นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

บริษัท มิลเลนเนียม กรุ๊ป คอร์ปอเรชั่น (เอเชีย) จำกัด (มหาชน)

ฉบับปรับปรุงครั้งที่: 1

วันที่มีผลบังคับใช้: 25 กุมภาพันธ์ 2568

อนุมัติโดย: คณะกรรมการบริษัท ครั้งที่ 1/2568

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

บริษัท มิลเลนเนียม กรุ๊ป คอร์ปอเรชั่น (เอเชีย) จำกัด (มหาชน) (“บริษัทฯ”) มีทรัพย์สินสารสนเทศเพื่อสนับสนุนประสิทธิภาพการดำเนินงานให้สามารถตอบสนองเป้าหมายทางธุรกิจ ซึ่งทรัพย์สินสารสนเทศดังกล่าวเป็นทรัพย์สินสำคัญที่ผู้ปฏิบัติงานจะต้องใช้และดูแลรักษาให้อยู่ในสภาพที่พร้อมใช้งานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา

ทั้งนี้ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเป็นงานที่ต้องได้รับความร่วมมือจากทุกหน่วยงานในการปฏิบัติตามอย่างต่อเนื่อง โดยต้องมีการตรวจสอบอย่างสม่ำเสมอ และต้องมีการปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ถูกกำหนดขึ้นนั้น จะเป็นเครื่องมือสำคัญสำหรับผู้ใช้บริการ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศในการใช้เป็นแนวทางเพื่อดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

วัตถุประสงค์

เพื่อให้องค์กรมีแนวนโยบายในการดำเนินงานหรือการจัดการทางด้านเทคโนโลยีสารสนเทศและให้ผู้ที่เกี่ยวข้องกับสารสนเทศทั้งผู้บริหารบุคลากรในองค์กรหน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศขององค์กรได้มีแผนงานและกรอบการปฏิบัติที่ชัดเจนอันจะนำไปสู่การประสานงานในการให้บริการที่มีประสิทธิภาพ มีความปลอดภัยในการให้บริการสูงสุด และมีมาตรฐานยิ่งขึ้น อีกทั้งกำหนดมาตรการป้องกันที่เหมาะสมเพื่อควบคุมและลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากกรณีที่ทรัพย์สินไม่สามารถใช้งานได้สูญหายเสียหายบกพร่องหรือถูกคุกคามด้านความมั่นคงปลอดภัย ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ คงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ จึงเห็นสมควรกำหนดนโยบายรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อให้ถือเป็นแนวทางในการปฏิบัติเดียวกัน

กฎหมายและกฎระเบียบที่เกี่ยวข้อง

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (รวมทั้งที่มีการแก้ไขเพิ่มเติม)
2. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 (รวมทั้งที่มีการแก้ไขเพิ่มเติม)
3. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
4. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

5. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย
6. พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 (รวมทั้งที่มีการแก้ไขเพิ่มเติม)
7. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (รวมทั้งที่มีการแก้ไขเพิ่มเติม)

บทบังคับใช้และบทลงโทษ

นโยบายด้านความมั่งคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ ให้มีผลบังคับใช้นับจากวันที่ประกาศให้มีผลบังคับใช้ต่อผู้ใช้งานระบบสารสนเทศของบริษัทฯ ทั้งหมดโดยไม่มีการยกเว้น ผู้ฝ่าฝืนจะมีความผิดและต้องได้รับการลงโทษทางวินัยตามระเบียบที่องค์กรกำหนดไว้

ลักษณะการกระทำที่ถือว่าเป็นความผิดทางวินัย

- ทำการเปลี่ยนแปลงแก้ไขข้อมูลในการติดต่อสื่อสารของบุคคลอื่น โดยไม่ได้รับอนุญาต
- เปิดเผยความรู้หรือข้อมูลข่าวสารทางธุรกิจอันเป็นเรื่องลับหรือปกปิดของบริษัทฯ ให้แก่ผู้อื่นโดยไม่ได้รับอนุญาตจากบริษัทฯ
- ทำการลักลอกปลอมแปลงรหัสผ่าน (Password) หรือรหัสประจำตัวผู้ใช้อื่นพื่อเข้าระบบงานคอมพิวเตอร์โดยจงใจเจตนา เพื่อกระทำการทุจริตต่อทรัพย์สินเงินทองทั้งของบริษัทฯ หรือลูกค้า หรือทำให้เสื่อมเสียชื่อเสียง
- ใช้รหัสผ่าน (Password) หรือรหัสประจำตัวผู้ใช้อื่น หรือรหัสผ่านแบบครั้งเดียว (OTP : One Time Password) ของบุคคลอื่นเข้าสู่ระบบคอมพิวเตอร์ของบริษัทฯ ทำการอ่าน คัดลอกข้อมูล อนุมัติ แก้ไขเปลี่ยนแปลง ลบทิ้งไม่ว่าเพื่อประโยชน์ใดทั้งของส่วนตัวหรือของบุคคลอื่น
- ประมาท เลินเล่อ ไม่ระมัดระวังการใช้รหัสผ่าน (Password) หรือรหัสประจำตัวผู้ใช้อื่น หรือรหัสผ่านแบบครั้งเดียว (OTP : One Time Password) หรือยินยอมจงใจให้บุคคลอื่นใช้รหัสผ่าน หรือรหัสประจำตัวผู้ใช้ และสิทธิในการใช้งานระบบคอมพิวเตอร์ของตนเอง
- จงใจ เจตนา ลักลอบ ส่งออก หรือนำข้อมูลของบริษัทฯ ไปเปิดเผย จำหน่าย แจกจ่าย แก่บุคคลอื่นเพื่อประโยชน์ส่วนตน หรือบุคคลอื่นโดยไม่ได้รับอนุญาตหรือทำให้บริษัทฯ เกิดความเสียหาย
- พยายามเข้าถึงระบบที่ไม่มีสิทธิ์ หรือไม่ได้รับอนุญาตให้ใช้งาน
- จงใจ หรือเจตนาก่อกวน หรือทำลายข้อมูลสารสนเทศ ระบบคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อสร้างความเสียหายต่อบริษัทฯ
- ทำการลักลอบ เฝ้าดู ดักฟัง ค้นหาเส้นทางหรือถอดรหัสข้อมูลอิเล็กทรอนิกส์ โดยใช้เครื่องมือหรือ

เทคโนโลยีอื่นใด เพื่อให้ได้มาซึ่งข้อมูล หรือความลับของบุคคลอื่นหรือของบริษัทฯ โดยจงใจก่อให้เกิดความเสียหายต่อบุคคลอื่นหรือต่อบริษัทฯ

- ทำการติดตั้ง หรือใช้งาน Software ประเภท Hacking Tools หรือ Software อื่นใดที่เกี่ยวข้องกับการตรวจสอบและเข้าถึงข้อมูลสำคัญของบริษัทฯ ยกเว้นบุคคลหรือหน่วยงานที่ทำหน้าที่เกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยเฉพาะ
- ทำการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่นใดเข้ากับระบบคอมพิวเตอร์หรือเครือข่ายของบริษัท โดยไม่ได้รับอนุญาตจากหน่วยงานที่รับผิดชอบ
- ทำการกำหนดและติดตั้ง หรือเปลี่ยนแปลง IP Address ด้วยตนเองโดยไม่ได้รับอนุญาตจากหน่วยงานที่รับผิดชอบ
- ทำการดึงข้อมูล หรือมีไว้ในครอบครองในสิ่งที่ไม่สมควร หรือเป็นการผิดกฎหมาย เช่น ข้อความ ภาพลามก อนาจาร ฯลฯ หรือสิ่งอื่นใดอันเป็นการดูหมิ่น บ่อนทำลายสถาบัน ชาติ ศาสนา และพระมหากษัตริย์ หรือที่เป็นการปลุกระดมให้เกิดความแตกแยกในหมู่ประชาชน หรือพนักงาน หรือสร้างความเสียหายแก่บริษัทฯ
- ทำการส่งข้อความหรือข้อมูลที่ไม่เหมาะสมโดยใช้ระบบ E-Mail หรือใช้เครื่องมือสื่อสารของบริษัทฯ เช่น หมิ่นประมาท คุกคาม ขู่กรรโชก กล่าวร้ายป้ายสี หยาบคายหรือส่งจดหมายลูกโซ่ เป็นต้น
- ใช้งานระบบ Intranet หรือระบบ Internet หรือ E-Mail ในเรื่องที่ไม่เกี่ยวข้องกับธุรกิจของบริษัทฯ ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ อันเป็นทรัพย์สินของบริษัทฯ เพื่อความบันเทิง หรือประโยชน์ส่วนตัว
- ใช้ Software ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย หรือที่บริษัทฯ ไม่ได้อนุญาตให้ใช้หรือที่อาจก่อให้เกิดความเสียหายต่อบริษัทฯ
- ให้ความช่วยเหลือ หรือร่วมมือกับบุคคลภายนอกเพื่อให้เข้าถึงระบบคอมพิวเตอร์หรือระบบข้อมูลสารสนเทศของบริษัทฯ กระทำการคัดลอกหรือทำลายข้อมูลสารสนเทศหรือระบบคอมพิวเตอร์ของบริษัทฯ

การลงโทษทางวินัย

- ตักเตือนด้วยวาจา
- ตักเตือนเป็นลายลักษณ์อักษร
- พักงานชั่วคราว โดยไม่ได้รับค่าจ้าง
- ปลดออก
- ไล่ออก

- การดำเนินทางกฎหมายอาญาหรือแพ่ง

  กรณีการลงโทษพนักงาน บริษัทฯ ไม่จำเป็นต้องปฏิบัติตามลำดับดังกล่าวข้างต้น บริษัทฯ อาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

การเผยแพร่นโยบาย

แผนกเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการประกาศและเผยแพร่นโยบายไปยังผู้ใช้งานระบบสารสนเทศขององค์กรเพื่อช่วยให้เกิดความเข้าใจในบทบาทของตนเองในการใช้งานเทคโนโลยีสารสนเทศและปกป้องทรัพย์สินของบริษัทฯ

