บริษัท พีอาร์ทีอาร์ กรุ๊ป จำกัด (มหาชน)
และบริษัทในเครือ

นโยบาย

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ฉบับนี้ เป็นลิขสิทธิ์ของ บริษัท พีอาร์ ทีอาร์ กรุ๊ป จำกัด (มหาชน) เพื่อมุ่งมั่นพัฒนาระบบการกำกับดูแลกิจการให้สอดคล้องตามหลักการกำกับดูแลกิจการ แนวปฏิบัติที่ดี รวมทั้งกฎ ระเบียบ ข้อกำหนดของทางการ และหน่วยงานที่ทำหน้าที่กำกับดูแล

คณะกรรมการบริษัทได้อนุมัตินโยบายการใช้งานระบบเทคโนโลยีสารสนเทศในบริษัท ฉบับนี้ ในการประชุมครั้งที่ 2/2567 วันที่ 27 กุมภาพันธ์ 2567 เพื่อให้ผู้บริหาร พนักงาน และผู้เกี่ยวข้องของบริษัทฯ และบริษัทย่อย ใช้เป็นหลักและแนวทางในการปฏิบัติ ทั้งนี้ ตั้งแต่วันที่ 1 มีนาคม 2567 เป็นต้นไป

เพื่อให้นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน เหมาะสมกับสถานการณ์ และการเปลี่ยนแปลง จึงกำหนดให้มีการทบทวนนโยบายการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ เป็นประจำอย่างน้อยปีละครั้ง การเปลี่ยนแปลงแก้ไขใด ๆ ต้องได้รับการอนุมัติโดยคณะกรรมการบริษัทเท่านั้น

(นิพนธ์ บุญเดชานันทน์)
รักษาการประธานกรรมการ

สารบัญ

1. บทนำ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของบริษัท บริษัท พีอาร์ทีอาร์ กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ร่วมกัน เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท บริษัทฯ จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

2. วัตถุประสงค์

2.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัทให้ดาเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและมีการปรับปรุงอย่างต่อเนื่อง

2.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและขั้นตอนปฏิบัติ ให้ผู้บริหาร พนักงาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2.4 นโยบายนี้ต้องมีการดำเนินการทบทวน ตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

2.5 เพื่อใช้เป็นเครื่องมือในการสื่อสารนโยบายการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศไว้เป็นลายลักษณ์อักษรให้บุคลากรของบริษัท บริษัทย่อยและบริษัทร่วม เพื่อสร้างความเข้าใจที่ตรงกัน

3. ขอบเขต

มีผลบังคับใช้กับบริษัท พีอาร์ทีอาร์ กรุ๊ป จำกัด (มหาชน) บริษัทย่อยและบริษัทร่วม ครอบคลุมหลักการ นโยบาย และแนวทางในการปฏิบัติ

4. คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานในนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

1. **“บริษัท”** หมายความว่า บริษัท พีอาร์ทีอาร์ กรุ๊ป จำกัด (มหาชน) บริษัทย่อย และบริษัทในเครือ ที่ใช้ระบบสารสนเทศ และระบบเครือข่ายและคอมพิวเตอร์ร่วมกัน
2. **“ฝ่ายทรัพยากรบุคคล”** หมายความว่า ฝ่ายทรัพยากรบุคคล ของ บริษัท พีอาร์ทีอาร์ กรุ๊ป จำกัด (มหาชน)
3. **“ส่วนเทคโนโลยีสารสนเทศ”** หมายความว่า ส่วนเทคโนโลยีสารสนเทศ ของ บริษัท พีอาร์ทีอาร์ กรุ๊ป จำกัด (มหาชน)
4. **“ผู้ใช้งาน”** หมายความว่า กรรมการบริษัท ผู้บริหาร ผู้ปฏิบัติงาน พนักงาน ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก ที่ ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเครือข่ายของบริษัท
5. **“ผู้ใช้งานภายนอก”** หมายความว่า บุคคล หรือนิติบุคคลนอกเหนือจากผู้ปฏิบัติงานและผู้ใช้งานที่เกี่ยวข้อง
6. **“ผู้ดูแลระบบ”** หมายความว่า ผู้จัดการส่วนเทคโนโลยีสารสนเทศ หรือผู้ปฏิบัติงานอื่น ที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป ให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแล รักษาระบบสารสนเทศ และระบบเครือข่าย ที่ใช้งานอยู่ในบริษัท หรือหน่วยงานที่มีหน้าที่ และรับผิดชอบในการดูแลระบบสารสนเทศ และระบบเครือข่าย โดยตรง
7. **“ระบบสารสนเทศ”** หมายความว่า ระบบงานของบริษัท ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผนการบริหาร และการสนับสนุนกลไกการทำงานของบริษัท
8. **“ระบบเครือข่าย”** หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่นๆ
9. **“สินทรัพย์”** หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับบริษัท ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัท

10. **“ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ”** หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศระบบเครือข่ายของบริษัท โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้าม ปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
11. **“สิทธิ์ของผู้ใช้งาน”** หมายความว่า ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ปฏิบัติงาน และผู้ใช้งานที่เกี่ยวข้อง ได้แก่ สิทธิ์ทั่วไป สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของบริษัท
12. **“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ”** หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ
13. **“บัญชีผู้ใช้งาน”** หมายความว่า รหัสพนักงาน อีเมลล์ (E-Mail) บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ปฏิบัติงานผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก
14. **“เหตุการณ์ด้านความมั่นคงปลอดภัย”** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือ เครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
15. **“การเข้ารหัส (Encryption)”** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ จะต้องมี โปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
16. **“การยืนยันตัวตน (Authentication)”** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
17. **“SSL (Secure Socket Layer)”** หมายความว่า เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน

18. **"VPN (Virtual Private Network)"** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

5. ความมั่นคงปลอดภัยสารสนเทศ (Information Security)

5.1 ความปลอดภัยสารสนเทศ

วัตถุประสงค์ : เพื่อทำให้การปฏิบัติงานของพนักงานที่เกี่ยวข้องกับข้อมูล รวมถึงระบบที่เกี่ยวข้องกับข้อมูลมีการปฏิบัติงานที่คำนึงถึงความปลอดภัยด้านสารสนเทศที่เพียงพอในการรองรับการดำเนินธุรกิจ และให้มั่นใจว่าข้อมูลของบริษัทมีความปลอดภัย รักษาความลับ ถูกต้อง และมีความพร้อมใช้ของข้อมูล เพื่อลดผลกระทบด้านการเงิน ความน่าเชื่อถือ และชื่อเสียงของบริษัท

ขอบเขต : ครอบคลุมการปกป้องข้อมูลของบริษัท ซึ่งจะเน้นข้อมูลที่อยู่ในรูปแบบปอิเล็กทรอนิกส์ และมีผลบังคับใช้กับพนักงานทุกระดับในบริษัท ตั้งแต่ผู้บริหาร พนักงาน รวมถึงบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลของบริษัท

5.2 การสื่อสารระเบียบฯ

บริษัทกำหนดให้พนักงานทุกท่านต้องได้รับการอบรมเกี่ยวกับการใช้งานระบบสารสนเทศในบริษัทอย่างปลอดภัย และให้มีการลงนามรับทราบเงื่อนไขการใช้งานระบบสารสนเทศ

5.3 การทบทวนระเบียบฯ

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศจะต้องทบทวนระเบียบฉบับนี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศของบริษัท เช่น การเปลี่ยนแปลงกลยุทธ์หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนแปลงโครงสร้างบริษัทหรือโครงสร้างเทคโนโลยี เป็นต้น เสนอต่อรองกรรมการผู้จัดการพิจารณาและลงนามผู้จัดทำ แล้วเสนอประธานเจ้าหน้าที่บริหารพิจารณาลงนามอนุมัติ

5.4 บทลงโทษ

ผู้ที่ฝ่าฝืนระเบียบฯ ฉบับนี้ ถือเป็นความผิดที่ร้ายแรง โดยมีบทลงโทษถึงขั้นสูงสุดตามข้อบังคับที่เกี่ยวกับการทำงานของบริษัท

6. โครงสร้างความปลอดภัยสารสนเทศ (Organization of Information Security)

6.1 โครงสร้างความมั่นคงปลอดภัยสารสนเทศภายในองค์กร (Internal organization)

วัตถุประสงค์ : เพื่อกำหนดบทบาทและหน้าที่รับผิดชอบในด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ อย่างเหมาะสมและปลอดภัยภายในองค์กร (Information security roles and responsibilities) โดยผู้บริหารระดับสูงสุดแต่งตั้งกลุ่มหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ และมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดตำแหน่งหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้เหมาะสม พร้อมทั้งควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

2) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตามและทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

3) ผู้บริหารต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

4) พนักงานและผู้ให้บริการภายนอกต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

การติดต่อกับหน่วยงานผู้มีอานาจ (Contact with authorities)

1) ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สาหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัย

การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษเรื่องเดียวกัน (Contact with special interest groups)

1) ต้องกำหนดรายชื่อ และข้อมูลสาหรับติดต่อกลุ่มที่มีความสนใจเป็นพิเศษเรื่องเดียวกันหรือกลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ

การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)

1) ต้องมีการกำหนดระเบียบ ข้อบังคับ กฎเกณฑ์ต่างๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูลเพื่อให้งานโครงการมีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน

กรณีโครงการที่จ้างผู้ให้บริการภายนอก ต้องปฏิบัติตามวิธีปฏิบัติงานด้านเทคโนโลยีสารสนเทศเพื่อให้การบริหารจัดการโครงการเกิดความมั่นคงปลอดภัย และลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น

7. การบริหารจัดการทรัพย์สิน (Asset Management)

7.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

วัตถุประสงค์ : เพื่อให้ระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์อย่าง เหมาะสม

