นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

บริษัท แอดเทค ฮับ จำกัด (มหาชน) และบริษัทย่อย (“**กลุ่มบริษัท**”) ได้จัดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่ออำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงานทั้งระบบ ทั้งนี้ เพื่อให้การใช้บริการและการให้บริการสามารถดำเนินการใช้งานร่วมกันได้อย่างเหมาะสมสอดคล้องกับนโยบายทางธุรกิจ มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายอื่นที่เกี่ยวข้อง และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ทั้งจากผู้ใช้งานและภัยคุกคามต่าง ๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของกลุ่มบริษัทให้ได้รับความเสียหายได้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมถึงผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ กลุ่มบริษัทจึงกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้ถือเป็นแนวทางในการปฏิบัติเดียวกันตามหัวข้อมาตรการควบคุมด้านต่าง ๆ ดังต่อไปนี้

- ด้านการบริหารจัดการองค์กร (Organization Control)
- ด้านการบริหารจัดการทรัพยากรบุคคล (People control)
- ด้านการบริหารจัดการทางกายภาพ (Physical Control)
- ด้านการควบคุมทางเทคโนโลยี (Technological Control)

1. **ด้านการบริหารจัดการองค์กร** (Organization Control)

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่าง ๆ ภายในบริษัทและเพื่อเป็นแนวทางควบคุมการใช้งานอุปกรณ์สื่อสารประเภทพกพาให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1.1 นโยบายสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Policy for Information Security)

- บริษัทจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากประธานกรรมการบริษัท หรือผู้บริหารระดับสูงที่ประธานกรรมการบริษัทมอบหมายให้เป็นผู้อนุมัติ
- บริษัทเผยแพร่นโยบายดังกล่าวให้ผู้ใช้งานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบและถือปฏิบัติเป็นไปตามที่นโยบายกำหนด โดยการเผยแพร่ต้องดำเนินการในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย
- ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการตรวจสอบ และทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามเงื่อนไขที่ได้กำหนดไว้ในหัวข้อ การทบทวนนโยบาย

1.2 การกำหนดบทบาทและหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities)

- ผู้บริหารระดับฝ่ายต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศสำหรับบุคลากรในหน่วยงานอย่างเป็นลายลักษณ์อักษร และให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำหนดไว้

1.3 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

- ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจนเพื่อให้มีการสอบทานระหว่างกันได้

1.4 หน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Management Responsibilities)

- ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุมและกำกับให้บุคลากรหรือหน่วยงานภายนอกที่ได้รับการว่าจ้างเพื่อปฏิบัติงานหรือให้บริการกับบริษัท ปฏิบัติงานตามนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่บริษัทได้ประกาศใช้

1.5 การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องด้านความมั่นคงปลอดภัย (Contact with authorities)

- ฝ่ายเทคโนโลยีสารสนเทศต้องรวบรวมรายชื่อและช่องทางการติดต่อของหน่วยงานที่จำเป็น เช่น หน่วยงานด้านกฎหมาย โรงพยาบาล สถานีตำรวจ สถานีดับเพลิง หรือ

หน่วยกู้ภัย เป็นต้น สำหรับติดต่อเมื่อเกิดเหตุฉุกเฉินพร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

1.6 การประสานงานกับกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความมั่นคงปลอดภัยของสารสนเทศ (Contact with special interest group)

- ฝ่ายเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และเพิ่มช่องทางการรับข่าวสารจากกลุ่มผู้เชี่ยวชาญเพื่อให้สามารถติดต่อประสานงานหรือรับข้อมูลข่าวสาร หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศได้ทันท่วงที พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

1.7 การเฝ้าติดตามภัยคุกคาม (Threat intelligence)

- ฝ่ายเทคโนโลยีสารสนเทศต้องรวบรวมข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความปลอดภัยและวิเคราะห์ผลกระทบ เพื่อสร้างข้อมูลความรู้ภายในบริษัทเกี่ยวกับภัยคุกคาม

1.8 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ (Information Security in Project Management)

- ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุมความเสี่ยง การติดตามการดำเนินงานโครงการรวมถึงการประเมินภาพรวมในการดำเนินงานโครงการ ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก
- ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศเพื่อนำมาใช้งานในบริษัท กำหนดคุณลักษณะความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งานหรือระบบที่จัดหามาใช้งาน
- ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศต้องติดตามการพัฒนาระบบสารสนเทศ เพื่อตรวจสอบว่าการพัฒนาระบบสารสนเทศตรงตามความต้องการด้านความมั่นคงปลอดภัย สารสนเทศรวมถึงความต้องการด้านการใช้งานที่กำหนดไว้

1.9 การจัดทำบัญชีทรัพย์สิน (Inventory of Information and other associated assets)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้หน่วยงานภายในฝ่ายจัดทำบัญชีทรัพย์สินสารสนเทศ เพื่อบริหารจัดการและควบคุมทรัพย์สินสารสนเทศอย่างเหมาะสมและให้มีการปรับปรุงบัญชีทรัพย์สินให้เป็นปัจจุบันอยู่เสมอ
- ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการระบุผู้ถือครองทรัพย์สิน ผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศและผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม

1.10 การใช้ทรัพย์สินสารสนเทศ (Acceptable Use of Information and other associated assets)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำข้อกำหนดในการใช้ทรัพย์สินเพื่อการบริหารจัดการอุปกรณ์คอมพิวเตอร์ให้เหมาะสมก่อให้เกิดประสิทธิภาพสูงสูด รวมทั้งมีความปลอดภัยจากความเสียหายที่อาจเกิดขึ้นได้ โดยต้องสื่อสาร ให้บุคลากรของบริษัทรับทราบและปฏิบัติตาม
- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมกำกับให้มีขั้นตอนการปฏิบัติงานในการบริหารจัดการทรัพย์สินสารสนเทศ เพื่อมิให้ข้อมูลสำคัญของบริษัทรั่วไหล หรือทรัพย์สินสารสนเทศถูกนำไปใช้ผิดประเภท
- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอรวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม
- การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ต้องมีความสอดคล้องกับการกำหนดลำดับชั้นความลับข้อมูล

