ประกาศ บริษัท บีบีจีไอ จำกัด (มหาชน)

ที่ : 10000/004/2567 **เริ่มใช้** : 1 มิถุนายน 2567

วันที่ : 21 พฤษภาคม 2567 **สิ้นสุด** : เมื่อมีการเปลี่ยนแปลง

เรื่อง : นโยบายและมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัท บีบีจีไอ จำกัด (มหาชน) ต่อไปนี้เรียกว่า “บริษัทฯ” มีนโยบายให้ระบบเทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญที่ช่วยสนับสนุนนโยบายการพัฒนาธุรกิจอย่างยั่งยืนไปกับสิ่งแวดล้อมและสังคมขององค์กร เพื่อรองรับการตอบสนองต่อความคาดหวังและความต้องการของผู้มีส่วนได้เสีย โดยเฉพาะการมีแนวปฏิบัติ มีเครื่องมือ มีมาตรฐานที่ใช้ดำเนินการที่ทันสมัย มีประสิทธิภาพ และมีความปลอดภัยสอดคล้องตามมาตรฐานสากล

เพื่อให้การดำเนินการใดๆ ด้านเทคโนโลยีสารสนเทศของบริษัทฯ และกลุ่มบริษัทในเครือ มีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนข้อมูลและสินทรัพย์สารสนเทศของบริษัทฯ ได้รับการดูแลรักษาอย่างเหมาะสม โดยคำนึงถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศและด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น มาตรการในการรักษาความลับ ความถูกต้อง ครบถ้วน สมบูรณ์ และความพร้อมใช้ต่อการดำเนินงานอย่างเหมาะสม รวมถึงสอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ จึงได้กำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ดังรายละเอียดปรากฏตามเอกสารแนบท้าย

ทั้งนี้ จึงแจ้งให้ทราบโดยทั่วกัน โดยให้มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2567 เป็นต้นไป

(นายกิตติพงศ์ ลิ่มสุวรรณโรจน์)
ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่

สำเนา : ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ รองกรรมการผู้จัดการใหญ่ ผู้ช่วยกรรมการผู้จัดการใหญ่ ผู้อำนวยการอาวุโส ผู้อำนวยการ ผู้จัดการอาวุโส ผู้จัดการส่วนหรือเทียบเท่า ป้ายประกาศ

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

สารบัญ

รายการปรับปรุงแก้ไข

Version	คำอธิบาย	เสนอโดย	อนุมัติโดย	วันประกาศใช้	
				เริ่มใช้	ยกเลิก

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

กำหนดให้นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศมีรายละเอียด ดังนี้

1) การตรวจสอบและประเมินความเสี่ยง

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทฯ ยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

2) การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

หน่วยงานเจ้าของโครงการ ต้องจัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์บริษัทฯ โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

3) การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

3.1) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทฯ ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัทฯ

3.2) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรการป้องกัน ควบคุมการใช้งาน และการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัทฯ ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

3.3) การจัดการข้อมูลสารสนเทศและการรักษาความลับ

(1) การจำแนกประเภททรัพย์สินสารสนเทศ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดแนวทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัทฯ มาร่วมพิจารณาการกำหนด

ชั้นความลับที่เหมาะสม รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้

(2) การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

(3) การควบคุมการเข้ารหัสข้อมูล

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

3.4) การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

(1) การควบคุมการใช้งานของผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีการควบคุมการใช้งานทรัพย์สินสารสนเทศและระบบสารสนเทศ ดังนี้

1. กำหนดมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่รหัสผ่าน และให้ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์ โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มีการล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม

2. กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกบริษัทฯ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดให้มีมาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัทฯ รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัทฯ

3. กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯ อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯ รับทราบและปฏิบัติตาม

(2) การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

3.5) การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

(1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

(2) การควบคุมการรับส่งข้อมูลสารสนเทศ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัทฯ และระหว่างบริษัทฯ กับหน่วยงานภายนอกบริษัทฯ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

1. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัทฯ และระหว่างบริษัทฯ กับหน่วยงานภายนอกบริษัทฯ อย่างเป็นลายลักษณ์อักษร

2. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

3. ผู้บริหารระดับฝ่ายต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทฯ มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทฯ อย่างเป็นลายลักษณ์อักษร

3.6) การป้องกันภัยคุกคามต่อระบบสารสนเทศ

(1) การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

(2) การบริหารจัดการช่องโหว่ทางเทคนิค

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องควบคุมให้ระบบสารสนเทศของบริษัทฯ ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

1. จัดให้มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (Untrusted Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Business Impact Analysis) ดังนี้

   1.1. กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ

   1.2. กรณีที่เป็นระบบงานที่มีความสำคัญอื่นๆ ต้องทดสอบอย่างน้อยทุก 5 ปี

2. จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไขและป้องกัน

3. จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศตามอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)

3.7) การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

4) การกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานที่สอดคล้องกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศได้ และต้องกำหนดผู้รับผิดชอบตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศดังกล่าวให้ชัดเจน โดยมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทฯ แบ่งออกเป็น 14 ข้อ ได้แก่

1. มาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard)
2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)
3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)
4. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)
5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)
6. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)
7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)
9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)
10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)
11. การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)
12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)
13. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)
14. การปฏิบัติตามข้อกำหนด (Compliance)

5) การทบทวนนโยบาย

กำหนดให้มีการทบทวนนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้ฝ่ายเทคโนโลยีสารสนเทศ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลง

6) การเผยแพร่นโยบาย

ทุกหน่วยงานมีหน้าที่รับผิดชอบโดยการประกาศให้ทราบ และเผยแพร่นโยบายเหล่านี้ รวมทั้งทำการสนับสนุนตอบสนอง นโยบายของบริษัทฯ

7) การรายงาน

ให้มีการรายงานการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดใดๆ ต่อคณะกรรมการของบริษัทฯ อย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีเหตุการณ์ใดๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดอย่างมีนัยสำคัญ เช่น ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหายหรืออันตรายใดๆ แก่บริษัทฯ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดที่บริษัทฯ กำหนดไว้ ทั้งนี้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

8) บทบังคับใช้

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศนี้ให้ใช้บังคับกับ พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของ บริษัท บีบีจีไอ จำกัด (มหาชน) และกลุ่มบริษัทในเครือ รวมถึงบุคคลภายนอก และหน่วยงานภายนอกที่ให้บริการแก่บริษัทฯ โดยมีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

มาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

สารบัญ

รายการปรับปรุงแก้ไข

Version	คำอธิบาย	เสนอโดย	อนุมัติโดย	วันประกาศใช้	
				เริ่มใช้	ยกเลิก

วัตถุประสงค์

บริษัท บีบีจีไอ จำกัด ต่อไปนี้เรียกว่า “บริษัทฯ” มีนโยบายให้ระบบเทคโนโลยีสารสนเทศ เป็นปัจจัยสำคัญที่ช่วยสนับสนุนนโยบายขององค์กร เพื่อรองรับการตอบสนองต่อความคาดหวังและความต้องการของผู้มีส่วนได้เสีย โดยเฉพาะการมีแนวปฏิบัติ เครื่องมือ มาตรฐานที่ใช้ที่ทันสมัย มีประสิทธิภาพ และมีความปลอดภัยสอดคล้องตามมาตรฐานสากล

เพื่อให้การดำเนินการใดๆ ด้านเทคโนโลยีสารสนเทศของ บริษัท บีบีจีไอ จำกัด และบริษัทในเครือ มีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนข้อมูลและสินทรัพย์สารสนเทศขององค์กร ได้รับการปกป้องด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และให้เกิดการปรับปรุงอย่างต่อเนื่อง รวมถึงเป็นไปตามข้อกำหนดของมาตรฐาน และนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ จึงได้มีการจัดทำมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อเป็นแนวปฏิบัติและขั้นตอนปฏิบัติขึ้น

บทบังคับใช้

มาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ฉบับนี้ ให้มีผลบังคับใช้กับหน่วยงานภายใต้บริษัท บีบีจีไอ จำกัด (มหาชน)

นิยาม

1. **บริษัทฯ** หมายถึง บริษัท บีบีจีไอ จำกัด (มหาชน)
2. **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งกำหนดไว้ดังนี้
   - **ผู้บริหาร** หมายถึง ผู้บริหารที่ดูแลรับผิดชอบด้านบริหารและเทคโนโลยีสารสนเทศ
   - **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
   - **เจ้าหน้าที่** หมายถึง พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของบริษัท บีบีจีไอ จำกัด (มหาชน) และกลุ่มบริษัทในเครือ บุคคลภายนอก และหน่วยงานภายนอก ที่ใช้งานระบบงานคอมพิวเตอร์ของบริษัทฯ หรือบุคคลใดที่ได้รับมอบหมายหน้าที่จากบริษัทฯ หรือพนักงาน ของบริษัทฯ และเจ้าหน้าที่ประจำโครงการของบริษัทฯ
3. **ข้อมูล หมายถึง ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ที่อยู่ในรูปของ** ตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์ หรือที่อยู่ในรูปสื่อสิ่งพิมพ์และให้ความหมายรวมถึงข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

4. **ข้อมูลสารสนเทศ** หมายถึง ข้อมูล ข่าวสาร ความรู้ ข้อเท็จจริง ที่นำมาบันทึกไว้ในทรัพยากรสารสนเทศของบริษัท ฯ ได้แก่ เอกสาร สื่อบันทึกข้อมูล เป็นต้น
5. **ข้อมูลอิเล็กทรอนิกส์** หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร
6. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
7. **สารสนเทศ** หมายถึง ข้อมูลต่างๆ ที่ได้ผ่านการเปลี่ยนแปลง การประมวลผล หรือวิเคราะห์ ผลสรุปด้วยวิธีการต่างๆ ให้สื่อความหมาย ตรงตามวัตถุประสงค์ที่ต้องการ หรือให้อยู่ในรูปแบบที่สามารถนำไปใช้ประโยชน์ในการใช้งานได้ เพื่อให้ความรู้ทำให้เกิดความคิดความเข้าใจ วิเคราะห์ผล การตัดสินใจ และการวางแผนการบริหารงาน
8. **หน่วยงานภายนอก/ผู้ให้บริการภายนอก** หมายถึง บุคคลที่สาม ผู้ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) และผู้มีสัญญาทำงานให้บริษัทได้รับอนุญาตให้ มีสิทธิเข้าถึงและใช้งานระบบสารสนเทศ ของบริษัท ตามอำนาจหน้าที่ที่รับผิดชอบ
9. **ระบบสารสนเทศ** หมายถึง ระบบคอมพิวเตอร์ ระบบเก็บข้อมูล ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสื่อสารข้อมูลทุกประเภท อุปกรณ์สื่อสาร เครื่องพิมพ์ เครื่องสแกนหรืออุปกรณ์ใดๆ ที่เกี่ยวข้องที่เป็นกรรมสิทธิ์ของบริษัท และ/หรือ ที่บริษัท ได้รับอนุญาตให้ใช้ได้ตามกฎหมาย
10. **ระบบเครือข่าย** หมายถึง กลุ่มของคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่ถูกนำมาเชื่อมต่อกันเพื่อให้ผู้ใช้งานในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่างๆ ในเครือข่ายร่วมกันได้
11. **ทรัพย์สิน** หมายถึง
    1) อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์อื่นใดที่ใช้งานร่วมกับอุปกรณ์เทคโนโลยี สารสนเทศที่เกี่ยวข้องทุกประเภท
    2) ชุดคำสั่ง โปรแกรมระบบงานสารสนเทศ และโปรแกรมอื่นใดที่ใช้งานร่วมกับโปรแกรม ระบบงานสารสนเทศ
    3) ข้อมูลสารสนเทศ หรือ ทรัพย์สินทางปัญญาใด ๆ
12. **อุปกรณ์พกพา** หมายถึง เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเล็ตคอมพิวเตอร์ (Tablet Computer) ที่บริษัทอนุญาตให้เชื่อมต่อและใช้งานสารสนเทศของบริษัทได้
13. **สื่อบันทึกข้อมูล** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard drive หรือ Flash drive หรือ Handy drive หรือ Thumb drive หรือ External hard drive เป็นต้น
14. **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว
15. **สถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งทำให้ระบบของบริษัทไม่สามารถใช้งานได้ ถูกบุกรุกหรือโจมตี หรือความมั่นคงปลอดภัยถูกคุกคาม