ทรัพย์สิน หมายถึง ข้อมูล ซอฟต์แวร์ รวมทั้งอุปกรณ์ที่เกี่ยวข้องในการประมวลผล ซึ่งบริษัทได้กำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน อย่างไรก็ดี เจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบทรัพย์สินดังกล่าว

7.1.1 การจัดการบัญชีทรัพย์สินที่เป็นอุปกรณ์และซอฟต์แวร์ บริษัทกำหนดให้ฝ่ายบัญชีเป็นผู้จัดทำบัญชีทรัพย์สินประเภทอุปกรณ์และซอฟท์แวร์ โดยระบุรายละเอียดต่างๆ ไว้ในทะเบียนทรัพย์สิน และทำการตรวจสอบทรัพย์สินร่วมกับผู้ถือครองทรัพย์สิน เพื่อปรับปรุงทะเบียนทรัพย์สิน อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

7.1.2 ในทะเบียนทรัพย์สินต้องระบุผู้ถือครองหรือผู้ดูแลทรัพย์สิน และสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สินตลอดจนการแจ้งถึงการเปลี่ยนแปลงในการโอนย้ายทรัพย์สินข้ามบริษัทในเครือที่เกิดขึ้นให้ฝ่ายบัญชีทราบ

7.1.3 การใช้ทรัพย์สินอย่างเหมาะสม กรณีพนักงานเข้าใหม่ ฝ่ายบริหารทรัพยากรมนุษย์จะส่งแบบฟอร์มขอเพิ่ม/เปลี่ยนแปลง/ยกเลิก สิทธิผู้ใช้งาน ให้หน่วยงานต้นสังกัดระบุสิทธิการเข้าถึงข้อมูลในระบบ และการใช้เครือข่าย รวมถึงการใช้อุปกรณ์ต่อพ่วง อย่างเหมาะสม และต้องมีการทบทวนสิทธิของพนักงานในสังกัดอย่างน้อยปีละ 1 ครั้ง

7.1.4 การคืนทรัพย์สิน พนักงานของบริษัทที่สิ้นสุดการจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง ลาออก หรือพ้นสภาพจากการเป็นพนักงานของบริษัท ต้องคืนทรัพย์สินของบริษัททั้งหมดที่ตนเองถือครอง โดยฝ่ายบริหารทรัพยากรมนุษย์จะส่ง เอกสารตรวจเช็คทรัพย์สินให้ผู้บังคับบัญชาต้นสังกัดเป็นผู้ติดตามการส่งมอบทรัพย์สินต่างๆ พร้อมทั้ง ตรวจสภาพทรัพย์สิน หากผลการตรวจสอบพบว่ามีความชำรุดเสียหาย หรือมีข้อมูลบางอย่างขาดหายไป พนักงานผู้นั้นต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

7.1.5 การระบุสิทธิ์ในทรัพย์สินทางปัญญา ฝ่ายบัญชีจัดทำทะเบียนคุมซอฟท์แวร์ลิขสิทธิ์เพื่อควบคุมลิขสิทธิ์ซอฟต์แวร์ และ สิทธิ์ในทรัพย์สินทางปัญญาของบริษัท และให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการจัดเก็บเอกสารหลักฐานแสดงสิทธิ์ความเป็นเจ้าของลิขสิทธิ์ที่ถูกต้องตามกฎหมาย ซึ่งฝ่ายบัญชีต้องสุ่มตรวจสอบเอกสารแสดงสิทธิ์อย่างน้อยปีละ 1 ครั้ง

7.2 การจัดชั้นความลับของสารสนเทศ (Information classification)

วัตถุประสงค์ : บริษัทได้กำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้นและได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้ ยังได้กำหนดให้เจ้าของข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้องต้องเป็นผู้จัดลำดับชั้นของข้อมูล เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อบริษัท

7.2.1 ขั้นความลับสารสนเทศ (Classification of Information) สารสนเทศต้องมีการจัดชั้นความลับ โดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ดังนี้

1) ชั้นที่ 1 ข้อมูลเปิดเผยได้ ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย
2) ชั้นที่ 2 ข้อมูลใช้ภายในบริษัทเท่านั้น เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่าสามารถเปิดเผยให้พนักงานทุกคนภายในบริษัททราบได้ แต่ไม่สามารถเปิดเผยต่อบุคคลภายนอกบริษัทได้ เนื่องจากอาจสร้างความเสียหายให้กับบริษัทได้
3) ชั้นที่ 3 ข้อมูลลับ เป็นข้อมูลใช้ภายในบริษัทที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน

7.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

วัตถุประสงค์ : เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบหรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

7.3.1 การบริหารจัดการสื่อบันทึกข้อมูล (Management of Media) ขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือ ขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้

1) สื่อบันทึกข้อมูลต้องตั้งชื่อตามที่กำหนด และต้องมีทะเบียนควบคุมการใช้งาน
2) การเบิกสื่อบันทึกข้อมูลจะต้องได้รับการอนุมัติจากผู้มีอำนาจของหน่วยงานผู้ใช้
3) สื่อบันทึกข้อมูลต้องมีการตรวจนับอย่างน้อยปีละ 1 ครั้ง

7.3.2 การทำลายข้อมูล หรือสื่อบันทึกข้อมูล (Disposal of Media) ต้องมีการกำจัดหรือทำลายด้วยการปฏิบัติตามขั้นตอนสำหรับการทำลายที่บริษัทกำหนดไว้ ข้อมูลที่เป็น

ความลับ ต้องได้รับการอนุมัติจากผู้มีอำนาจและต้องมีการบันทึกการทำลายทุกครั้งเพื่อเป็นหลักฐานในการตรวจสอบในภายหน้า

1) ที่เป็นเอกสาร : ให้ทำลายโดยการเข้าเครื่องย่อยกระดาษ เผาทำลาย หรือด้วยวิธีการอื่นที่จะไม่สามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้

2) ที่เป็นสื่อบันทึกข้อมูล : ต้องทำด้วยวิธีที่มั่นใจได้ว่าข้อมูลที่อยู่ในสื่อไม่สามารถนำกลับมาใช้ได้อีก

7.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer) ต้องมีการป้องกันข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต หรือการนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

7.3.4 Removable media เช่น USB Drive, Flash drive, External Hard disk, Memory card จะต้องได้รับการอนุญาตให้ใช้งาน และ ควบคุมการใช้งาน โดยจะต้องมีการ เข้ารหัสข้อมูลในสื่อบันทึกนั้นๆด้วย

8. การควบคุมการเข้าถึง (Access Control)

8.1 ความต้องการทางธุรกิจเกี่ยวกับการเข้าถึง (Business Requirements of Access Control)

วัตถุประสงค์ : เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ และลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม

8.1.1 การควบคุมการเข้าถึง (Access Control) ฝ่ายเทคโนโลยีสารสนเทศจัดทำรายการการเข้าถึงระบบสารสนเทศ และนำรายการดังกล่าวมาทบทวนตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

8.2 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

วัตถุประสงค์ : เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือผู้ที่ไม่มีสิทธิเข้าใช้งานในระดับระบบปฏิบัติการ (Operating System) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีข้อความเตือนก่อนการเข้าสู่ระบบ การตรวจสอบผู้ใช้ และการบริหารรหัสผ่านสำหรับผู้ใช้งาน รวมถึงการควบคุมเวลาในการเชื่อมต่อสู่ระบบข้อมูล

8.2.1 การจัดการเข้าถึงสารสนเทศ (Information Access Restriction) การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับการควบคุมการเข้าถึง ผู้ดูแลระบบต้องจัดการให้ระบบแสดงข้อความเตือนถึง “การอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าใช้งาน” ก่อนที่จะทำการเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ของบริษัท และระบบต้อง

เปิดโอกาสให้ผู้ใช้สามารถยกเลิกการเชื่อมต่อเข้าสู่ระบบในกรณีที่ทราบว่าระบบนั้น ๆ ไม่ได้เกี่ยวข้องกับตนเอง

1) ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้ (User-ID) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้แต่ละคนได้
2) ผู้ใช้ควรออกจากระบบเครือข่าย (Log-off) ทันที เมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก
3) ผู้ใช้ถูกติดตั้งโปรแกรมถนอมหน้าจอ (Screen Saver) ที่มีรหัสผ่านบนเครื่องคอมพิวเตอร์ โดยโปรแกรมเหล่านี้จะเริ่มทำงาน หลังจากไม่มีการใช้งานใด ๆ บนเครื่องคอมพิวเตอร์นั้น ๆ ตามเวลาที่กำหนดไว้
4) หากไม่มีการใช้งานเป็นเวลานาน ผู้ใช้ต้องปิดเครื่องคอมพิวเตอร์ หรือเครื่องปลายทางให้เรียบร้อย
5) ต้องควบคุมและจากัดการใช้งานบัญชีผู้ดูแลระบบ (Administrator Account) โดยต้องพิจารณาให้สิทธิ์ตามหน้าที่รับผิดชอบและความจำเป็น โดยให้ถือหลักการให้สิทธิ์ที่น้อยที่สุดก่อน
6) ต้องดำเนินการทบทวน และตรวจสอบสิทธิ์การเข้าถึงระบบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

8.3 การจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

<u>วัตถุประสงค์</u> : เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต ด้วยการควบคุมสิทธิในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบ เริ่มตั้งแต่การขอเพิ่ม เปลี่ยนแปลง และยกเลิกสิทธิ รวมไปถึงการควบคุมสิทธิของผู้ใช้ ซึ่งมีสิทธิพิเศษที่สามารถแก้ไขสิทธิต่าง ๆ ของระบบได้

8.3.1 การขอเพิ่ม เปลี่ยนแปลง และยกเลิกสิทธิผู้ใช้งาน เพื่อเป็นการให้สิทธิการเข้าถึง