1.11 การคืนทรัพย์สิน (Return of Assets)

- ฝ่ายบริหารทรัพยากรบุคล หัวหน้างาน หรือผู้บังคับบัญชาต้องกำกับและติดตามให้บุคลากรในหน่วยงานหรือหน่วยงานภายนอกที่เข้ามาใช้บริการดำเนินการคืนทรัพย์สิน อาทิ เครื่องคอมพิวเตอร์พกพา เอกสาร กุญแจ บัตรพนักงานที่เป็นทรัพย์สินของบริษัทให้กับหน่วยงานที่เกี่ยวข้อง

1.12 การจัดลำดับชั้นความลับของสารสนเทศ (Classification of Information)

- บริษัทกำหนดให้มีการจัดหมวดหมู่ของทรัพย์สินสารสนเทศและจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับโดยให้นำกฎหมายและข้อกำหนดที่เกี่ยวกับบริษัทมาร่วมพิจารณาการกำหนดชั้นความลับที่เหมาะสม
- หน่วยงานภายในบริษัทต้องจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศที่ใช้ในการดำเนินงานของบริษัท และกำหนดลำดับชั้นความลับของข้อมูลและทรัพย์สินสารสนเทศ
- หน่วยงานภายในบริษัทต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้ในระเบียบการปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.13 การบ่งชี้สารสนเทศ (Labeling of Information)

- บริษัทต้องควบคุมให้ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นมีการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้บุคลากรและผู้ที่เกี่ยวข้องต้องปฏิบัติตาม เพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

- ฝ่ายเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้องต้องทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สินและขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

1.14 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้ประเภทของข้อมูลและลำดับชั้นความลับของข้อมูล
- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุม กำกับให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศ ทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท และระหว่างบริษัทกับหน่วยงานภายนอก ซึ่งเป็นไปตามคู่มือการปฏิบัติงานระบบสารสนเทศและเทคโนโลยี
- การแลกเปลี่ยนข้อมูลสารสนเทศภายในบริษัทกับหน่วยงานภายนอกต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อนทุกครั้ง และมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลสารสนเทศตามลำดับชั้นความลับข้อมูลอย่างเหมาะสม
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

1.15 นโยบายควบคุมการเข้าถึง (Access Control)

- บริษัทกำหนดให้มีนโยบายควบคุมการเข้าถึง (Access Control Policy) อย่างเป็นลายลักษณ์อักษรและปรับปรุงนโยบายให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม
- ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้มีการขอเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานโดยต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น
- ฝ่ายเทคโนโลยีสารสนเทศจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้ เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตให้เข้าถึงเท่านั้น โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

1.16 การบริหารจัดการการยืนยันตัวตน (Identity management)

- ฝ่ายเทคโนโลยีสารสนเทศและเจ้าของข้อมูลต้องร่วมกันกำหนดวิธีการบริหารจัดการการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม

1.17 การใช้งานข้อมูลการพิสูจน์ตัวตน (Authentication Information)

- ผู้ใช้งานจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการคาดเดา และไม่ใช้รหัสผ่านซึ่งเคยใช้มาแล้ว

- ผู้ใช้งานจะต้องไม่เขียนหรือบันทึกรหัสผ่านที่ใช้และเก็บหรือแสดงให้เห็นไว้ใกล้กับระบบหรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น
- ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใด ๆ โดยใช้บัญชีผู้ใช้งานของตนหรือกระทำการใด ๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ
- ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการบริหารจัดการรหัสผ่านอื่น ๆ ที่บริษัทกำหนดไว้

1.18 ระบบสำหรับบริหารจัดการรหัสผ่าน (Password Management System)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีระบบสำหรับบริหารจัดการบัญชีผู้ใช้และรหัสผ่านสำหรับการเข้าถึงระบบสารสนเทศของผู้ใช้งานภายในบริษัท เพื่อให้เกิดการบริหารจัดการที่เป็นมาตรฐานเดียวกัน

1.19 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (Access Rights)

- ฝ่ายเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดให้มีการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ
- ฝ่ายเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องจัดทำเอกสารการมอบหมายสิทธิการเข้าถึงข้อมูลหรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน
- ฝ่ายเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดกระบวนการในการบริหารจัดการสิทธิการเข้าถึง ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องใช้งานข้อมูลหรือระบบสารสนเทศเกินสิทธิที่ได้รับมอบหมาย
- ฝ่ายเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องจัดทำขั้นตอนปฏิบัติการทบทวนสิทธิการเข้าถึงข้อมูล ระบบสารสนเทศและโปรแกรมประยุกต์ (Application) อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม
- ฝ่ายเทคโนโลยีสารสนเทศและเจ้าของข้อมูล ต้องกำหนดรอบในการทบทวนสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศอย่างชัดเจนและแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ
- การทบทวนสิทธิการเข้าถึงต้องพิจารณาประเด็น ดังต่อไปนี้
  - รอบการทบทวนสิทธิที่กำหนดไว้
  - การพ้นสภาพการเป็นบุคลากรของบริษัท
  - การเปลี่ยนแปลงโยกย้ายหน้าที่การปฏิบัติงาน
  - การขอใช้สิทธินอกเหนือจากหน้าที่ความรับผิดชอบที่กำหนดไว้
- เมื่อดำเนินการทบทวนสิทธิเรียบร้อยแล้ว ให้เจ้าของข้อมูลหรือผู้ดูแลระบบจัดเก็บหลักฐานการทบทวนสิทธิโดยให้แยกหลักฐานตามช่วงเวลาการทบทวนสิทธิ

- เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเกณฑ์การพิจารณาการถอดถอนสิทธิการเข้าถึงและวิธีการถอดถอนสิทธิในการเข้าถึงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม

1.20 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับหน่วยงานภายนอก (Information Security Policy for Supplier Relationships)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน่วยงานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาหรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้หน่วยงานภายนอกหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของบริษัท
- ผู้ดูแลระบบและหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอกต้องควบคุมกำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการและระดับการให้บริการ

1.21 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้มีการกำหนดข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศเพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร
- ผู้ดูแลระบบและหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอกต้องควบคุมให้หน่วยงานภายนอกสามารถเข้าถึงสารสนเทศของบริษัทเฉพาะส่วนที่มีความจำเป็นต้องรู้ และต้องได้รับการยินยอมจากเจ้าของข้อมูลสารสนเทศอย่างเป็นลายลักษณ์อักษรเท่านั้น
- ผู้ดูแลระบบและหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอกต้องควบคุมดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างบริษัทและหน่วยงานภายนอก

1.22 การบริหารจัดการและการสื่อสารต่อผู้รับจ้างช่วงของหน่วยงานภายนอก (Managing information security in the ICT supply chain)

- ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมถึงผู้รับจ้างช่วงที่หน่วยงานภายนอกเป็นผู้จัดหา

1.23 การติดตามและทบทวนการให้บริการของหน่วยงานภายนอก (Monitoring and Review of Supplier Services)

- ผู้ดูแลระบบและหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอกต้องติดตามและตรวจทานการดำเนินงานของหน่วยงานภายนอกซึ่งมีหน้าที่ในการบริหารจัดการระบบ ประมวลผลข้อมูลสารสนเทศให้กับบริษัท ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการอย่างสม่ำเสมอ

1.24 การบริหารจัดการการเปลี่ยนแปลงบริการของหน่วยงานภายนอก (Managing Changes to Supplier Services)

- กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอกต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหารและผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการ บริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

1.25 การบริหารจัดการเพื่อใช้ระบบคลาวด์ (Information security for use of cloud services)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีกระบวนการในการได้มา การใช้งาน การจัดการและการยกเลิกการใช้บริการคลาวด์โดยจะต้องจัดทำขึ้นตามข้อกำหนดด้านความปลอดภัยข้อมูลของบริษัท

1.26 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Information security incident management planning and preparation)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และมอบหมายสิทธิการดำเนินงานอย่างชัดเจนให้บุคลากรภายในฝ่าย
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิดออกจากเหตุขัดข้องด้านการปฏิบัติงานทั่วไปเพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดช่องทางและเกณฑ์ในการรายงานเหตุการณ์หรือจุดอ่อนหรือเหตุขัดข้องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศและสื่อสารให้บุคลากรในบริษัทและหน่วยงานภายนอกรับทราบ

1.27 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment and Decision on Information Security Events)

- ผู้ดูแลระบบต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทำการจัดแยกกลุ่มเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัยและจัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้และแจ้งผู้ที่เกี่ยวข้องรับทราบเพื่อแก้ไขในกรณีที่

พบว่าเหตุการณ์หรือจุดอ่อนนั้น อาจเป็นเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศ

1.28 การตอบสนองต่อเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents)

- บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ต้องดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้
- บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ต้องดำเนินการตอบสนองและแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หากไม่สามารถแก้ไขได้ตามเวลาที่กำหนด ต้องแจ้งให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด

1.29 การเรียนรู้จากเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)

- บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้จะต้องจัดเตรียมรายงานผลการวิเคราะห์และการแก้ไขเหตุขัดข้อง จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และจัดเก็บไว้เป็นองค์ความรู้เพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต

1.30 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

- บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้จะต้องดำเนินการเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อรวบรวมหลักฐานให้เพียงพอต่อการนำเสนอผู้บริหารหน่วยงานที่เกี่ยวข้องและใช้ในการดำเนินการด้านกฎหมายต่อไป

1.31 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security during disruption)

- เจ้าของข้อมูลและฝ่ายเทคโนโลยีสารสนเทศต้องร่วมกันระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ประเมินความเสี่ยงเหตุการณ์ และระบบงานสำคัญเพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้องและครบถ้วน เพื่อใช้ในการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ
- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้เป็นส่วนหนึ่งของแผนและให้มีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจของบริษัท

- ฝ่ายเทคโนโลยีสารสนเทศต้องทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างน้อย ปีละ 1 ครั้ง และจัดให้มีการบันทึกผลการทดสอบเพื่อให้มั่นใจว่าแผนงานที่จัดทำมีความถูกต้องและสามารถตอบสนองต่อการดำเนินงานได้เป็นอย่างดี
- บุคลากรผู้ซึ่งมีส่วนเกี่ยวข้องในการปฏิบัติงานกู้คืนระบบสารสนเทศต้องมีความรู้ด้านเทคนิคที่จำเป็นต่อการกู้คืนระบบและเข้าร่วมการซักซ้อมแผน
- เจ้าของข้อมูลและผู้ใช้งานระบบที่เกี่ยวข้องกับแผนรองรับการดำเนินการทางธุรกิจอย่างต่อเนื่องต้องเข้าร่วมการทดสอบแผนและดำเนินงานตามแผนที่กำหนดไว้

1.32 ความพร้อมของอุปกรณ์การสื่อสารและเทคโนโลยีสำหรับความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้มีความพร้อมด้านอุปกรณ์การสื่อสารและเทคโนโลยี โดยจะต้องมีการวางแผน นำไปใช้ บำรุงรักษา และทดสอบตามวัตถุประสงค์ด้านความต่อเนื่องทางธุรกิจและข้อกำหนดด้านความต่อเนื่องของอุปกรณ์การสื่อสารและเทคโนโลยี

1.33 การระบุกฎหมายและข้อกำหนดในสัญญาจ้าง (Legal, Statutory, Regulatory and Contractual Requirements)