บทบาทและความรับผิดชอบ

ผู้บริหารระดับสูง :

1. อนุมัติมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ
2. ตัดสินใจในการติดต่อกับหน่วยงานบังคับใช้กฎหมาย และหน่วยงานสืบสวน เมื่อมีข้อสงสัยว่า มีการกระทำผิดร้ายแรงเกิดขึ้น
3. รับผิดชอบโดยรวมในความปลอดภัยของทรัพย์สิน เพื่อให้มีความมั่นใจว่า การปฏิบัติตามวัตถุประสงค์ทางธุรกิจของบริษัทและความต้องการภายนอกเป็นไปอย่างต่อเนื่อง

ผู้บริหารที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศ :

1. กำหนดทิศทาง และให้การสนับสนุนเรื่องนโยบายความมั่นคงปลอดภัยสารสนเทศ ให้แก่ เจ้าหน้าที่ที่รับผิดชอบดูแลรักษาระบบความปลอดภัยระบบสารสนเทศ
2. อนุมัติ และสนับสนุนกิจกรรมโครงการด้านความปลอดภัยสารสนเทศและเป็นหลักในการริเริ่มให้มีการสร้างความตระหนักเรื่องการรักษาด้านความปลอดภัยสารสนเทศ
3. ทบทวน สรุป และนำเสนอต่อผู้บริหารระดับสูงและคณะกรรมการบริษัท เพื่ออนุมัตินโยบายความมั่นคงปลอดภัยสารสนเทศ รวมถึงข้อยกเว้นและการเปลี่ยนแปลงที่อาจจะมีขึ้น
4. วิเคราะห์ ประเมิน สรุปผล และนำเสนอต่อผู้บริหารระดับสูงและคณะกรรมการบริษัท ประเด็นซึ่งมีการกระทบอย่างยิ่งยวดต่อทั้งบริษัทฯ อาทิ สัญญากับผู้ขาย ผู้ซึ่งฝ่าฝืนนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทอย่างรุนแรง การขาย จำหน่าย จ่ายแจก หรือการถ่ายโอนซอฟต์แวร์ของบริษัท รวมทั้งทรัพย์สินทางปัญญาไปยังบุคคลอื่น การเปิดเผยข้อมูลสารสนเทศที่สำคัญ การเปลี่ยนแปลงที่สำคัญต่อเว็บไซต์ของบริษัท
5. ทบทวนและอนุมัติความต้องการด้านความปลอดภัยของระบบที่จะนำไปใช้กับข้อมูล สารสนเทศที่มีความอ่อนไหว (Sensitive) หรือสำคัญมากต่อการปฏิบัติงานทางธุรกิจก่อนเริ่มต้นพัฒนาโครงการ (Project Development)

บุคลากรที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศ :

1. พัฒนาขั้นตอนการปฏิบัติงาน รวบถึงเอกสารสนับสนุน การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
2. ระบุทรัพย์สินที่ตนบริหารอยู่ตามแนวทางในเชิงธุรกิจของตน และได้ชื่อว่าเป็นเจ้าของทรัพย์สินนั้น นอกจากนั้นยังเป็นผู้วิเคราะห์ความเสี่ยงของทรัพย์สินที่ครอบครองอยู่
3. บริหารจัดการทรัพย์สินที่อยู่ภายใต้การควบคุมของตน และระมัดระวังตามความจำเป็นที่ จะป้องกันความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้งานของทรัพย์สินที่ใช้ในหน่วยธุรกิจ
4. กำหนดลำดับความสำคัญ ริเริ่ม และลงมือปฏิบัติ เพื่อให้ผู้ใช้งานที่อยู่ในหน่วยธุรกิจนั้น ปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ อาทิ การสร้างและการวางวิธีในการตรวจสภาพแวดล้อมของการรักษาด้านความปลอดภัยสารสนเทศของบริษัท
5. กำหนดให้มีการควบคุมที่เหมาะสมเพื่อรักษาไว้ซึ่งความปลอดภัยระบบสารสนเทศของบริษัท สำหรับการใช้ซอฟต์แวร์สำเร็จรูปทางการค้าหรือว่าจ้างผู้อื่นพัฒนา

6. สนองตอบต่อเหตุการณ์ด้านความปลอดภัยสารสนเทศ ซึ่งเป็นเหตุการณ์ที่มีผลกระทบด้านลบต่อหน่วยธุรกิจอื่นหรือทั้งบริษัทฯ อาทิ มีผลอย่างยิ่งต่อภาพพจน์ของบริษัทความเชื่อมั่นของลูกค้าการดำเนินการของบริษัท โดยต้องรายงานต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศรับทราบ
7. ให้การสนับสนุนในการสืบสวน และเสนอแนวทางแก้ไขต่อทรัพย์สินที่เกี่ยวข้องกับการสูญเสีย และเหตุการณ์ด้านความปลอดภัยสารสนเทศที่เกิดขึ้น
8. ดูแลรักษาและปรับปรุงระบบคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ รวมทั้งสอดส่องดูแลการใช้งานเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย
9. ให้การสนับสนุนในการสอบสวน และแก้ไขปัญหา ในส่วนที่ทราบหรือสงสัยว่าทรัพย์สินสำคัญของบริษัทถูกคุกคาม เหตุการณ์ที่ต้องสงสัยว่ามีการโจมตีระบบรักษาด้านความปลอดภัยสารสนเทศ หรือเป็นการกระทำที่ไม่เหมาะสมและแจ้งผลลัพธ์ให้เจ้าของทรัพย์สินที่ทราบ

เจ้าของทรัพย์สิน :

1. กำหนดลำดับชั้นความปลอดภัยของทรัพย์สินตามความอ่อนไหว และความสำคัญต่อบริษัทฯ ตามมาตรฐานของบริษัท พร้อมทั้งแจ้งให้กลุ่มผู้เกี่ยวข้องรับทราบในการเปลี่ยนแปลงชั้นของข้อมูลสารสนเทศที่เกิดขึ้น
2. พัฒนา และปรับปรุงโครงสร้างการแบ่งลำดับชั้นของทรัพย์สิน และมีการจัดทำป้ายแสดงลำดับชั้น และข้อกำหนดในการบริหารจัดการ
3. ระบุกฎเกณฑ์การกำหนดสิทธิในการเข้าถึงทรัพย์สิน เช่น บทบาทของผู้ใช้งานหรือของบริษัทฯ วิถีทางที่จะเข้าถึงที่ต้องได้รับการอนุมัติ พร้อมทั้งแจ้งให้กลุ่มผู้เกี่ยวข้องรับทราบในการเปลี่ยนแปลงกฎเกณฑ์ที่เกิดขึ้น
4. ระบุกลุ่มการดำเนินงานในหน่วยธุรกิจที่รับผิดชอบในการอนุญาต และเตรียมเรื่องการเข้าถึงทรัพย์สินรวมถึงการบริหารจัดการบัญชีของผู้ใช้งาน การพิจารณาการแบ่งแยกหน้าที่ให้เหมาะสม และให้สิทธิในการตรวจสอบ

ฝ่ายตรวจสอบภายใน :

1. สอบทานการนำนโยบายความมั่นคงปลอดภัยสารสนเทศมาใช้ และประเมินการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานด้านความปลอดภัยสารสนเทศ รวมถึงประสิทธิภาพของนโยบาย และมาตรฐานด้านความปลอดภัยสารสนเทศ ตลอดจน การวัดผลการควบคุมภายใน โดยถือเป็นส่วนหนึ่งของตารางการตรวจสอบเป็นประจำ อย่างน้อยปีละ 1 ครั้ง และทำการสื่อสารความเห็นประกอบการประเมินไปยังผู้บริหารที่เกี่ยวข้องได้รับทราบ
2. กำหนดวิธีการสอบทานให้มีการควบคุมอย่างเพียงพอ อาทิ การป้องกันและรักษา ระบบปฏิบัติการหรือเครื่องมือที่ใช้ในการตรวจสอบ เพื่อมิให้เกิดความเสียหายในระหว่างการตรวจสอบ

ผู้ใช้งาน :

1. ทำความเข้าใจกับนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความปลอดภัย สารสนเทศปฏิบัติตามนโยบายของบริษัท และให้การร่วมมือการใช้กฎข้อบังคับต่าง ๆ
2. ใช้ทรัพย์สินของบริษัทอย่างมีประสิทธิภาพ มีจริยธรรม และถูกต้องตามกฎหมาย
3. รายงานเหตุการณ์ที่เกี่ยวกับด้านความปลอดภัยสารสนเทศแก่หัวหน้างาน และฝ่ายเทคโนโลยีสารสนเทศให้ทราบโดยทันที และช่วยเหลือในการสนองตอบต่อเหตุการณ์เหล่านั้น

ฝ่ายบริหารทรัพยากรบุคคล และหน่วยงานที่เกี่ยวข้อง :

1. เผยแพร่ให้ผู้ใช้งานทราบถึงนโยบายความมั่นคงปลอดภัยสารสนเทศ ของบริษัท
2. จัดเตรียมแนวทาง เพื่อให้มั่นใจว่าพนักงาน และลูกจ้างทุกคนตระหนักถึงนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ มาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ระเบียบปฏิบัติและข้อกำหนดต่าง ๆ รวมถึงกฎหมายลิขสิทธิ์ทางปัญญา และบทบัญญัติอื่น ๆ ที่ใช้บังคับอยู่ในปัจจุบัน

ฝ่ายกฎหมาย :

1. จัดเตรียมข้อแนะนำทางกฎหมายที่เกี่ยวข้องกับระเบียบวิธีการปฏิบัติของพนักงานในบริษัท

หน่วยงานภายนอก :

1. ลงนาม และปฏิบัติตามข้อตกลงไม่เปิดเผยความลับของบริษัท
2. ปฏิบัติตามนโยบาย ระเบียบ และข้อกำหนดที่เกี่ยวข้องกับด้านความปลอดภัยสารสนเทศ หรือข้อบังคับอื่นของบริษัท
3. รายงานเหตุการณ์ที่เกี่ยวข้องกับด้านความปลอดภัยสารสนเทศที่เกิดขึ้นทันที ให้แก่ เจ้าของโครงการ พร้อมทั้งช่วยเหลือในการสนองตอบต่อเหตุการณ์นั้น ๆ

มาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

1. มาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard)

1.1. ฝ่ายเทคโนโลยีสารสนเทศ สารสนเทศ ต้องดำเนินการทบทวนมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard) อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อบริษัทฯ

1.2. ฝ่ายเทคโนโลยีสารสนเทศ ต้องเผยแพร่ให้หน่วยงานภายในและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

2.1. โครงสร้างทางด้านความปลอดภัยสารสนเทศภายในของบริษัท

2.1.1. การกำหนดหน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศ

ผู้บริหารระดับสูงร่วมกับหน่วยงานที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทไว้อย่างชัดเจน

2.1.2. การแบ่งแยกหน้าที่

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจน เพื่อให้มั่นใจว่าจะไม่มีบุคคลใดบุคคลหนึ่งสามารถเข้าถึง แก้ไข และใช้ทรัพย์สินนั้นได้โดยไม่ได้รับอนุญาต หรือไม่สามารถตรวจพบได้

2.1.3. การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อหน่วยงานที่จำเป็นสำหรับติดต่อเมื่อเกิดเหตุฉุกเฉิน