1) พนักงานทุกคนที่มีสิทธิเข้าใช้งานระบบข้อมูลต้องมีรหัสผู้ใช้เฉพาะบุคคลในการเข้าสู่ระบบ
2) รหัสผู้ใช้เป็นรหัสเฉพาะบุคคล โดยไม่มีการใช้รหัสผู้ใช้ร่วมกัน (Shared User ID) ในกรณีที่พนักงานลาออก รหัสผู้ใช้รายนั้น ต้องไม่ถูกนำกลับมาใช้ใหม่
3) ในการร้องขอเพื่อเข้าใช้งานระบบใดๆ ผู้บังคับบัญชาในหน่วยงานต้องทำการพิจารณาเพื่อเห็นชอบ

4) ผู้บังคับบัญชาในหน่วยงานและฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการร่วมกันในการยกเลิกสิทธิของผู้ใช้ ซึ่งไม่มีความต้องการใช้ระบบอีกต่อไปโดยทันที

8.3.2 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ผู้บังคับบัญชาในหน่วยงานต้องทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง

8.4 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์ : เพื่อให้ผู้ใช้งานระบบมีความตระหนักถึงความปลอดภัยในการใช้งานระบบข้อมูล โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่าน และต้องทราบถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานคอมพิวเตอร์

8.4.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information) ผู้ใช้งานต้องพิสูจน์ตัวตน ดังนี้

1) รหัสผ่านสำหรับการเข้าสู่ระบบถือเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสผู้ใช้ของตนให้บุคคลอื่น
2) ผู้ใช้ต้องกำหนดและใช้รหัสผ่านที่มีประกอบด้วย ตัวเลข อักขระพิเศษ ตัวพิมพ์ใหญ่และเล็ก รวมกันไม่น้อยกว่า 8 ตัวอักษร
3) ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำทุก ๆ 90 วัน ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตาม และผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำกับของเดิม หรือไม่ใช้วิธีเปลี่ยนตัวเลขต่อท้ายในรหัสผ่าน
4) ผู้ใช้ต้องตรวจสอบว่าสิทธิที่ตนได้รับในการเข้าใช้ระบบเหมาะสมกับหน้าที่ที่ตนรับผิดชอบหรือไม่ ถ้าพบว่าสิทธิที่ได้รับไม่เหมาะสมต้องแจ้งผู้บังคับบัญชาให้รับทราบเพื่อพิจารณาและปรับเปลี่ยนให้เหมาะสม
5) ในกรณีที่โปรแกรมไม่สามารถตั้งค่ารหัสผ่านตามนโยบายด้วยข้อจำกัดของโปรแกรม อนุโลมให้ตั้งค่าตามโปรแกรมนั้นๆ
6) ต้องเปลี่ยนรหัสผ่าน (Password) ตามที่บริษัทฯ กำหนดหรือหรือเปลี่ยนเมื่อต้องสงสัยว่ามีบุคคลอื่นล่วงรู้รหัสผ่านของตนเอง
7) เมื่อต้องเปลี่ยนรหัสผ่านใหม่ ผู้ใช้ไม่สามารถใช้รหัสผ่านเดิมซ้ำได้ (Password History) เป็นจำนวน 4 รหัสล่าสุด
8) หากผู้ใช้งานพยายามล็อกอินเข้าสู่ระบบแต่ใส่รหัสผ่านผิด 3 ครั้งติดต่อกัน ระบบจะ "ระงับ" หรือ "ล็อก" บัญชีอย่างถาวร ไม่สามารถปลดล็อกได้โดย

อัตโนมัติ ต้องติดต่อเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเพื่อปลดล็อกบัญชีผู้ใช้งานเท่านั้น

9) ข้อยกเว้นสำหรับบัญชีระบบและข้อจำกัดทางเทคนิค (Exceptions for System, Service & Database Accounts) ในกรณีที่บัญชีผู้ใช้งานไม่สามารถปฏิบัติตามมาตรฐานการตั้งรหัสผ่านที่บริษัทกำหนดได้ เนื่องจากข้อจำกัดทางเทคนิคของซอฟต์แวร์ หรือความจำเป็นในการเชื่อมต่อระบบงาน ให้ปฏิบัติตามแนวทางข้อยกเว้น

- ข้อยกเว้นด้านอายุรหัสผ่าน (Maximum Password Age / Expiry): สำหรับบัญชีระบบ (System Account), บัญชีบริการ (Service Account) หรือบัญชีในฐานข้อมูล (Database) ที่ใช้เชื่อมต่อกับระบบรายงาน (Report) หรือแอปพลิเคชันอื่น ซึ่งหากรหัสผ่านหมดอายุจะส่งผลกระทบต่อความต่อเนื่องของธุรกิจ (Business Continuity) อนุโลมให้ตั้งค่ารหัสผ่านแบบไม่มีวันหมดอายุได้
- ข้อยกเว้นด้านมาตรฐานความปลอดภัยและการล็อกบัญชี (Complexity & Lockout Policy): หากระบบไม่รองรับการตั้งค่าความซับซ้อน (Complexity), การเก็บประวัติรหัสผ่าน (Password History), การจำกัดจำนวนครั้งที่ใส่รหัสผิด (Account Lockout Threshold) หรือระยะเวลาการล็อกบัญชี (Lockout Duration) ให้ใช้มาตรการควบคุมทดแทนโดยการกำหนดรหัสผ่านที่มีความซับซ้อนและมีความยาวอย่างน้อย 14-16 ตัวอักษร หรือยาวที่สุดเท่าที่ระบบจะรองรับ (Maximum Length) เพื่อชดเชยมาตรการความปลอดภัยส่วนที่ไม่สามารถตั้งค่าได้
- การบันทึกและทบทวนข้อยกเว้น: ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำบัญชีรายชื่อข้อยกเว้น (Exception List) โดยระบุรายละเอียดส่วนที่ไม่สามารถตั้งค่าได้ตามมาตรฐานและมาตรการป้องกันทดแทนไว้เป็นหลักฐาน และต้องทำการทบทวนความเหมาะสมร่วมกับผู้บังคับบัญชาอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการปรับปรุงระบบ

9 การเข้ารหัสข้อมูล (Cryptography)

9.1 มาตรการเข้ารหัสข้อมูล (Cryptographic Controls)

วัตถุประสงค์ : เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม และได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศเพื่อรักษาความปลอดภัยของข้อมูลทั้งในด้านความลับและความถูกต้องของข้อมูลจำเป็นต้องพิจารณาถึงการนำซอฟต์แวร์และเทคนิคต่าง ๆ มาให้ในการเข้ารหัสข้อมูลที่มีความเสี่ยงเนื้อหา

9.1.1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอก เพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยทรัพย์สินของบริษัทโดยอย่างน้อยครอบคลุม

1) รหัสผ่านต่าง ๆ ที่เก็บอยู่ในระบบฐานข้อมูลจะถูกเข้ารหัสไว้ เจ้าของรหัสรวมถึงซอฟต์แวร์เจ้าของข้อมูลเท่านั้นที่ทราบรหัสผ่านดังกล่าว
2) ในการรับส่ง Email ได้ทำการเปิดใช้งานการเข้ารหัส (Encryption) โดยทำการเข้ารหัสในระดับของ Field ข้อมูล
3) การส่ง Email ที่มีข้อมูลสำคัญต้องอยู่ในรูปแบบที่เข้ารหัส และต้องเข้ารหัสไฟล์ข้อมูลที่เป็นความลับกรณีส่งไปยังบุคคลอื่น และแยกช่องทางการส่งไฟล์ข้อมูลและรหัสผ่านต้องไม่อยู่ใน Email ฉบับเดียวกัน

10 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

10.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์ : เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในบริษัท และกำหนดมาตรการป้องกันที่เหมาะสมตามระดับของความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศของบริษัทขั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับการอนุญาต ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคาม และการรบกวนไม่ว่าโดยตั้งใจหรือจากภัยธรรมชาติ

10.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ หน่วยงานได้จัดหาที่ตั้งห้อง Server ที่มีสภาพแวดล้อมภายนอกปลอดภัยจากภัยคุกคามภายนอก คือ อยู่ในสถานที่ ๆ เข้าถึงได้โดยยากจากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้ พื้นที่โดยรอบโปร่ง และสามารถมองเห็นได้ชัดหากมีการเข้าถึงห้อง Server

10.1.2 การรักษาความมั่นคงปลอดภัย บริษัทกำหนดให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศหรือผู้เกี่ยวข้องเท่านั้นที่มีสิทธิ์ในการเข้าถึงห้อง Server กรณีมีบุคคลภายนอกที่ไม่เกี่ยวข้องจำเป็นต้องเข้าไปให้บริการใดๆ ภายในห้อง Server จะต้องได้รับการอนุมัติก่อน

ทุกครั้ง พร้อมทั้งให้บันทึกรายละเอียดต่าง ๆ ในแบบฟอร์มการเข้า-ออก ห้อง Server ของบุคคลภายนอก ทุกครั้ง รวมทั้งต้องมีการจัดเตรียมอุปกรณ์รักษาความปลอดภัยในการเข้าถึงห้อง Server ดังนี้

1) ติดตั้งกล้องวงจรปิด และบันทึกภาพภายในห้องตลอดเวลา โดยสามารถดูข้อมูลย้อนหลังได้ 30 วัน

10.1.3 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม ต้องดำเนินการ ดังนี้

1) ศูนย์คอมพิวเตอร์ ต้องมีระบบป้องกันอัคคีภัย ระบบปรับอากาศและความชื้น ระบบกระแสไฟฟ้า

2) เครื่องปรับอากาศ มี 2 ชุดทำงานสลับกัน โดยตั้งความเย็นอยู่ที่ 20 -25 องศาเซลเซียส และมีความชื้นไม่เกิน 50%

