เอกสารแนบท้ายประกาศ ๒

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศ พ.ศ. ๒๕๖๒

การอนุมัติเอกสาร

ผู้อนุมัติ

ตำแหน่ง	ชื่อ	ลายมือชื่อ	วัน/เดือน/ปี
กรรมการผู้อำนวยการใหญ่	นายสมนึก รงค์ทอง		๒ ส.ค. ๖๒

ผู้ตรวจสอบ

ตำแหน่ง	ชื่อ	ลายมือชื่อ	วัน/เดือน/ปี
รองกรรมการผู้อำนวยการใหญ่ (วิศวกรรม)	นายณัฐวัฒน์ สุภานันท์		๑ ส.ค. ๖๒

ผู้จัดทำ

ตำแหน่ง	ชื่อ	ลายมือชื่อ	วัน/เดือน/ปี
ผู้อำนวยการ ฝ่ายเทคโนโลยีสารสนเทศ	นายไพบูลณ์ ประจำวงษ์		๑๘ ก.พ. ๖๐
ผู้อำนวยการกองบริหาร ระบบเทคโนโลยีสารสนเทศ	นายเมธี เสรีอรุโณ		๑๘ ก.พ. ๖๐

บันทึกการแก้ไขเอกสาร

ครั้งที่แก้ไข	วันที่แก้ไข	รายละเอียดการแก้ไข	ผู้จัดทำ

สารบัญ

หน้า

คำนิยาม

"บริษัท" หมายความว่า บริษัท วิทยุการบินแห่งประเทศไทย จำกัด

"หน่วยงานภายใน" หมายความว่า หน่วยงานตามโครงสร้างองค์กรของบริษัท อันมีพนักงานตั้งแต่ระดับฝ่ายจัดการขึ้นไปเป็นผู้บังคับบัญชา

"ผู้ใช้งาน" หมายความว่า คณะกรรมการบริษัท พนักงาน ลูกจ้าง หน่วยงานภายในและบุคคลภายนอกที่เข้าใช้งานหรือดำเนินการเกี่ยวกับระบบสารสนเทศ

"ผู้บังคับบัญชา" หมายความว่า พนักงานตั้งแต่ระดับฝ่ายจัดการขึ้นไปซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท

"บุคคลภายนอก" หมายความว่า บุคคลที่มิใช่คณะกรรมการบริษัท พนักงาน หรือลูกจ้าง และได้รับอนุญาตจากบริษัท ให้เข้าใช้งานหรือดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทภายใต้เงื่อนไข ข้อกำหนดหรือแนวปฏิบัติที่บริษัทกำหนดไว้

"ผู้ดูแลจัดการระบบงาน (Application Administrator)" หมายความว่า พนักงาน ลูกจ้างที่ได้รับมอบหมายจากผู้บังคับบัญชาของผู้ดูแลจัดการระบบงาน หรือบุคคลที่มิใช่พนักงานแต่ปฏิบัติงานตามสัญญาหรือข้อตกลง ให้มีหน้าที่ดูแลระบบสารสนเทศ โดยต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหน่วยงานภายในที่เป็นเจ้าของระบบสารสนเทศ

"ผู้ดูแลระบบคอมพิวเตอร์ (Computer System Administrator)" หมายความว่า พนักงาน ลูกจ้าง ที่ได้รับมอบหมายจากผู้บังคับบัญชาของผู้ดูแลระบบคอมพิวเตอร์ หรือบุคคลที่มิใช่พนักงานแต่ปฏิบัติงานตามสัญญาหรือข้อตกลง ให้มีหน้าที่ดูแลระบบคอมพิวเตอร์ โดยต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหน่วยงานภายในที่เป็นเจ้าของระบบคอมพิวเตอร์

"ผู้ดูแลระบบเครือข่าย (Network Administrator)" หมายความว่า พนักงาน ลูกจ้าง ที่ได้รับมอบหมายจากผู้บังคับบัญชาของผู้ดูแลระบบเครือข่าย หรือบุคคลที่มิใช่พนักงานแต่ปฏิบัติงานตามสัญญาหรือข้อตกลง ให้มีหน้าที่ดูแลระบบเครือข่าย โดยต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหน่วยงานภายในที่เป็นเจ้าของระบบเครือข่าย

"ผู้ดูแลฐานข้อมูล (Database Administrator)" หมายความว่า พนักงาน ลูกจ้าง ที่ได้รับมอบหมายจากผู้บังคับบัญชาของผู้ดูแลฐานข้อมูล หรือบุคคลที่มิใช่พนักงานแต่ปฏิบัติงานตามสัญญาหรือข้อตกลง ให้มีหน้าที่ดูแลฐานข้อมูล โดยต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหน่วยงานภายในที่เป็นเจ้าของฐานข้อมูล

"ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน (User Account Administrator)" หมายความว่า พนักงาน ลูกจ้าง ที่ได้รับมอบหมายจากผู้บังคับบัญชาของผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน หรือบุคคลที่มิใช่พนักงานแต่ปฏิบัติงานตามสัญญาหรือข้อตกลง ให้มีหน้าที่ดูแลบริหารจัดการบัญชีผู้ใช้งาน โดยต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหน่วยงานภายในที่เป็นเจ้าของระบบสารสนเทศ

"ผู้ปฏิบัติการ (Operator)" หมายความ ผู้ทำหน้าที่ตามสิทธิที่ได้รับจากผู้ดูแลบริหาร