2.1.4. การประสานงานกับกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อกลุ่มผู้เชี่ยวชาญและเพิ่มช่องทางการรับข่าวสารจากกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเพิ่มพูนความรู้และสามารถหาข้อมูลสารสนเทศเพิ่มเติมในเรื่องอันตรายหรือภัยคุกคามด้านความปลอดภัยสารสนเทศได้

2.1.5. การควบคุมความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ ที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก

2.2. การใช้งานอุปกรณ์พกพาและการปฏิบัติงานจากนอกบริษัท

2.2.1. การป้องกันอุปกรณ์พกพา

(1) ติดตั้ง Anti-Virus Software ซึ่งถูกกำหนดมาตรการให้มีการทำ Automatic Update กับผู้ผลิตเสมอ หรือมี Software ควบคุม จัดการป้องกันความไม่ปลอดภัย หรือมีวิธีการสามารถ Lock ป้องกัน ไม่ให้ติดตั้งโปรแกรมอื่น ๆ หรืออนุญาตให้เฉพาะโปรแกรมทำงานได้ เช่น Antivirus Software Mobile Device Management หรือการ Hardening

(2) กำหนดให้มีการลงทะเบียนอุปกรณ์พกพา หรือ นำเข้าระบบ (Enroll) เช่น ยี่ห้อ รุ่น ระบบปฏิบัติการ รหัสประจำเครื่อง (serial number) หรือหมายเลขอ้างอิงอุปกรณ์เครือข่าย (MAC address) การ Join Domain หรือติดตั้ง Agent เพื่อให้มีข้อมูลในระบบที่ใช้บริหารจัดการเป็นต้น ก่อนการใช้งาน รวมถึงจัดให้มีการทบทวนทะเบียนดังกล่าวตามรอบอายุการใช้งานที่กำหนด และเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าว มีความสอดคล้องเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(3) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) กรณีที่อุปกรณ์เคลื่อนที่สูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (lock screen) หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น

(4) กำหนดประเภทบริการการใช้งาน (application service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์เคลื่อนที่ และกำหนดมาตรการควบคุมการเข้าถึงบริการการใช้งานดังกล่าวโดยคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่น จำกัดให้เข้าถึงบริการการใช้งานบางประเภทหากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น

(5) จัดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์

(6) จัดให้มีการสื่อสารให้ผู้ใช้งานรับทราบ เพื่อสร้างความตระหนักและทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงดังกล่าว

(7) ควบคุมให้มีการติดตั้งเฉพาะซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (patches) ที่เหมาะสม และกำหนดมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (malware)

(8) ทั้งนี้ เพื่อป้องกันการบุกรุกหรือก่อให้เกิดความเสียหายต่อข้อมูลที่เป็นความลับและมีความสำคัญที่จัดเก็บในอุปกรณ์เคลื่อนที่จัดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ เช่น ตัดการเชื่อมต่อโดยทันทีที่ทราบเหตุ เป็นต้น

(9) ทั้งนี้ หากอุปกรณ์เคลื่อนที่เป็นทรัพย์สินของพนักงาน จะใช้งานได้เฉพาะระบบและวิธีการเข้าถึงที่บริษัทฯ จัดให้ไว้เท่านั้น เช่น การเข้าถึง e-mail หรือ web site หรือการเข้าปฏิบัติงานจากภายนอกบริษัท

2.2.2. การปฏิบัติงานจากภายนอกบริษัท (Teleworking)

(1) ผู้ใช้งานที่มีการทำงานจากภายนอกทั้งหมดจะต้องปฏิบัติตามนโยบายการใช้งานด้านความปลอดภัยสารสนเทศของบริษัทเช่นเดียวกันกับการทำงานภายในบริษัท

(2) ผู้ใช้งานที่มีการใช้ข้อมูลสารสนเทศของบริษัทในการทำงานนอกสถานที่ หรือการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากเจ้าของข้อมูลสารสนเทศ และหน่วยงานต้นสังกัด โดยมีเหตุผลทางธุรกิจอันควร

(3) ผู้ใช้งานที่ต้องจะเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากผู้ดูแลระบบเทคโนโลยีสารสนเทศ และจะต้องมีการพิสูจน์ตัวตน โดยใช้ระบบ Virtual Private Network (VPN) หรือระบบ Remote Desktop ก่อนเข้าสู่ระบบโครงข่ายสารสนเทศภายใน

2.3. การใช้บริการ Cloud Computing

2.3.1. การใช้บริการ Cloud Computing กับระบบสารสนเทศที่มีความสำคัญ ฝ่ายเทคโนโลยีสารสนเทศสารสนเทศ และหน่วยงานที่ใช้บริการ ต้องจัดให้มีการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศการใช้งานดังต่อไปนี้

(1) ประเมินความเสี่ยงเกี่ยวกับการใช้บริการ และกำหนดประเภทงานที่จะใช้บริการ Cloud Computing

(2) กำหนดรูปแบบของการใช้บริการ เช่น Software as a service (SAAS), Platform as a service (PAAS) และ Infrastructure as a service (IAAS)

(3) กำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ (Due Diligence) โดยควรให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (Availability)

(4) กำหนดแนวทางการควบคุมความปลอดภัยของข้อมูลแต่ละประเภทที่จะใช้ใน Cloud Computing โดยแบ่งชั้นความลับของข้อมูลและกำหนดวิธีปฏิบัติแต่ละระดับชั้นความลับของข้อมูล

(5) กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภทเพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

(6) กำหนดให้มีการตรวจสอบบันทึกหลักฐานต่างๆ และติดตามปัญหาที่อาจส่งผลต่อการใช้บริการ

(7) จัดให้มีการเผยแพร่นโยบายการบริหารจัดการเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสื่อสารให้พนักงานที่เกี่ยวข้องรับทราบ เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ Cloud Computing

2.3.2. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ใช้บริการ ต้องกำหนดข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ โดยครอบคลุมเนื้อหา ดังนี้

(1) กำหนดให้บริษัทฯ ถือเป็นเจ้าของข้อมูลสารสนเทศ

(2) กำหนดประเภทบริการที่จะใช้ Cloud Computing

(3) กำหนดมาตรฐานความปลอดภัยด้านเครือข่าย เช่น การเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีในลักษณะ DDOS (Distributed Denial Of Service) การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี การป้องกันภัยคุกคามในรูปแบบใหม่ (Advanced Persistent Threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอพพลิเคชั่น (Application) การป้องกันการบุกรุกแบบลำดับชั้น (Defense-in-Depth) และการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ (Hardening) เป็นต้น

(4) ระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพ และสภาพโดยรวมของระบบอย่างชัดเจน

(5) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล การรับเรื่องแก้ไขปัญหา ขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อ ระดับการให้บริการ (Service Level Agreement) ระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (Recovery Time Objectives : RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective : RPO) อย่างชัดเจน

(6) กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามที่กำหนดในข้อตกลง

(7) ระบุรายละเอียดที่เกี่ยวข้องกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการไว้ในเอกสารสัญญาหรือข้อตกลงการให้บริการ

(8) ไม่อนุญาตให้ผู้ให้บริการมีสิทธิเข้าถึงและเปิดเผยข้อมูลของของบริษัทฯ เว้นแต่จะแจ้งและได้รับความยินยอมจากบริษัทฯ หรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล (Cloud Server Hosting Country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (Origin Country)

(9) กำหนดให้ผู้ให้บริการปรับปรุงการปฏิบัติงานให้เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากลฉบับปัจจุบันโดยไม่ชักช้า หากมาตรฐานดังกล่าวได้ถูกปรับปรุงให้เป็นปัจจุบัน

(10) กำหนดให้ผู้ให้บริการต้องได้รับการตรวจสอบขั้นตอนการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง จากผู้ตรวจสอบอิสระ

(11) กำหนดข้อตกลงที่ผู้ให้บริการต้องปฏิบัติเมื่อสิ้นสุดการให้บริการ เช่น กำหนดระยะเวลารักษาข้อมูลและวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้

(12) จัดให้มีข้อกำหนดในกรณีที่มีการใช้บริการ Cloud Computing ต่อจากผู้ให้บริการรายอื่น (Subcontract) โดยอย่างน้อยควรมีเงื่อนไขกำหนดให้บริการดังกล่าวเป็นส่วนหนึ่งของผู้ให้บริการ และผู้ให้บริการควรรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการกระทำหรือการดำเนินการใด ๆ ของผู้ให้บริการรายอื่น

2.3.3. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ใช้บริการ ต้องติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ ดังนี้

(1) ติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่างๆ หรือข้อตกลงในการให้บริการ

(2) ประเมินความเพียงพอของระบบงานของผู้ให้บริการ (Capacity Planning) อย่างสม่ำเสมอ

(3) ทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท

(4) ทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น เพื่อให้มั่นใจว่าผู้ให้บริการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการของบริษัทฯ อย่างต่อเนื่อง

2.4. การใช้งานระบบคลาวด์สาธารณะ (Public cloud)

2.4.1. ผู้ใช้งานต้องไม่นำข้อมูลที่เป็นข้อมูลสำคัญของบริษัทไปจัดเก็บหรือเผยแพร่ผ่านระบบคลาวด์ สาธารณะ

2.4.2. ต้องดำเนินการขออนุมัติจากผู้บังคับบัญชา หากมีความจำเป็นต้องใช้งานระบบคลาวด์สาธารณะเพื่อเผยแพร่ข้อมูลของบริษัทเป็นเป็นข้อมูลทั่วไป

2.4.3. ผู้ใช้งาน ต้องพิจารณาข้อตกลงหรือสัญญาการให้บริการระบบคลาวด์สาธารณะ โดยข้อตกลงหรือสัญญาการให้บริการดังกล่าว ต้องไม่ขัดต่อนโยบายความมั่นคงปลอดภภัยสารสนเทศของบริษัทฯ

2.4.4. รหัสผ่านที่ใช้ในการยืนยันตัวตนการเข้าถึงระบบคลาวด์สาธารณะ จะต้องมีความปลอดภัยเทียบเท่าหรือดีกว่านโยบายความมั่นคงปลอดภภัยสารสนเทศของบริษัทฯ

2.4.5. ผู้ใช้งาน ต้องเก็บรักษาข้อมูลที่ใช้ในการระบุและยืนยันตัวตนการเข้าถึงระบบคลาวด์สาธารณะ และไม่เปิดเผยให้ผู้อื่นได้รับทราบ

2.4.6. ต้องกำหนดสิทธิการเข้าถึงระบบคลาวด์สาธารณะอย่างเหมาะสมตามหน้าที่และความรับผิดชอบ และต้องมีการทบทวนสิทธิอย่างสม่ำเสมอ

3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

3.1. ก่อนการจ้าง

3.1.1. การตรวจสอบประวัติ

ผู้สมัครงาน และหน่วยงานภายนอกที่ได้รับการคัดเลือก ควรได้รับการตรวจสอบ ประวัติที่เพียงพอ โดยเฉพาะอย่างยิ่งในขอบเขตงานที่อาจก่อให้เกิดความอ่อนไหวต่อความเสียหายกับบริษัท

3.1.2. เงื่อนไขในการจ้างงาน

(1) หน่วยงานทรัพยากรบุคคล ต้องกำกับให้มีการลงนามในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ซึ่งได้มีการระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญาหรือข้อตกลงไว้ผู้ใช้งานต้องรับทราบ และยอมรับระเบียบปฏิบัติของทางบริษัท โดยจะต้องอ่านทำความเข้าใจและปฏิบัติตามนโยบาย กฎ ระเบียบที่บริษัทได้กำหนดไว้

(2) ผู้ใช้งาน ต้องลงนามรับทราบหน้าที่และความรับผิดชอบในหนังสือยอมรับนโยบายการใช้งานด้านความปลอดภัยสารสนเทศ