- ฝ่ายเทคโนโลยีสารสนเทศต้องร่วมกับฝ่ายกฎหมาย และฝ่ายบริหารทรัพยากรบุคคลในการรวบรวมกฎหมาย กฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ
- บุคลากรทั้งหมดต้องรับผิดชอบในการปฏิบัติตามข้อกำหนดที่ได้มีการระบุไว้อย่างเคร่งครัด
- ห้ามเจ้าหน้าที่ในบริษัทใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัทกระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม
- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมการเข้ารหัสลับข้อมูลให้มีความสอดคล้องกับกฎหมาย ประกาศ หลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่าง ๆ ที่มีผลบังคับใช้กับบริษัท

1.34 การป้องกันสิทธิ และทรัพย์สินทางปัญญา (Intellectual Property Rights)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำกระบวนการสำหรับการบริหารจัดการการใช้ซอฟต์แวร์ลิขสิทธิ์และทรัพย์สินทางปัญญา เพื่อให้มั่นใจว่าการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ

- ผู้ใช้งานต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่บริษัทได้จัดซื้อลิขสิทธิ์ เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น
- ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบสารสนเทศของบริษัทโดยเด็ดขาด
- ซอฟต์แวร์ที่พัฒนาเพื่อบริษัททั้งโดยหน่วยงานภายนอกหรือบุคลากรในหน่วยงานของบริษัท ถือว่าเป็นทรัพย์สินของบริษัท ซึ่งไม่อนุญาตให้หน่วยงานภายนอกหรือบุคลากรในหน่วยงานของบริษัททำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินของบริษัทโดยไม่ได้รับอนุญาต
- ผู้ใช้งานที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศของบริษัทต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์ นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

1.35 การป้องกันข้อมูลของบริษัท (Protection of Records)

- เจ้าของข้อมูลต้องปฏิบัติตามข้อบังคับทางกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศบางประเภท เช่น ด้านบัญชี ด้านลูกค้า และต้องจัดทำข้อกำหนดในการจัดการข้อมูลสารสนเทศ ระยะเวลาในการจัดเก็บให้สอดคล้องกับข้อบังคับดังกล่าว
- เจ้าของข้อมูลต้องควบคุมป้องกันมิให้ข้อมูลบันทึกหลักฐาน (Logs) ต่าง ๆ เกิดความเสียหาย สูญหาย ถูกเปลี่ยนแปลงแก้ไข ถูกเข้าถึง หรือเผยแพร่ โดยไม่ได้รับอนุญาต โดยการควบคุมต้องให้สอดคล้องกับกฎหมาย ข้อกำหนด และความต้องการทางธุรกิจ

1.36 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information,(PII))

- บริษัทต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายประกาศ หลักเกณฑ์ที่รัฐบาลได้ประกาศไว้รวมถึงข้อบังคับต่าง ๆ ที่มีผลบังคับใช้กับบริษัท
- ข้อมูลสารสนเทศรายละเอียดที่เกี่ยวกับลูกค้าถือว่ามีความสำคัญ หน่วยงานผู้รับผิดชอบในการดูแลข้อมูลต้องกำหนดให้บุคลากรและลูกจ้างที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศดังกล่าวได้
- ข้อมูลสารสนเทศส่วนบุคคลของบุคลากร ลูกจ้าง และลูกค้าถือว่าเป็นความลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิตามที่บริษัทกำหนดเท่านั้น

1.37 การตรวจประเมินระบบสารสนเทศจากผู้ตรวจสอบอิสระ (Independent Review of Information Security)

- บริษัทต้องจัดให้มีการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศโดยส่วนตรวจสอบระบบงานหรือผู้ตรวจสอบอิสระภายนอก เพื่อตรวจสอบการปฏิบัติตาม

นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนทบทวนถึงความพอเพียงของการควบคุมระบบสารสนเทศและการปฏิบัติตามการควบคุมต่าง ๆ

1.38 การปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยสารสนเทศ (Compliance with policies, rules and Standards for information security)

- ผู้บังคับบัญชาของแต่ละแผนกต้องรับผิดชอบในการสอบทานการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรใต้บังคับบัญชาอย่างสม่ำเสมอ
- กรณีที่ผู้บังคับบัญชาของแต่ละฝ่ายตรวจพบการปฏิบัติงานที่ไม่สอดคล้องกับนโยบาย มาตรฐานและขั้นตอนปฏิบัติซึ่งยังไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ผู้บังคับบัญชาต้องชี้แจงให้บุคลากรใต้บังคับบัญชารับทราบและทำความเข้าใจ แต่หากความไม่สอดคล้องที่พบส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ผู้บังคับบัญชาต้องดำเนินการลงโทษทางวินัยตามกฎระเบียบที่บริษัทกำหนดไว้
- ฝ่ายเทคโนโลยีสารสนเทศต้องให้การสนับสนุนด้านการให้คำแนะนำในการใช้งานหรือการปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศต่อหน่วยงานอื่นเมื่อได้รับคำร้องขอ

1.39 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีขั้นตอนปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษร โดยต้องแบ่งแยกอำนาจหน้าที่ของบุคลากรตามโครงสร้างการปฏิบัติหน้าที่ที่ชัดเจนเพื่อให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท
- หน่วยงานในฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำคู่มือเอกสารประกอบระบบงานและฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงานและกระบวนการทำงาน
- หน่วยงานในฝ่ายเทคโนโลยีสารสนเทศต้องทบทวนวิธีปฏิบัติ คู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ดังกล่าวให้เป็นปัจจุบันอยู่เสมอรวมทั้งจัดให้ขั้นตอนปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้และต้องสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม

2. **การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล** (People control)

เพื่อกำหนดมาตรการควบคุม การกำกับและติดตามการสรรหาบุคลากรเข้ามาปฏิบัติงานภายในบริษัท การบริหารจัดการบุคลากรระหว่างการจ้างงาน และการบริหารจัดการบุคลากรเมื่อพ้นสภาพการเป็นลูกจ้าง หรือเมื่อมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงาน

2.1 การตรวจสอบประวัติ (Screening)