การทบทวนนโยบาย

นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ต้องได้รับการทบทวน ปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญของสภาพแวดล้อมต่างๆ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมายและเทคโนโลยี เป็นต้น โดยถือเป็นหน้าที่ของแผนกเทคโนโลยีสารสนเทศในการทบทวนและปรับปรุงโดยมีผู้บริหารแผนกเทคโนโลยีสารสนเทศเป็นผู้ควบคุมดูแลให้เกิดการทบทวนและปรับปรุงตามที่ได้กำหนดไว้

วิธีการปฏิบัติให้เป็นไปตามนโยบาย

แผนกเทคโนโลยีสารสนเทศ ได้จัดนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001:2022 (Information Security Management Systems) เพื่อให้เกิดความมั่นคงปลอดภัยแก่สารสนเทศ

องค์ประกอบของนโยบาย

1.1. คำนิยาม

1.2. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

1.3. การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

1.4. การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

1.5. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

1.6. การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

1.7. การรักษาความมั่นคงปลอดภัยของอีเมล์

1.8. การรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต

1.9. การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

1.10. ความมั่นคงปลอดภัยของการสำรองข้อมูล

1.11. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งพนักงานของบริษัทฯ และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

ในการรักษาความมั่นคงปลอดภัยอย่างได้ผล จำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย

- การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของพนักงานและบุคคลภายนอกทุกคน
- การบริหาร และการปฏิบัติในการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา
- การรู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนด ไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่าง ๆ ถือเป็นสิ่งที่สำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้พนักงานและบุคคลภายนอกทราบอย่างชัดเจน เพื่อให้มีความเข้าใจในหน้าที่ และความรับผิดชอบในการรักษาความมั่นคงปลอดภัย ที่ตนเองรับผิดชอบเป็นที่สิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

คำนิยาม

นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้กำหนดคำนิยามของคำศัพท์ที่ใช้ในนโยบายฉบับนี้ เพื่อให้เข้าใจถึงความหมายตรงกันและอ้างอิงได้ถูกต้อง ดังต่อไปนี้

คำศัพท์	ความหมาย
หน่วยงาน	
องค์กร	บริษัท มิลเลนเนียม กรุ๊ป คอร์ปอเรชั่น (เอเชีย) จำกัด (มหาชน)
บริษัทย่อย	บริษัทที่บริษัท มิลเลนเนียม กรุ๊ป คอร์ปอเรชั่น (เอเชีย) จำกัด (มหาชน) มีอำนาจควบคุมได้
แผนกเทคโนโลยีสารสนเทศ	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร
บุคคล	
ผู้บริหารระดับฝ่าย	ผู้บริหารสูงสุดของแต่ละฝ่ายงาน
ผู้มีอำนาจ	ผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไปหรือผู้ที่ได้รับมอบหมายให้มีหน้าที่ ตัดสินใจ
ผู้ดูแลระบบ (Administrator)	เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบใน การดูแลรักษาระบบ หรือเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการใช้ งานระบบสารสนเทศในด้านต่างๆ ซึ่งสามารถเข้าถึงโปรแกรมหรือเครือข่าย คอมพิวเตอร์เพื่อการจัดการต่างๆ ได้
บุคลากร	บุคลากรของบริษัท มิลเลนเนียม กรุ๊ป คอร์ปอเรชั่น (เอเชีย) จำกัด (มหาชน)
บุคคลภายนอก	บุคคลหรือพนักงานของหน่วยงานภายนอกที่มาติดต่อสื่อสารและมีการเข้าถึง ทรัพย์สินสารสนเทศขององค์กร
ผู้ให้บริการภายนอก/หน่วยงานภายนอก (Third party)	ผู้ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) พนักงานสัญญาจ้าง (Outsource) และบุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศและต่างประเทศที่ ให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการ ให้บริการให้กับองค์กร รวมถึงหน่วยงานผู้รับจ้างช่วงที่ผู้ให้บริการภายนอกเป็นผู้จัดจ้าง โดยได้รับอนุญาตให้มีสิทธิเข้าถึงสถานที่หรือทรัพย์สินสารสนเทศของ องค์กร และใช้งานระบบสารสนเทศขององค์กรตามอำนาจหน้าที่ที่รับผิดชอบ
ผู้ใช้งาน (User)	พนักงานของบริษัทฯ รวมไปถึงบุคคลภายนอก และหน่วยงานภายนอกที่ได้รับอนุญาตใช้งานระบบงานคอมพิวเตอร์ ขององค์กร

คำศัพท์	ความหมาย
เจ้าของโครงการ	หน่วยงานภายในบริษัท มิลเลนเนียม กรุ๊ป คอร์ปอเรชั่น (เอเชีย) จำกัด (มหาชน) ที่เป็นผู้รับผิดชอบในการดำเนินงานโครงการที่มีการจัดจ้างผู้ให้บริการภายนอก / หน่วยงานภายนอกเข้ามาปฏิบัติงาน ให้กับองค์กร
เจ้าของทรัพย์สิน / เจ้าของข้อมูล (Data Owner)	บุคคล ส่วนงาน หรือฝ่ายงานผู้เป็นเจ้าของข้อมูล หรือเป็นผู้ที่ได้รับความเสียหาย สูงสุดเมื่อข้อมูลนั้นเสียหายหรือถูกเปิดเผย
คำอื่นๆ	
ข้อมูล	ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ ที่อยู่ในรูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล ทั้งที่อยู่ ในรูปอิเล็กทรอนิกส์หรือที่อยู่ ในรูปสื่อสิ่งพิมพ์ และให้ความหมายรวมถึง ข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
ข้อมูลอิเล็กทรอนิกส์	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมาย อิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ใน สภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูล อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
ข้อมูลสำคัญ	หรือ ข้อมูลที่เป็นความลับ (Sensitive Information) หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัทมีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำไปเปิดเผยต่อบุคคลอื่นหรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพหรือบริษัทเสื่อมเสียชื่อเสียง
ระบบคอมพิวเตอร์	เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสาย

คำศัพท์	ความหมาย
	และไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่าง ๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อโทรคมนาคมต่าง ๆ ที่สามารทำงานหรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัทฯ ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือมช้งานภายในสถานประกอบการของบริษัทฯ
ระบบที่มีความสำคัญ (Important System)	ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์ เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัทฯ ให้เป็นปกติ และระบบที่ได้รับการกำหนดโดยหน่วยงานด้านความปลอดภัยข้อมูลและระบบสารสนเทศของบริษัทฯ ทั้งนี้หากระบบที่มีความสำคัญดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทฯ ต้องหยุดชะงักหรือด้อยประสิทธิภาพ
เจ้าของระบบ (System Owner)	หน่วยงานภายในซึ่งเป็นเจ้าของระบบ คอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้น ๆ
ผู้ดูแลข้อมูล (Custodian)	ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศในการสนับสนุนการดูแล จัดการ และควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศที่กำหนด
ผู้ดูแลระบบ (Administrator)	ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ไดรับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของบริษัทฯ ทำงานได้อย่างถูกต้องมีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปอลดภัย
บุคคลภายนอก (External Party)	บุคคลหรือหน่วยงานภายนอกที่ดำเนินธุรกิจ หรือให้บริการที่อาจได้รับสิทธิพิเศษเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น ■ บริษัทฯ คู่ค้า (Business Partner)

คำศัพท์	ความหมาย
	■ ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource) ■ ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ (Supplier/Vendor) ■ ผู้ให้บริการต่าง ๆ (Service Provider) ■ ที่ปรึกษา (Consultant)
Remote Access หรือ Virtual Private Network (VPN)	การเข้าสู่ระบบสารสนเทศของบริษัทฯ จากระยะไกล
บัญชีผู้ใช้ (Username หรือ Account)	กลุ่มของข้อมูล ที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิการเข้าถึง และข้อจำกัดต่างๆ ในการเข้าถึงระบบสารสนเทศ
รหัสผ่าน (Password)	กลุ่มอักขระที่ใช้ในการพิสูจน์ตัวตน ใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศหรือข้อมูลสารสนเทศ
สิทธิ์ระดับสูง (Privilege)	สิทธิ์ที่สามารถใช้งาน โดยได้รับสิทธิ์ที่มากกว่าสิทธิ์ของผู้ดูแลระบบหรือผู้ใช้งานทั่วไปในระบบ เช่น Root หรือ Administrator
ระบบสารสนเทศ	ระบบคอมพิวเตอร์ ระบบเก็บข้อมูล ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสื่อสารข้อมูลทุกประเภท อุปกรณ์สื่อสาร เครื่องพิมพ์ เครื่องสแกนหรือ อุปกรณ์ใดๆ ที่เกี่ยวข้องที่เป็นกรรมสิทธิ์ขององค์กรและ/หรือที่องค์กรได้รับอนุญาตให้ใช้ได้ตามกฎหมาย
ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และ สภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธ ความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความ เป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการ ป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคง ปลอดภัย
เหตุขัดข้อง (Incident)	เหตุขัดข้องที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามที่กำหนดไว้ หรือคุณภาพในการให้บริการลดลง เช่น ระบบอีเมลไม่สามารถใช้งานได้ เครื่องแม่ ข่ายขัดข้อง หรือ ระบบงานประมวลช้าผิดปกติ เป็นต้น