3.2. ระหว่างการจ้างงาน

3.2.1. หน้าที่ในการบริหารจัดการด้านความปลอดภัยสารสนเทศ

ทุกหน่วยงาน ต้องควบคุม และกำกับให้บุคลากรหรือหน่วยงานภายนอกที่ได้ว่าจ้างเพื่อปฏิบัติงานหรือให้บริการกับบริษัทปฏิบัติงานตามนโยบาย ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่บริษัทได้ประกาศใช้

3.2.2. การสร้างความตระหนัก การให้ความรู้

หน่วยงานทรัพยากรบุคคล และฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมกำกับให้พนักงานทุกคนได้รับข้อมูลข่าวสาร และการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความปลอดภัยสารสนเทศอย่างสม่ำเสมอ โดยเนื้อหาต้องครอบคลุมถึงนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความ ปลอดภัยสารสนเทศ ตามลักษณะงานที่รับผิดชอบ

3.2.3. กระบวนการลงโทษทางวินัย

บริษัทต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษผู้ใช้งานที่ฝ่าฝืนหรือละเมิดนโยบาย หรือขั้นตอนการปฏิบัติงานด้านความปลอดภัยสารสนเทศของบริษัท

3.3. การสิ้นสุดหรือการปรับเปลี่ยนตำแหน่งงาน

3.3.1. ความรับผิดชอบเมื่อสิ้นสุดการจ้างงาน

หน่วยงานทรัพยากรบุคคล ต้องกำหนดความรับผิดชอบที่เกี่ยวข้องกับการรักษาความปลอดภัยสารสนเทศของพนักงานหรือหน่วยงานภายนอกภายหลังจากที่บริษัทยกเลิก การจ้าง หรือหมดสัญญาจ้าง

4. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

4.1. หน้าที่ความรับผิดชอบต่อทรัพย์สิน

4.1.1. การจัดทำบัญชีทรัพย์สิน

เจ้าของทรัพย์สิน ต้องจัดเตรียม และปรับปรุงรายการ ทรัพย์สิน ที่ใช้เพื่อธุรกิจของบริษัทอย่างสม่ำเสมอ

4.1.2. การระบุผู้เป็นเจ้าของทรัพย์สิน

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดบุคลากรผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม

4.1.3. การยอมรับการใช้งานทรัพย์สิน

(1) หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกฎ ระเบียบ หรือหลักเกณฑ์ที่เหมาะสมในการใช้งานทรัพย์สินสารสนเทศอย่างเป็นลายลักษณ์อักษร

(2) ผู้ใช้งานทรัพย์สิน จะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ อย่างเคร่งครัด

4.1.4. การคืนทรัพย์สิน

(1) หน่วยงานทรัพยากรบุคคล และหน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ มีหน้าที่กำกับ ติดตามให้พนักงาน หน่วยงานหรือบุคคลภายนอกภายใต้สัญญาจ้าง ที่ได้พ้นสภาพการจ้างงานส่งคืนทรัพย์สินของบริษัทที่อยู่ในความครอบครองเมื่อพ้นสภาพการจ้างงาน

(2) เมื่อใดก็ตามที่พนักงาน หน่วยงานหรือบุคคลภายนอกภายใต้สัญญาจ้างได้พ้นสภาพการจ้างงานจะต้องดำเนินการส่งคืนทรัพย์สิน อาทิ เครื่องคอมพิวเตอร์พกพา เอกสาร กุญแจ บัตรพนักงาน ที่เป็นทรัพย์สินของบริษัทให้กับฝ่ายที่เกี่ยวข้อง

4.2. การจัดหมวดหมู่ข้อมูลสารสนเทศ

4.2.1. แนวทางการจัดหมวดหมู่ข้อมูลสารสนเทศ

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีกระบวนการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นลับที่เหมาะสม โดยบริษัทเป็นผู้มีสิทธิตามกฎหมายในความเป็นเจ้าของข้อมูล

สารสนเทศเหล่านั้น ไม่ว่าจะเป็นเนื้อหาข้อมูลสารสนเทศ หรือระหว่างการรับส่ง ซึ่งบริษัทสงวนสิทธิในการเข้าถึงข้อมูลสารสนเทศดังกล่าวโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

4.2.2. การจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศ

(1) เจ้าของทรัพย์สิน ต้องกำหนดให้มีการแสดงลำดับชั้นความปลอดภัยของข้อมูลสารสนเทศทุกระดับมีวิธีการบริหารจัดการที่เหมาะสม และต้องมีขั้นตอนปฏิบัติในการทบทวนข้อมูลสารสนเทศ

(2) หากระบบสารสนเทศประกอบไปด้วยข้อมูลสารสนเทศซึ่งมีการกำหนดระดับชั้นความลับที่แตกต่างกัน มาตรการที่ใช้ควบคุม ต้องครอบคลุมข้อมูลสารสนเทศที่มีระดับชั้นความลับสูงที่สุดบนระบบนั้น

4.2.3. ขั้นตอนการปฏิบัติสำหรับการจัดการทรัพย์สินสารสนเทศ

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการจัดการและจัดการทรัพย์สินสารสนเทศ เพื่อมิให้ข้อมูลสำคัญของบริษัทรั่วไหลหรือทรัพย์สินสารสนเทศถูกนำไปใช้ผิดประเภท

4.3. การจัดการกับสื่อบันทึกข้อมูลสารสนเทศ

4.3.1. การบริหารจัดการสื่อบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้ (Removable media)

4.3.2. การทำลายสื่อบันทึกข้อมูลสารสนเทศ

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการทำลายสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้ (Removable media) โดยการทำลายต้องเป็นไปอย่างมั่นคงปลอดภัย

5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

5.1. ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ

5.1.1. นโยบายควบคุมการเข้าถึง

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการกำหนดนโยบายและขั้นตอนปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

5.1.2. นโยบายการใช้งานบริการเครือข่าย

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้ เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตให้เข้าถึงเท่านั้น โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

5.2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน

5.2.1. การลงทะเบียนผู้ใช้งาน

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนการลงทะเบียนผู้ใช้งานอย่างเป็นลายลักษณ์อักษร เช่น ผ่านระบบให้บริการ หรือ e-mail ผ่านผู้บังคับบัญชา

5.2.2. การบริหารจัดการสิทธิการใช้งานของผู้ใช้งาน

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการบริหารจัดการบัญชีชื่อผู้ใช้งาน (User Name) ดังนี้

(1) บัญชีชื่อผู้ใช้งาน (User Name) ซึ่งใช้งานบนระบบสารสนเทศของบริษัทตลอดจนเครือข่ายของบริษัทจะต้องถูกสร้างตามมาตรฐานการสร้างบัญชีชื่อผู้ใช้งาน และจะต้องกำหนดหน้าที่หรือสิทธิให้ชัดเจนในแต่ละบุคคล โดยไม่แสดงชื่อหรือรายละเอียดของระบบจนกว่าจะ login สำเร็จ

(2) สำหรับบัญชีชื่อผู้ใช้งานที่สร้างขึ้นสำหรับบุคคลภายนอก เพื่อปฏิบัติงานกับบริษัท จะต้องมีการกำหนดวันหมดอายุ หรือเปิดสิทธิ์เมื่อจำเป็นต้องใช้ทำงาน และปิดสิทธิ์เมื่อสิ้นสุดการทำงาน

(3) สิทธิการเข้าถึงของระบบสารสนเทศของบริษัทจะต้องยกเลิกเมื่อผู้ใช้งานสิ้นสุดการปฏิบัติงานที่เกี่ยวข้องกับสารสนเทศของบริษัท

5.2.3. การบริหารจัดการสิทธิการใช้งานระบบ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดให้มีการควบคุมผู้ใช้งาน ให้ได้รับสิทธิการเข้าถึงระบบสารสนเทศ และระบบการสื่อสารของบริษัทเท่าที่จำเป็นเพียงพอต่อการปฏิบัติงาน โดยบัญชีชื่อผู้ใช้งาน สิทธิในการเข้าใช้งานระบบสารสนเทศ และสิทธิในการเข้าถึงระบบอื่น ที่นอกเหนือจากที่ให้กับผู้ใช้งานทั่วไปจะต้องได้รับการยินยอมจากผู้บังคับบัญชาของ ผู้ใช้งาน และเจ้าของทรัพย์สินนั้น

5.2.4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดให้มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นลายลักษณ์อักษร เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย และผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม โดยมีแนวทางดังนี้

(1) รหัสผ่านจะต้องไม่ถูกฝังไว้ในระบบที่ถูกพัฒนาขึ้น (Hard-Coded)

(2) หากระบบสารสนเทศซึ่งมีผู้ใช้งานจำนวนมาก มีการใช้งานรหัสผ่านแบบตายตัว (Fixed Password) เป็นกลไกควบคุมการเข้าถึงระบบเป็นหลัก รหัสผ่านทั้งหมดบนระบบ จะต้อง

ถูกเปลี่ยนทันทีถ้าพบหลักฐานว่าระบบถูกคุกคาม รวมถึงผู้ใช้งานทั้งหมดจะต้อง เปลี่ยนรหัสผ่านบนเครื่องอื่นถ้ารหัสผ่านนั้นมีการใช้งานบนเครื่องอื่นด้วย

(3) ถ้าบัญชีชื่อผู้ใช้งานที่มีสิทธิ ถูกคุกคามโดยผู้บุกรุกหรือผู้ใช้งานอื่นซึ่งไม่มีสิทธิ รหัสผ่านทั้งหมดบนระบบนั้นจะต้องถูกเปลี่ยนในทันที

(4) ผู้ใช้งานจะต้องถูกพิสูจน์ตัวตนก่อนจะได้รับรหัสผ่านใหม่หรือเปลี่ยนรหัสผ่าน

(5) ผู้ใช้งานจะต้องพิสูจน์ตัวตนที่แน่ชัดก่อนที่จะเริ่มใช้งานระบบสารสนเทศหลักหรือทรัพยากรด้านระบบการสื่อสาร

(6) หลังจากระบบได้ถูกติดตั้งเสร็จเรียบร้อยแล้ว ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องยกเลิกบัญชีผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของทุกบัญชีชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

5.2.5. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีกระบวนการทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งานตามรอบระยะเวลาที่กำหนด โดยดำเนินการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อได้รับแจ้งการเปลี่ยนแปลงสถานภาพพนักงาน (พ้นสภาพ/โยกย้าย) ในระบบที่สำคัญ

5.2.6. การถอดถอนสิทธิการเข้าถึง

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ มีหน้าที่กำกับ ติดตามให้มีการถอดถอนสิทธิทั้งหมดที่ใช้ในการเข้าถึงทรัพย์สินของบริษัทของพนักงาน หน่วยงานหรือบุคคลภายนอกภายใต้สัญญาจ้าง ที่บริษัทได้ยุติหรือสิ้นสุดการจ้างงาน

5.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน

5.3.1. การใช้งานรหัสผ่าน

บริษัทกำหนดให้ผู้ใช้งาน ใช้งานรหัสผ่านอย่างมั่นคงปลอดภัย โดยมีแนวทางดังนี้

(1) ผู้ใช้งานทั้งหมดจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการเดา อาทิ ศัพท์ในพจนานุกรม คัดลอกหรือผสมจากชื่อผู้ใช้ อักขระเรียงลำดับ ข้อมูลส่วนบุคคล หรือประโยควลี

(2) ผู้ใช้งานจะต้องไม่เขียนหรือบันทึกรหัสผ่านที่ใช้ และเก็บหรือแสดงให้เห็นไว้ใกล้กับ ระบบหรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น

(3) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใด ๆ โดยใช้บัญชีผู้ใช้งานของตน หรือกระทำการใด ๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ

(4) ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการใช้รหัสผ่านอื่น ๆ ที่บริษัทกำหนด