จัดการบัญชีผู้ใช้งาน

“ผู้พัฒนาระบบสารสนเทศ (Information System Developer)” หมายความว่า พนักงาน ลูกจ้าง ที่ได้รับมอบหมายจากผู้บังคับบัญชาของผู้พัฒนาระบบสารสนเทศ หรือบุคคลที่มิใช่พนักงาน แต่ปฏิบัติงานตามสัญญาหรือข้อตกลง ให้มีหน้าที่พัฒนาระบบสารสนเทศ โดยต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหน่วยงานภายในที่เป็นผู้พัฒนาระบบสารสนเทศ

“ผู้ดูแลระบบฯ (System Administrator)” หมายความว่า ผู้ดูแลจัดการระบบงาน ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย ผู้ดูแลฐานข้อมูล และผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน

“เจ้าของระบบสารสนเทศ (Information System Owner)” หมายความว่า หน่วยงานภายในซึ่งเป็นเจ้าของระบบสารสนเทศ

“เจ้าของข้อมูล (Information Owner)” หมายความว่า หน่วยงานภายในที่ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบข้อมูลที่อยู่ในระบบสารสนเทศ

“ผู้ดูแลงานอาคารและสถานที่” หมายความว่า หน่วยงานภายในที่มีหน้าที่ควบคุมดูแลและบริหารจัดการระบบสาธารณูปโภคต่าง ๆ เช่น ไฟฟ้า เครื่องปรับอากาศ ระบบน้ำ ระบบแสงสว่าง ระบบดับเพลิง ระบบเตือนไฟไหม้ และระบบความปลอดภัย เป็นต้น

“ผู้ดูแลงานทรัพยากรบุคคล” หมายความว่า หน่วยงานภายในที่มีหน้าที่ในการตรวจสอบภูมิหลัง ของบุคคล ทำข้อตกลงและเงื่อนไขทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดการจ้างงานเพื่อป้องกันและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

“ผู้ดูแลงานนิติการ” หมายความว่า หน่วยงานภายในที่มีหน้าที่ให้ความคิดเห็นหรือตีความเกี่ยวกับ ระเบียบ ข้อบังคับ คำสั่ง หรือแนวปฏิบัติ ให้สอดคล้องกับกฎหมาย

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานภายใน

“สินทรัพย์ (Asset)” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับบริษัท

“ทรัพย์สินสารสนเทศ” หมายความว่า

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นที่เกี่ยวข้องกับสารสนเทศ

(๓) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

“เทคโนโลยีสารสนเทศและการสื่อสาร” หมายความว่า เทคโนโลยีทางด้านคอมพิวเตอร์และเทคโนโลยีทางด้านการสื่อสารที่ถูกนำมาใช้ในกระบวนการจัดการสารสนเทศได้อย่างสะดวก ถูกต้องและรวดเร็ว

“เครื่องคอมพิวเตอร์” หมายความว่า เครื่องมือ หรืออุปกรณ์อิเล็กทรอนิกส์ที่มีความสามารถในการรับข้อมูลเข้าประมวลผลตามโปรแกรม และแสดง บันทึก ส่งออกข้อมูล ซึ่งเป็น

ผลที่ได้จากการประมวลผล

“อุปกรณ์คอมพิวเตอร์” (Computer) หมายความว่า อุปกรณ์คอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ และอุปกรณ์ต่อพ่วง รวมถึงโปรแกรมคอมพิวเตอร์ และชุดคำสั่งคอมพิวเตอร์ทุกประเภทที่นำมาใช้ร่วมกับอุปกรณ์ดังกล่าว เพื่อใช้ในการปฏิบัติงาน

“เครื่องคอมพิวเตอร์แม่ข่าย” (Server) หมายความว่า อุปกรณ์คอมพิวเตอร์หลักในเครือข่ายซึ่งทำหน้าที่ควบคุมอุปกรณ์คอมพิวเตอร์อื่น ๆ หรือทำหน้าที่ในการให้บริการด้านฐานข้อมูลและโปรแกรมระบบงานต่าง ๆ ของบริษัท

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์ หรือชุดของเครื่องคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางการปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ

“ระบบสารสนเทศ” หมายความว่า ระบบของการรวบรวม (Input) ประมวลผล (Processing) เผยแพร่ (Output) และจัดเก็บข้อมูล (Storage) ที่ใช้เทคโนโลยีสารสนเทศและการสื่อสารในการดำเนินการ เพื่อให้ได้สารสนเทศที่เหมาะสมกับงานหรือภารกิจแต่ละอย่าง ซึ่งประกอบด้วย ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล (Data) บุคคล (People) กระบวนการ (Procedure) และการสื่อสารข้อมูล (Data Communication)

“ข้อมูลสารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นกับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

“ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมถึงคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non–repudiation) และความน่าเชื่อถือ (Reliability)

“ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS)” หมายความว่า ระบบการจัดการความปลอดภัยของข้อมูล ที่มีการหมุนเพื่อปรับปรุงอย่างต่อเนื่องอยู่ตลอดเวลาเมื่อครบวงรอบ (Plan Do heck Act) เพื่อให้ข้อมูลขององค์กร มีการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

รวมถึงคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่พึงประสงค์ที่อาจเกี่ยวข้องกับความมั่นคงปลอดภัย หรือเหตุการณ์อันเป็นการแทรกแซงโดยมิชอบด้วยกฎหมาย (Unlawful Interference)

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบสารสนเทศของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"พื้นที่ควบคุม" หมายความว่า พื้นที่ที่ถูกกำหนดมีการควบคุมการเข้า-ออกของบุคคลและยานพาหนะ เพื่อตรวจสอบการเข้าถึงพื้นที่ภายในบริษัท และอาคารสำนักงาน