10.2 การจัดการอุปกรณ์ (Equipment Management)

<u>วัตถุประสงค์</u> : เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่ออุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่าย และป้องกันการหยุดชะงักต่อการดำเนินการของบริษัท

10.2.1 การติดตามการทำงานของเครื่องแม่ข่าย (Server Monitor) มีการจัดทำรายงานสถานะการทำงานของเครื่องแม่ข่ายต่าง ๆ รวมถึงอุปกรณ์รอบข้างที่จำเป็น เป็นประจำทุกวัน โดยผู้ปฏิบัติจะทำการบันทึกสถานการณ์การทำงานต่าง ๆ ในรายการสถานะการทำงานของคอมพิวเตอร์แม่ข่าย และมีการจัดทำรายงาน สรุปสถานะการทำงานของเครื่อง Server ให้กับทางผู้บริหารให้ทราบเป็นประจำทุกไตรมาส

10.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) อุปกรณ์ต้องได้รับการป้องกันการล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบ และอุปกรณ์สนับสนุนการทำงานต่างๆ

1) อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สำคัญต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน (UPS) เพื่อให้ระบบทำงานต่อเนื่องหรือสิ้นสุดการทำงานอย่างเหมาะสมเมื่อระบบไฟฟ้าขัดข้อง

ต้องทำการตรวจสอบอุปกรณ์สำรองไฟฟ้าฉุกเฉินตามขั้นตอนของผู้ผลิตอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าว สามารถรองรับการทำงานได้เมื่อเกิดปัญหาไฟฟ้าขัดข้อง

11 ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

11.1 การปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

วัตถุประสงค์ : เพื่อให้การปฏิบัติงานด้านระบบประมวลผลที่มีความปลอดภัยและถูกต้อง โดยคำนึงถึงการแบ่งแยกหน้าที่ที่เหมาะสม

การบริหารจัดการขีดความสามารถของระบบ (Capacity Management) การใช้ทรัพยากรของระบบต้องมีการติดต่อ ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ ฝ่ายเทคโนโลยีสารสนเทศ จึงได้จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ (IT Master Plan) เพื่อทำให้เกิดความมั่นใจว่าสารสนเทศของบริษัทมีความปลอดภัย และสามารถเข้าถึงและใช้งานได้ตามสิทธิ์โดยง่าย มีการจัดเตรียมซอฟต์แวร์ คอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่คอยสนับสนุนการทำงานของหน่วยงานต่าง ๆ ตามแผนกลยุทธ์ภาพรวมบริษัท

11.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์ : เพื่อควบคุม และป้องกัน ซอฟต์แวร์ และข้อมูล จากโปรแกรมที่ไม่ประสงค์ดีและซอฟต์แวร์อันตราย

11.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against Malware) มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนัก ผู้ใช้งานที่เหมาะสม

1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกัน Virus Version ล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่อง Server โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา
2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้โปรแกรมค้นหา Virus ทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย
3) ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตมีการตรวจหา Virus ก่อนนำไปใช้งาน
4) ห้ามพนักงานดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนา Virus หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ
5) ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้นต้องตรวจสอบ Virus คอมพิวเตอร์ก่อนใช้งานทุกครั้ง

11.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์ : เพื่อป้องกันการสูญหายของข้อมูล และให้อุปกรณ์ประมวลผลสารสนเทศถูกต้องสมบูรณ์และพร้อมใช้งานเสมอ

11.3.1 การสำรองข้อมูล (Information Backup) ข้อมูลสำหรับสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการสำรองไว้ และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอ

1) มีการจัดเตรียมแผนในการสำรองข้อมูล และทดสอบกู้คืนระบบ/ข้อมูล ในแผนสำรองข้อมูลและทดสอบการกู้คืน และมีการปรับปรุงทบทวนแผนทุกปี
2) จัดทำคู่มือในการสำรองข้อมูล รวมถึงกู้คืนระบบและข้อมูลกับระบบสำคัญต่าง ๆ ทั้งหมด โดยจัดทำอยู่ในคู่มือการสำรอง และกู้คืนข้อมูล
3) ฝ่ายเทคโนโลยีสารสนเทศ ทำการตรวจสอบการสำรองข้อมูลในระบบทุกวัน ว่ามีสถานะเป็นอย่างไร พร้อมทั้งบันทึกสถานการณ์สำรองข้อมูลลงใน รายการสถานการณ์สำรองข้อมูล
4) ฝ่ายเทคโนโลยีสารสนเทศ ทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยระบบหลักต้องมีการทดสอบตามแผนการกู้คืน พร้อมทั้งสรุปเป็นรายงานเพื่อแจ้งคณะกรรมการความมั่นคงสารสนเทศตามกำหนดระยะเวลา อย่างน้อยปีละครั้ง
5) คอมพิวเตอร์ส่วนบุคคล ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลไฟล์ที่สำคัญ

11.4 การบันทึกข้อมูล Log และการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์ : เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

11.4.1 การบันทึกข้อมูล Log แสดงเหตุการณ์ (Event Logging) ข้อมูล Log แสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บ และทบทวนอย่างสม่ำเสมอ อุปกรณ์บันทึกข้อมูล Log จะได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไข และการเข้าถึงโดยไม่ได้รับอนุญาต

11.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)

วัตถุประสงค์ : เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

11.5.1 การติดตั้งซอฟต์แวร์ระบบให้บริการ (Installation of Software on Operational Systems) ซอฟต์แวร์คอมพิวเตอร์ทุกเครื่อง จะถูกติดตั้งโดยฝ่ายเทคโนโลยีสารสนเทศ

เท่านั้น โดยมีการตรวจสอบตามข้อกำหนด เรื่อง การบริหารจัดการทรัพย์สิน (Asset Management)

11.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์ : เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

11.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities) ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิค จุดอ่อนต่อช่องโหว่ของบริษัท มีการเก็บรวบรวม การประเมิน และเตรียมมาตรการที่เหมาะสมต้องถูกนำมาใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง โดยช่องโหว่ทั้งหมดจะถูกจัดเก็บไว้ที่เอกสารช่องโหว่ทางเทคนิค และช่องโหว่ทั้งหมดจะต้องรายงานต่อผู้บริหารระดับสูงอย่างน้อยปีละ 1 ครั้ง

11.6.2 ดำเนินการประเมินช่องโหว่อย่างน้อยปีละ 1 ครั้ง ให้ครอบคลุมทุกระบบสารสนเทศ รวมถึงเซิร์ฟเวอร์ ระบบฐานข้อมูล แอปพลิเคชัน เครือข่าย และอุปกรณ์โครงสร้างพื้นฐาน

11.6.3 ช่องโหว่ที่ตรวจพบต้องได้รับการประเมินระดับความเสี่ยงโดยแบ่งระดับความเสี่ยงเป็น ต่ำ (Low), ปานกลาง (Medium), สูง (High), และวิกฤต (Critical) และกำหนดระยะเวลาในการแก้ไข

Critical: ภายใน 7 วัน

High: ภายใน 14 วัน

Medium: ภายใน 30 วัน

Low: ตามความเหมาะสม

11.6.4 ทดสอบการทดสอบเจาะระบบ (Penetration Testing) ระบบสำคัญอย่างน้อยปีละ 1 ครั้ง หรือหลังการอัพเกรด/เปลี่ยนแปลงระบบที่สำคัญ

11.7 ตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations)

วัตถุประสงค์ : เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินระบบให้บริการ

11.7.1 มาตรการตรวจประเมินระบบ (Information Systems Audit Controls) ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการ ต้องมีการวางแผนและตกลงร่วมกันอย่างระมัดระวัง เพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ ฝ่ายเทคโนโลยีสารสนเทศ จะทำการกำหนดแผนการประเมินระบบสำคัญต่าง ๆ ไว้ในรายการตรวจประเมินระบบ และนำผลการตรวจประเมินเสนอผู้บริหารระดับสูงตามกำหนดระยะเวลา

12 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

12.1 การจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

วัตถุประสงค์ : เพื่อให้มั่นใจว่าระบบเครือข่ายมีความปลอดภัย และสามารถใช้เป็นสื่อในการรับส่งข้อมูลต่าง ๆ ได้อย่างมีประสิทธิภาพ

12.1.1 มาตรการเครือข่าย (Network Controls) เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่าง ๆ ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการควบคุมการปฏิบัติการด้านเครือข่าย ดังนี้

1) กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร (Network Configuration) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สายที่ใช้ในการสื่อสารของเครือข่ายทั้งหมด โดยจัดทำและปรับปรุง แผนภาพเครือข่าย ตำแหน่งเครื่องเซิร์ฟเวอร์ และ ตารางช่องบริการของเครื่องเซิร์ฟเวอร์ ให้ทันสมัยอยู่เสมอ
2) ควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่จัดไว้
3) มีมาตรการในการควบคุมดูแลสภาพและประเมินประสิทธิภาพการใช้งานของคู่สาย สายสื่อสาร และอุปกรณ์ในเครือข่ายสื่อสาร เพื่อให้พร้อมใช้งานตลอดเวลา
4) บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ
5) ประเมินประสิทธิภาพของระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และวางแผนในการปรับปรุงระบบเครือข่ายให้สามารถรองรับปริมาณงานที่จะขยายตัวในอนาคต

12.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services) กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าบริการเหล่านี้จะมีการให้บริการโดยบริษัทเองหรือจ้างการให้บริการก็ตาม ผู้ให้บริการทางเครือข่าย ต้องได้รับการตรวจสอบ และวิเคราะห์ในเรื่องระดับการให้บริการ รูปแบบความปลอดภัยของเครือข่าย การจัดการ ความต้องการของบริษัท