5.4. การควบคุมการเข้าถึงโปรแกรมประยุกต์และข้อมูลสารสนเทศ

5.4.1. การจำกัดการเข้าถึงข้อมูลสารสนเทศ

ผู้ควบคุมดูแลระบบสารสนเทศ ต้องกำหนดสิทธิของผู้ใช้งานในการเข้าใช้ข้อมูล สารสนเทศ ในโปรแกรมประยุกต์ให้อยู่ในระดับน้อยที่สุดตามความจำเป็นในการใช้งาน

5.4.2. กระบวนการปฏิบัติในการเข้าใช้งานระบบ (log on/sign on) อย่างปลอดภัย

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีกระบวนการปฏิบัติในการเข้าใช้งานระบบ โดยมีแนวทางดังนี้

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดการไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์ เพื่อป้องกันผู้บุกรุกในการนำข้อมูลดังกล่าวไปใช้ประโยชน์ในการลักลอบเชื่อมต่อเข้าสู่ระบบของบริษัท

(2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดการให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทางและระบบ ควรมีการจำกัดเวลาหรือจำกัดจำนวนครั้ง สำหรับใช้ในการป้อนรหัสผ่าน เพื่อป้องกัน การบุกรุกจากผู้บุกรุก

(3) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดการให้ระบบแสดงข้อความเตือนถึงการอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าใช้งาน ก่อนที่จะทำการเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ของบริษัท และระบบต้องเปิดโอกาสให้ผู้ใช้สามารถยกเลิกการเชื่อมต่อเข้าสู่ระบบในกรณีที่ทราบว่าระบบนั้น ๆ ไม่ได้เกี่ยวข้องกับตนเอง

(4) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการตัดการใช้งาน ได้แก่ การล็อคหน้าจอ เมื่อไม่มีการใช้งานมาระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ และต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูงตามความเหมาะสมในการใช้งาน โดยระบบงานที่มีความสำคัญ ผู้พัฒนาระบบจะต้องพัฒนาระบบงานให้มีการตัดการเชื่อมต่อทางเครือข่ายเมื่อผู้ใช้งานไม่ได้ใช้งานมาเกินกว่าระยะเวลาหนึ่ง (Session Timeout) เช่น 15 นาที

5.4.3. ระบบบริหารจัดการรหัสผ่าน

ผู้ควบคุมดูแลระบบสารสนเทศควรจัดให้มีระบบการจัดการรหัสผ่านสำหรับระบบต่าง ๆ ภายในบริษัทตามมาตรฐานระบบการจัดการรหัสผ่าน โดยระบบควรมีความสามารถในการรองรับการบริหารจัดการรหัสผ่าน ดังนี้

(1) การตั้งบัญชีผู้ใช้งานของแต่ละบุคคล

(2) การกำหนดรหัสผ่านที่มีความซับซ้อน

(3) การเปลี่ยนรหัสผ่านตามรอบที่กำหนด

(4) ไม่อนุญาตให้ใช้รหัสผ่านซ้ำตามจำนวนครั้งที่กำหนด

(5) ตัดการเชื่อมต่อหากตรวจสอบพบว่ามีการยืนยันตัวตนไม่ถูกต้องติดต่อกัน 10 ครั้ง

(6) ไม่แสดงรหัสผ่านจริงบนหน้าจอในขณะที่มีการเข้าสู่ระบบ

(7) รับส่ง และเก็บรหัสผ่านแยกจากข้อมูลอื่นในรูปแบบที่ปลอดภัย เช่น การเข้ารหัส หรือ Hash เป็นต้น

5.4.4. การใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบ (System Utilities)

ผู้ควบคุมดูแลระบบสารสนเทศ ต้องควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการหลีกเลี่ยงมาตรการป้องกันทางด้านความปลอดภัยของระบบ

5.4.5. การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ

กำหนดให้มีแนวทางการควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ ดังต่อนี้

(1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องแต่งตั้งเจ้าหน้าที่ผู้ดูแล Program Source Libraries

(2) เจ้าหน้าที่ผู้ดูแล Program Source Libraries ต้องจำกัดสิทธิในการเข้าถึง Program Source Libraries ที่เก็บซอร์สโค้ดของ โปรแกรม (Program Source Code)

(3) การปรับปรุงซอร์สโค้ดของโปรแกรมใน Program Source Libraries และการนำซอร์สโค้ดของโปรแกรมให้กับผู้พัฒนาระบบจะต้องดำเนินการโดยเจ้าหน้าที่ผู้ที่ได้รับมอบหมายในแต่ละระบบ

(4) ในกรณีที่ต้องมีการจัดเก็บโปรแกรมเวอร์ชั่นเก่า เจ้าหน้าที่ผู้ดูแล Program Source Libraries ควรบันทึกรายละเอียดที่ชัดเจน ได้แก่ วันเดือนปีที่โปรแกรมเวอร์ชั่นนี้ได้ยกเลิกการใช้งาน

(5) การปรับปรุงเปลี่ยนแปลง Program Source Code จะต้องปฏิบัติตามขั้นตอนปฏิบัติควบคุมการเปลี่ยนแปลง

6. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

6.1 นโยบายการใช้งานการเข้ารหัสข้อมูล

(1) หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล โดยเมื่อใดก็ตามที่ผู้ปฏิบัติงานทำการเข้ารหัสข้อมูลลับของบริษัท ผู้ปฏิบัติงานจะต้องใช้ วิธีการเข้ารหัสข้อมูลที่เป็นมาตรฐาน และได้รับการอนุมัติจากบริษัทเท่านั้น

(2) มีการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่ายกับเครื่อง Server สำหรับระบบงานที่มีข้อมูลที่มีความสำคัญสูง เช่น ใช้โพรโตคอล https

6.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล

ผู้ดูแลระบบเทคโนโลยีสารสนเทศแต่ละระบบ เป็นผู้จัดการกุญแจรหัสในระบบของตน โดยให้ใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานของบริษัท

7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

7.1. พื้นที่ความปลอดภัย

7.1.1. ความปลอดภัยทางกายภาพบริเวณล้อมรอบ

บริษัทจะต้องพิจารณา และจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัยโดยจะประกอบด้วยพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทาง เข้า-ออกหลัก และระบบรักษาความปลอดภัยอย่างเหมาะสม

7.1.2. การควบคุมการเข้าออก

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้การเข้าถึงพื้นที่ที่ต้องการรักษาความปลอดภัย เช่น พื้นที่ศูนย์คอมพิวเตอร์ และพื้นที่ปฏิบัติงานซึ่งมีข้อมูลสำคัญ สามารถเข้าถึงได้เฉพาะพนักงานผู้ได้รับอนุญาตเท่านั้น และรายชื่อผู้ได้รับอนุญาต จะต้องได้รับการตรวจสอบ ปรับปรุง ดูแลให้เหมาะสมอย่างสม่ำเสมอ

(2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ที่ต้องการรักษาความปลอดภัย (Secure area) ได้แก่ ศูนย์คอมพิวเตอร์ และห้องปฏิบัติงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ และบันทึกการเข้าออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

7.1.3. การรักษาความปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่น ๆ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่ห้องปฏิบัติงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ หรืออุปกรณ์สารสนเทศต่าง ๆ ที่ใช้ในการปฏิบัติงาน

7.1.4. การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยคุกคามจากภายนอก ทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

7.1.5. การปฏิบัติงานภายในพื้นที่ที่ต้องรักษาความปลอดภัย

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำกับให้มีการกำหนดแนวปฏิบัติของการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ที่ต้องการรักษาความปลอดภัยด้านกายภาพ (Secure area) ได้แก่ ศูนย์คอมพิวเตอร์ และห้องปฏิบัติงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ และกำหนดให้มีการนำแนวปฏิบัติไปใช้งาน

7.1.6. การจัดบริเวณพื้นที่รับส่งของ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ โดยต้องกำหนดพื้นที่การส่งมอบสินค้า และพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าศูนย์คอมพิวเตอร์ แยกเป็นสัดส่วนที่ชัดเจน เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

7.2. ความมั่นคงปลอดภัยสำหรับอุปกรณ์

7.2.1. การจัดวางและการป้องกันอุปกรณ์

อุปกรณ์สารสนเทศจะต้องถูกวางไว้ในห้องหรือบริเวณที่ปลอดภัย อุปกรณ์ที่มีตู้ประตูของตู้วางคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารเครือข่ายจะต้องล็อคตลอดเวลา มีเพียงเจ้าหน้าที่เทคนิคที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการเปิด เพื่อซ่อม บำรุง หรือการปรับปรุง ค่าคอนฟิกกูเรชัน (Reconfiguration) เพื่อลดความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

7.2.2. ระบบและอุปกรณ์สนับสนุนการทำงาน

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้มีการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ ได้แก่ อุปกรณ์ดับเพลิง อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิและความชื้น ระบบเตือนภัยน้ำรั่ว หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น

7.2.3. ความปลอดภัยในการเดินสายสัญญาณสื่อสาร

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้การติดตั้งและการบำรุงรักษาสายไฟฟ้าและสายสื่อสาร เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรม เพื่อป้องกันไม่ให้มีการเข้าถึงหรือดักจับข้อมูล หรือเกิดความเสียหายทางด้านกายภาพ

7.2.4. การบำรุงรักษาอุปกรณ์

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้อุปกรณ์ระบบสารสนเทศหลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ จะต้องได้รับการบำรุงดูแลรักษาตามช่วงเวลา และตามข้อกำหนดที่ผู้ผลิตแนะนำไว้สำหรับการซ่อมบำรุง เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

7.2.5. การนำทรัพย์สินออกนอกบริษัท

(1) ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ ต้องไม่อนุญาตให้นำอุปกรณ์สารสนเทศออกจากบริษัท ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

(2) ผู้ใช้งานต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากบริษัทยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

7.2.6. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน

ต้องมีการดำเนินการให้ผู้มีอำนาจอนุมัติให้นำอุปกรณ์สารสนเทศของบริษัทไปใช้งานภายนอกบริษัท และต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่าง ๆ ที่ใช้งานอยู่ภายนอกบริษัทเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

7.2.7. การกำจัดอุปกรณ์และการนำกลับมาใช้ใหม่

(1) พนักงานจะต้องทำการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลสารสนเทศที่สำคัญ หรือซอฟต์แวร์ลิขสิทธิ์ว่ามีการลบ ย้าย หรือทำลายอย่างเหมาะสมตามระดับชั้นความลับ ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์ หรือนำอุปกรณ์กลับมาใช้ใหม่

(2) เจ้าของข้อมูลสารสนเทศ มีหน้าที่ในการทำลายข้อมูลสารสนเทศที่ไม่จำเป็นต่อกิจการของบริษัทที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลที่สามารถนำกลับมาใช้ใหม่ได้ ซึ่งต้องเป็นไปตามกระบวนการขั้นตอนที่ได้กำหนด

7.2.8. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล

ผู้ใช้งานจะต้องไม่ออกห่างจากเครื่องคอมพิวเตอร์ โดยไม่มีการออกจากระบบ (Log out/Sign off) หรือทำการล็อคหน้าจอ หากไม่มีความจำเป็นต้องใช้ให้ต้องปิดเครื่อง (Turn off) เสมอ

7.2.9. นโยบายการควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ไม่ปลอดภัย (Clear desk and clear screen policy)

ผู้ใช้งาน ต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ

8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

8.1. การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน

8.1.1. ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการจัดทำเอกสารพร้อมด้วยขั้นตอนปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญ รวมทั้งดำเนินการทบทวนและปรับปรุงขั้นตอนหรือวิธีการปฏิบัติงานให้เป็นปัจจุบันอยู่เสมอ เพื่อให้บุคลากรสามารถนำไปปฏิบัติได้

8.1.2. การบริหารการเปลี่ยนแปลง

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ เพื่อควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใด ๆ ซึ่งส่งผลต่อระบบประมวลผลข้อมูลสารสนเทศ

