ประกาศ หลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับองค์กร

1.14.2 การทบทวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Reviews)

1) การตรวจประเมินระบบสารสนเทศจากผู้ตรวจสอบอิสระ (Independent Review of Information Security)

1.1) องค์กรต้องจัดให้มีการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศ โดยส่วนตรวจสอบระบบงานหรือผู้ตรวจสอบอิสระภายนอก เพื่อตรวจสอบการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนทบทวนถึงความพอเพียงของการควบคุมระบบสารสนเทศ และการปฏิบัติตามการควบคุมต่างๆ

2) การปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยสารสนเทศ (Compliance with Security Policies and Standards)

2.1) ผู้บังคับบัญชาของแต่ละแผนกต้องรับผิดชอบในการสอบทานการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรใต้บังคับบัญชาอย่างสม่ำเสมอ

2.2) กรณีที่ผู้บังคับบัญชาของแต่ละแผนกตรวจพบการปฏิบัติงานที่ไม่สอดคล้องกับนโยบาย มาตรฐาน และขั้นตอนปฏิบัติซึ่งยังไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ผู้บังคับบัญชาต้องชี้แจงให้บุคลากรใต้บังคับบัญชารับทราบและทำความเข้าใจ แต่หากความไม่สอดคล้องที่พบส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ผู้บังคับบัญชาต้องดำเนินการลงโทษทางวินัยตามกฎระเบียบที่องค์กรกำหนดไว้

2.3) หน่วยงานเทคโนโลยีสารสนเทศ ต้องให้การสนับสนุนด้านการให้คำแนะนำในการใช้งาน หรือการปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศต่อหน่วยงานอื่นเมื่อได้รับคำร้องขอ

3) การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

3.1) ต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค เช่น การทดสอบการบุกรุกระบบสารสนเทศ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษา

ความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

3.2) ส่วนตรวจสอบระบบงาน ต้องตรวจสอบการควบคุมทางเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอเหมาะสม และมีการปฏิบัติตามการควบคุมเหล่านั้น

3.3) ผู้ดูแลระบบ ต้องจัดให้มีการทดสอบระดับมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การตรวจหาช่องโหว่ของระบบสารเทศ (Vulnerability Assessment) หรือการทดสอบการบุกรุกระบบ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