"พื้นที่ควบคุมเฉพาะ" หมายความว่า พื้นที่ที่มีความสำคัญต่อการให้บริการจราจรทางอากาศของบริษัท ซึ่งจะต้องพิทักษ์ดูแลควบคุมการเข้า-ออกพื้นที่อย่างสูงสุด

"รหัสผ่าน" หมายความว่า ข้อมูลซึ่งเป็นที่รู้อยู่เฉพาะบุคคลจำกัดหรือกลุ่มบุคคลจำกัดที่ป้อนเข้าสู่อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย หรือระบบคอมพิวเตอร์ เพื่อให้บุคคลหรือกลุ่มบุคคลดังกล่าวสามารถใช้อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย หรือระบบคอมพิวเตอร์ได้

"ชุดคำสั่งไม่พึงประสงค์" (Malicious Code) หมายความว่าชุดคำสั่งคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลที่ได้รับการออกแบบขึ้นมาเพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยทางตรงหรือทางอ้อมแก่ อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย หรือระบบคอมพิวเตอร์

ส่วนที่ ๑
การจัดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดบทบาทและหน้าที่รับผิดชอบของผู้ที่เกี่ยวข้องในการกำกับ ดูแล และปฏิบัติตามหน้าที่รักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑. คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร

๒. คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. โครงสร้างด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๑ *บริษัท*ต้องกำหนดให้มีโครงสร้างในระดับบริหารงานเพื่อทำหน้าที่สนับสนุนกิจกรรมต่าง ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ และให้มีโครงสร้างในระดับการปฏิบัติงานเพื่อปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศตามหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

๑.๒ ต้องมีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจนตามนโยบายและแนวปฏิบัติฯ เพื่อลดโอกาสความผิดพลาดในการเข้าถึง เปลี่ยนแปลง แก้ไข และใช้งาน*ทรัพย์สินสารสนเทศ*ของ*บริษัท* ที่ผิดประเภทหรือไม่ถูกต้องหรือไม่ได้รับอนุญาต

๑.๓ ต้องมีการจัดทำและปรับปรุงทะเบียนรายชื่อ เบอร์โทรศัพท์ หรือช่องทางการติดต่ออื่น ๆ ที่สามารถติดต่อประสานงานกับเจ้าหน้าที่ของรัฐผู้บังคับใช้กฎหมาย เพื่อใช้สำหรับการแจ้งเหตุอย่างทันท่วงที ในกรณีที่ตรวจพบเหตุการณ์ละเมิดด้านความมั่นคงปลอดภัยเกิดขึ้น

๑.๔ ต้องมีการจัดทำและปรับปรุงทะเบียนรายชื่อ เบอร์โทรศัพท์ หรือช่องทางการติดต่ออื่น ๆ ที่สามารถติดต่อประสานงานกับหน่วยงานภายนอกหรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้*บริษัท*ได้รับทราบข้อมูลที่เกี่ยวข้องกับการโจมตี หรือช่วงโหว่ต่าง ๆ ที่ตรวจพบใหม่ และสามารถขอคำแนะนำในการปฏิบัติเพื่อลดความเสี่ยงที่อาจเกิดขึ้นได้

ส่วนที่ ๒
การสร้างความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

วัตถุประสงค์

๑. เพื่อให้*ผู้ใช้งาน*เข้าใจหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ของตนเองที่ได้รับ

๒. เพื่อให้*ผู้ใช้งาน*ตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

๓. เพื่อป้องกันผลประโยชน์ของ*บริษัท*ซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

ผู้รับผิดชอบ

๑. *ผู้ดูแลงานทรัพยากรบุคคล*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. ความมั่นคงปลอดภัยก่อนเข้าทำงาน (Prior to Employment)

๑.๑ ในการพิจารณารับพนักงาน ลูกจ้าง หรือการว่าจ้างหน่วยงานหรือ*บุคคลภายนอก*เข้าทำงาน ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยให้คำนึงถึงระดับชั้นความลับของ*ข้อมูลสารสนเทศ*ที่จะให้เข้าถึง

๑.๒ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน ลูกจ้าง หรือสัญญาว่าจ้างหน่วยงานหรือ*บุคคลภายนอก* ให้ระบุบทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศและข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

๑.๓ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้*ผู้ใช้งาน*ที่เป็น*บุคคลภายนอก*เข้าถึง*ระบบสารสนเทศ* หรือใช้*ข้อมูลสารสนเทศ*ของ*หน่วยงานภายใน*

๒. ความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During Employment)

การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้*ผู้ใช้งาน*ได้ทราบ

๒.๒ จัดฝึกอบรมนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศให้กับ*ผู้ใช้งาน*

๓. การสิ้นสุดหรือเปลี่ยนการจ้างงาน (Termination and Change of Employment)

๓.๑ *ผู้ใช้งาน*ต้องส่งคืน*ทรัพย์สินสารสนเทศ*ของ*หน่วยงานภายใน*ผู้เป็นเจ้าของ*ทรัพย์สินสารสนเทศ* เมื่อสิ้นสุดสภาพการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับ*บริษัท*

ส่วนที่ ๓
การบริหารจัดการทรัพย์สินสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการระบุ*ทรัพย์สินสารสนเทศ*ของ*บริษัท*และกำหนดหน้าที่ความรับผิดชอบในการป้องกัน*ทรัพย์สินสารสนเทศ*อย่างเหมาะสม