8.1.3. การบริหารจัดการความต้องการทรัพยากรสารสนเทศ (Capacity Management)

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมีประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งานในอนาคต

8.1.4. การแยกระบบสำหรับการพัฒนา การทดสอบและระบบปฏิบัติการจริง (Production)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการแยกระบบแอพพลิเคชันที่สำคัญของบริษัทซึ่งอยู่ในระหว่างการพัฒนาและการทดสอบออกจากระบบปฏิบัติการจริง มีการควบคุมการเข้าถึงอย่างเข้มงวด

8.2. การป้องกันซอฟต์แวร์ไม่ประสงค์ดี (Malicious Software)

8.2.1. การป้องกันซอฟต์แวร์ไม่ประสงค์ดี

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้อง ให้กับผู้ใช้งานอย่างเหมาะสม

8.3. การสำรองข้อมูลสารสนเทศ

8.3.1. การสำรองข้อมูลสารสนเทศ

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องดำเนินการสำรองข้อมูลในลักษณะรายวัน หรือรายสัปดาห์ตามที่บริษัทกำหนด เพื่อป้องกันการสูญหายของข้อมูล

(2) เจ้าของข้อมูลสารสนเทศ ต้องดำเนินการ หรือกำหนดให้มีการสำรองข้อมูลสารสนเทศและการทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ

8.4. การบันทึกเหตุการณ์ (Event Logging)

8.4.1. การตรวจสอบบันทึกเหตุการณ์

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวข้องกับความปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ เช่น ข้อมูลที่มีการแก้ไขเพื่อที่จะได้ตรวจสอบได้ในภายหลัง (Audit Log) เป็นต้น

(2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ จะต้องเฝ้าติดตาม (Monitoring) การใช้งานระบบสารสนเทศ โดยผลของการเฝ้าติดตามจะต้องถูกสอบทานอย่างสม่ำเสมอ เพื่อตรวจหาความผิดปกติ

(3) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการบันทึกเหตุการณ์ความผิดพลาด (Fault Logging) ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ รวมถึงวิเคราะห์ ดำเนินการแก้ไข ตลอดจน วางแนวทางป้องกันการเกิดปัญหา ซ้ำอีกในอนาคต

8.4.2. การป้องกันข้อมูลบันทึกเหตุการณ์ (Log)

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับไม่ให้บันทึกเหตุการณ์ (Log) ของระบบและโปรแกรมทั้งหมด ถูกแก้ไขหรือเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

8.4.3. การปรับเวลาให้ตรงกัน

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของบริษัทได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง

8.5. การสร้างความปลอดภัยสารสนเทศให้กับไฟล์ของระบบที่ให้บริการ

8.5.1. การควบคุมการติดตั้งโปรแกรมลงไปยังระบบที่ให้บริการ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติในการควบคุมการติดตั้งโปรแกรมลงไปยังระบบที่ให้บริการ

8.6. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

8.6.1. มาตรการควบคุมช่องโหว่ทางเทคนิค

(1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้ระบบสารสนเทศสำคัญของบริษัท ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้

(2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องดูแลและบำรุงรักษาระบบ เพื่อรักษาระดับความปลอดภัยสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ที่ตรวจสอบพบ และการปรับปรุงแก้ไขช่องโหว่ของระบบสารสนเทศ

8.6.2. การกำหนดและควบคุมการติดตั้งซอฟต์แวร์

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดและควบคุมให้ผู้ใช้งานติดตั้งเฉพาะซอฟต์แวร์ที่ได้รับอนุญาต และเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ที่มีหลักฐานแสดงสิทธิการใช้งาน

(2) ผู้ใช้งาน ต้องไม่นำซอฟต์แวร์ที่ไม่ได้รับอนุมัติให้ใช้งานมาติดตั้งบนเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของบริษัท

8.7. การตรวจประเมินระบบสารสนเทศ

8.7.1. มาตรการการตรวจประเมินระบบสารสนเทศ

หน่วยงานตรวจสอบภายในหรือผู้ตรวจสอบอิสระภายนอก จะต้องทำการตรวจสอบตามการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความปลอดภัยสารสนเทศ ตามแผนที่ที่ได้กำหนดไว้กับผู้ที่เกี่ยวข้อง เพื่อลดความเสี่ยงที่จะอาจทำให้ระบบหรือกระบวนการทางธุรกิจต้องหยุดชะงัก

9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

9.1. การบริหารความมั่นคงปลอดภัยเครือข่าย

9.1.1. การควบคุมเครือข่าย

แผนกโครงข่ายโทรคมนาคม ต้องจัดให้มีมาตรฐานการให้บริการเครือข่ายสื่อสาร เพื่อให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ ป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

9.1.2. ความปลอดภัยของการให้บริการด้านเครือข่าย

แผนกโครงข่ายโทรคมนาคม ต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมด ลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ไม่ว่าจะเป็นการให้บริการจากภายในหรือภายนอก

9.1.3. การแบ่งแยกเครือข่าย

แผนกโครงข่ายโทรคมนาคม ต้องแบ่งแยกเครือข่ายออกเป็นเครือข่ายย่อยตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่ายผลกระทบทางด้านความปลอดภัย และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น โดยมีการจัดทำการแบ่ง Zone (Network Segmentation) เพื่อให้มีระบบการป้องกัน ตามขอบ และภายใน Zone ต่าง ๆ ด้วยมาตรการที่เหมาะสม

9.2. การแลกเปลี่ยนข้อมูลสารสนเทศ

9.2.1. นโยบายและขั้นตอนการปฏิบัติในการแลกเปลี่ยนข้อมูลสารสนเทศ

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลสารสนเทศ

9.2.2. ข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศ โดยการแลกเปลี่ยนข้อมูลสารสนเทศภายในบริษัทกับหน่วยงานภายนอกนั้นจะต้องมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร ซึ่งกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลสารสนเทศอย่างเหมาะสม

9.2.3. ข้อความทางอิเล็กทรอนิกส์

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ EDI (Electronic Data Interchange) หรือ Instant messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

9.2.4. ข้อตกลงในการไม่เปิดเผยความลับ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้ผู้ที่เกี่ยวข้องกับระบบและข้อมูลสารสนเทศลงนามในข้อตกลงไม่เปิดเผยความลับ รวมถึงต้องควบคุมให้ผู้รับผิดชอบดำเนินการทบทวนเอกสารอย่างสม่ำเสมอ

10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

10.1. ข้อกำหนดด้านความปลอดภัยสารสนเทศ

10.1.1. การวิเคราะห์และการระบุข้อกำหนดทางด้านความปลอดภัยสารสนเทศ

(1) ผู้พัฒนาระบบ และผู้บังคับบัญชาของกลุ่มผู้ใช้งานจะต้องมีการกำหนดคุณลักษณะความต้องการด้านความปลอดภัยสารสนเทศให้ชัดเจน เมื่อต้องการพัฒนาระบบสารสนเทศใหม่ หรือปรับปรุงระบบ เช่น กรณีที่เป็น Web application ผู้พัฒนาจะต้องพัฒนาระบบให้สามารถป้องกันภัยคุกคามที่ได้ระบุไว้ใน OWASP Top 10 (The Open Web Application Security Project) เป็นต้น

(2) บริษัท จะต้องเลือกใช้ผลิตภัณฑ์รักษาด้านความปลอดภัยสารสนเทศที่ได้รับการทดสอบ อย่างเป็นทางการมากกว่าผลิตภัณฑ์ที่ไม่ได้รับการทดสอบ

(3) ผู้พัฒนาจะต้องมีการจัดทำ Prototype เพื่อแสดงกระบวนการทำงานสำหรับระบบงานที่สำคัญ

10.1.2. การควบคุมการให้บริการสารสนเทศผ่านเครือข่ายสาธารณะ

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลไม่ให้เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการพาณิชย์อิเล็กทรอนิกส์เก็บข้อมูลสารสนเทศทางธุรกิจที่สำคัญของบริษัทไว้

(2) ข้อมูลของผู้ใช้งานระบบ จะต้องได้รับการป้องกันอย่างเหมาะสมหากมีการเก็บข้อมูลเหล่านี้ไว้ในสารสนเทศซึ่งสามารถเข้าถึงได้ทางระบบเครือข่ายอินเทอร์เน็ต

(3) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการป้องกันความถูกต้องและสมบูรณ์ของสารสนเทศที่มีการเปิดเผยออกสู่สาธารณะ

10.1.3. ธุรกรรมออนไลน์

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญทั้งหมดซึ่งเกี่ยวข้องกับธุรกรรมออนไลน์ โดยข้อมูลสารสนเทศต้องได้รับการป้องกันอย่างเหมาะสมจากภัยคุกคามที่อาจเกิดขึ้นได้ อาทิ การส่งข้อมูลผิดเส้นทาง (Miss-Routing) ข้อมูลถูกเปิดเผยจากผู้ไม่ได้รับอนุญาต ข้อมูลถูกทำซ้ำ

10.2. ความปลอดภัยสารสนเทศในกระบวนการพัฒนาระบบและการสนับสนุน

10.2.1. ความมั่นคงปลอดภัยในกระบวนการพัฒนาและบำรุงรักษาระบบสารสนเทศ

หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดกฎระเบียบสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย ตลอดทั้งวงจรการพัฒนาระบบ

10.2.2. ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ

ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติควบคุม การเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร

10.2.3. การตรวจสอบแอพพลิเคชันหลังการเปลี่ยนแปลงระบบปฏิบัติการ

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบที่อาจเกิดขึ้นเมื่อต้องการที่จะเปลี่ยนแปลงหรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชั่นและการแก้ไข ข้อบกพร่องด้านความปลอดภัย เป็นต้น โดยจะต้องมีการทดสอบบนเครื่องทดสอบ (Test Environment) ได้แก่ การทำ User Acceptance Test (UAT) จนมั่นใจว่าระบบงานต่าง ๆ ที่ประมวลผลบนเครื่องดังกล่าวสามารถทำงานได้ตามปกติ จึงจะทำการเปลี่ยนแปลงหรือปรับปรุง บนเครื่อง สภาวการณ์ที่ใช้งานจริง (Production Environment)

(2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศจะต้องทำการตรวจสอบทางเทคนิคภายหลังการเปลี่ยนแปลงระบบปฏิบัติการบนระบบจริง เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่มีผลกระทบต่อการทำงานของระบบ

10.2.4. การจำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่มาจากผู้ผลิต

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่มาจากผู้ผลิต โดยมีแนวทางดังต่อไปนี้

(1) ซอฟต์แวร์สำเร็จรูปควรใช้งานโดยปราศจากการแก้ไข ถ้ามีความจำเป็นในการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูปต้องมีการพิจารณาการควบคุมต่าง ๆ อย่างเข้มงวด

(2) ดำเนินการเปลี่ยนแปลง ตามขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงของบริษัท

10.2.5. หลักการความมั่นคงปลอดภัยในการพัฒนาระบบ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบดังต่อไปนี้

(1) การให้สิทธิต่ำที่สุด (least privilege) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

(2) การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (need to know) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ

(3) การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (defense in-depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(4) การออกแบบในลักษณะเปิด (open design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (algorithm) ที่เป็นมาตรฐานและสามารถตรวจสอบการทำงานได้

(5) ระบบจะต้องมีการทำ Validate Input เพื่อป้องกันการโจมตีในรูปแบบต่าง ๆ ผ่านทางการรับ ข้อมูลจากผู้ใช้โดยมีรายละเอียดดังนี้