12.1.3 การแบ่งแยกเครือข่าย (Network Segregation and Segmentation) โดยกำหนดสถาปัตยกรรมเครือข่ายโดยแบ่งแยกส่วนการทำงานระหว่าง เครือข่ายภายใน (Internal Network) และ เครือข่ายภายนอก (External Network) ออกจากกันอย่างชัดเจน รวมถึงการแบ่งส่วนเครือข่ายย่อยตามระดับความสำคัญของข้อมูล เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและจำกัดขอบเขตความเสียหายหากเกิดการบุกรุก โดยมีแนวทางปฏิบัติดังนี้

1) การควบคุมเครือข่าย: ติดตั้งอุปกรณ์จัดเก็บและควบคุมการเข้าออกข้อมูล (เช่น Firewall หรือ Gateway) เพื่อคัดกรอง Traffic ระหว่างเครือข่ายภายในและภายนอกตามนโยบายความมั่นคงปลอดภัย

2) การจำกัดสิทธิ์การเข้าถึง: กำหนดสิทธิ์ให้ผู้ใช้งานหรือระบบงานสามารถเข้าถึงได้เฉพาะส่วนของเครือข่ายที่จำเป็นต่อการปฏิบัติงานเท่านั้น

12.2 การถ่ายโอนสารสนเทศ (Information Transfer)

<u>วัตถุประสงค์</u> : เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในบริษัทและถ่ายโอนกับหน่วยงานนอกบริษัท

12.2.1 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) สารสนเทศที่เกี่ยวข้องกับการส่งข้อความอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม

12.2.2 การตรวจสอบรายการการใช้งานเครือข่าย (Network Monitoring) ฝ่ายเทคโนโลยีสารสนเทศทำการตรวจสอบการใช้งานเครือข่ายของฝ่ายต่าง ๆ และจัดทำรายงานสรุปการใช้งานเครือข่าย เพื่อนำเสนอต่อผู้บริหารระดับสูงอย่างสม่ำเสมอ

12.3 การปฏิบัติงานจากระยะไกลและมาตรการความปลอดภัย (Remote Access Policy)

<u>วัตถุประสงค์</u> : เพื่อรักษาความมั่นคงปลอดภัยของการเข้าถึงระบบภายในจากระยะไกล (Remote Access) ให้มีประสิทธิภาพและป้องกันภัยคุกคามทางไซเบอร์

12.3.1 มาตรการควบคุมการเข้าถึงจากระยะไกล (Remote Access Controls)

12.3.1.1 สิทธิ์และการยืนยันตัวตน (Access Rights & Authentication)

1. ระบุตัวบุคคลที่มีสิทธิ์เข้าถึงระบบจากระยะไกลอย่างชัดเจน โดยกำหนดสิทธิ์ตามหน้าที่งาน (Role-based Access Control) เพื่อจำกัดการเข้าถึงเฉพาะส่วนที่จำเป็น
2. ห้ามผู้ใช้งานแบ่งปันบัญชี (Shared Account) หรือเปิดเผยรหัสผ่านแก่บุคคลอื่นโดยเด็ดขาด

3. การเข้าถึงโดยหน่วยงานภายนอก (External Parties) ต้องใช้บัญชีเฉพาะกิจสำหรับผู้ใช้ภายนอก และจำกัดสิทธิ์ตามความจำเป็น (Least Privilege) และต้องเปลี่ยนรหัสผ่านทันทีหลังเสร็จสิ้นการใช้งาน หรือกำหนดวันหมดอายุของบัญชี (Expired Account) และเฝ้าตรวจสอบการเข้าถึงทุกครั้ง

12.3.1.2 การควบคุมตามพื้นที่ภูมิศาสตร์ (Geographic Access Control - O365)

1. กำหนดให้ระบบ Microsoft 365 (O365) อนุญาตการเข้าใช้งานเฉพาะภายในประเทศไทยเท่านั้น และทำการปิดกั้น (Block) การเข้าถึงจากต่างประเทศทุกกรณีเพื่อลดความเสี่ยงจากการโจมตีทางไซเบอร์
2. หากมีความจำเป็นต้องเข้าใช้งานจากต่างประเทศ ผู้ใช้งานต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศ (IT) ล่วงหน้า เพื่อพิจารณาขอยกเว้นการปิดกั้นเป็นรายกรณี (Temporary White-list) ตามช่วงเวลาที่กำหนด
3. ผู้ที่ได้รับอนุญาตให้ใช้งานจากต่างประเทศ ต้อง ยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) และเชื่อมต่อผ่านช่องทางที่องค์กรกำหนดเท่านั้น

12.3.1.3 ความปลอดภัยของอุปกรณ์ (Device Security)

1. อุปกรณ์พกพาทุกเครื่องต้องเข้ารหัสข้อมูล (Disk Encryption) และติดตั้ง Antivirus / Endpoint Protection
2. กำหนดให้การเชื่อมต่อระยะไกลเข้าสู่ระบบภายในต้องผ่านเครือข่ายเสมือนส่วนตัว (VPN) ขององค์กรเท่านั้น
3. กำหนดระยะเวลาสิ้นสุดการเชื่อมต่อ (Session Timeout) หากไม่มีการใช้งานตามเวลาที่กำหนด ระบบต้องทำการล็อกหน้าจอหรือตัดการเชื่อมต่อโดยอัตโนมัติ

13 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

13.1 ด้านความมั่นคงปลอดภัยของระบบ (Security Requirements of Information Systems)

วัตถุประสงค์ : เพื่อให้มั่นใจได้ว่าการพัฒนาระบบงานได้คำนึงถึงความปลอดภัย และการควบคุมที่เพียงพอ บริษัทต้องมีการกำหนดให้มีการพิจารณาถึงความต้องการด้านความปลอดภัยของระบบงาน ก่อนที่จะมีการพัฒนาระบบงาน รวมถึงการกำหนดให้มีควบคุมภายในของระบบงาน

13.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification) ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องมีการรวมเข้ากับความต้องการสำหรับระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้ว

1) เจ้าของระบบงานธุรกิจ ต้องกำหนดความต้องการด้านความปลอดภัยสารสนเทศ ก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นเอกสารฟอร์มร้องขอพัฒนาโปรแกรม ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน
2) ความต้องการที่เกิดขึ้น จะต้องได้รับการอนุมัติจากผู้มีอำนาจ ก่อนส่งมายังฝ่ายเทคโนโลยีสารสนเทศ เพื่อพิจารณาความเป็นไปได้ในการพัฒนา

13.2 การพัฒนาและสนับสนุน (Security in Development and Support)

วัตถุประสงค์ : เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบ และดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

13.2.1 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures) การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบ มีการควบคุมโดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ โดยฝ่ายเทคโนโลยีสารสนเทศ จะทำการปรับปรุงเอกสารการควบคุมเวอร์ชั่นของระบบ

13.2.2 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing) แผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการจัดทำสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชั่น ใหม่

1) กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อให้มั่นใจว่า ข้อมูลมีความถูกต้อง สมบูรณ์
2) ผู้ร้องขอ จะต้องเป็นผู้ทดสอบ และตรวจรับระบบในฟอร์มร้องขอพัฒนาโปรแกรม

13.3 การทดสอบข้อมูล (Test Data)

วัตถุประสงค์ : เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

13.1.1 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments) สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกันเพื่อลดความเสี่ยงของการเข้าถึง หรือ การเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

1) ในการพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) และ ระบบที่ใช้งานจริง (Production System)

2) ต้องจัดให้มีระเบียบปฏิบัติที่ชัดเจนในการโอนย้ายโปรแกรมที่พัฒนาเสร็จแล้ว ไปยังระบบที่ใช้งานจริง

14 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

14.1 ความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship)

วัตถุประสงค์ : เพื่อให้มีการป้องกันทรัพย์สินของบริษัทที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

14.1.1 ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships) เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินของบริษัท จะต้องมีการกำหนดข้อตกลงกับผู้ให้บริการภายนอกเป็นลายลักษณ์อักษร และฝ่ายเทคโนโลยีสารสนเทศจะต้องจัดเก็บสัญญาการให้บริการไว้เป็นหลักฐาน

14.2 ให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

วัตถุประสงค์ : เพื่อรักษาระดับความปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่ได้จัดทำไว้

14.2.1 ติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

1) ต้องมีการตรวจสอบการให้บริการจากหน่วยงานภายนอก ผู้ทำหน้าที่ตรวจสอบจำเป็นต้องมีความรู้ ความเข้าใจในเรื่องความปลอดภัยสารสนเทศ ตลอดจนเงื่อนไขและข้อตกลงต่าง ๆ

2) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการเพื่อรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมายในกรณีที่จำเป็น

กำหนดให้มีการตรวจประเมินผู้ให้บริการภายนอกเป็นประจำทุกปี ตามเงื่อนไขที่ระบุไว้ในสัญญา พร้อมทั้งจัดทำรายงานสรุปผลการประเมินผู้ให้บริการภายนอก เพื่อรายงานให้ผู้บริหารรับทราบ

15 การบริหารจัดการผู้ให้บริการภายนอก (Third-party management)

วัตถุประสงค์ : เพื่อให้การบริหารจัดการผู้ให้บริการภายนอกด้านสารสนเทศ หรือพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัทหรือสามารถเข้าถึงข้อมูลสำคัญหรือลูกค้าของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพและมั่นคงปลอดภัย

กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอก เพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยทรัพย์สินของบริษัทโดยอย่างน้อยครอบคลุม

1) ก่อนใช้บริการ บริษัทจะดำเนินการระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึง โดยอย่างน้อยควรพิจารณาขอบเขต เหตุผล ระยะเวลาและ ความจำเป็นในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจและการยกเลิกหรือสิ้นสุดสัญญา