๒. เพื่อให้ข้อมูลได้รับระดับการปกป้องที่เหมาะสมโดยสอดคล้องกับความสำคัญของข้อมูลนั้นที่มีต่อ*บริษัท*

๓. เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลงการขนย้าย การลบ หรือการทำลายข้อมูลที่จัดเก็บอยู่ในสื่อบันทึกข้อมูล

ผู้รับผิดชอบ

๑. *เจ้าของระบบสารสนเทศ*

๒. *เจ้าของข้อมูล*

๓. *ผู้ดูแลจัดการระบบงาน*

๔. *ผู้ดูแลระบบคอมพิวเตอร์*

๕. *ผู้ใช้งาน*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. หน้าที่รับผิดชอบต่อทรัพย์สินสารสนเทศ (Responsibility of Assets)

๑.๑ บัญชี*ทรัพย์สินสารสนเทศ* (Inventory of Assets)

กำหนดให้*เจ้าของระบบสารสนเทศ*ต้องจัดทำบัญชี*ทรัพย์สินสารสนเทศ*ที่อยู่ในความรับผิดชอบของตน โดยระบุผู้รับผิดชอบใน*ทรัพย์สินสารสนเทศ*นั้นอย่างชัดเจน และปรับปรุงให้ทันสมัยอยู่เสมอ

๑.๒ ความเป็นเจ้าของ*ทรัพย์สินสารสนเทศ* (Ownership of Assets)

(๑) *เจ้าของระบบสารสนเทศ*ต้องควบคุมดูแลเพื่อให้มั่นใจได้ว่ามีการจัดหมวดหมู่ข้อมูลและ*ทรัพย์สินสารสนเทศ* รวมถึงจัดทำแนวทางการป้องกัน*ทรัพย์สินสารสนเทศ*อย่างเหมาะสมตามลำดับชั้นความลับ

(๒) *เจ้าของระบบสารสนเทศ*ต้องกำหนดและทบทวนสิทธิในการเข้าถึง*ทรัพย์สินสารสนเทศ*อย่างสม่ำเสมอ

(๓) *เจ้าของระบบสารสนเทศ*ต้องควบคุมดูแลเพื่อให้มั่นใจได้ว่า*ทรัพย์สินสารสนเทศ*ถูกลบหรือทำลายอย่างเหมาะสม

๑.๓ การใช้งาน*ทรัพย์สินสารสนเทศ*อย่างเหมาะสม (Acceptable Use of Assets)

(๑) *เจ้าของข้อมูล*ต้องกำหนดขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บ*ทรัพย์สินสารสนเทศ* เพื่อมิให้*ข้อมูลสารสนเทศ*รั่วไหลหรือถูกนำไปใช้ผิดประเภท

(๒) *ผู้ใช้งาน*ต้องไม่ทิ้งหรือปล่อยให้*ทรัพย์สินสารสนเทศ*ที่มีความสำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล ให้อยู่ในสถานที่ที่ไม่มีความปลอดภัย สถานที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น

(๓) แนวทางปฏิบัติในการใช้งาน*เครื่องคอมพิวเตอร์*ส่วนบุคคล

๑) *เครื่องคอมพิวเตอร์*ที่อนุญาตให้ใช้งานเป็น*สินทรัพย์*ของ*บริษัท ผู้ใช้งาน*ต้องระมัดระวังการใช้งานและสงวนรักษา*เครื่องคอมพิวเตอร์*ที่ครอบครองใช้งานอยู่เสมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งาน

๒) โปรแกรมที่ได้ถูกติดตั้งลงบน*เครื่องคอมพิวเตอร์*ของ*บริษัท* ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้าม*ผู้ใช้งาน*คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบน*เครื่องคอมพิวเตอร์*หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓) ไม่อนุญาตให้*ผู้ใช้งาน*ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมใน*เครื่องคอมพิวเตอร์*ของ*บริษัท* ก่อนได้รับอนุญาตจาก*ผู้ดูแลระบบคอมพิวเตอร์*

๔) ไม่อนุญาตให้*ผู้ใช้งาน*ทำการติดตั้ง*เครื่องคอมพิวเตอร์*ใด ๆ ใน*ระบบเครือข่าย*คอมพิวเตอร์ก่อนได้รับอนุญาตจาก*ผู้ดูแลระบบฯ*

๕) การเคลื่อนย้ายหรือส่ง*เครื่องคอมพิวเตอร์*ตรวจซ่อมต้องดำเนินการโดยเจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบ*เครื่องคอมพิวเตอร์*นั้น

๖) *ผู้ใช้งาน*ต้องตรวจสอบสื่อบันทึกข้อมูลแบบพกพาชนิดต่าง ๆ ด้วยโปรแกรมป้องกันไวรัสก่อนนำมาใช้งาน

๗) *ผู้ใช้งาน*ต้องดูแลอัพเดทฐานข้อมูลของโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอหรือตามที่*ผู้ดูแลระบบคอมพิวเตอร์*กำหนดไว้ หากตรวจพบไวรัสฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายโดยเร็วที่สุด

๘) *ผู้ใช้งาน*ต้องสำรองข้อมูลสำคัญที่อยู่ใน*เครื่องคอมพิวเตอร์*สม่ำเสมอ

๙) *ผู้ใช้งาน*ต้องให้ความร่วมมือและอำนวยความสะดวกแก่*ผู้ดูแลระบบฯ* และผู้ที่เกี่ยวข้องในการตรวจสอบความมั่นคงปลอดภัยของ*เครื่องคอมพิวเตอร์* และระบบคอมพิวเตอร์ที่ใช้งานอยู่ รวมทั้งจะต้องปฏิบัติตามคำแนะนำของ*ผู้ดูแลระบบฯ* หรือผู้ที่เกี่ยวข้องอย่างเคร่งครัด