คำศัพท์	ความหมาย
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
การเข้ารหัสลับ (Encryption)	การเปลี่ยนแปลงรูปแบบของข้อมูลให้อยู่ในรูปแบบที่มีความมั่นคงปลอดภัย โดยใช้กุญแจในการเข้ารหัสลับ เพื่อที่ผู้เข้าถึงข้อมูลจะไม่สามารถทราบเนื้อหาที่แท้จริงของข้อมูลได้ ถ้าไม่มีการถอดรหัสลับจากกุญแจที่ใช้ในการถอดรหัสที่ถูกต้อง ทั้งนี้ ขึ้นอยู่กับเทคนิคการเข้ารหัสลับข้อมูลที่ใช้โดยลักษณะของการเข้ารหัสลับมี ด้วยกัน 2 ประเภทคือ ● การเข้ารหัสแบบสมมาตร (Symmetric Key Encryption) เป็นการเข้ารหัส ที่ใช้กุญแจรหัสเดียวในการเข้ารหัสและถอดรหัส เรียกว่า กุญแจลับ (Secret Key) ● การเข้ารหัสแบบอสมมาตร (Asymmetric Key Encryption or Public Key Cryptography) เป็นการเข้ารหัสในลักษณะที่มีกุญแจคู่เรียกว่ากุญแจ ส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) โดยใน นโยบายฉบับนี้เรียกว่ากุญแจคู่
กุญแจ (Key)	กุญแจที่ใช้ในกระบวนการเข้ารหัสลับ หรือถอดรหัสลับขึ้นอยู่กับการใช้งาน เทคนิคการเข้ารหัสลับข้อมูล โดยแยกเป็น 2 ประเภท คือ ● กุญแจลับ (Secret Key) ซึ่งใช้ในการเข้ารหัสลับแบบสมมาตร (Symmetric Key Encryption) ตัวอย่างของอัลกอริทึมสำหรับการเข้ารหัสแบบสมมาตร เช่น 3DES, RC5, RC6, AES เป็นต้น ● กุญแจคู่ ซึ่งใช้ในการเข้ารหัสแบบอสมมาตร (Asymmetric Key Encryption or Public Key Cryptography) ประกอบไปด้วย กุญแจ ส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ตัวอย่างของ อัลกอริทึมสำหรับการเข้ารหัสแบบอสมมาตร เช่น RSA (Rivest-Shamir Adleman), Diffie-Hellman Key Exchange Protocol, Elliptic Curve Cryptography (ECC) เป็นต้น

คำศัพท์	ความหมาย
ช่องโหว่ (Vulnerability)	สภาพหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ของทรัพย์สินสารสนเทศ ซึ่ง อาจเกิดจากความบกพร่องในการผลิต หรือการออกแบบ หรือการบริหารจัดการ ทำให้เกิดจุดอ่อน โดยมีความเสี่ยงที่จะเกิดภัยคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของโปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ ต้องผ่านการพิสูจน์ตัวตน
การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness)	การให้ความรู้ความเข้าใจทางด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อสร้าง ความตระหนักถึงภัยคุกคามและปัญหาทางด้านความมั่นคงปลอดภัยสารสนเทศ แก่บุคลากร
การสำรองข้อมูล (Data Backup)	การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมี การแก้ไข เปลี่ยนแปลง หรือสูญหายให้สามารถนำกลับมาใช้งานได้
แหล่งข้อมูล (Source of Data and Information)	ที่เก็บข้อมูล หรือสารสนเทศทั้งที่อยู่ในรูปแบบต่างๆ กัน เช่น ข้อมูล แหล่งข้อมูล เฉพาะและแหล่งข้อมูลส่วนกลาง เป็นต้น
ทรัพย์สินสารสนเทศ	หมายถึง ● อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์อื่นใดที่ใช้งานร่วมกับอุปกรณ์ เทคโนโลยีสารสนเทศที่เกี่ยวข้องทุกประเภท ● ชุดคำสั่ง โปรแกรมระบบงานสารสนเทศ และโปรแกรมอื่นใดที่ใช้งาน ร่วมกับโปรแกรมระบบงานสารสนเทศ ● ข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ และ/หรือทรัพย์สินทางปัญญาใดๆ
พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Area)	คือ บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ แบ่งได้ เป็น 3 ประเภท คือ 1) พื้นที่ห้อง Patching Room 2) พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ (Computer Operation) 3) พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)
พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ (Computer Operation)	พื้นที่ที่ใช้ในการป้อนข้อมูล ออกรายงาน และปฏิบัติงานเกี่ยวกับระบบงาน สารสนเทศขององค์กร

คำศัพท์	ความหมาย
พื้นที่ห้อง Patching Room	พื้นที่ที่ใช้เก็บอุปกรณ์ในการเชื่อมต่อเครือข่ายคอมพิวเตอร์ และโทรศัพท์ในแต่ละชั้น
ห้องคอมพิวเตอร์ (Data Center)	พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ที่ใช้เก็บอุปกรณ์คอมพิวเตอร์และเครื่อง คอมพิวเตอร์หลักที่สำคัญในระบบงาน เช่น เครื่องคอมพิวเตอร์แม่ข่าย และระบบ เครือข่ายหลัก
บันทึกเหตุการณ์ (Logs)	บันทึกเหตุการณ์การใช้งานของระบบสารสนเทศ การเข้าใช้งานระบบงานหรือ ระบบสารสนเทศ การประมวลผลกิจกรรมของระบบสารสนเทศ และเหตุการณ์ ทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบถึงประสิทธิภาพความปลอดภัย และ ความผิดปกติที่เกิดจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ
การเฝ้าระวัง (Monitoring)	การเฝ้าระวังทางด้านความมั่นคงปลอดภัยสารสนเทศเพื่อตรวจสอบความผิดปกติ จากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศจากบันทึกเหตุการณ์ (Logs) เช่น การเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การใช้งานสารสนเทศผิดวัตถุประสงค์ และปัญหาที่เกิดจากระบบงาน
ความเสี่ยง (Risk)	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือ เหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายของการให้บริการ
โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	โปรแกรมหรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของ ระบบสารสนเทศไม่ทางใดก็ทางหนึ่ง เช่น ไวรัส (Virus) เวิร์ม (Worm) หรือโทรจัน (Trojan) เป็นต้น
แผนการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	การสร้างความต่อเนื่องทางธุรกิจ เพื่อป้องกันการติดขัดหรือการหยุดชะงักของ ระบบงานธุรกรรมที่สำคัญซึ่งอาจมีสาเหตุมาจากภัยทางด้านสิ่งแวดล้อม เหตุการณ์ทางด้านความมั่นคงปลอดภัยหรือภัยคุกคามอื่นๆ
แผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP: Disaster Recovery Plan)	การเตรียมความพร้อมรองรับเหตุฉุกเฉินและแผนการปฏิบัติงานเมื่อเกิดเหตุ ฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงาน ไปจนถึงการใช้งานระบบสารสนเทศสำรอง

คำศัพท์	ความหมาย
แผนสำหรับย้อนกลับสู่สภาวะเดิม (Fallback Plan)	แผนการดำเนินงานเพื่อใช้ในการกลับสู่สถานการณ์ดำเนินงานครั้งล่าสุด เพื่อใช้ใน กรณีที่การแก้ไขเหตุฉุกเฉินไม่เป็นผลสำเร็จ
ระยะเวลาเป้าหมายในการฟื้นคืน สภาพ (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อส่งมอบผลิตภัณฑ์ บริการ และ กิจกรรม หรือกระบวนการกลับสู่สภาวะปกติหลังจากเกิดสถานการณ์ไม่พึง ประสงค์ที่มีความเสียหายระดับรุนแรง
ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายจากระบบได้ และเพื่อเป็นข้อมูลในการ ออกแบบวิธีการสำรองข้อมูลเพื่อให้ข้อมูลไม่สูญหายเกินกว่าที่กำหนดไว้
ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD)	ช่วงเวลาสูงสุดที่การดำเนินงานหยุดชะงัก หากเกินกำหนดช่วงเวลานี้แล้วจะไม่ สามารถทำให้การดำเนินงานฟื้นคืนสู่สภาพปกติได้
ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้รับบริการที่อธิบายถึงรายละเอียดการ บริการ ระดับการให้บริการที่จะถูกวัดและประเมินผล เป้าหมายของระดับการ ให้บริการ รวมไปถึงระบุหน้าที่ความรับผิดชอบที่ชัดเจนของทั้งผู้ให้บริการและ ผู้รับบริการ
ข้อตกลงการให้บริการระดับปฏิบัติงาน (Operational Level Agreement: OLA)	ข้อตกลงในการให้บริการสำหรับปฏิบัติงานร่วมกันระหว่างหน่วยงานภายใน เพื่อสนับสนุนให้การบริการของผู้รับบริการเป็นไปตามข้อตกลงระดับการให้บริการ (SLA)
สัญญาการให้บริการ (Underpinning Contracts: UC)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้รับบริการ/ผู้จำหน่ายระบบ (Vendor) เพื่อให้บริการผู้รับบริการได้ตามข้อตกลงการให้บริการ (SLA)
ระบบงานที่สำคัญ (High Priority Application System)	หมายถึง ระบบที่ให้บริการธุรกรรมหลักที่ใช้ในการให้บริการลูกค้า หรือระบบงาน ที่นำส่งข้อมูลรายงานแก่ทางราชการ
ระบบพัฒนา (Development Area)	ระบบสารสนเทศที่ใช้ในการพัฒนาระบบงาน โดยเป็นการจำลองทรัพยากรและ สภาพแวดล้อมของระบบให้บริการจริง เพื่อใช้พัฒนาระบบงานใหม่
ระบบทดสอบ (User Acceptance Area)	ระบบสารสนเทศที่ใช้ในการทดสอบโดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริงมาเพื่อทดสอบประสิทธิภาพและความ ปลอดภัยของระบบที่ได้พัฒนาขึ้น

คำศัพท์	ความหมาย
ระบบสารสนเทศสำรอง (Disaster Recovery Center: DRC)	ระบบงาน ข้อมูล และระบบเครือข่ายสำรองนอกเหนือจากระบบสารสนเทศหลัก เพื่อให้สามารถทำธุรกรรมหลักได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิด เหตุการณ์ฉุกเฉิน
ระบบให้บริการจริง (Production Area)	ระบบสารสนเทศที่ให้บริการจริงแก่ผู้ใช้งานซึ่งต้องมีการรักษาความมั่นคง ปลอดภัย และการควบคุมการเข้าถึงจากการพัฒนาระบบและการทดสอบระบบ อย่างเคร่งครัด
อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)	เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บ เล็ตคอมพิวเตอร์ (Tablet Computer) ที่องค์กรอนุญาตให้เชื่อมต่อและใช้งาน ระบบสารสนเทศขององค์กรได้
สื่อบันทึกข้อมูล (Media)	อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard Drive หรือ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Drive เป็นต้น

นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1. <u>นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ</u>

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่างๆ โดยองค์กรต้องจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวทางปฏิบัติดังนี้

- **ทิศทางการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Management Directions for Information Security)**

1. นโยบายสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Policy for Information Security)

    1.1 องค์กรต้องจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่าง เป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากคณะกรรมการบริษัท หรือผู้ที่คณะกรรมการบริษัทมอบหมายให้เป็นผู้อนุมัติ

    1.2 องค์กรต้องเผยแพร่นโยบายดังกล่าวให้ผู้ใช้งานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบและถือปฏิบัติเป็นไปตามที่นโยบายกำหนด โดยการเผยแพร่ต้องดำเนินการในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย

2. การทบทวนนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Review of the Policies for Information Security)

    2.1 ต้องดำเนินการตรวจสอบ และทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามเงื่อนไขที่กำหนดไว้ในส่วนการทบทวนนโยบาย

2. <u>การจัดโครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security)</u>

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่างๆ ภายในองค์กร และเพื่อเป็นแนวทางควบคุมการใช้งานอุปกรณ์สื่อสารประเภท พกพา ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

- **การจัดโครงสร้างภายในองค์กร (Internal Organization)**

1. การกำหนดบทบาทและหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities)

    1.1 ผู้บริหารระดับฝ่ายต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความ มั่นคง

ปลอดภัยระบบสารสนเทศสำหรับบุคลากรในหน่วยงานอย่างเป็นลายลักษณ์อักษร และให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำหนดไว้

2. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

    2.1 ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ ในการปฏิบัติงานด้านต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจน เพื่อให้มีการสอบทานระหว่างกันได้

3. การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องด้านความมั่นคงปลอดภัย (Contact with authorities)

    3.1 แผนกเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อและช่องทางการติดต่อของหน่วยงานที่จำเป็น เช่น หน่วยงานด้านกฎหมาย โรงพยาบาล สถานีตำรวจ สถานีดับเพลิง หรือหน่วยกู้ภัย เป็นต้น สำหรับติดต่อเมื่อเกิดเหตุฉุกเฉิน พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

4. การประสานงานกับกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Contact with special interest groups)

    4.1 แผนกเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และเพิ่มช่องทางการรับข่าวสารจากกลุ่มผู้เชี่ยวชาญเพื่อให้สามารถติดต่อประสานงาน หรือรับข้อมูลข่าวสาร หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศได้ทันท่วงที พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

5. การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ (Information Security in Project Management)

    5.1 ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุมความเสี่ยงการติดตามการดำเนินงานโครงการ รวมถึงการประเมินภาพรวมในการดำเนินงานโครงการ ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก

    5.2 ผู้บังคับบัญชา ต้องชี้แจงและส่งเสริมให้ผู้ใช้งานปฏิบัติงานตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัย กรณีพบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

6. หน้าที่ของผู้ใช้งาน

6.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาบการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยเคร่งครัด

6.2 ให้ความร่วมมือกับบริษัทฯ อย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัทฯ สอดส่องดูแล ปกป้องข้อมูลสารสนเทศของบริษัทฯ ให้มีความปลอดภัย

6.3 รายงานต่อบริษัทฯ ทันที เมื่อพบว่าอุปกรณ์หรือข้อมูลสารสนเทศสำคัญสูญหายหรือพบเห็นการบุกรุก ขโมย ทำลายหรือโจรกรรมสารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียต่อบริษัทฯ

7. หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

7.1 จัดให้มีการจัดทำเอกสาร มาตรการ และขั้นตอนการควบคุมการเข้าถึงข้อมูลให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ

7.2 ดูแลให้พนักงานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ

7.3 ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และรบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ

7.4 แจ้งหน่วยงานเทคโนโลยีสารสนเทศที่รับผิดชอบด้านการบริหารบัญชีผู้ใช้งานและสิทธิ์ในการใช้ระบบสารสนเทศเพื่อลบ / เปลี่ยนแปลงสิทธิ์ / เมื่อมีการเปลี่ยนแปลงพนักงาน / อำนาจหน้าที่ / โยกย้าย

- **การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile Computing and Teleworking)**

1. การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communication)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีมาตรการที่เหมาะสมเพื่อรับรองความปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ขององค์กร และเมื่อนำอุปกรณ์ออกไปใช้งานนอกสถานที่

1.2 ผู้ใช้งานที่มีการใช้งานอุปกรณ์สื่อสารประเภทพกพาเพื่อเชื่อมต่อกับระบบสารสนเทศขององค์กรทั้งหมดต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและตระหนักถึงการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯ ต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานหรือผู้บังคับบัญชาสูงสุด

1.3 บริษัทฯ ขอสงวนสิทธิ์ในการตรวจสอบ ระงับ เพิกถอนการใช้งาน และลบข้อมูลทั้งหมด บนอุปกรณ์พกพาทั้งที่เป็นของบริษัทฯ และของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บข้อมูล

สารสนเทศของบริษัทฯ หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐาน หรือข้อมูลและสารสนเทศของบริษัทฯ

2. การปฏิบัติงานภายนอกสำนักงาน (Teleworking)

2.1 ผู้ใช้งานที่มีการทำงานจากภายนอกสำนักงานทั้งหมด จะต้องปฏิบัติตามนโยบายด้านการ รักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรเช่นเดียวกันกับการทำงานภายในสำนักงาน

2.2 ผู้ใช้งานที่มีการใช้ข้อมูลสารสนเทศขององค์กรในการทำงานนอกสำนักงาน หรือการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากเจ้าของข้อมูลสารสนเทศ และหน่วยงานต้นสังกัดโดยต้องมีเหตุผลอันควร

2.3 ผู้ใช้งานที่ต้องการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งาน

3. <u>การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)</u>

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการกำกับ และติดตามการสรรหาบุคลากรเข้ามาปฏิบัติงานภายในองค์กร การบริหารจัดการบุคลากรระหว่างการจ้างงานและการบริหารจัดการบุคลากรเมื่อพ้นสภาพการเป็นลูกจ้างหรือเมื่อมี การเปลี่ยนแปลงหน้าที่การปฏิบัติงาน

- **การบริหารจัดการบุคลากรก่อนการจ้างงาน (Prior to Employment)**

1. การตรวจสอบประวัติ (Screening)

1.1 องค์กรต้องกำหนดให้มีการตรวจสอบประวัติของผู้สมัครงานและหน่วยงานภายนอกที่ต้อง เข้ามาให้บริการภายในหน่วยงาน

2. ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

2.1 แผนกทรัพยากรมนุษย์ต้องกำกับให้มีการลงนามในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของบุคลากร หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ซึ่งได้มีการระบุหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญาหรือข้อตกลงการปฏิบัติงาน ซึ่งผู้ใช้งานต้องรับทราบและยอมรับระเบียบปฏิบัติขององค์กร โดยจะต้องอ่านทำความเข้าใจและปฏิบัติตามนโยบาย กฎ ระเบียบที่องค์กรได้กำหนดไว้

- **การบริหารจัดการบุคลากรระหว่างการจ้างงาน (During employment)**

1. หน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Management Responsibilities)

1.1 ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุม และกำกับให้บุคลากร หรือหน่วยงาน ภายนอกที่ได้รับการว่าจ้างเพื่อปฏิบัติงานหรือให้บริการกับองค์กร ปฏิบัติงานตามนโยบาย ด้านความมั่งคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศที่องค์กรได้ประกาศใช้

2. การอบรม การสร้างความตระหนัก การให้ความรู้ในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information security awareness, education and training)

2.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดช่องทางให้บุคลากรสามารถทำการศึกษาและทำความเข้าใจในนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของตนเองก่อนที่จะอนุญาตให้เริ่มต้น ปฏิบัติงานกับองค์กร

2.2 แผนกเทคโนโลยีสารสนเทศ ต้องจัดให้มีการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไปโดยหน่วยงานผู้รับผิดชอบ เพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เช่น วิธีการใช้ระบบงานวิธีการใช้งานซอฟต์แวร์สำเร็จรูป การแก้ปัญหาการใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมายระเบียบและข้อบังคับที่เกี่ยวข้อง เป็นต้น

2.3 แผนกเทคโนโลยีสารสนเทศ ต้องจัดการอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยเพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เพื่อช่วยให้ผู้รับการว่าจ้างสามารถปฏิบัติงานที่ตนเองรับผิดชอบได้เป็นอย่างดีและอย่างมั่นคงปลอดภัย

3. กระบวนการลงโทษทางวินัย (Disciplinary Process)

3.1 องค์กรต้องจัดให้มีกระบวนการลงโทษทางวินัยเพื่อลงโทษผู้ใช้งานที่ฝ่าฝืนหรือละเมิด นโยบายด้านความมั่งคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการ รักษาความมั่นคงปลอดภัยด้านสารสนเทศหรือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับความ มั่นคงปลอดภัยด้านสารสนเทศขององค์กร

- **การสิ้นสุดการจ้างงานหรือโยกย้ายตำแหน่งงาน (Termination or Change of Employment)**

1. การบริหารจัดการบุคลากรพ้นสภาพหรือเปลี่ยนหน้าที่ความรับผิดชอบในการปฏิบัติงาน (Termination or Change of Employment Responsibilities)

1.1 แผนกทรัพยากรมนุษย์ต้องกำหนดกฎระเบียบและความรับผิดชอบที่เกี่ยวข้องกับการ รักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรและหน่วยงานภายนอกภายหลังจากที่ พ้นสภาพการจ้างงาน หรือมีการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงานอย่างเป็นลายลักษณ์อักษร

1.2 แผนกทรัพยากรมนุษย์ต้องควบคุมดูแลให้บุคลากร และหน่วยงานภายนอก ปฏิบัติตามกฎระเบียบที่กำหนดไว้อย่างเคร่งครัด

4. <u>การบริหารจัดการทรัพย์สิน (Asset Management)</u>

วัตถุประสงค์

เพื่อให้สินทรัพย์และระบบสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม เพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลขององค์กรโดยไม่ได้รับอนุญาต รวมถึงป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์ และเกิดความเสียหายกับทรัพย์สินสารสนเทศขององค์กร