- บริษัทกำหนดให้มีการตรวจสอบประวัติของผู้สมัครงานและหน่วยงานภายนอกที่ต้องเข้ามาให้บริการภายในหน่วยงาน

2.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

- ฝ่ายบริหารทรัพยากรบุคคลต้องกำกับให้มีการลงนามในสัญญาจ้าง หรือข้อตกลงการปฏิบัติงานของบุคลากร หรือสัญญาว่าจ้างหน่วยงาน หรือบุคคลภายนอก ซึ่งได้มีการระบุหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญาหรือข้อตกลง การปฏิบัติงาน ซึ่งผู้ใช้งานต้องรับทราบและยอมรับระเบียบปฏิบัติของบริษัท โดยจะต้องทำความเข้าใจและปฏิบัติตามนโยบาย กฎ ระเบียบที่บริษัทได้กำหนดไว้

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

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดช่องทางให้บุคลากรสามารถทำการศึกษาและทำความเข้าใจในนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ บทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยก่อนที่จะขออนุญาตให้เริ่มต้นปฏิบัติงานกับบริษัท
- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไปโดยหน่วยงานผู้รับผิดชอบ เพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เช่น วิธีการใช้ระบบงาน วิธีการใช้งานซอฟต์แวร์สำเร็จรูป การแก้ปัญหาการใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง เป็นต้น
- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัย เพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เพื่อช่วยให้ผู้รับการว่าจ้างสามารถปฏิบัติงานที่ตนเองรับผิดชอบได้เป็นอย่างดีและอย่างมั่นคงปลอดภัย

2.4 กระบวนการลงโทษทางวินัย (Disciplinary Process)

- บริษัทจัดให้มีการลงโทษทางวินัยเพื่อลงโทษผู้ใช้งานที่ฝ่าฝืนหรือละเมิดนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศหรือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

2.5 การบริหารจัดการบุคลากรพ้นสภาพหรือเปลี่ยนหน้าที่ความรับผิดชอบในการปฏิบัติงาน (Responsibilities after Termination or Change of Employment)

- ฝ่ายบริหารทรัพยากรบุคคลต้องกำหนดกฎระเบียบและความรับผิดชอบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรและหน่วยงานภายนอกภายหลังจากที่พ้นสภาพการจ้างงาน หรือมีการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงานอย่างเป็นลายลักษณ์อักษร

- ฝ่ายบริหารทรัพยากรบุคคลต้องควบคุมดูแลให้บุคลากรและหน่วยงานภายนอกปฏิบัติตามกฎระเบียบที่กำหนดไว้อย่างเคร่งครัด

2.6 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements)

- ผู้บริหารระดับฝ่ายต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัท มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทอย่างเป็นลายลักษณ์อักษร

2.7 การปฏิบัติงานภายนอกสำนักงาน (Remote working)

- ผู้ใช้งานที่มีการทำงานจากภายนอกสำนักงานทั้งหมด จะต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทเช่นเดียวกับการทำงานภายในสำนักงาน
- ผู้ใช้งานที่มีการใช้ข้อมูลสารสนเทศของบริษัทในการทำงานนอกสำนักงาน หรือการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากเจ้าของข้อมูลสารสนเทศและหน่วยงานต้นสังกัดโดยต้องมีเหตุผลอันควร
- ผู้ใช้งานที่ต้องการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งาน

2.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event Reporting)

- ผู้ใช้งานและหน่วยงานภายนอกต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของบริษัทต่อผู้บังคับบัญชาและฝ่ายเทคโนโลยีสารสนเทศโดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด
- ผู้ใช้งานและหน่วยงานภายนอกต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของบริษัทต่อผู้บังคับบัญชาและฝ่ายเทคโนโลยีสารสนเทศ โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด
- ผู้ใช้งานและหน่วยงานภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศหรือจุดอ่อนใด ๆ ของระบบสารสนเทศในบริษัท ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่นยกเว้นผู้บังคับบัญชาและฝ่ายเทคโนโลยีสารสนเทศ และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคง ปลอดภัยสารสนเทศนั้นด้วยตนเอง

3. **การควบคุมการทางกายภาพ** (Physical Control)

เพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงทางกายภาพและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัท

3.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeters)

- บริษัทต้องพิจารณาและจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัยโดยจะประกอบด้วยพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกหลัก และระบบรักษาความปลอดภัยอย่างเหมาะสม

3.2 การควบคุมการเข้าออกทางกายภาพ (Physical Entry)

- บริษัทต้องควบคุมการเข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญให้เข้าถึงได้เฉพาะบุคลากรผู้ได้รับอนุญาตเท่านั้น
- รายชื่อผู้ได้รับอนุญาตให้เข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ต้องได้รับการตรวจสอบ ปรับปรุง และดูแลให้เหมาะสมอย่างสม่ำเสมอ
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความปลอดภัย (Secure Area) อาทิเช่น ห้องเซิร์ฟเวอร์ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์และบันทึกการเข้าออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก วัตถุประสงค์การผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
- ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึง อาจสามารถเข้าถึงได้โดยต้องกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์ ทั้งนี้ให้แยกเป็นสัดส่วนที่ชัดเจนเพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศ และข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

3.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่น ๆ (Securing Offices, Rooms, and Facilities)

- ฝ่ายเทคโนโลยีสารสนเทศต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ห้องคอมพิวเตอร์และพื้นที่ปฏิบัติงานของผู้ดูแลระบบหรืออุปกรณ์สารสนเทศ ต่าง ๆ ที่ใช้ในการปฏิบัติงานอันเนื่องจากการได้รับความเสียหายและถูกเข้าถึงโดยไม่ได้รับอนุญาต

3.4 การเฝ้าติดตามการรักษาความปลอดภัยทางกายภาพ (Physical security monitoring)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการตรวจสอบพื้นที่ควบคุมด้านความมั่นคงปลอดภัยข้อมูลอย่างต่อเนื่องเพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