(๔) การควบคุม*เครื่องคอมพิวเตอร์*แบบพกพา

๑) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งาน*เครื่องคอมพิวเตอร์*ประเภทพกพาเป็นประจำทุกปี

๒) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องสร้างความตระหนักเพื่อให้*ผู้ใช้งาน*ระมัดระวังและป้องกันการใช้งานก่อนครอบครอง*เครื่องคอมพิวเตอร์*ประเภทพกพา เช่น การใช้งานในพื้นที่สาธารณะ การเข้ารหัสข้อมูลที่สำคัญ การสำรองข้อมูล เป็นต้น

๓) กำหนดให้ใช้งานการพิสูจน์ตัวตนของ*ผู้ใช้งาน*บนระบบปฏิบัติการ

๔) ข้อมูลที่มีชั้นความลับที่ถูกจัดเก็บไว้บน*เครื่องคอมพิวเตอร์*แบบพกพาต้องได้รับการเข้ารหัสข้อมูล

๕) *ผู้ใช้งาน*ต้องสำรองข้อมูลสำคัญที่อยู่ใน*เครื่องคอมพิวเตอร์*ประเภทพกพาอย่างสม่ำเสมอ

๖) ห้าม*ผู้ใช้งาน*ติดตั้งโปรแกรมละเมิดลิขสิทธิ์หรือมีแหล่งที่มาที่ไม่มีความน่าเชื่อถือ

๗) *ผู้ใช้งาน*ต้องทำการล็อกหน้าจอทุกครั้งเมื่อไม่มีการใช้งาน

(๕) การควบคุมอุปกรณ์แท็บเล็ตหรือสมาร์ทโฟน

๑) *ผู้ใช้งาน*ต้องทำการล็อกหน้าจอทุกครั้งเมื่อไม่มีการใช้งาน

๒) ข้อมูลที่มีชั้นความลับที่ไม่ควรถูกจัดเก็บไว้บนอุปกรณ์แท็บเล็ตหรือสมาร์ทโฟน หากมีความจำเป็นต้องจัดเก็บ ข้อมูลที่มีชั้นความลับต้องได้รับการเข้ารหัสข้อมูล

๓) *ผู้ใช้งาน*ไม่ควรติดตั้งโปรแกรมจากแหล่งที่มาที่ไม่มีความน่าเชื่อถือ

๔) หากพบว่าอุปกรณ์แท็บเล็ตหรือสมาร์ทโฟนสูญหาย *ผู้ใช้งาน*ต้องทำการสั่งลบข้อมูลจากระยะไกลในทันที

(๖) แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๑) *ผู้ใช้งาน*ต้องใช้งานอินเทอร์เน็ตด้วยบัญชีผู้ใช้งานของตนเองเท่านั้น

๒) *ผู้ใช้งาน*ต้องตรวจสอบโปรแกรมป้องกันไวรัสลงใน*เครื่องคอมพิวเตอร์*ส่วนบุคคลหรือ*เครื่องคอมพิวเตอร์*แบบพกพา ก่อนการเชื่อมต่อกับอินเทอร์เน็ต ในกรณีไม่มีโปรแกรมป้องกันไวรัสให้ใช้งานอินเทอร์เน็ตด้วยความระมัดระวังอย่างสูง

๓) *ผู้ใช้งาน*ต้องไม่ใช้*ระบบเครือข่าย*อินเทอร์เน็ตของ*บริษัท* เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวหรือเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

๔) ห้าม*ผู้ใช้งาน*เปิดเผยข้อมูลที่เป็นความลับของ*บริษัท* โดยไม่ได้รับอนุญาตผ่านเครือข่ายอินเทอร์เน็ต

๕) *ผู้ใช้งาน*มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งานหรือเผยแพร่แก่ผู้อื่น

๖) เมื่อ*ผู้ใช้งาน*เสร็จสิ้นการใช้งานอินเทอร์เน็ต ต้องออกจากระบบ (Logout) หรือปิดเว็บเบราเซอร์ (Web browser) ทุกครั้ง

(๗) แนวทางปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

๑) *ผู้ดูแลจัดการระบบงาน*ต้องกำหนดสิทธิการใช้งานจดหมายอิเล็กทรอนิกส์ที่เหมาะสมให้กับ*ผู้ใช้งาน*

๒) *ผู้ใช้งาน*ต้องไม่รับส่งข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานโดยผ่านทางจดหมายอิเล็กทรอนิกส์ที่ไม่ใช่ระบบจดหมายอิเล็กทรอนิกส์ของ*บริษัท*

๓) *ผู้ใช้งาน*ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณพื้นที่จัดเก็บจดหมายอิเล็กทรอนิกส์

๔) *ผู้ใช้งาน*ต้องตรวจสอบไฟล์แนบจากจดหมายอิเล็กทรอนิกส์ด้วยโปรแกรมป้องกันไวรัสก่อนทำการเปิดไฟล์แนบ

๕) การส่งข้อมูลที่มีชั้นความลับ *ผู้ใช้งาน*ต้องทำการเข้ารหัสข้อมูลก่อนทำการส่ง

๖) ห้าม*ผู้ใช้งาน*ส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะ ดังนี้

- จดหมายขยะ (Spam mail)
- จดหมายลูกโซ่ (Chain mail)
- จดหมายที่มีลักษณะละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
- จดหมายที่มีไวรัสซึ่งส่งไปหาผู้อื่นโดยเจตนา