- **หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)**

1. การจัดทำบัญชีทรัพย์สิน (Inventory of Assets)

    1.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมให้หน่วยงานภายในจัดทำบัญชีทรัพย์สินสารสนเทศเพื่อบริหารจัดการและควบคุมทรัพย์สินสารสนเทศอย่างเหมาะสม และให้มีการปรับปรุงบัญชีทรัพย์สินให้เป็นปัจจุบันอยู่เสมอ

2. การระบุผู้ถือครองทรัพย์สิน (Ownership of Assets)

    2.1 ผู้บังคับบัญชาแผนกเทคโนโลยีสารสนเทศต้องกำหนดให้มีการระบุผู้ถือครองทรัพย์สิน ผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม

3. การใช้ทรัพย์สินสารสนเทศ (Acceptable Use of Assets)

    3.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำข้อกำหนดในการใช้ทรัพย์สินเพื่อการบริหารจัดการอุปกรณ์คอมพิวเตอร์ให้เหมาะสมก่อให้เกิดประสิทธิภาพสูงสุด รวมทั้งมีความปลอดภัยจากความเสียหายที่อาจเกิดขึ้นได้ โดยต้องสื่อสารให้บุคลากรขององค์กรรับทราบและปฏิบัติตาม

4. การคืนทรัพย์สิน (Return of Assets)

    4.1 แผนกทรัพยากรมนุษย์หัวหน้างาน หรือผู้บังคับบัญชาต้องกำกับและติดตามให้บุคลากรในหน่วยงานหรือหน่วยงานภายนอกที่เข้ามาให้บริการดำเนินการคืนทรัพย์สิน (Return of Assets) อาทิ เครื่องคอมพิวเตอร์พกพา เอกสาร กุญแจ บัตรพนักงาน ที่เป็นทรัพย์สินขององค์กรให้กับหน่วยงานที่เกี่ยวข้อง

- **การจัดลำดับชั้นความลับของสารสนเทศ (Information Classification)**

1. การจัดลำดับชั้นความลับของสารสนเทศ (Classification of Information)

    1.1 องค์กรต้องกำหนดให้มีการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับโดยให้นำกฎหมายและข้อกำหนดที่เกี่ยวข้อง กับองค์กรมาร่วมพิจารณาการกำหนดชั้นความลับที่เหมาะสม

    1.2 หน่วยงานภายในองค์กรต้องจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศที่ใช้ในการดำเนินงานขององค์กร และกำหนดลำดับชั้นความลับของข้อมูลและทรัพย์สินสารสนเทศ

    1.3 หน่วยงานภายในองค์กรต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้ในระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2. การบ่งชี้สารสนเทศ (Labeling of Information)

    2.1 องค์กรต้องควบคุมให้ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นมีการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้บุคลากรและผู้ที่เกี่ยวข้องต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

    2.2 แผนกเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง ต้องทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สิน และขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

3. การบริหารจัดการทรัพย์สิน (Handling of Assets)

    3.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการบริหารจัดการทรัพย์สินสารสนเทศเพื่อมิให้ข้อมูลสำคัญขององค์กรรั่วไหลหรือทรัพย์สินสารสนเทศถูกนำไปใช้ผิดประเภท

- **การจัดการสื่อบันทึกข้อมูล (Media Handling)**

1. การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Management of Removable Media)

    1.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

    1.2 การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ต้องมีความสอดคล้องกับการกำหนดลำดับชั้นความลับข้อมูล

2. การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

2.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติงานทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับหรือมีความสำคัญ

2.2 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการทำลายสื่อบันทึกข้อมูลโดยอ้างอิงมาตรฐานซึ่งเป็นที่ยอมรับในสากล

3. การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

3.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติงานหรือข้อกำหนดในการดูแล รักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออก จากพื้นที่ติดตั้งหรือพื้นที่ปฏิบัติงาน

5. <u>การควบคุมการเข้าถึง (Access Control)</u>

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกรวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะ สร้างความเสียหายให้แก่ข้อมูลขององค์กร

- **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 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการขอเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานโดยต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น

2.2 แผนกเทคโนโลยีสารสนเทศ ต้องจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้ เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตให้เข้าถึงเท่านั้น โดยสิทธิ์ที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

- **การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)**

1. การลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration)

    1.1 แผนกเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องร่วมกันกำหนดวิธีการบริหารจัดการการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

2. การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

    2.1 แผนกเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดให้มีการมอบหมายหรือกำหนด สิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ

    2.2 แผนกเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องจัดทำเอกสารการมอบหมายสิทธิ์การเข้าถึงข้อมูลหรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน

    2.3 แผนกเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดกระบวนการในการบริหารจัดการสิทธิการเข้าถึง ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องใช้งานข้อมูลหรือระบบสารสนเทศเกินสิทธิ์ที่ได้รับมอบหมาย

3. การบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิระดับสูง (Management of Privileged Access Right)

    3.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดเก็บรหัสผู้ใช้งานที่มีสิทธิระดับสูง เช่น Administrator/root บนเครื่องแม่ข่าย หรือ Administrator ของระบบ Application และให้มีการเบิกใช้งานตามความจำเป็นเท่านั้น

    3.2 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิระดับสูงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม

4. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้ (Management of Secret Authentication Information of Users)

    4.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

5. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

    5.1 แผนกเทคโนโลยีสารสนเทศและเจ้าของข้อมูลต้องจัดทำขั้นตอนปฏิบัติงานทบทวนสิทธิการเข้าถึงข้อมูลระบบสารสนเทศ และโปรแกรมประยุกต์ (Application) อย่างเป็นลายลักษณ์

อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กร รับทราบและปฏิบัติตาม

5.2 แผนกเทคโนโลยีสารสนเทศและเจ้าของข้อมูลต้องกำหนดรอบในการทบทวนสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศอย่างชัดเจนและแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ

5.3 การทบทวนสิทธิการเข้าถึง ต้องพิจารณาประเด็นดังต่อไปนี้

- รอบการทบทวนสิทธิที่กำหนดไว้
- การพ้นสภาพการเป็นบุคลากรขององค์กร
- การเปลี่ยนแปลงโยกย้ายหน้าที่การปฏิบัติงาน
- การขอใช้สิทธินอกเหนือจากหน้าที่ความรับผิดชอบที่กำหนดไว้

5.4 เมื่อดำเนินการทบทวนสิทธิเรียบร้อยแล้วให้เจ้าของข้อมูลหรือผู้ดูแลระบบจัดเก็บหลักฐาน การทบทวนสิทธิโดยให้แยกหลักฐานตามช่วงเวลาการทบทวนสิทธิ

6. การถอดถอนสิทธิในการเข้าถึง (Removal of Access Rights)

6.1 เจ้าของข้อมูล และผู้ดูแลระบบ ต้องกำหนดเกณฑ์การพิจารณาการถอดถอนสิทธิการเข้าถึงและวิธีการถอดถอนสิทธิในการเข้าถึงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

- **หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)**

1. การใช้งานข้อมูลการพิสูจน์ตัวตน (Use of Secret Authentication Information)

1.1 ใช้งานจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการเดา อาทิ คำศัพท์ในพจนานุกรมหรือคัดลอกหรือผสมจากชื่อผู้ใช้หรืออักขระเรียงลำดับหรือข้อมูลส่วนบุคคล หรือประโยควลีใดๆ ที่สามารถคาดเดาได้ง่าย

1.2 ผู้ใช้งานจะต้องไม่เขียนหรือบันทึกรหัสผ่านที่ใช้ และเก็บหรือแสดงให้เห็นไว้ใกล้กับระบบ หรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น

1.3 ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานของตน หรือกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ์

1.4 ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการบริหารจัดการรหัสผ่านอื่นๆ ที่องค์กรกำหนดไว้

1.5 ผู้ใช้งานหรือพนักงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติดังต่อไปนี้

- ต้องออกจากระบบ (Log – Out, Log – Off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานานและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน
- ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอื่นเป็นระยะเวลาสั้น ๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน
- ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้งโดยใช้โปรแกรมป้องกันไวรัส (Anti-Virus) ที่มีข้อมูลไวรัสที่ทันสมัย
- ต้องระมัดระวังการโพสต์ข้อความ หรือการแสดงความคิดเห็นต่าง ๆ ผ่านสื่อโซเชียลมีเดีย (Social Media) ต่าง ๆ ที่อาจเข้าข่ายละเมิดบุคคลอื่น ๆ หรืออันทำให้เกิดความเข้าใจผิดต่อบริษัทฯ ได้
- ต้องระมัดระวังการได้รับข้อมูลปลอมต่าง ๆ หรือเรียกว่าการหลอกหลวง “ฟิชชิ่ง” ซึ่งเป็นการหลอกให้ผู้ใช้งานคลิก หรือกรอกข้อมูลต่าง ๆ ทั้งจากอีเมล เว็บ ไลน์ หรืออื่น ๆ อันมีเจตนาที่จะได้ข้อมูลสำคัญจากผู้ใช้งาน
- ต้องใช้อีเมลประจำตัวพนักงานที่ทางบริษัทสร้างให้เพื่อใช้สำหรับติดต่อสื่อสารภายในบริษัทฯ และบริษัทฯในเครือ รวมถึงลูกค้า หรือคู่ค้าภายนอก ห้ามผู้ใช้นำ E-Mail ส่วนตัวของพนักงานมาใช้ในการติดต่อสื่อสารถึงข้อความใดๆที่มีเนื้อหาเกี่ยวข้องกับธุรกิจของบริษัทกับบุคคลภายนอก หรือบริษัทคู่ค้าทั้งหมด
- ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทฯ กำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทฯ เป็นความลับเฉพาะตกเองเท่านั้น ห้ามมิให้ผู้อื่นล่วงรู้ และใช้งานร่วมกัน
- ต้องระมัดระวังการใช้งานจดหมายอิเล็กทรอนิกส์ส่วนบุคคล เพื่อใช้ในการส่งออก หรือเผยแพร่ข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับ (Sensitive Information) ของบริษัทฯ
- พนักงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอกจะต้องสื่อสารและดำเนินการให้บุคคลภายนอกนั้นปฏิบัติตามนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ ด้วย