1. ระบบต้องปิด Tracing และ Debugging ของระบบก่อนส่ง Production
2. การตรวจสอบข้อมูลที่เข้าสู่ระบบ (Input Validation) ต้องทำการตรวจสอบข้อมูลที่เข้าสู่ระบบได้เฉพาะข้อมูลที่ถูกต้องตาม Format, Type, Length ที่ต้องการเท่านั้น
3. เมื่อโปรแกรมมีการทำงานผิดพลาดเกิดขึ้นจะต้องมีกระบวนการป้องกันและตรวจสอบ Error โดยระบบต้องไม่เปิดเผยข้อมูลการ Display Error Code ที่เครื่อง Client รวมถึงไม่แสดงข้อมูลที่สำคัญของระบบออกไป
4. ระบบต้องป้องกัน Cross Side Scripting (XSS)
5. เชื่อมต่อฐานข้อมูล ต้องเชื่อมต่อด้วยสิทธิ์ของเจ้าของฐานข้อมูลเท่านั้น
6. ระบบต้องป้องกันการทำ SQL Injection โดยตรวจสอบข้อมูลที่ป้อนเข้าทาง URL Header และ Input Form ที่ได้ออกแบบไว้
7. ระบบต้องเข้ารหัสข้อมูลที่เป็นความลับ เช่น Username, Password, Connection Strings ข้อมูลที่อยู่ในระดับ Confidential หรือ Secret

(6) ระบบจะต้องมีการออกแบบ และกำหนด Password policy สำหรับ Application เช่น

1. รองรับการตั้งรหัสผ่านเพื่อเข้าสู่ระบบสารสนเทศโดยมีความยาวของรหัสผ่านอย่างน้อย 8 ตัวอักษร
2. รูปแบบของรหัสผ่านต้องประกอบไปด้วยตัวอักษรและตัวเลขรวมถึงอักขระพิเศษ
3. การจัดเก็บรหัสผ่านควรเก็บในฐานข้อมูลและจะต้องมีการเข้ารหัสผ่านเพื่อมิให้ผู้อื่น ๆ สามารถเข้าใจรหัสผ่านได้
4. จะต้องระงับการใช้งานของผู้ใช้งานในระบบสารสนเทศ หากมีการป้อนรหัสผ่านผิดเกิน 10 ครั้ง
5. รองรับการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด
6. พัฒนาระบบการตรวจสอบตัวตน (Authorization) สามารถกำหนดให้ผู้ใช้งานแก้ไขรหัสผ่านโดยทันทีเมื่อมีการใช้งานในครั้งแรก พร้อมฟังก์ชันการแก้ไข รหัสผ่าน/การขอรหัสผ่าน เมื่อผู้ใช้งานลืม / การ Reset รหัสผ่าน สำหรับ Administrator
7. ต้อง Encrypt ชื่อผู้ใช้งาน/รหัสผ่าน ในช่วงการส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์และเครื่องแม่ข่าย
8. ต้องไม่เก็บข้อมูลสำคัญเช่น รหัสผ่านไว้ใน Log file เป็นต้น

(7) ผู้พัฒนาระบบจะต้องออกแบบรูปแบบของการ Authentication และ Authorization โดยการกำหนด Username และ Password ในการเข้าใช้ Application โดยแบ่งแยกหน้าที่และสิทธิของแต่ละ User อย่างชัดเจน

(8) ผู้พัฒนาระบบจะต้องพัฒนาระบบงานให้สอดคล้องกับมาตรฐานในการ Login เข้าสู่ระบบงานให้มีความปลอดภัยดังนี้

1. ไม่แสดงชื่อหรือรายละเอียดของระบบจนกว่าจะ login สำเร็จ
2. มีการบันทึกจัดเก็บการ login ทั้งที่สำเร็จและไม่สำเร็จ และแสดงประวัติการ login 3 ครั้งล่าสุด
3. เมื่อมีการใส่ข้อมูลชื่อผู้ใช้งานและรหัสผ่านไม่ถูกต้อง ให้แสดงข้อความรวมๆ เพียง “ข้อมูลการ Login ไม่ถูกต้อง”

(9) ผู้พัฒนาระบบจะต้องพัฒนาระบบงานให้มีการตัดการเชื่อมต่อหลังจากที่ทำการ Login ไม่สำเร็จเกินกว่า 10 ครั้ง

(10) ผู้พัฒนาระบบจะต้องพัฒนาระบบงานให้มีหน้าจอสำหรับผู้ดูแลระบบงานให้สามารถบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

(11) ผู้พัฒนาระบบจะต้องพัฒนาระบบงานให้มีการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่ายกับเครื่อง Server สำหรับระบบงานที่มีข้อมูลที่มีความสำคัญสูง เช่น โดยใช้โพรโตคอล https

(12) สำหรับระบบงานที่มีความสำคัญ ผู้พัฒนาระบบจะต้องพัฒนาระบบงานให้มีการตัดการเชื่อมต่อทางเครือข่ายเมื่อผู้ใช้งานไม่ได้ใช้งานมาเกินกว่าระยะเวลาหนึ่ง เช่น 30 นาที รวมทั้งประกาศให้ผู้ใช้งานได้รับทราบว่าระบบงานจะมีการตัดการเชื่อมต่อเมื่อผู้ใช้งานไม่ได้ใช้งานเกินกว่าระยะเวลาดังกล่าว

(13) สำหรับข้อมูลที่มีความสำคัญ ผู้พัฒนาระบบจะต้องพัฒนาระบบงานให้มีการจัดเก็บ Log ของข้อมูลที่มีการแก้ไขเพื่อที่จะได้ตรวจสอบได้ในภายหลัง (Audit Log)

10.2.6. การควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบ (system development and integration)

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และผู้พัฒนาระบบ และผู้นำมาใช้ปฏิบัติการ ต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนาการรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบ

10.2.7. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ กำหนดให้มีมาตรการควบคุมหน่วยงานภายนอกที่ทำหน้าที่พัฒนาซอฟต์แวร์เพื่อใช้งานภายในบริษัท ดังนี้

(1) กำหนดเรื่องสิทธิบัตรหรือลิขสิทธิ์ความเป็นเจ้าของซอฟต์แวร์ และสิทธิความเป็นเจ้าของในซอร์สโค้ดของโปรแกรม ลงในข้อตกลงหรือสัญญาให้ชัดเจน

(2) กำหนดสัญญาหรือข้อตกลงด้านความปลอดภัยในการพัฒนาโปรแกรม อาทิ การไม่เขียนโปรแกรมแอบแฝง

(3) กำหนดความรับผิดชอบหากเกิดปัญหาที่เกี่ยวข้องกับซอฟต์แวร์

10.2.8. การทดสอบฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศ

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องมีการทดสอบฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือทุกครั้งที่มีการเปลี่ยนแปลง เช่น การทำ Code review เพื่อให้ source code มีความมั่นคงปลอดภัย เป็นต้น โดยต้องทดสอบโปรแกรมในระบบทดสอบ (Test Environment) ก่อนจะนำโปรแกรมขึ้นระบบจริง (Production)

(2) ผู้พัฒนาจะต้องมีการทำ User Acceptance Test (UAT) และการทดสอบประสิทธิภาพการทำงานของระบบ ก่อนที่จะนำขึ้นระบบจริง (Production)

10.2.9. การตรวจรับระบบ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และผู้พัฒนาระบบ ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ หรือที่ปรับปรุงเพิ่มเติม รวมทั้งต้องดำเนินการทดสอบก่อนที่จะนำระบบดังกล่าวมาใช้งาน

10.3. ข้อมูลที่ใช้สำหรับการทดสอบ

10.3.1. การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ

ผู้พัฒนาระบบ ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง โดยการควบคุมต่าง ๆ ต้องประกอบด้วย

(1) ต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อนการนำสำเนาข้อมูลจริงไปยัง ระบบงานทดสอบในแต่ละครั้ง

(2) มีการควบคุมการเข้าถึงข้อมูลที่ใช้ในการทดสอบระบบ

(3) มีการดัดแปลงข้อมูลจริงที่สำคัญบางส่วนก่อนนำมาใช้ในการทดสอบ

(4) ทำการลบข้อมูลทดสอบออกจากระบบทันทีเมื่อเสร็จสิ้นการทดสอบ

(5) มีการจัดเก็บบันทึกการนำสำเนาข้อมูลจริงที่ใช้ในการทดสอบ เพื่อตรวจสอบ กิจกรรมการทดสอบ (Audit Trail)

11. การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

11.1. การประสานงานกับหน่วยงานภายนอก

11.1.1. ความมั่นคงปลอดภัยเกี่ยวข้องกับหน่วยงานภายนอก

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน่วยงานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาหรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของบริษัท

11.1.2. การระบุข้อกำหนดด้านความปลอดภัยสารสนเทศในสัญญากับหน่วยงานภายนอก

(1) หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง ต้องควบคุมให้มีการกำหนดข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศ เพื่อการอ่าน การประมวลผลการบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ โดยควรมีเนื้อหาอย่างน้อยดังนี้

1. รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยผู้รับดำเนินการรวมทั้งวิธีการเข้าถึงข้อมูล
2. การจัดแบ่งประเภทข้อมูลซึ่งสอดคล้องกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ
3. มีมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับหรือมีความสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ของผู้ประกอบธุรกิจได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมายและหลักเกณฑ์ของทางการที่เกี่ยวข้อง
4. กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการในการปฏิบัติงานภายใต้การควบคุมต่าง ๆ เช่น กำหนดเงื่อนไขการเข้าถึงข้อมูลของผู้ประกอบธุรกิจ ติดตามตรวจสอบการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงของผู้ประกอบธุรกิจ กำหนดให้ผู้รับดำเนินการรายงานผลการปฏิบัติงานให้ผู้ประกอบธุรกิจทราบเมื่อร้องขอ การแก้ไขปัญหาต่าง ๆ ภายในระยะเวลาที่กำหนด รวมทั้งการปฏิบัติงานให้เป็นไปตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจ
5. แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม
6. แนวทางการแก้ไขปัญหากรณีที่เกิดข้อผิดพลาดจากการปฏิบัติหน้าที่
7. รายชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่ง

บุคคลหรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

8. มีข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีที่ผู้ให้บริการภายนอกมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ (Sub-Contracting to Another Supplier)

9. กำหนดให้ผู้ให้บริการภายนอกยินยอมให้บริษัทเรียกดู ตรวจสอบเอกสารหลักฐานที่เกี่ยวข้อง หรือสามารถเข้าตรวจสอบการปฏิบัติงานของให้บริการภายนอก

(2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้หน่วยงานภายนอกสามารถเข้าถึงสารสนเทศของบริษัทเฉพาะส่วนที่มีความจำเป็นต้องรู้ และต้องได้รับการยินยอมจากเจ้าของข้อมูลสารสนเทศอย่างเป็นลายลักษณ์อักษร

(3) บริษัทจะไม่ยินยอมให้หน่วยงานภายนอกมีสิทธิในการเข้าถึงระบบสารสนเทศ ผ่านทาง ระบบโทรศัพท์ (Dial-up) เครือข่ายอินเทอร์เน็ต หรือเครือข่ายเสมือนส่วนตัว (VPN) จนกว่าเจ้าของข้อมูลสารสนเทศ และ ผู้ดูแลระบบเทคโนโลยีสารสนเทศจะพิจารณาเห็นชอบว่าหน่วยงานภายนอกนั้นมีสิทธิโดยชอบด้วยกฎหมายตามความต้องการของธุรกิจ โดยมีเงื่อนไขจะต้องพิจารณาเป็นกรณีไป และมีการกำหนดช่วงเวลาสำหรับสิทธินั้น ๆ

(4) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างบริษัทและผู้ให้บริการ

11.1.3. การบริหารจัดการผู้รับจ้างช่วงของหน่วยงานภายนอก

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้าง

11.2. การบริหารจัดการการให้บริการจากหน่วยงานภายนอก

11.2.1. การติดตามและสอบทานการให้บริการจากหน่วยงานภายนอก

หน่วยงานเจ้าของโครงการ ต้องติดตามและตรวจทานการดำเนินงานของผู้ให้บริการจากภายนอกซึ่งมีหน้าที่ในการบริหารจัดการระบบประมวลผลข้อมูลสารสนเทศให้กับบริษัท อย่างสม่ำเสมอ