๗) *ผู้ใช้งาน*ควรสำรองข้อมูลจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ

๘) หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์เสร็จสิ้น *ผู้ใช้งาน*ต้องออกจากระบบ (Logout) ทุกครั้ง

๑.๔ การคืน*ทรัพย์สินสารสนเทศ* (Return of Assets)

(๑) เมื่อมี*ผู้ใช้งาน*พ้นจากหน้าที่หรือไม่มีหน้าที่รับผิดชอบใน*ระบบสารสนเทศ*ที่ได้รับสิทธิในการใช้งาน ให้คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งาน*ระบบสารสนเทศ* เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่*เจ้าของระบบสารสนเทศ*ในทันทีที่พ้นจากหน้าที่

๒. การจัดชั้นความลับของข้อมูล (Information Classification)

๒.๑ แบ่งข้อมูลออกเป็น ๓ ประเภท

(๑) ข้อมูลที่มีชั้นความลับ (Secret)

๑) ข้อมูลลับที่สุด (Top Secret) หมายถึง ข้อมูลที่มีความสำคัญต่อ*บริษัท*ในระดับสูงที่สุด หากสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อ*บริษัท*ในระดับร้ายแรงที่สุด

๒) ข้อมูลลับมาก (Secret) หมายถึง ข้อมูลที่มีความสำคัญต่อ*บริษัท*ในระดับสูงมาก หากสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อ*บริษัท*ในระดับร้ายแรงมาก

๓) ข้อมูลลับ (Confidential) หมายถึง ข้อมูลที่มีความสำคัญต่อ*บริษัท*ในระดับสูง หากสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อ*บริษัท*

(๒) ข้อมูลใช้ภายใน (Internal Use Only) หมายถึง ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของ*บริษัท* ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต

(๓) ข้อมูลเปิดเผยได้ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไป โดยไม่ก่อให้เกิดความเสียหายใด ๆ แก่*บริษัท*

๒.๒ จัดแบ่งระดับชั้นการเข้าถึงออกเป็น ๔ ระดับ

(๑) ข้อมูลลับที่สุด (Top Secret) และข้อมูลลับมาก (Secret) กำหนดให้มีสิทธิเข้าถึงได้เฉพาะผู้ที่ได้รับการระบุชื่อเท่านั้น และต้องปกป้องข้อมูลจากการเข้าถึงโดย*บุคคลภายนอก* พนักงานและลูกจ้างที่ไม่ได้รับอนุญาตด้วยวิธีการควบคุมการเข้าถึงทางเทคนิคและการเข้ารหัสข้อมูล

(๒) ข้อมูลลับ (Confidential) กำหนดให้มีสิทธิเข้าถึงได้เฉพาะบุคคลบางกลุ่มเท่านั้น และต้องปกป้องข้อมูลจากการเข้าถึงโดย*บุคคลภายนอก* พนักงานและลูกจ้างที่ไม่ได้รับอนุญาตด้วยวิธีการควบคุมการเข้าถึงทางเทคนิคและการเข้ารหัสข้อมูล

(๓) ข้อมูลใช้ภายใน (Internal use only) กำหนดให้มีสิทธิเข้าถึงได้เฉพาะพนักงานและลูกจ้างเท่านั้น และต้องปกป้องข้อมูลจากการเข้าถึงโดย*บุคคลภายนอก*ด้วยวิธีการควบคุมการเข้าถึงทางเทคนิค

(๔) ข้อมูลเปิดเผยได้ (Public) ไม่กำหนดสิทธิการเข้าถึง

๒.๓ จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๒ ระดับ

(๑) ข้อมูลที่มีระดับความสำคัญมาก

(๒) ข้อมูลที่มีระดับความสำคัญน้อย

๒.๔ การบ่งชี้สารสนเทศ (Labeling of Information)

(๑) *เจ้าของข้อมูล*เป็นผู้จำแนกและกำหนดระดับชั้นความลับของข้อมูล

(๒) ให้มีการกำหนดระดับชั้นการเข้าถึงให้สอดคล้องกับระดับชั้นความลับของข้อมูล

(๓) *เจ้าของระบบสารสนเทศ*ต้องจัดทำป้ายชื่อสำหรับปิดฉลากบนเอกสารข้อมูล หรืออุปกรณ์ที่เป็น*ทรัพย์สินสารสนเทศ*

๒.๕ การถือครอง*ทรัพย์สินสารสนเทศ* (Handing of Assets)

(๑) ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย

(๒) ห้ามเปิดเผยข้อมูลที่มีชั้นความลับแก่ผู้อื่น ยกเว้นกรณีที่การเปิดเผยนั้นถูกครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

(๓) *ผู้ใช้งาน*ต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ใน*เครื่องคอมพิวเตอร์*ของ*ผู้ใช้งาน* โดยเฉพาะอย่างยิ่ง*เครื่องคอมพิวเตอร์*ที่มีการใช้งานร่วมกันกับผู้อื่น ข้อมูลที่มีชั้นความลับจะต้องได้รับการเข้ารหัสข้อมูล

(๔) *ผู้ใช้งาน*ต้องเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในสถานที่จัดเก็บที่สามารถปิดล็อกได้เมื่อไม่ได้ใช้งาน

(๕) ข้อมูลที่มีชั้นความลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร ฯลฯ โดยทันที

(๖) ต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

(๗) สื่อบันทึกข้อมูล และ*เครื่องคอมพิวเตอร์*พกพาต่าง ๆ ที่มีข้อมูลที่มีชั้นความลับบันทึกอยู่ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