2) ข้อกำหนดในการรักษาความมั่นคงปลอดภัยของหน่วยงานภายนอก รวมถึง sub-contract ต้องปฏิบัติ โดยควรสอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่บริษัทกำหนด

3) ข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement)

4) สัญญาการให้บริการและเงื่อนไขระหว่างบริษัทและผู้ให้บริการภายนอก สอดคล้องตามนโยบาย การรักษาความมั่นคงปลอดภัยที่บริษัทกาหนด เช่น การทำลายข้อมูลของบริษัทหรือลูกค้าทั้งหมด เมื่อสิ้นสุดการใช้บริการ ความรับผิดชอบต่อการรั่วไหลของข้อมูลอันเนื่องมาจากการนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงในการให้บริการ เป็นต้น

5) มีกระบวนการติดตาม ประเมิน ทบทวน และรายงานผลการปฏิบัติงานของหน่วยงานภายนอก

16 จัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และการปรับปรุง (Management of Information Security Incidents and Improvements)

วัตถุประสงค์ : เพื่อให้มีวิธีการที่สอดคล้อง และได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

16.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการต้องมีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำเอกสารสำหรับการรับแจ้งปัญหาใน ฟอร์มการรับแจ้งปัญหา

16.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events) ประเด็นปัญหาต่าง ๆ ที่ได้รับแจ้ง และได้ดำเนินการแก้ไขเสร็จแล้วตามกำหนดระยะเวลา จะถูกนำข้อมูลดังกล่าวมาประมวลผล เพื่อสรุปออกมาเป็นรายงาน เพื่อแสดงให้เห็นว่าในช่วงเวลาที่ผ่านมานั้น มีปัญหาเรื่องอะไรมากที่สุด สาเหตุของปัญหาดังกล่าวเกิดจากอะไร และจะมีวีการป้องกันไม่ให้ปัญหานั้นเกิดขึ้นมาได้อย่างไร โดยฝ่ายเทคโนโลยีสารสนเทศ จะทำรายงานสรุปดังกล่าว เพื่อนำเสนอคณะกรรมการความมั่นคงปลอดภัยสารสนเทศเป็นประจำทุก 3 เดือน เพื่อร่วมพิจารณาปัญหาและวางแนวทางป้องกันปัญหาที่เกิดขึ้นในอนาคต

17 การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)

วัตถุประสงค์ : เพื่อป้องกันและรับมือกับการหยุดชะงักของการดำเนินธุรกิจ อันเนื่องมาจากภัยคุกคามต่อการทำงานของระบบ ให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักของบริษัทต่อไปได้

17.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity) บริษัทต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสภาพการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดภัยพิบัติ ผู้บริหารหรือหน่วยงานที่เกี่ยวข้องต้องมีการจัดการกระบวนการต่าง

ๆ เพื่อพัฒนาและคงไว้ซึ่งความต่อเนื่องทางธุรกิจ การจัดการกระบวนการต่าง ๆ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจดังกล่าว ต้องคำนึงถึงสิ่งต่าง ๆ ดังต่อไปนี้

1) การวิเคราะห์และการประเมินความเสี่ยงที่กระทบต่อการดำเนินธุรกิจของบริษัท

2) การจัดทำเอกสารกลยุทธ์เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ ต้องสอดคล้องกับเป้าหมายทางธุรกิจ ของบริษัท
3) การฝึกอบรมพนักงาน เพื่อให้ตระหนักถึงความมั่นคงปลอดภัย และเข้าใจในแผนฯ พร้อมทั้งสามารถปฏิบัติตามแผนฯ ได้
4) การกำหนดหน้าที่ความรับผิดชอบในการประสานงาน การพัฒนา การตรวจทาน และการปรับปรุงแผน

17.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity) บริษัทต้องกำหนด จัดทำเอกสารบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ และปรับปรุง กระบวนการ ขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

1) มีการสื่อสารไปยังพนักงานทุกคนทราบถึงแผนการดำเนินการเมื่อเกิดเหตุฉุกเฉิน

2) แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่าง ๆ ต้องมีการทดลอง ซักซ้อมตามระยะเวลาที่กำหนด
3) เจ้าของแผนงานและแนวทางปฏิบัติซึ่งเจ้าของแผนฯ ต้องรับผิดชอบในการบำรุงรักษา และทดสอบ พัฒนาหลักเกณฑ์ความต้องการและเงื่อนไขสำหรับการนำแผนฯ ไปใช้

17.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity) บริษัทต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมไว้ ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้อง และได้รับผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น พื้นฐานของการจัดการเพื่อให้เกิดความต่อเนื่องในการดำเนินธุรกิจคือ เข้าใจถึงกระบวนการ และเหตุการณ์ที่สามารถก่อให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจ ดังนั้น หน่วยงานเจ้าของกระบวนการรวมถึงหน่วยงานเจ้าของระบบงานธุรกิจที่สนับสนุนกระบวนการธุรกิจนั้น ต้องเข้าร่วมในการดำเนินการระบุเหตุการณ์ที่อาจส่งผลกระทบกับ

กระบวนการทางธุรกิจ ตลอดจนการประเมินความเสี่ยง เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วนในการดำเนินการจัดทำแผนบริหารจัดการความต่อเนื่องทางธุรกิจในการดำเนินธุรกิจลำดับต่อไป

17.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์ : เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

17.2.1 สภาพพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities) อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

18 การใช้บริการคลาวด์ (Cloud services policy)

วัตถุประสงค์ : เพื่อกำหนดเป็นมาตรการในการรักษาความปลอดภัยในการใช้บริการคลาวด์ รวมถึงปกป้องระบบ สารสนเทศ และแอปพลิเคชันที่มีการจัดเก็บไว้ในระบบคลาวด์ให้มีความมั่นคงปลอดภัย ไม่ถูกเข้าถึงได้โดย ไม่ได้รับอนุญาต

18.1 ต้องมีการบริหารจัดการระบบบริการคลาวด์อย่างมั่นคงปลอดภัย

18.2 ต้องมีการกำหนดสิทธิในการเข้าถึงระบบสารสนเทศ และแอปพลิเคชัน ให้สามารถเข้าถึง ได้เฉพาะผู้ที่มีส่วนเกี่ยวข้อง โดยควรตั้งค่าให้เฉพาะเจาะจง เช่น ผู้ที่มีสิทธิแก้ไขข้อมูล, ผู้ที่มีสิทธิดูเท่านั้น และผู้ที่ไม่มีสิทธิเข้าถึง

18.3 ต้องกำหนดเกณฑ์การเลือกบริการคลาวด์ โดยผู้ให้บริการคลาวด์ควรมีมาตรการป้องกันความ มั่นคงปลอดภัยบนโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ดังนี้

18.3.1 ผู้ให้บริการคลาวด์ต้องกำหนดให้มีวิธีการพิสูจน์ตัวตนในการเข้าถึงระบบที่มีความมั่นคง ปลอดภัย

18.3.2 ผู้ให้บริการคลาวด์ต้องมีแนวทางในการรักษาความมั่นคงปลอดภัยให้กับโครงสร้างพื้นฐานของการให้บริการคลาวด์

18.3.3 ผู้ให้บริการคลาวด์ต้องมีวิธีการในการบริหารจัดการและแก้ไขช่องโหว่เพื่อให้โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของตนเองมีความมั่นคงปลอดภัยอยู่เสมอ

18.3.4 ผู้ให้บริการคลาวด์ต้องมีกลไกหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการการ เปลี่ยนแปลงที่จำเป็นต้องดำเนินการกับโครงสร้างพื้นฐานของการให้บริการ และต้องดำเนินการแจ้งการเปลี่ยนแปลงใดๆ ก็ตามที่กระทบกับบริษัทฯ ให้ได้รับทราบก่อนล่วงหน้า

18.3.5 ผู้ให้บริการคลาวด์ต้องมีข้อมูลสำหรับการติดต่อ เพื่อใช้ในการแจ้งและประสาน งาน การแก้ไขปัญหาต่างๆ ที่เกิดขึ้นได้อย่างสะดวกและรวดเร็ว

18.3.6 ผู้ให้บริการคลาวด์ต้องมีโครงสร้างและทีมสำหรับการเฝ้าระวังติดตาม และบริหาร จัดการเหตุการณ์ด้านความมั่นคงปลอดภัย และประสานงานแจ้งให้บริษัทฯได้รับทราบ ตามความจำเป็น

18.3.7 กรณีที่จำเป็นต้องใช้หลักฐานข้อมูลด้านคอมพิวเตอร์ที่เป็นส่วนของผู้ให้บริการคลาวด์ ผู้ให้บริการคลาวด์ต้องช่วยเหลือและมอบหลักฐานข้อมูลดังกล่าว

18.4 บริษัทต้องกำหนดบทบาท และความรับผิดชอบที่เกี่ยวข้องกับการใช้และการบริหารจัดการบริการคลาวด์

18.5 มีการควบคุมการรักษาความปลอดภัยสารสนเทศที่ดำเนินการโดยผู้ให้บริการระบบคลาวด์

18.6 มีการบริหารจัดการการควบคุมส่วนต่อประสาน และการเปลี่ยนแปลงต่าง ๆ ในบริการเมื่อบริษัทฯ ใช้บริการคลาวด์หลายรายการ

18.7 กำหนดขั้นตอนในการบริหารจัดการเหตุการณ์การรักษาความปลอดภัยสารสนเทศที่เกิดขึ้น เกี่ยวกับการใช้บริการคลาวด์

18.8 กำหนดแนวทางสำหรับการติดตาม ทบทวน และประเมินการใช้บริการคลาวด์อย่างต่อเนื่องเพื่อบริหารจัดการความเสี่ยงด้านการรักษาความปลอดภัย

19 การทบทวนความสอดคล้องของความมั่นคงปลอดภัยสารสนเทศ (Compliance)