- **การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)**

1. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการเข้าถึงข้อมูลระบบสารสนเทศและฟังก์ชั่นในระบบงาน โดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

1.2 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดวิธีการใช้งานระบบสารสนเทศที่สำคัญไม่ว่าจะเป็นข้อมูล ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้ สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของฝ่ายงานนั้นๆ เป็นลายลักษณ์อักษร

2. การเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)

2.1 แผนกเทคโนโลยีสารสนเทศต้องกำหนดวิธีการเข้าสู่ระบบสารสนเทศที่มีความมั่นคง ปลอดภัย อย่างเป็นลายลักษณ์อักษร โดยอ้างอิงวิธีการที่เป็นมาตรฐานสากลและปรับปรุง ให้เป็นปัจจุบัน เสมอรวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

3. ระบบสำหรับบริหารจัดการรหัสผ่าน (Password Management System)

3.1 แผนกเทคโนโลยีสารสนเทศต้องจัดให้มีระบบสำหรับบริหารจัดการบัญชีผู้ใช้และรหัสผ่านสำหรับการเข้าถึงระบบสารสนเทศของผู้ใช้งานภายในองค์กร เพื่อให้เกิดการบริหารจัดการที่เป็นมาตรฐานเดียวกัน

4. การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

4.1 แผนกเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ และจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบสารสนเทศหรือโปรแกรม คอมพิวเตอร์ที่สำคัญเพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ ได้กำหนดไว้ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

5. การเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

5.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม และการนำซอร์สโค้ดของโปรแกรมไปใช้ในการพัฒนา เพื่อป้องกันการเกิดข้อผิดพลาดในการพัฒนาระบบสารสนเทศ และระบบงานขององค์กร

6. <u>การเข้ารหัสลับข้อมูล (Cryptographic)</u>

วัตถุประสงค์

เพื่อกำหนดแนวทางการเข้ารหัสลับข้อมูล และทำให้ระบบสารสนเทศธำรงไว้ซึ่งการรักษาความลับของ ข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และ/หรือ ป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต อย่างมีความเหมาะสม มีประสิทธิภาพ โดยมีข้อปฏิบัติดังนี้

- **มาตรการการเข้ารหัสลับข้อมูล (Cryptographic Controls)**

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

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการ เลือกมาตรฐานการเข้ารหัสลับข้อมูลโดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้

2. การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล (Key Management)

2.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล โดยให้ครอบคลุมวงจรการบริหารจัดการกุญแจ (key Management Life Cycle) รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

7. <u>การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)</u>

วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกันควมคุมการใช้งานและการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศขององค์กรให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

- **พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Area)**

1. ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

1.1 องค์กรต้องพิจารณาและจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัยโดยจะประกอบด้วย พื้นที่กั้นบริเวณจัดทำผนังหรือกำแพงล้อมรอบจัดทำประตูทางเข้า - ออกหลักและระบบรักษาความปลอดภัยอย่างเหมาะสม

2. การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)

2.1 องค์กร ต้องควบคุมการเข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญให้เข้าถึงได้เฉพาะบุคลากรผู้ได้รับอนุญาตเท่านั้น

2.2 รายชื่อผู้ได้รับอนุญาตให้เข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ต้องได้รับการตรวจสอบ ปรับปรุง และดูแลให้เหมาะสมอย่างสม่ำเสมอ

2.3 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความปลอดภัย (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ รวมถึงพื้นที่ปฏิบัติงานของผู้ดูแลระบบ

โดยต้องกำหนดให้เฉพาะผู้มีสิทธิ์ที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้า - ออกห้องคอมพิวเตอร์ และบันทึกการเข้า - ออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก วัตถุประสงค์การผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

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

    3.1 แผนกเทคโนโลยีสารสนเทศ ต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบหรืออุปกรณ์สารสนเทศต่างๆ ที่ใช้ในการปฏิบัติงานอันเนื่องจากการได้รับความเสียหายและถูกเข้าถึงโดยไม่ได้รับอนุญาต

4. การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against External and Environmental Threats)

    4.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมกำกับให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยคุกคามจากภายนอก ทั้งที่ก่อโดยมนุษย์ หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

5. การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

    5.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำกับให้มีการกำหนดแนวปฏิบัติของการป้องกันทางกายภาพสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบ และกำหนดให้มีการนำแนวปฏิบัติไปใช้งานอย่างเคร่งครัด

6. พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas)

    6.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิ์เข้าถึงอาจสามารถเข้าถึงได้ โดยต้องกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์ ทั้งนี้ให้แยกเป็นสัดส่วนที่ชัดเจนเพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

- **อุปกรณ์ (Equipment)**

1. การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

    1.1 แผนกเทคโนโลยีสารสนเทศต้องจัดวางอุปกรณ์สารสนเทศไว้ในห้องหรือบริเวณที่ปลอดภัย อุปกรณ์ที่มีตู้ ประตูของตู้วางคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารเครือข่ายต้องถูกล็อคอยู่เสมอ

โดยกำหนดให้มีเพียงเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้นมีสิทธิ์ในการเปิดเพื่อซ่อมบำรุง หรือการปรับปรุงค่าคอนฟิเกอเรชัน (Reconfiguration) เพื่อลดความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

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

3. ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

    3.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้การติดตั้งและการบำรุงรักษาสายไฟฟ้าและสายสื่อสารในพื้นที่ปฏิบัติงานและห้องคอมพิวเตอร์เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรม เพื่อป้องกันไม่ให้มีการเข้าถึงหรือดักจับข้อมูลหรือเกิดความเสียหายทางด้านกายภาพ

4. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

    4.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้อุปกรณ์ระบบสารสนเทศหลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนการทำงานได้รับการบำรุง ดูแลรักษาตามช่วงเวลาและตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่าง ต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

    4.2 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุง อุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

5. การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets)

    5.1 ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ต้องไม่อนุญาตให้นำอุปกรณ์สารสนเทศออกจากองค์กร ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

    5.2 ผู้ใช้งาน ต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกนอกองค์กร ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

5.3 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการนำทรัพย์สินออกนอกสำนักงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

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

6.1 กำหนดให้ผู้บริหารระดับฝ่ายขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์สารสนเทศขององค์กรไปใช้งานภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่างๆ ที่ใช้งานอยู่ภายนอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

6.2 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการความมั่นคงปลอดภัยในการควบคุมทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินขององค์กรออกไปใช้งาน

7. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานซ้ำ (Secure Disposal or Re-Use of Equipment)

7.1 ผู้ใช้งาน ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลายอย่างเหมาะสมตามลำดับชั้นความลับข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่

7.2 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลหรือทรัพย์สินสารสนเทศ และมาตรการหรือเทคนิคสำหรับการทำลายข้อมูลเพื่อนำอุปกรณ์สารสนเทศกลับมาใช้งานซ้ำ โดยต้องมีความสอดคล้องกับการจัดลำดับชั้นความลับข้อมูล

7.3 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดผู้รับผิดชอบในการทำหน้าที่ทำลายข้อมูลสารสนเทศที่ไม่จำเป็นต่อการดำเนินกิจการขององค์กรซึ่งจัดเก็บอยู่บนสื่อบันทึกข้อมูล

8. การป้องกันอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)

8.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศที่ทิ้งไว้โดยไม่มีผู้ดูแล เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ ไม่ได้รับอนุญาต

8.2 ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

8.3 ผู้ใช้งานต้องออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งานหรือเครื่องคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน

8.4 ผู้ใช้งาน ต้องล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์

9. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

9.1 ผู้ดูแลระบบ ต้องควบคุมให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session Time Out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

9.2 ผู้ใช้งาน ต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูลให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ์

9.3 ผู้ใช้งานต้องไม่จัดเก็บข้อมูลสำคัญไว้บนหน้าเดสท็อป (Desktop) ของเครื่องคอมพิวเตอร์ โดยผู้ใช้งานต้องจัดสรรพื้นที่ในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์และควบคุมการเข้าถึงอย่างเหมาะสม เพื่อป้องกันผู้อื่นเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

8. <u>การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security)</u>

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมให้การดำเนินงาน การจัดการด้านการสื่อสารความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรมีแนวทางปฏิบัติที่มีขั้นตอนชัดเจนและมีความมั่นคงปลอดภัย

- **ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operations Procedures and Responsibilities)**

1. ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดให้มีขั้นตอนปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษรโดยต้องแบ่งแยกอำนาจหน้าที่ของบุคลากรตามโครงสร้างการปฏิบัติหน้าที่ที่ชัดเจนเพื่อให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร

1.2 หน่วยงานในแผนกเทคโนโลยีสารสนเทศ ต้องจัดทำคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงาน และกระบวนการทำงาน

1.3 หน่วยงานในแผนกเทคโนโลยีสารสนเทศ ต้องทบทวนวิธีปฏิบัติคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้ขั้นตอน

ปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้และต้องสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม

2. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

   2.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของการเปลี่ยนแปลงโครงสร้างองค์กร ขั้นตอนการปฏิบัติงานระบบสารสนเทศ เพื่อ ควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใดๆ ซึ่งส่งผลต่อการดำเนินงานของระบบงานต่างๆ ทั้งนี้ให้ปฏิบัติตามที่กำหนดไว้ในนโยบายการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (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 และต้องวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมีประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งานในอนาคต

4. การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)

   4.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) การทดสอบระบบงาน (Test Environment) และระบบที่ให้บริการจริง (Production Environment) ออกจากกัน

   4.2 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดสิทธิ์การเข้าถึงในแต่ละสภาพแวดล้อม และจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไขรวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ+

- **การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)**

1. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

- **การสำรองข้อมูล (Back up)**

1. การสำรองข้อมูล (Information Backup)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการสำรองข้อมูล และรอบการสำรองข้อมูลของระบบสารสนเทศที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล

1.2 เจ้าของข้อมูลสารสนเทศ ต้องดำเนินการหรือกำหนดให้มีการสำรองข้อมูลสารสนเทศและการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ

1.3 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น External Hard Disk เป็นต้น ให้เป็นปัจจุบันอย่างสม่ำเสมอ รวมถึงให้จัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

- **การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)**

1. การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)

1.1 ผู้ดูแลระบบ ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ

1.2 ผู้ดูแลระบบ ต้องเฝ้าติดตาม (Monitoring) การใช้งานระบบสารสนเทศ โดยผลของการเฝ้าติดตามจะต้องถูกสอบทานอย่างสม่ำเสมอเพื่อตรวจหาความผิดปกติ

1.3 ผู้ดูแลระบบ ต้องควบคุมและกำกับให้มีการบันทึกเหตุการณ์ความผิดพลาด (Fault Logging) ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ รวมถึงวิเคราะห์ ดำเนินการแก้ไขตลอดจนวางแนวทางป้องกันการเกิดปัญหาซ้ำอีกในอนาคต

2. การป้องกันข้อมูลล็อก (Protection of Log Information)

2.1 ผู้ดูแลระบบ ต้องจัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ถูกทำความเสียหายหรือเข้าถึงโดยไม่ได้รับอนุญาต

3. การบันทึกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs)

3.1 ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบและผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ อาทิ เวลาเปิดและปิดระบบ การเปลี่ยนแปลงการตั้งค่าของระบบ ความผิดพลาดของระบบ และการดำเนินการแก้ไข และต้องมีการสอบทานบันทึกกิจกรรมอย่างสม่ำเสมอ

4. การตั้งเวลาระบบสารสนเทศ (Clock Synchronization)

4.1 ผู้ดูแลระบบ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศและระบบสารสนเทศขององค์กรได้รับการกำหนดเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องและตรงกับเวลาอ้างอิงสากล

4.2 ผู้ดูแลระบบ ต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศและระบบสารสนเทศขององค์กร รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอเพื่อป้องกันไม่ให้เกิดการบันทึกเวลาที่ไม่ถูกต้อง

- **การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)**

1. การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน

1.2 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ขององค์กรอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

- **การบริหารจัดการช่องโหว่ทางเทคนิคในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)**

1. การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมให้ระบบสารสนเทศขององค์กรได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง

1.2 ผู้ดูแลระบบ ต้องดูแลและบำรุงรักษาระบบ เพื่อรักษาระดับความมั่นคงปลอดภัยด้านสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ที่ตรวจสอบพบและการปรับปรุงแก้ไขช่องโหว่ของระบบสารสนเทศ

2. การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

2.1 ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์และไม่ติดตั้งซอฟต์แวร์ที่ ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ขององค์กร

- **สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)**

1. มาตรการการตรวจประเมินระบบ (Information System Audit Controls)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ เช่น แผนการตรวจสอบช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) เป็นต้น

1.2 แผนกเทคโนโลยีสารสนเทศ ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบก่อนดำเนินการตรวจสอบระบบสารสนเทศทุกครั้ง

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

9. <u>การสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ (Communications Security)</u>

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการบริหารจัดการเครือข่าย และการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกองค์กรให้มีความมั่นคงปลอดภัย

- **การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)**

1. การควบคุมเครือข่าย (Network Controls)

1.1 ผู้ดูแลระบบ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

2. ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

2.1 ผู้ดูแลระบบ ต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมดลง

ในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการ จากภายในหรือภายนอก

3. การแบ่งแยกเครือข่าย (Segregation in Network)

3.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตาม ความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศและระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

- **การแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer)**

1. นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer Policies and Procedures)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล

2. ข้อตกลงสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Agreements on Information Transfer)

2.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอกองค์กร

2.2 การแลกเปลี่ยนข้อมูลสารสนเทศภายในองค์กรกับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อนทุกครั้ง และมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลสารสนเทศตามลำดับชั้นความลับข้อมูลอย่างเหมาะสม

3. การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)

3.1 แผนกเทคโนโลยีสารสนเทศ 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 ผู้บริหารระดับฝ่ายต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้องค์กร มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลขององค์กรอย่างเป็นลายลักษณ์อักษร

10. <u>การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)</u>

วัตถุประสงค์

เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

- **ความต้องการด้านความมั่นคงปลอดภัยระบบ (Security Requirements of Information Systems)**

1. การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

   1.1 หน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศเพื่อนำมาใช้งานในองค์กร กำหนดคุณลักษณะความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งานหรือระบบที่จัดหามาใช้งาน

   1.2 หน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศ ต้องติดตามการพัฒนาระบบสารสนเทศ เพื่อตรวจสอบว่าการพัฒนาระบบสารสนเทศตรงตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงความต้องการด้านการใช้งานที่กำหนดไว้

2. ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Service on Public Networks)

   2.1 ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกันการกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission or Miss-Routing) หรือการเปิดเผย คัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

3. การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting Application Services Transactions)

   3.1 ข้อมูลสารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง (Miss-Routing) การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการสำเนาข้อมูลโดยไม่ได้รับอนุญาต

- **ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes)**

    1. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

        1.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดกฎระเบียบสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยและครอบคลุมตลอดทั้งวงจรการพัฒนาระบบสารสนเทศ

    2. ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

        2.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษรโดยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ

    3. การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical Review of Applications after Operating Platform Changes)

        3.1 ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบที่อาจเกิดขึ้นเมื่อต้องการที่จะเปลี่ยนแปลงหรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชัน และการแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัย เป็นต้น โดยจะต้องมีการทดสอบบนเครื่องทดสอบ (Test Environment) จนมั่นใจว่าระบบงานต่างๆ ที่ประมวลผลบนเครื่องดังกล่าวสามารถทำงานได้ตามปกติและมีความมั่นคงปลอดภัย 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 ต้องดำเนินการเปลี่ยนแปลงตามขั้นตอนปฏิบัติงานควบคุมการเปลี่ยนแปลงที่แผนกเทคโนโลยีสารสนเทศกำหนดไว้

    5. หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)

        5.1 หน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องยึดหลักการความมั่นคง ปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้เป็นอย่างน้อย

- การให้สิทธิ์ต่ำที่สุด (Least Privilege) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
- การให้สิทธิ์เฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
- การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (Defense In-Depth) เพื่อลด ความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การออกแบบในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกันและสามารถตรวจสอบการทำงานได้

6. สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)

   6.1 หน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของ ระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ

7. การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)

   7.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดข้อตกลงในการพัฒนาระบบสำหรับหน่วยงานภายนอกที่ทำหน้าที่พัฒนาซอฟต์แวร์เพื่อใช้งานภายในองค์กรอย่างเป็นลายลักษณ์อักษร

   7.2 หน่วยงานที่ได้รับมอบหมายให้ดำเนินการจัดจ้างหน่วยงานภายนอกเข้ามาพัฒนาระบบสารสนเทศให้องค์กรต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้เกิดความเสียหายใดๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

8. การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

   8.1 หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งาน ต้องร่วมกันทดสอบฟังก์ชันการทำงานของระบบสารสนเทศ และฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงทุกครั้ง

   8.2 การทดสอบการพัฒนาระบบสารสนเทศ ต้องดำเนินการทดสอบระหว่างการพัฒนา และก่อนนำระบบขึ้นใช้งานจริง โดยต้องจัดเก็บหลักฐานในการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงอย่างเป็นทางการ

9. การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

9.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากส่วนพัฒนาระบบเทคโนโลยีสารสนเทศพัฒนาขึ้นหรือที่มีการจัดหาจากหน่วยงานภายนอก และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้ งานจริง

- **ข้อมูลสำหรับการทดสอบ (Test Data)**

1. การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

1.1 หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบ

1.2 ใช้งานจริง

11. <u>การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)</u>

วัตถุประสงค์

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงานของหน่วยงานภายนอกในการให้บริการหรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศให้มีประสิทธิภาพมีความมั่นคงปลอดภัยและได้รับผลประโยชน์สูงสุดแก่องค์กร

- **ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับหน่วยงานภายนอก (Information Security in Supplier Relationships)**

1. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับหน่วยงานภายนอก (Information Security Policy for Supplier Relationships)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน่วยงานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาหรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้หน่วยงานภายนอกหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศขององค์กร

1.2 ผู้ดูแลระบบและหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมกำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการและระดับการให้บริการ

2. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

    2.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศ เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศหรือการพัฒนาระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร

    2.2 ผู้ดูแลระบบและหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมให้หน่วยงานภายนอกสามารถเข้าถึงสารสนเทศขององค์กรเฉพาะส่วนที่มีความจำเป็นต้องรู้และต้องได้รับการยินยอมจากเจ้าของข้อมูลสารสนเทศอย่างเป็นลายลักษณ์อักษรเท่านั้น

    2.3 ผู้ดูแลระบบและหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอกต้องควบคุมดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่าง องค์กรและหน่วยงานภายนอก

3. การบริหารจัดการและการสื่อสารต่อผู้รับจ้างช่วงของหน่วยงานภายนอก (Information and Communication Technology Supply Chain)

    3.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมถึงผู้รับจ้างช่วงที่หน่วยงานภายนอกเป็นผู้จัดหา

- **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 และหน่วยงานที่ได้รับมอบหมายให้

ประสานงานกับ หน่วยงานภายนอก ต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหารและผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

12. การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศการเรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้นและการปรับปรุงแก้ไข ซึ่งเป็นการป้องกันไม่ให้เกิดเหตุการณ์ทางด้านความมั่นคง ปลอดภัยสารสนเทศซ้ำขึ้นอีก

- **การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Management of Information Security Incidents and Improvements)**

1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

    1.1 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดหน้าที่ในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิดและมอบหมายสิทธิ์การดำเนินงานอย่างชัดเจนให้บุคลากรภายในฝ่าย

    1.2 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคง ปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิดออกจากเหตุขัดข้องด้านการปฏิบัติงานทั่วไป เพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม

    1.3 แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดช่องทางและเกณฑ์ในการรายงานเหตุการณ์หรือจุดอ่อน หรือเหตุขัดข้องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และสื่อสารให้บุคลากรในองค์กรและหน่วยงานภายนอกรับทราบ

2. การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)

    2.1 ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้บังคับบัญชาและแผนกเทคโนโลยีสารสนเทศโดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

3. การรายงานจุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

    3.1 ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้บังคับบัญชาและแผนกเทคโนโลยีสารสนเทศ โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

3.2 ผู้ใช้งานและหน่วยงานภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศหรือจุดอ่อนใดๆ ของระบบสารสนเทศในองค์กร ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชาและแผนกเทคโนโลยีสารสนเทศ 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 บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ต้องดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้

5.2 บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ต้องดำเนินการตอบสนองและแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หากไม่สามารถแก้ไขได้ตามเวลาที่กำหนดต้องแจ้งให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด

6. การเรียนรู้จากเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)

6.1 บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องจัดเตรียมรายงานผลการวิเคราะห์และการแก้ไขเหตุขัดข้อง จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และจัดเก็บไว้เป็นองค์ความรู้ เพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต

7. การเก็บรวบรวมหลักฐาน (Collection of Evidence)

7.1 บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องดำเนินการเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อรวบรวมหลักฐานให้

เพียงพอต่อการนำเสนอผู้บริหารหน่วยงานที่เกี่ยวข้อง และใช้ในการดำเนินการด้านกฎหมายต่อไป

13. ความมั่นคงปลอดภัยสำหรับการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อป้องกันการติดขัดหรือหยุดชะงักของการดำเนินธุรกิจขององค์กรและป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวของระบบสารสนเทศและเพื่อให้สามารถกู้ระบบสารสนเทศกลับคืนมาได้ใน ระยะเวลาอันเหมาะสม

- **ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)**

1. การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity)

   1.1 เจ้าของข้อมูลและแผนกเทคโนโลยีสารสนเทศต้องร่วมกันระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ประเมินความเสี่ยงเหตุการณ์และระบบงานสำคัญ เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้องและครบถ้วน เพื่อใช้ในการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

2. การสร้างกระบวนการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)

   2.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้เป็นส่วนหนึ่งของแผนและให้มีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจขององค์กร

3. การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)

   3.1 แผนกเทคโนโลยีสารสนเทศ ต้องทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ 1 ครั้ง และจัดให้มีการบันทึกผลการทดสอบ เพื่อให้มั่นใจว่าแผนงานที่จัดทำมีความถูกต้องและสามารถตอบสนองต่อการดำเนินงานได้เป็นอย่างดี

   3.2 บุคลากรผู้ซึ่งมีส่วนเกี่ยวข้องในการปฏิบัติงานกู้คืนระบบสารสนเทศ ต้องมีความรู้ด้านเทคนิคที่จำเป็นต่อการกู้คืนระบบและเข้าร่วมการซักซ้อมแผน

   3.3 เจ้าของข้อมูลและผู้ใช้งานระบบที่เกี่ยวข้องกับแผนรองรับการดำเนินการทางธุรกิจอย่างต่อเนื่อง ต้องเข้าร่วมการทดสอบแผนและดำเนินงานตามแผนที่กำหนดไว้

- **การจัดให้มีอุปกรณ์หรือระบบสารสนเทศสำรอง (Redundancies)**

1. สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

1.1 องค์กรต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่มีความสำคัญสูง

1.2 องค์กรต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

14. <u>การปฏิบัติตามกฎระเบียบและข้อบังคับ (Compliance)</u>

วัตถุประสงค์

เพื่อให้การดำเนินงานต่างๆ ขององค์กรเป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ ที่องค์กรและบุคลากรขององค์กรต้องปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

- **การปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง (Compliance with Legal and Contractual Requirements)**

1. การระบุกฎหมายและข้อกำหนดในสัญญาจ้าง (Identification of Applicable Legislation and Contractual Requirements)

1.1 แผนกเทคโนโลยีสารสนเทศ ต้องร่วมกับฝ่ายกฎหมายและแผนกทรัพยากรมนุษย์ในการรวบรวมกฎหมาย กฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ และจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

1.2 บุคลากรทั้งหมดต้องรับผิดชอบในการปฏิบัติตามข้อกำหนดที่ได้มีการระบุไว้อย่างเคร่งครัด

1.3 ห้ามเจ้าหน้าที่ในองค์กรใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศขององค์กรกระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

2. การป้องกันสิทธิ์และทรัพย์สินทางปัญญา (Intellectual Property Rights)

2.1 แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำกระบวนการสำหรับการบริหารจัดการการใช้ซอฟต์แวร์ลิขสิทธิ์และทรัพย์สินทางปัญญา เพื่อให้มั่นใจว่าการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ

2.2 ผู้ใช้งานต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

2.3 ห้ามผู้ใช้งานทำการใช้งานทำซ้ำหรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์หรือติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กรโดยเด็ดขาด

2.4 ซอฟต์แวร์ที่พัฒนาเพื่อองค์กร ทั้งโดยหน่วยงานภายนอกหรือบุคลากรในหน่วยงานขององค์กร ถือว่าเป็นทรัพย์สินขององค์กร องค์กรไม่อนุญาตให้หน่วยงานภายนอกหรือบุคลากรในหน่วยงานขององค์กรทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินขององค์กรโดยไม่ได้รับอนุญาต

2.5 ผู้ใช้งานที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรต้องยึดถือและปฏิบัติตามกฎหมาย นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

2.6 ห้ามมิให้พนักงานเปิดเพลงที่ไม่มีใบอนุญาตและเพลงที่ทางบริษัทไม่ได้เป็นผู้จัดส่งให้เข้าในระบบกระจายเสียงของบริษัท ทั้งนี้รวมถึงการเปิดเพลงจากแผ่นเสียงที่มีลิขสิทธิ์ถูกต้องหรือจากเครือข่ายสาธารณะ เช่น วิทยุ YouTube เป็นต้น เนื่องจากการกระทำดังกล่าวอาจถือเป็นการละเมิดลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 (และที่แก้ไขเพิ่มเติม) ในเรื่องของการเผยแพร่ผลงานต่อสาธารณชนโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

3. การป้องกันข้อมูลขององค์กร (Protection of Records)

3.1 เจ้าของข้อมูล ต้องปฏิบัติตามข้อบังคับทางกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศบางประเภท เช่น ด้านบัญชี ด้านลูกค้า และต้องจัดทำข้อกำหนดในการจัดการข้อมูลสารสนเทศ ระยะเวลาในการจัดเก็บให้สอดคล้องกับข้อบังคับดังกล่าว

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

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

4.1 องค์กรต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย ประกาศหลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับองค์กร

4.2 ข้อมูลสารสนเทศรายละเอียดที่เกี่ยวกับลูกค้าถือว่ามีความสำคัญ หน่วยงานผู้รับผิดชอบในการดูแลข้อมูลต้องกำหนดให้บุคลากรและลูกจ้างที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศดังกล่าวได้

4.3 ข้อมูลสารสนเทศส่วนบุคคลของบุคลากร ลูกจ้าง และลูกค้า ถือว่าเป็นความลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิตามที่องค์กรกำหนดเท่านั้น

5. ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสลับข้อมูล (Regulation of Cryptographic Controls)

5.1 แผนกเทคโนโลยีสารสนเทศ ต้องควบคุมการเข้ารหัสลับข้อมูลให้มีความสอดคล้องกับกฎหมายประกาศหลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับองค์กร

- **การทบทวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Reviews)**

1. การตรวจประเมินระบบสารสนเทศจากผู้ตรวจสอบอิสระ (Independent Review of Information Security)

1.1 องค์กรต้องจัดให้มีการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศ โดยส่วนตรวจสอบระบบงานหรือผู้ตรวจสอบอิสระภายนอก เพื่อตรวจสอบการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนทบทวนถึงความ พอเพียงของการควบคุมระบบสารสนเทศ และการปฏิบัติตามการควบคุมต่างๆ

2. การปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยสารสนเทศ (Compliance with Security Policies and Standards)

2.1 ผู้บังคับบัญชาของแต่ละแผนกต้องรับผิดชอบในการสอบทานการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศของ บุคลากรใต้บังคับบัญชาอย่างสม่ำเสมอ

2.2 กรณีที่ผู้บังคับบัญชาของแต่ละแผนกตรวจพบการปฏิบัติงานที่ไม่สอดคล้องกับนโยบาย มาตรฐาน และขั้นตอนปฏิบัติซึ่งยังไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ผู้บังคับบัญชาต้องชี้แจงให้บุคลากรใต้บังคับบัญชารับทราบและทำความเข้าใจ แต่หากความไม่สอดคล้องที่พบส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของ องค์กร ผู้บังคับบัญชาต้องดำเนินการลงโทษทางวินัยตามกฎระเบียบที่องค์กรกำหนดไว้

2.3 แผนกเทคโนโลยีสารสนเทศ ต้องให้การสนับสนุนด้านการให้คำแนะนำในการใช้งาน หรือการปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศต่อหน่วยงานอื่นเมื่อได้รับคำร้องขอ

3. การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

3.1 ต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค เช่น การทดสอบการบุกรุกระบบสารสนเทศ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

3.2 ส่วนตรวจสอบระบบงานต้องตรวจสอบการควบคุมทางเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอเหมาะสมและมีการปฏิบัติตามการควบคุมเหล่านั้น

3.3 ผู้ดูแลระบบต้องจัดให้มีการทดสอบระดับมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การตรวจหาช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) หรือการทดสอบการบุกรุกระบบ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้ สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และ มาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Information Security Policy) นี้ ได้รับอนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2568 เมื่อวันที่ 25 กุมภาพันธ์ 2568 และมีผลบังคับใช้ตั้งแต่วันที่ 25 กุมภาพันธ์ 2568 เป็นต้นไป

- ลงนาม -

(นายพชร ยุติธรรมดำรง)

ประธานคณะกรรมการบริษัท