๓. การจัดการสื่อบันทึกข้อมูล (Media Handling)

๓.๑ สื่อบันทึกข้อมูลแบบถอดแยกได้ (Removable Media)

(๑) ให้*เจ้าของระบบสารสนเทศ*เป็นผู้พิจารณาอนุญาตให้ใช้งานสื่อบันทึกข้อมูลแบบถอดแยกได้บน*เครื่องคอมพิวเตอร์*ที่ตนดูแลรับผิดชอบ

(๒) ในกรณีที่*เจ้าของระบบสารสนเทศ*อนุญาตให้ใช้งานสื่อบันทึกข้อมูลแบบถอดแยกก่อนการใช้งานสื่อบันทึกข้อมูลแบบถอดแยกต้องได้รับการสแกนไวรัสจากโปรแกรมป้องกันไวรัสที่ได้รับการอัพเดทอยู่เสมอ

(๓) ห้ามใช้งานสื่อบันทึกข้อมูลแบบถอดแยกได้ที่ไม่สามารถระบุเจ้าของหรือแหล่งที่มาได้และให้ส่งมอบแก่*ผู้ดูแลระบบฯ* เพื่อทำการตรวจสอบความมั่นคงปลอดภัย

๓.๒ การทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

(๑) *เจ้าของข้อมูล*เป็นผู้ทำลายข้อมูลบนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

(๒) กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้

ประเภทสื่อบันทึก	นำสื่อบันทึกกลับมาใช้ใหม่	บันทึกข้อมูลที่มีชั้นความลับและนำสื่อบันทึกกลับมาใช้ใหม่	ไม่นำสื่อบันทึกกลับมาใช้ใหม่
CD/DVD	–	–	ใช้การทุบ หรือทำลายให้เสียหาย หรือเผา
สื่อบันทึกข้อมูลแบบมีระบบปฏิบัติการ	ใช้การ Factory Data Reset	– ระบบปฏิบัติการ IOS ใช้การ Factory Data Reset – ระบบปฏิบัติการอื่น ๆ ใช้การลบและเขียนข้อมูลทับจนเต็มพื้นที่จัดเก็บ	ใช้การทุบ หรือทำลายให้เสียหาย หรือเผา
สื่อบันทึกข้อมูลแบบถอดแยกได้	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย หรือเผา
เทปบันทึกข้อมูล	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย หรือเผา
ฮาร์ดไดรฟ์ (Hard Drive)	ใช้วิธีการ Format โดยการเขียนทับข้อมูลเป็นจำนวนหลาย ๆ รอบ	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย หรือเผา
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse	ห้ามนำกลับมาใช้ใหม่	ใช้เครื่องทำลายเอกสารก่อนทิ้ง

(๓) *เจ้าของข้อมูล*ต้องจัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูล และสื่อบันทึกข้อมูลสำคัญและมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

(๔) *เจ้าของข้อมูล*ต้องจัดทำบันทึกรายละเอียดการปฏิบัติงาน (Log) ในการทำลายข้อมูล เพื่อให้สามารถตรวจสอบได้ภายหลัง

๓.๓ การขนย้ายสื่อบันทึกข้อมูล

ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บ*ข้อมูลสารสนเทศ* ให้มีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลดังกล่าว เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือ*ข้อมูลสารสนเทศ*ได้รับความเสียหาย

ส่วนที่ ๔

การควบคุมการเข้าถึง

วัตถุประสงค์

๑. เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึง*ระบบสารสนเทศ*ของ*บริษัท* และสามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งาน*ระบบสารสนเทศ*ของ*บริษัท*ได้อย่างถูกต้อง

๒. เพื่อควบคุมการเข้าถึงของ*ผู้ใช้งาน*เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

๓. เพื่อให้ผู้ปฏิบัติการและ*ผู้ใช้งาน*มีความรับผิดชอบในการป้องกันข้อมูล

๔. เพื่อป้องกันการเข้าถึง*ระบบสารสนเทศ*โดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

๑. *เจ้าของระบบสารสนเทศ*

๒. *เจ้าของข้อมูล*

๓. *ผู้ดูแลระบบฯ*

๔. *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*

๕. *ผู้ดูแลระบบคอมพิวเตอร์*

๖. *ผู้พัฒนาระบบสารสนเทศ*

๗. ผู้ปฏิบัติการและ*ผู้ใช้งาน*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirements of Access Control)

๑.๑ *เจ้าของระบบสารสนเทศ*เป็นผู้อนุญาตและให้สิทธิการเข้าถึง*ระบบสารสนเทศ*แก่*ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ตามเหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของ*ผู้ปฏิบัติการ*และ*ผู้ใช้งาน* รวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ โดยให้ผู้ดูแลจัดการบัญชี*ผู้ใช้งาน*เป็นผู้กำหนดสิทธิการเข้าถึงของ*ผู้ใช้งาน*ใน*ระบบสารสนเทศ*ตามสิทธิการเข้าถึงที่*เจ้าของระบบสารสนเทศ*มอบให้แก่*ผู้ใช้งาน*

๑.๒ การเข้าถึง*ระบบเครือข่าย*และบริการทางเครือข่าย (Access to network and Network services) *ผู้ดูแลระบบเครือข่าย*เป็นผู้ให้สิทธิการเข้าถึง*ระบบเครือข่าย*และบริการทางเครือข่ายแก่*ผู้ใช้งาน*ตามความจำเป็นเท่านั้น

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ การลงทะเบียนและลบบัญชี*ผู้ใช้งาน* (User Registration and De-registration)