วัตถุประสงค์ : เพื่อให้มั่นใจว่าการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทมีความสอดคล้องกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัย บริษัทจึงกำหนดให้ผู้บริหารที่เกี่ยวข้องมีหน้าที่ต้องทบทวนความสอดคล้องของขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง เช่น การทบทวนสิทธิการเข้าถึงข้อมูลแต่ละระบบ การทบทวนแผนสำรองฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง เป็นต้น

20 การทำลายสื่อบันทึกข้อมูล (Media disposal)

วัตถุประสงค์ : เพื่อให้มั่นใจว่าสื่อบันทึกข้อมูลที่ไม่ใช้งานแล้วหรือมีข้อมูลที่ไม่ต้องการถูกทำลายหรือลบออกอย่างปลอดภัย ป้องกันไม่ให้เกิดการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และลดความเสี่ยงที่ข้อมูลสำคัญจะรั่วไหลหรือถูกนำไปใช้ในทางที่ไม่ถูกต้อง

20.1 ต้องส่งคืนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ของบริษัทฯ ให้ฝ่ายเทคโนโลยีสารสนเทศ เมื่อไม่มีความจำเป็นต้องใช้งานสื่อบันทึกข้อมูล หรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ไม่สามารถใช้งานได้

20.2 ต้องมั่นใจว่าสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่ถูกทำลายแล้ว จะต้องไม่สามารถกู้คืนกลับมาได้ ไม่ว่าจะโดยวิธีการใดก็ตาม

20.3 ต้องทำลายสื่อบันทึกข้อมูลประเภทกระดาษ เมื่อไม่มีความจำเป็นต้องจัดเก็บหรือใช้งาน โดยให้เป็นไปตามระดับชั้นความลับและเป็นไปตามระเบียบปฏิบัติที่กำหนดขึ้น

21 การใช้งานอุปกรณ์เคลื่อนที่และอุปกรณ์ส่วนตัว (Mobile Device and BYOD Management)

วัตถุประสงค์ : เพื่อกำหนดแนวทางและมาตรการในการใช้งานอุปกรณ์เคลื่อนที่ (Mobile Devices) และอุปกรณ์ส่วนตัว (Bring Your Own Device - BYOD) ในการเข้าถึงทรัพยากรและข้อมูลขององค์กรอย่างปลอดภัย ลดความเสี่ยงของการรั่วไหลของข้อมูล และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

21.1 อุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ที่นำมาใช้ทำงานจะต้องนำมาลงทะเบียนและได้รับอนุมัติจากผู้มีบังคับบัญชา และไม่ได้เชื่อมต่อเข้าระบบของบริษัทหรือฐานข้อมูล

21.2 อุปกรณ์เคลื่อนที่และอุปกรณ์ส่วนตัว (Mobile Device and BYOD) ต้องมีการติดตั้ง Anti-Virus ทุกเครื่อง และต้องมีการตรวจสอบความทันสมัยของ Anti-Virus ทุก 6 เดือน

21.3 ต้องจัดเก็บอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ที่นำมาใช้ทำงานในที่ปลอดภัย ไม่วางทิ้งไว้ในที่เสี่ยงต่อการสูญหาย

21.4 บริษัทฯ ไม่อนุญาตให้ใช้อุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ทำการดาวน์โหลดโปรแกรม ข้อมูล จัดเก็บข้อมูล จากระบบของบริษัทฯ หรือของลูกค้า หรือข้อมูลส่วนบุคคลที่ไม่จำเป็นไว้ในอุปกรณ์พกพาโดยเด็ดขาด

21.5 อุปกรณ์เคลื่อนที่ของบริษัทฯ หรือที่บริษัทฯ ดูแล (Mobile device) และอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ที่ได้รับอนุมัติให้สามารถใช้งานภายในบริษัทฯ ได้ ต้องปฏิบัติตามนโยบายดังต่อไปนี้

1) พนักงานของบริษัทฯ ที่ใช้งานอุปกรณ์ดังกล่าว ต้องมีความตระหนักในการใช้งานอุปกรณ์ให้มีความมั่นคงปลอดภัย ดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอย่างสม่ำเสมอ และต้องป้องกันระวังอุปกรณ์ไม่ให้ถูกโจรกรรมหรือสูญหาย

2) อุปกรณ์เคลื่อนที่ (Mobile Device) และอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ที่จะนำมาใช้เชื่อมต่อกับระบบของบริษัทฯ จะต้องได้รับอนุมัติก่อน ถึงจะนำมาเชื่อมต่อได้

3) ห้ามนำอุปกรณ์เคลื่อนที่ (Mobile Device) และอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ที่หลบเลี่ยงการควบคุมความมั่นคงปลอดภัย เช่น การ jailbreaking หรือการ rooting มาเชื่อมต่อกับระบบของบริษัทฯ โดยเด็ดขาด

4) ในการติดตั้งแอพพลิเคชั่นเพื่อใช้งานในอุปกรณ์ดังกล่าว ต้องเป็นแอพพลิเคชั่นที่อยู่ในรายการที่บริษัทอนุมัติแล้วเท่านั้น และต้องติดตั้งหรือดาวน์โหลดร้านค้า (Store) ได้รับอนุมัติแล้วเท่านั้น

5) ห้ามติดตั้งแอพพลิเคชั่นที่อยู่นอกรายการอนุมัติหรือจากร้านค้าอื่น (Store) นอกเหนือจากที่บริษัทฯ ได้กำหนดไว้

6) พนักงานต้องยอมให้บริษัทฯ ทำการตรวจสอบอุปกรณ์เคลื่อนที่ (Mobile Device) และอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ที่นามาใช้งาน

7) อุปกรณ์เคลื่อนที่ (Mobile Device) และอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) จะต้องทำการล็อคหน้าจอตามที่บริษัทฯ กำหนดไว้

8) พนักงานต้องปกป้องข้อมูลจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาติจากอุปกรณ์เคลื่อนที่ (Mobile Device) โดยวิธีการเข้ารหัสเครื่องหรือการเข้ารหัสข้อมูลตามระดับชั้นความลับของเอกสาร

9) พนักงานต้องเปิดใช้งานความสามารถ geo-location ของ อุปกรณ์เคลื่อนที่ (Mobile Device) จากระยะไกลทั้งหมด

21.6 พนักงานต้องทำการสำรองข้อมูลบนอุปกรณ์เคลื่อนที่ (Mobile Device) และอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) เท่าที่จำเป็น และต้องจัดเก็บข้อมูลที่สำรองไว้ในที่ที่บริษัทฯ กำหนดเท่านั้น

21.7 พนักงานต้องยอมให้บริษัทฯ ทำการลบข้อมูลอุปกรณ์เคลื่อนที่ (Mobile Device) และอุปกรณ์เคลื่อนที่ส่วนตัว (BYOD) ที่นำมาใช้งาน เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ถึงแม้ว่าอุปกรณ์เหล่านั้นจะมีข้อมูลส่วนตัวของพนักงานก็ตาม

21.8 บริษัทฯ มีสิทธิ์ในการปฏิเสธการเข้าใช้งานจากอุปกรณ์ส่วนตัวของพนักงาน ในการเข้าถึงข้อมูลและระบบของทางบริษัท หากบริษัทพบว่าอุปกรณ์ดังกล่าวอาจก่อให้เกิดความเสี่ยงต่อข้อมูล ระบบ พนักงาน และลูกค้าของบริษัท

21.9 บริษัทฯ มีสิทธิ์ในการทำลายข้อมูล (Self-Destruct) บนอุปกรณ์ส่วนตัวของพนักงานที่นำมาใช้ปฏิบัติงาน โดยบริษัทอาจจะมีการสั่งลบข้อมูลบนอุปกรณ์พกพาในกรณีที่เกิดเหตุการณ์ที่ทาให้เกิดการรั่วไหลหรือความไม่ปลอดภัยของข้อมูล

21.10 บริษัทฯ มีสิทธิ์ในการตรวจสอบใช้งานจากอุปกรณ์ส่วนตัวของพนักงาน เมื่อมีความจำเป็นต้องตรวจสอบหรือเมื่อกำหนดให้มีการตรวจสอบ

22 ความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ด้านทรัพยากรบุคคล (Human Resource Security)

วัตถุประสงค์ : เพื่อกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคลากรในองค์กร ทั้งก่อน ระหว่าง และหลังการปฏิบัติงาน โดยมีเป้าหมายในการลดความเสี่ยงจากการกระทำโดยไม่ตั้งใจหรือโดยเจตนาที่ส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และเพื่อให้เป็นไปตามข้อกฎหมายและข้อกำหนดที่เกี่ยวข้อง เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

22.1 ต้องตรวจสอบประวัติผู้สมัครงานที่ประสงค์จะมาเป็นพนักงานของบริษัทฯ ตามความเหมาะสมกับตำแหน่งของพนักงาน

22.2 ต้องจัดทำสัญญาไม่เปิดเผยความลับของข้อมูลสารสนเทศ (non-disclosure agreement-NDA) ให้แก่พนักงานหรือผู้ที่เกี่ยวข้องตามความเหมาะสม

22.3 ต้องแจ้งให้พนักงานทราบถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

22.4 ต้องจัดให้มีการอบรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงการคุ้มครองข้อมูลส่วนบุคคลและผลกระทบที่อาจจะเกิดขึ้น เพื่อสร้างความตระหนักให้พนักงาน อย่างน้อยปีละ 1 ครั้ง

22.5 จำกัดการเข้าถึงข้อมูลเฉพาะเท่าที่จำเป็น

22.6 ยกเลิกสิทธิ์การเข้าถึงระบบและข้อมูลทั้งหมดทันทีเมื่อสิ้นสุดการจ้างงาน

23 การพัฒนา และการบำรุงรักษาระบบให้มีความมั่นคงปลอดภัย (System development and maintenance)