11.2.2. การบริหารการเปลี่ยนแปลงในการให้บริการจากหน่วยงานภายนอก

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

12.1. การบริหารจัดการสถานการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศและการปรับปรุงอย่างต่อเนื่อง

12.1.1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ซึ่งมีหน้าที่ในการบริหารจัดการสถานการณ์ที่เกี่ยวข้องกับระบบความปลอดภัยสารสนเทศจะต้องได้รับการกำหนด และมอบหมายสิทธิอย่างชัดเจนในการดำเนินการจัดการแก้ไขเหตุการณ์ต่าง ๆ รวมถึงการกำหนดขั้นตอนปฏิบัติในการบริหารจัดการสถานการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

12.1.2. การรายงานเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

ผู้ใช้งานจะต้องรายงานเหตุการณ์ที่มีผลกระทบกับความปลอดภัยสารสนเทศที่เกิดขึ้นให้ผู้บังคับบัญชาและฝ่ายเทคโนโลยีสารสนเทศทราบโดยเร็วที่สุด

12.1.3. การรายงานจุดอ่อนหรือช่องโหว่ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

(1) เมื่อใดก็ตามที่ผู้ใช้งานพบจุดอ่อนหรือช่องโหวในระบบสารสนเทศ ผู้ใช้งานจะต้องรายงานปัญหาที่พบต่อผู้บังคับบัญชา และฝ่ายเทคโนโลยีสารสนเทศโดยด่วนที่สุด

(2) ผู้ใช้งาน ซึ่งพบจุดอ่อนหรือช่องโหวในระบบสารสนเทศจะต้องไม่เปิดเผย การสนทนาหรือกระทำการใด ๆ อันเป็นการเผยแพร่ต่อผู้อื่นที่ทำให้เกิดความเสียหายกับบริษัท นอกเหนือจากฝ่ายเทคโนโลยีสารสนเทศ

12.1.4. การประเมินเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศทำการจัดแยกกลุ่มและลำดับความสำคัญตามเกณฑ์ที่บริษัทกำหนด และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าจุดอ่อนหรือช่องโหว่นั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

12.1.5. การแก้ไขสถานการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

ผู้ที่ทำหน้าที่แก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่ ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และผู้ให้บริการภายนอกที่เป็นผู้มีสัญญาทำงานให้ต้องดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการแก้ไขเหตุการณ์ ด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้

12.1.6. การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศ จะต้องจัดเตรียมรายงานผลการวิเคราะห์ เหตุการณ์ จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ เพื่อใช้ในการลดโอกาสเกิดในอนาคต

12.1.7. การเก็บรวบรวมหลักฐาน

หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ จะต้องดำเนินการการเก็บรวบรวมหลักฐานด้านความมั่นคงปลอดภัยสารสนเทศ โดยเมื่อใดก็ตามที่มีหลักฐานบ่งชี้ชัดว่าระบบสารสนเทศได้ถูกกระทำการละเมิดโดยการกระทำผิดกฎหมายทางคอมพิวเตอร์ จะต้องเริ่มดำเนินการกระบวนการตรวจสอบเพื่อเป็นการรวบรวมหลักฐานให้เพียงพอต่อการนำเสนอผู้บริหารหน่วยงานที่เกี่ยวข้อง และใช้ในการดำเนินการด้านกฎหมายต่อไป รวมถึงเพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ

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

13.1. การดำเนินการทางธุรกิจอย่างต่อเนื่อง

13.1.1. การวางแผนในการสร้างการดำเนินการทางธุรกิจอย่างต่อเนื่อง

เจ้าของข้อมูลสารสนเทศ หน่วยงานเทคโนโลยีสารสนเทศ และหน่วยงานบริหารความเสี่ยง จะต้องเข้าร่วมในการดำเนินการระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ และการประเมินความเสี่ยง เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วน ในการดำเนินการจัดทำแผนการดำเนินการทางธุรกิจอย่างต่อเนื่อง

13.1.2. การสร้างกระบวนการการจัดการเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ

(1) บริษัทต้องควบคุม กำกับให้มีการจัดทำกระบวนการเพื่อก่อให้เกิดความต่อเนื่องในการ ให้บริการในกรณีที่เกิดเหตุการณ์ที่ส่งผลให้การดำเนินธุรกิจต้องหยุดชะงัก

(2) คณะกรรมการบริหารการดำเนินการทางธุรกิจอย่างต่อเนื่องจะต้องทำการกำหนดกรอบมาตรฐาน (Framework) เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ และสะดวกในการจัดลำดับความสำคัญของแผนและกิจกรรมที่ต้องดำเนินการ

(3) คณะกรรมการบริหารการดำเนินการทางธุรกิจอย่างต่อเนื่องต้องควบคุม กำกับให้มีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง โดยแผนต้องถูกจัดทำขึ้นภายใต้กรอบมาตรฐานการ ดำเนินธุรกิจอย่างต่อเนื่อง

13.1.3. การทดสอบและการปรับปรุงแผนรองรับการดำเนินการทางธุรกิจอย่างต่อเนื่อง

(1) เจ้าของข้อมูลสารสนเทศ หน่วยงานเทคโนโลยีสารสนเทศ และหน่วยงานบริหารความเสี่ยง มีหน้าที่ปรับปรุงบทบาทและหน้าที่ความรับผิดชอบ คู่มือและแผนการสร้างความต่อเนื่องให้กับธุรกิจ และต้องจัดให้มีการทดสอบแผนอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าธุรกิจจะดำเนินต่อไปได้เมื่อเกิดเหตุการณ์ที่กระทบกับกระบวนการทางธุรกิจของบริษัท

(2) พนักงานผู้ซึ่งมีส่วนเกี่ยวข้องในการปฏิบัติงานกู้คืนระบบสารสนเทศไปยังศูนย์สำรองจะต้องจะต้องมีความรู้ด้านเทคนิคที่จำเป็นต่อการกู้คืนระบบ และเข้าร่วมในการซักซ้อมแผน

(3) เจ้าของข้อมูลสารสนเทศ และผู้ใช้งานระบบที่เกี่ยวข้องกับแผนรองรับการดำเนินการทางธุรกิจอย่างต่อเนื่องต้องเข้าร่วมการทดสอบแผน และดำเนินงานตามแผนที่กำหนดไว้

13.2. การจัดให้มีอุปกรณ์หรือระบบสารสนเทศสำรอง (Redundancy)

13.2.1. การรักษาความต่อเนื่องของอุปกรณ์หรือระบบสารสนเทศ

หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบที่มีความสำคัญสูง และกำกับให้การติดตั้งอุปกรณ์หรือระบบสำหรับรักษาการให้บริการเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ ที่เหมาะสม

14. การปฏิบัติตามข้อกำหนด (Compliance)

14.1. การปฏิบัติตามข้อกำหนดทางกฎหมาย

14.1.1. การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย

(1) หน่วยงานกฎหมาย และหน่วยงานกำกับดูแลกิจการ ต้องรวบรวมและจัดทำเป็นเอกสารที่ระบุถึงกฎหมาย กฎระเบียบ พระราชบัญญัติหรือข้อบังคับตามสัญญาต่าง ๆ ที่มีผลบังคับใช้ กับบริษัท ทั้งนี้รวมถึงข้อบังคับด้านกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศแต่ละระบบของบริษัท

(2) หน่วยงานที่เกี่ยวข้องในแต่ละระบบสารสนเทศต้องรับผิดชอบในการปฏิบัติตาม ข้อบังคับด้านกฎหมายหรือกฎระเบียบที่เกี่ยวข้อง

14.1.2. การป้องกันสิทธิ และทรัพย์สินทางปัญญา

(1) พนักงานต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่บริษัทได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

(2) ซอฟต์แวร์ที่พัฒนาโดยหรือเพื่อบริษัท ทั้งโดยหน่วยงานภายนอกหรือพนักงานของบริษัท ถือว่าเป็นทรัพย์สินบริษัท บริษัทไม่อนุญาตให้พนักงานทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินของบริษัทโดยไม่ได้รับอนุญาต

(3) พนักงานที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศของบริษัท ต้องยึดถือ และปฏิบัติตาม กฎหมาย ลิขสิทธิ์ นโยบายการใช้งานด้านความปลอดภัยสารสนเทศ และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

14.1.3. การป้องกันข้อมูลสารสนเทศสำคัญที่เกี่ยวข้องกับบริษัท

เจ้าของข้อมูลสารสนเทศ จำเป็นต้องปฏิบัติตามข้อบังคับทางกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศบางประเภท เช่น ทางด้านบัญชี ทางด้านลูกค้า และต้องจัดทำข้อกำหนดในการจัดการข้อมูลสารสนเทศ ระยะเวลาในการจัดเก็บ ให้สอดคล้องกับข้อบังคับดังกล่าว นอกจากนี้เจ้าของข้อมูลสารสนเทศต้องควบคุม กำกับให้ผู้ดูแลข้อมูลสารสนเทศได้ปฏิบัติงานให้สอดคล้องกับข้อกำหนดดังกล่าว

14.1.4. การป้องกันข้อมูลสารสนเทศส่วนบุคคล

(1) ข้อมูลสารสนเทศรายละเอียดที่เกี่ยวกับลูกค้าถือว่ามีความสำคัญ พนักงานและลูกจ้างที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศดังกล่าวได้

(2) ข้อมูลสารสนเทศส่วนบุคคลของพนักงาน ลูกจ้าง และลูกค้า ถือว่าเป็นความลับ และ สามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ ตามที่บริษัทกำหนด

14.1.5. การเข้ารหัสลับ

ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายพระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

14.2. การตรวจประเมินระบบสารสนเทศ

14.2.1. การตรวจประเมินระบบสารสนเทศจากผู้ตรวจสอบอิสระ

หน่วยงานตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอก จะต้องทำการตรวจสอบตามการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความปลอดภัย สารสนเทศ ตลอดจนทบทวนถึงความพอเพียงของการควบคุมระบบสารสนเทศ และการปฏิบัติตามการควบคุมนั้น ๆ

14.2.2. การปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยสารสนเทศ

กำหนดให้มีแนวทางการตรวจสอบการปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยสารสนเทศดังต่อไปนี้

(1) ผู้บังคับบัญชาของแต่ละหน่วยงานต้องรับผิดชอบในการสอบทานอย่างสม่ำเสมอถึงการ ใช้งาน หรือการปฏิบัติงานว่าสอดคล้องกับนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการสนับสนุนด้านการให้คำแนะนำในการใช้งาน หรือการปฏิบัติตาม ข้อกำหนดด้านความปลอดภัยสารสนเทศที่เกี่ยวข้อง

(2) บริษัทจะต้องมีการสอบทานการปฏิบัติตามข้อกำหนดด้านความปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยหน่วยงานตรวจสอบภายใน และแจ้งให้คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศทราบถึงผลการตรวจสอบ ซึ่งการตรวจสอบดังกล่าวในเรื่องใด ๆ จะครอบคลุมถึงการปฏิบัติงานที่สอดคล้องกับนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ

14.2.3. การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิค

กำหนดให้มีแนวการตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิค ดังต่อไปนี้

(1) หน่วยงานตรวจสอบภายใน ต้องตรวจสอบการควบคุมทางเทคนิคของระบบสารสนเทศเพื่อตรวจสอบว่ามีความเพียงพอ เหมาะสม และมีการปฏิบัติตามการควบคุมเหล่านั้น

(2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้ระบบสารสนเทศ โดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ให้ได้รับการทดสอบระดับมาตรฐานความปลอดภัยสารสนเทศของระบบสารสนเทศอย่างสม่ำเสมอ อาทิ การทดสอบการเจาะระบบ เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของ การควบคุมด้านความปลอดภัยสารสนเทศ