3.5 การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against Physical and Environmental Threats)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมกำกับให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยคุกคามจากภายนอก ทั้งที่ก่อโดย

มนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

3.6 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำกับให้มีการกำหนดแนวปฏิบัติของการป้องกันทางกายภาพ สำหรับการปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบ และกำหนดให้มีการนำแนวปฏิบัติไปใช้งานอย่างเคร่งครัด

3.7 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen)

- ผู้ดูแลระบบต้องควบคุมให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session Time Out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น
- ผู้ใช้งานต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูลให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะหรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ

3.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดวางอุปกรณ์สารสนเทศไว้ในห้อง หรือบริเวณที่ปลอดภัย อุปกรณ์ที่มีตู้ ประตูของตู้วางคอมพิวเตอร์แม่ข่าย และอุปกรณ์สื่อสารเครือข่ายต้องถูกล็อคอยู่เสมอ โดยกำหนดให้มีเพียงเจ้าหน้าที่ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการเปิดเพื่อซ่อมบำรุง หรือการปรับปรุงค่าคอนฟิเกอเรชั่น (Reconfiguration) เพื่อลดความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

3.9 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of Asset Off-Premises)

- กำหนดให้ผู้บริหารระดับฝ่ายขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์สารสนเทศของบริษัทไปใช้งานภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่าง ๆ ที่ใช้งานอยู่ภายนอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการความมั่นคงปลอดภัยในการควบคุมทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของบริษัทออกไปใช้งาน

3.10 การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets)

- ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ต้องไม่อนุญาตให้นำอุปกรณ์สารสนเทศออกจากบริษัท ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

- ผู้ใช้งานต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกนอกบริษัท ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดขั้นตอนปฏิบัติสำหรับการนำทรัพย์สินออกนอกสำนักงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม

3.11 การจัดการสื่อบันทึกข้อมูล (Storage of Media)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับหรือมีความสำคัญ
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการควบคุมการทำลายสื่อบันทึกข้อมูลโดยอ้างอิงมาตรฐานซึ่งเป็นที่ยอมรับในสากล
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดขั้นตอนปฏิบัติงานหรือข้อกำหนดในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ติดตั้งหรือพื้นที่ปฏิบัติงาน

3.12 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมดูแลให้มีการติดตั้งอุปกรณ์ป้องกันการล้มเหลวของระบบ และอุปกรณ์สนับสนุนการทำงานต่าง ๆ ภายในห้องเซิร์ฟเวอร์ ได้แก่ อุปกรณ์ดับเพลิง อุปกรณ์ดักจับควันไฟ หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น และต้องบำรุงดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ

3.13 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมดูแลให้การติดตั้งและการบำรุงรักษาสายไฟฟ้าและสายสื่อสารในพื้นที่ปฏิบัติงานและห้องคอมพิวเตอร์เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรมเพื่อป้องกันไม่ให้มีการเข้าถึง หรือดักจับข้อมูลหรือเกิดความเสียหายทางด้านกายภาพ

3.14 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมดูแลให้อุปกรณ์ระบบสารสนเทศหลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนการทำงานได้รับการบำรุงดูแลรักษาตามช่วงเวลาและตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน
- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้มีการบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

3.15 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานซ้ำ (Secure Disposal or Re-Use of Equipment)

- ผู้ใช้งานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลาย

อย่างเหมาะสม ตามลำดับชั้นความลับข้อมูลก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลหรือทรัพย์สินสารสนเทศ และมาตรการหรือเทคนิคสำหรับการทำลายข้อมูลเพื่อนำอุปกรณ์สารสนเทศกลับมาใช้งานซ้ำโดยต้องมีความสอดคล้องกับการจัดลำดับชั้นความลับข้อมูล
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดผู้รับผิดชอบในการทำหน้าที่ทำลายข้อมูลสารสนเทศที่ไม่จำเป็นต่อการดำเนินกิจการของบริษัทซึ่งจัดเก็บอยู่บนสื่อบันทึกข้อมูล

4. **การควบคุมทางเทคโนโลยี** (Technological Control)

เพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการด้านเทคนิคต่าง ๆ ที่ส่งผลกระทบต่อความปลอดภัยข้อมูลของบริษัท

4.1 การป้องกันอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (User Endpoint Devices)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศที่ทิ้งไว้โดยไม่มีผู้ดูแลเพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต
- ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์
- ผู้ใช้งานต้องออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน
- ผู้ใช้งานต้องล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์
- ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีมาตรการที่เหมาะสมเพื่อรับรองความปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัท และเมื่อนำอุปกรณ์ออกไปใช้งานนอกสถานที่
- ผู้ใช้งานที่มีการใช้งานอุปกรณ์สื่อสารประเภทพกพาซึ่งเชื่อมต่อกับระบบสารสนเทศของบริษัททั้งหมดต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและตระหนักถึงการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

4.2 ข้อจำกัดสำหรับผู้ใช้งานที่มีสิทธิพิเศษในการเข้าถึง (Privileged access restriction)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุม การจัดสรร และการใช้สิทธิพิเศษในการเข้าถึงระบบสารสนเทศสำหรับผู้ใช้งานระบบที่มีสิทธิพิเศษ

4.3 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

- เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดวิธีการเข้าถึงข้อมูลระบบสารสนเทศและฟังก์ชันในระบบงานโดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

- เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดวิธีการใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นข้อมูลระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของฝ่ายงานนั้น ๆ เป็นลายลักษณ์อักษร

4.4 การเข้าถึงซอร์สโค้ดของโปรแกรม (Access to source code)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม และการนำซอร์สโค้ดของโปรแกรมไปใช้ในการพัฒนาเพื่อป้องกันการเกิดข้อผิดพลาดในการพัฒนาระบบสารสนเทศและระบบงานของบริษัท

4.5 การเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย (Secure Authentication)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดวิธีการเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร โดยอ้างอิงวิธีการที่เป็นมาตรฐานสากลและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม

4.6 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

- ผู้ดูแลระบบต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ
- ผู้ดูแลระบบต้องประเมินสมรรถภาพและความเพียงพอ (Capacity) ของทรัพยากรสารสนเทศ เช่น การใช้งานของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (Memory) หน่วยจัดเก็บข้อมูล (Disk) หรือปริมาณการใช้งานระบบเครือข่าย (Bandwidth) เป็นต้น และต้องวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งานในอนาคต

4.7 การป้องกันโปรแกรมที่ไม่พึงประสงค์ (Protecting against malware)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

4.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้ระบบสารสนเทศของบริษัทได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง
- ผู้ดูแลระบบต้องดูแลและบำรุงรักษาระบบเพื่อรักษาระดับความมั่นคงปลอดภัยด้านสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่การประเมินความเสี่ยงของช่องโหว่ที่ตรวจสอบพบ และการปรับปรุงแก้ไขช่องโหว่ของระบบสารสนเทศ

- ต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค เช่น การทดสอบการบุกรุกระบบสารสนเทศ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
- ส่วนตรวจสอบระบบงานต้องตรวจสอบการควบคุมทางเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอเหมาะสมและมีการปฏิบัติตามการควบคุมเหล่านั้น
- ผู้ดูแลระบบต้องจัดให้มีการทดสอบระดับมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การตรวจหาช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) หรือการทดสอบการบุกรุกระบบ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

4.9 การบริหารจัดการค่าที่ปรับตั้ง (Configuration management)

- ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดค่าความปลอดภัยให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยข้อมูลสำหรับฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่าย โดยจัดทำเป็นเอกสารอย่างเป็นลายลักษณ์อักษร เพื่อบันทึก นำไปใช้ตรวจสอบ และทบทวนอย่างสม่ำเสมอ

4.10 การลบข้อมูล (Information deletion)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการในการจัดการข้อมูลที่จัดเก็บไว้ในระบบข้อมูล อุปกรณ์ หรือในสื่อบันทึกข้อมูลอื่นใด ซึ่งจะต้องถูกลบเมื่อไม่ต้องการอีกต่อไป

4.11 การปกปิดข้อมูล (Data masking)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการในการปกปิดข้อมูลให้เป็นไปตามนโยบายของบริษัทเกี่ยวกับการควบคุมการเข้าถึงข้อมูล ข้อกำหนดทางธุรกิจ และกฎหมายที่เกี่ยวข้องซึ่งมีผลบังคับใช้

4.12 การป้องกันการรั่วไหลของข้อมูล (Data leakage prevention)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการการป้องกันการรั่วไหลของข้อมูลโดยนำไปใช้กับระบบ เครือข่าย และอุปกรณ์อื่น ๆ ที่ประมวลผล จัดเก็บ หรือส่งข้อมูล สำหรับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้

4.13 การสำรองข้อมูล (Information Backup)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการในการสำรองข้อมูลและรอบการสำรองข้อมูลของระบบสารสนเทศที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล
- เจ้าของข้อมูลสารสนเทศต้องดำเนินการหรือกำหนดให้มีการสำรองข้อมูลสารสนเทศและการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ

- ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น External Hard Disk เป็นต้น ให้เป็นปัจจุบันอย่างสม่ำเสมอ รวมถึงให้จัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

4.14 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Redundancy of information processing facilities)

- บริษัทต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่มีความสำคัญสูง
- บริษัทต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

4.15 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Logging)

- ผู้ดูแลระบบต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ
- ผู้ดูแลระบบต้องเฝ้าติดตาม (Monitoring) การใช้งานระบบสารสนเทศโดยผลของการเฝ้าติดตามจะต้องถูกสอบทานอย่างสม่ำเสมอเพื่อตรวจหาความผิดปกติ
- ผู้ดูแลระบบต้องควบคุมและกำกับให้มีการบันทึกเหตุการณ์ความผิดพลาด (Fault Logging) ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ รวมถึงวิเคราะห์ ดำเนินการแก้ไขตลอดจนวางแนวทางป้องกันการเกิดปัญหาซ้ำอีกในอนาคต
- ผู้ดูแลระบบต้องจัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ถูกทำความเสียหายหรือเข้าถึงโดยไม่ได้รับอนุญาต
- ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบและผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ อาทิ เวลาเปิดและปิดระบบ การเปลี่ยนแปลงการตั้งค่าของระบบ ความผิดพลาดของระบบ และการดำเนินการแก้ไข และต้องมีการสอบทานบันทึกกิจกรรมอย่างสม่ำเสมอ

4.16 การเฝ้าติดตามกิจกรรมต่าง ๆ (Monitoring activities)

- ฝ่ายเทคโนโลยีสารสนเทศต้องตรวจสอบพฤติกรรมที่ผิดปกติ และมีกระบวนการที่เหมาะสมเพื่อประเมินเหตุการณ์ด้านความปลอดภัยของข้อมูลที่อาจเกิดขึ้นของเครือข่าย ระบบ และแอปพลิเคชันอย่างสม่ำเสมอ

4.17 การตั้งเวลาระบบสารสนเทศ (Clock Synchronization)

- ผู้ดูแลระบบต้องควบคุมกำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของบริษัทได้รับการกำหนดเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องและตรงกับเวลาอ้างอิงสากล

- ผู้ดูแลระบบต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศและระบบสารสนเทศของบริษัท รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอเพื่อป้องกันไม่ให้เกิดการบันทึกเวลาที่ไม่ถูกต้อง

4.18 การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์และจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบสารสนเทศหรือโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการ ป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

4.19 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดรายการซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม

4.20 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

- ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์และไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของบริษัท

4.21 การควบคุมเครือข่าย (Network security)

- ผู้ดูแลระบบต้องควบคุม กำกับ ให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคามและมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

4.22 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

- ผู้ดูแลระบบต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการและความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมดลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่าง ๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก

4.23 การแบ่งแยกเครือข่าย (Segregation in Network)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบ

เครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

4.24 การคัดกรองเว็บไซต์ที่ไม่ปลอดภัย (Web filtering)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการการควบคุมการเข้าถึงเว็บไซต์ภายนอกเพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ของบริษัทจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

4.25 นโยบายการใช้มาตรการการเข้ารหัสลับข้อมูล (Use of Cryptographic)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้

4.26 การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล (Key Management)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล โดยให้ครอบคลุมวงจรการบริหารจัดการกุญแจ (Key Management Life Cycle) รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

4.27 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Life Cycle)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดกฎระเบียบสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย และครอบคลุมตลอดทั้งวงจรการพัฒนาระบบสารสนเทศ

4.28 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Application Securing Requirements)

- ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ (Application Service) การใช้งานทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกันการกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission or Miss-Routing) หรือการเปิดเผย คัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
- ข้อมูลสารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง (Miss-Routing) การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการสำเนาข้อมูลโดยไม่ได้รับอนุญาต

4.29 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Architecture and Engineering Principles)

- ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบดังต่อไปนี้เป็นอย่างน้อย

- การให้สิทธิต่ำที่สุด (Least Privilege) แก่ผู้ใช้งานระบบสารสนเทศเพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
- การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้งานระบบสารสนเทศเพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
- การออกแบบระบบให้สามารถป้องกันได้หลายระดับขั้น (In-Depth Defense) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การออกแบบในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกันและสามารถตรวจสอบการทำงานได้

4.30 การเขียนโปรแกรมโดยคำนึงถึงความปลอดภัย(Secure Coding)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดหลักการรักษาความปลอดภัยสำหรับการเขียนโปรแกรมและนำไปใช้กับกระบวนการพัฒนาซอฟต์แวร์

4.31 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (Security Testing in Development and acceptance)

- ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ หน่วยงานที่ได้รับมอบหมายและผู้ใช้งานต้องร่วมกันทดสอบฟังก์ชันการทำงานของระบบสารสนเทศ และฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงทุกครั้ง
- การทดสอบการพัฒนาระบบสารสนเทศ ต้องดำเนินการทดสอบระหว่างการพัฒนาและก่อนนำระบบขึ้นใช้งานจริง โดยต้องจัดเก็บหลักฐานในการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาขึ้นใหม่หรือระบบที่มีการเปลี่ยนแปลงอย่างเป็นทางการ
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากส่วนพัฒนาระบบเทคโนโลยีสารสนเทศพัฒนาขึ้นหรือที่มีการจัดหาจากหน่วยงานภายนอก และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง

4.32 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)

- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดข้อตกลงในการพัฒนาระบบสำหรับหน่วยงานภายนอกที่ทำหน้าที่พัฒนาซอฟต์แวร์เพื่อใช้งานภายในบริษัท อย่างเป็นลายลักษณ์อักษร
- หน่วยงานที่ได้รับมอบหมายให้ดำเนินการจัดจ้างหน่วยงานภายนอกเข้ามาพัฒนาระบบสารสนเทศให้บริษัทต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้เกิดความเสียหายใด ๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

4.33 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน (Separation of Development, Testing and Production Environments)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุม กำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) การทดสอบระบบงาน (Testing Environment) และระบบที่ให้บริการจริง (Operational Environment) ออกจากกัน
- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้มีการกำหนดสิทธิการเข้าถึงในแต่ละสภาพแวดล้อม และจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจนโดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหาและวิธีการแก้ไขรวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ
- ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ

4.34 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

- ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมกำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของการเปลี่ยนแปลงโครงสร้างองค์กร ขั้นตอนการปฏิบัติงาน ระบบสารสนเทศ เพื่อควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใด ๆ ซึ่งส่งผลต่อการดำเนินงานของระบบงานต่าง ๆ ทั้งนี้ ให้ปฏิบัติตามที่กำหนดไว้ในนโยบายการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษรโดยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ
- ผู้ดูแลระบบจะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบที่อาจเกิดขึ้น เมื่อต้องการที่จะเปลี่ยนแปลงหรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชัน และการแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัย เป็นต้น โดยจะต้องมีการทดสอบบนเครื่องทดสอบ (Testing Environment) จนมั่นใจว่าระบบงานต่าง ๆ ที่ประมวลผลบนเครื่องดังกล่าวสามารถทำงานได้ตามปกติและมีความมั่นคงปลอดภัย จึงจะทำการเปลี่ยนแปลงหรือปรับปรุงบนเครื่องที่ใช้งานจริง (Operational Environment)
- ผู้ดูแลระบบจะต้องทำการตรวจสอบทางเทคนิคภายหลังการเปลี่ยนแปลงระบบปฏิบัติการบนระบบจริง เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่มีผลกระทบต่อการทำงานของระบบและไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศ

- ซอฟต์แวร์สำเร็จรูปที่นำมาใช้งานในบริษัทควรใช้งานโดยปราศจากการแก้ไข หากในกรณีที่มีความจำเป็นต้องดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป หน่วยงานที่ได้รับมอบหมายให้ดำเนินการต้องพิจารณาการควบคุมการแก้ไขอย่างเข้มงวด
- การเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูปต้องดำเนินการเปลี่ยนแปลงตามขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดไว้

4.35 การป้องกันข้อมูลสำหรับการทดสอบ (Test information)

ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง

4.36 มาตรการการตรวจประเมินระบบ (Protection of information systems during audit testing)

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ เช่น แผนการตรวจสอบช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) เป็นต้น
- ฝ่ายเทคโนโลยีสารสนเทศต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบก่อนดำเนินการตรวจสอบระบบสารสนเทศทุกครั้ง
- ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ โดยกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (System Availability) ต้องจัดให้มีการทดสอบนอกเวลาทำการ

นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศฉบับนี้ พิจารณาและอนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2567 เมื่อวันที่ 12 พฤศจิกายน 2567 และมีผลบังคับใช้ทันที