วัตถุประสงค์ : เพื่อกำหนดแนวทางในการพัฒนา แก้ไข และบำรุงรักษาระบบสารสนเทศขององค์กรให้มีความมั่นคงปลอดภัย ตั้งแต่กระบวนการวางแผน พัฒนา ทดสอบ ไปจนถึงการนำไปใช้งานจริง โดยมุ่งเน้นการลดความเสี่ยงจากช่องโหว่หรือการถูกโจมตีจากภัยคุกคามทางไซเบอร์

23.1 ต้องมีการแยกสภาพแวดล้อมที่เกี่ยวข้องกับการพัฒนาแอปพลิเคชันออกจากระบบปฏิบัติงานจริง

23.2 ในการจ้างผู้ให้บริการจากภายนอกพัฒนาระบบแอปพลิเคชัน ต้องมีการระบุ จัดทำสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศเสมอ

23.3 ในการพัฒนาระบบต้องได้รับการควบคุมและทดสอบก่อนนำระบบไปใช้งานจริง

23.4 ให้ใช้หรือพัฒนาช่องทางการเชื่อมต่อระบบ (API: Application Programming Interface) ที่เป็นมาตรฐานสากลและต้องทดสอบความเข้ากันได้ของระบบก่อนนำมาใช้ปฏิบัติการจริง

24 บริหารจัดการความเสี่ยง (Risk Management Policy)

วัตถุประสงค์ : เพื่อกำหนดแนวทางและหลักเกณฑ์ในการระบุ ประเมิน จัดการ และติดตามความเสี่ยงที่อาจเกิดขึ้นกับองค์กร โดยเฉพาะความเสี่ยงที่เกี่ยวข้องกับข้อมูล ระบบสารสนเทศ ทรัพยากรบุคคล และกระบวนการทางธุรกิจ เพื่อให้มั่นใจว่าองค์กรสามารถดำเนินงานได้อย่างต่อเนื่อง ปลอดภัย และสอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง

24.1 กำหนดให้มีการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยของระบบ และให้มีการทบทวนการประเมินความเสี่ยงประจำสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือมีการเปลี่ยนแปลงรายการบัญชีทรัพย์สินสารสนเทศ (การเพิ่ม การลด การเปลี่ยนแปลงรายละเอียดสำคัญ) หรือ มีการเปลี่ยนแปลงที่มีแนวโน้มกระทบต่อมาตรการควบคุมและป้องกัน ด้านความมั่นคงปลอดภัยต่อสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

24.2 เสนอรายงานผลการประเมินความเสี่ยง (Risk Assessment Report) และแผนลดความเสี่ยง (Risk Treatment) ต่อผู้บริหารให้รับทราบและอนุมัติการจัดการต่อความเสี่ยง

25 ความมั่นคงปลอดภัยในการใช้ Generative AI (Generative AI Security Policy)

วัตถุประสงค์ : เพื่อการใช้ Generative AI ให้เหมาะสมสำหรับพนักงาน และผู้ปฏิบัติงานที่เกี่ยวข้อง ให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง และป้องกันผลกระทบที่อาจเกิดขึ้นกับบุคคล องค์กร และสังคม

25.1 แนวทางกาใช้ Generative AI

1) การใช้ Generative AI ต้องเป็นไปเพื่อประโยชน์ของบริษัทและสอดคล้องตามภารกิจของบริษัทเท่านั้น

2) ต้องไม่ใช้ Generative AI ในการสร้างเนื้อหาที่ผิดกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง หรือสร้างเนื้อหาที่เป็นอันตราย ทำให้เสื่อมเสียชื่อเสียง หรือเนื้อหาที่เป็นการล่วงละเมิดหรือไม่เหมาะสม

3) ต้องไม่ใช้ Generative AI ในการสร้างและแจกจ่ายเนื้อหาที่มีเจตนาบิดเบือน แสดงข้อมูลไม่ถูกต้อง หรือทำให้ผู้อื่นเข้าใจผิด

4) ไม่นำข้อมูลภายในองค์กรและข้อมูลที่มีชั้นความลับ (เช่น รหัสผ่าน เอกสารสัญญา เอกสารลับ ข้อมูลโครงการภายใน ฯลฯ) ไปใช้งานร่วมกับ Generative AI

5) ไม่นำข้อมูลส่วนบุคคล (เช่น ชื่อ-สกุล เลขประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์) และ ข้อมูลส่วนบุคคลที่อ่อนไหว ไปใช้งานร่วมกับ Generative AI

6) ไม่นำข้อมูลที่ส่งผลต่อความมั่นคงปลอดภัยของระบบ (เช่น API Key, การตั้งค่าระบบ) ไปใช้งานร่วมกับ AI

7) หากพบเหตุการณ์ละเมิดความมั่นคงปลอดภัยจากการใช้ AI ต้องแจ้งผู้บังคับบัญชาและปฏิบัติตามขั้นตอนการจัดการเหตุการณ์ความมั่นคงปลอดภัย (Incident Response) ทันที

8) ต้องตรวจสอบเนื้อหาที่สร้างโดย AI ก่อนนำไปใช้งานหรือเผยแพร่ เพื่อหลีกเลี่ยงการเกิดอคติหรือการเลือกปฏิบัติที่ไม่เป็นธรรม

9) ผู้ใช้งานต้องระมัดระวังไม่ให้การใช้ AI นำไปสู่การละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือสิทธิในทรัพย์สินทางปัญญาของผู้อื่น

10) หากเกิดความผิดพลาดหรือผลกระทบเชิงลบจากการใช้ AI ผู้ใช้งานต้องรายงานผู้บริหารตามสายงานทันที

26 การบริหารจัดการความเปลี่ยนแปลง (Change Management Policy)

วัตถุประสงค์ : เพื่อให้การเปลี่ยนแปลงระบบสารสนเทศทั้งหมดเป็นไปอย่างเป็นระบบ ลดความเสี่ยงจากความผิดพลาด และป้องกันผลกระทบที่อาจเกิดขึ้นกับความมั่นคงปลอดภัยและความต่อเนื่องทางธุรกิจ

26.1 ประเภทของการเปลี่ยนแปลง (Change Categories)

1) Standard Change: งานประจำที่มีขั้นตอนมาตรฐานชัดเจน (เช่น Patch ประจำเดือน) โดยต้องตรวจสอบการสำรองข้อมูล (Backup) ก่อนเริ่มงานทุกครั้ง

2) Normal Change: การแก้ไขฟังก์ชันหรือโครงสร้างระบบที่ต้องส่งใบคำขอเพื่อประเมินผลกระทบก่อนดำเนินการ แบ่งเป็น:

- Minor Change: การแก้ไขจุดเล็กๆ และไม่มีการหยุดให้บริการระบบ (No Downtime)
- Major Change: การอัพเดตใหญ่ที่ต้องมีการหยุดใช้ระบบตามแผน (Planned Downtime)

ทุก Normal Change ต้องส่งใบคำขอเพื่อประเมินผลกระทบและขออนุมัติก่อนเริ่มงาน

3) Bug Fix: การแก้ไขข้อผิดพลาดซอฟต์แวร์ที่ไม่เร่งด่วน โดยต้องระบุอาการและสาเหตุ (Root Cause) พร้อมผ่านการทดสอบในระบบจำลอง (UAT) ก่อนนำขึ้นระบบจริง เพื่อป้องกันผลกระทบต่อฟังก์ชันส่วนอื่น

4) Emergency Change: การแก้ไขเหตุฉุกเฉินหรือปิดช่องโหว่ความปลอดภัยร้ายแรง ให้ขออนุมัติผ่านผู้มีอำนาจโดยเร็วที่สุด (อนุมัติด้วยวาจาหรือช่องทางด่วนได้) โดยต้องมีแผน Backup เพื่อลดความเสี่ยง และจัดทำเอกสารบันทึกย้อนหลังให้ครบถ้วนภายใน 24 ชั่วโมง

26.2 ข้อปฏิบัติในการดำเนินการ (Implementation Rules)

1) การอนุมัติ (Approval): ทุกการเปลี่ยนแปลง (ยกเว้น Standard) ต้องผ่านการพิจารณาและอนุมัติจากผู้มีอำนาจ

2) แผนสำรอง (Roll-back Plan): ต้องจัดเตรียมแผนกู้คืนระบบกลับสู่สถานะเดิมเสมอ หากการดำเนินการไม่เป็นไปตามแผนหรือเกิดความล้มเหลว

3) การแยกสภาพแวดล้อม (Isolation): ห้ามแก้ไขหรือทดสอบบนระบบใช้งานจริง (Production) โดยตรง ต้องทดสอบในระบบจำลอง (Test/Staging) ให้เสร็จสิ้น และได้รับการยืนยันผลก่อนเสมอ

4) การบันทึก (Logging): ต้องบันทึกรายละเอียดประวัติการเปลี่ยนแปลง (ผู้ขอ, ผู้อนุมัติ, วันที่ดำเนินการ, รายการแก้ไข) เพื่อรองรับการตรวจสอบ (Audit) ย้อนหลัง

ประวัติการแก้ไข

ครั้งที่	ผู้ดำเนินการ	วันที่ทบทวน	วันที่บังคับใช้	รายละเอียดการแก้ไข
0	ปภพ พลาพิริยกิจ	15 ก.พ. 2567	1 มี.ค. 2567	จัดทำเอกสารเป็นครั้งแรก
1	ปภพ พลาพิริยกิจ	17 เม.ย. 2568	15 พ.ค. 2568	ทบทวนและปรับปรุงนโยบาย
2	ปภพ พลาพิริยกิจ	10 ก.พ. 2569	26 ก.พ. 2569	ทบทวนและปรับปรุงนโยบาย