(๑) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*สามารถลงทะเบียนได้โดยทันทีเมื่อ*ผู้ใช้งาน*มีสถานะเป็นคณะกรรมการ*บริษัท* และพนักงาน

(๒) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องเปลี่ยนสถานะบัญชี*ผู้ใช้งาน*ที่เป็นคณะกรรมการ*บริษัท* และพนักงาน เมื่อพ้นสภาพแล้วให้มีสถานะห้ามใช้งาน (Disable) ไว้เป็นเวลาอย่างน้อย ๑ ปี และดำเนินการลบบัญชี*ผู้ใช้งาน*ได้ทันทีเมื่อครบกำหนดเวลาดังกล่าว

(๓) ให้*หน่วยงานภายใน*ที่เป็นต้นสังกัดของ*ผู้ใช้งาน*แจ้งข้อมูลการลงทะเบียน*ผู้ใช้งานระบบสารสนเทศ*ต่อ*เจ้าของระบบสารสนเทศ*อย่างเป็นลายลักษณ์อักษร

(๔) *เจ้าของระบบสารสนเทศ*ตรวจสอบข้อมูลการขอลงทะเบียน*ผู้ใช้งาน* และพิจารณาให้สิทธิกับ*ผู้ใช้งาน*ในการเข้าสู่*ระบบสารสนเทศ*เฉพาะในส่วนที่จำเป็นต้องใช้งานตามหน้าที่เท่านั้น

(๕) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*เป็นผู้ลบบัญชี*ผู้ใช้งาน*ระบบตามที่*เจ้าของระบบสารสนเทศ*กำหนด เมื่อ*ผู้ใช้งาน*พ้นจากหน้าที่หรือไม่มีหน้าที่รับผิดชอบใน*ระบบสารสนเทศ*ที่ขอสิทธิในการใช้งาน

๒.๒ การจัดการสิทธิการเข้าถึงของ*ผู้ใช้งาน* (User Access Provisioning)

(๑) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องกำหนดสิทธิการเข้าถึงข้อมูลและ*ระบบสารสนเทศ* ให้เหมาะสมกับหน้าที่ความรับผิดชอบของ*ผู้ใช้งาน*ในการปฏิบัติงานตามการให้สิทธิการเข้าถึง*ระบบสารสนเทศที่เจ้าของระบบสารสนเทศ*ได้กำหนดไว้ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๒) ข้อมูลพื้นฐานที่ใช้ประกอบการควบคุมและจำกัดสิทธิสำหรับ*ผู้ใช้งาน*

๑) ตำแหน่ง

๒) *หน่วยงานภายใน*ที่เป็นต้นสังกัด

๓) คำสั่งมอบหมายงานและหน้าที่รับผิดชอบ (Job Assignment)

๔) สัญญาจ้างงาน (ถ้ามี)

๕) ลายเซ็นอนุมัติจาก*ผู้บังคับบัญชา*ของ*หน่วยงานภายใน*ที่เป็นสังกัดหรือจ้างงาน

(๓) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึง*ระบบสารสนเทศ*การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

(๔) แบ่งประเภทของสิทธิการใช้งาน*ระบบสารสนเทศ* ดังนี้

๑) สิทธิการใช้งาน*ระบบสารสนเทศ*ขั้นพื้นฐาน

ระบบสารสนเทศ	คณะกรรมการบริษัท	พนักงาน	ลูกจ้าง	บุคคลภายนอก
– ระบบ Internet	✓	✓	✓	✓
– ระบบจดหมายอิเล็กทรอนิกส์ (E–mail)	✓	✓		
– เว็บไซต์ home.aerothai.co.th	✓	✓	✓	
– ระบบ File and print sharing	✓	✓		
– เว็บไซต์ www.aerothai.co.th	✓	✓	✓	✓
– ระบบสารบรรณอิเล็กทรอนิกส์		✓		
– ระบบ http://portal.aerothai.co.th		✓		
– ระบบ Wi–Fi	✓	✓	✓	
– ระบบ VPN	✓	✓		

๒) สิทธิการใช้งาน*ระบบสารสนเทศ*ตามภารกิจ ได้แก่ *ระบบสารสนเทศ*อื่นที่นอกเหนือจากข้อ ๑)

(๕) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องกำหนดให้*ผู้ใช้งาน*ที่เป็นพนักงานของ*บริษัท*มีสิทธิการใช้งาน*ระบบสารสนเทศ*ขั้นพื้นฐาน โดยไม่ต้องได้รับอนุมัติจาก*ผู้บังคับบัญชา*ของ*หน่วยงานภายใน*ที่เป็นสังกัดหรือจ้างงาน

(๖) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องกำหนดให้*ผู้ใช้งาน*ใช้งาน*ระบบสารสนเทศ*ได้แต่เพียงที่ได้รับอนุญาตจาก*เจ้าของระบบสารสนเทศ*เท่านั้น

(๗) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องกำหนดบัญชีผู้ใช้งาน แยกกันเป็นรายบุคคลโดยไม่ซ้ำซ้อนกัน และให้ถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของ*ผู้ใช้งาน*ต่อไป

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับ*ผู้ใช้งาน*เพื่อให้มีสิทธิสูงสุด *ผู้ใช้งาน*ต้องได้รับความเห็นชอบและอนุมัติจาก*เจ้าของระบบสารสนเทศ* โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือเมื่อพ้นจากหน้าที่

(๙) ในกรณี*ระบบคอมพิวเตอร์*หรือ*ระบบสารสนเทศ*ที่มีข้อจำกัดเกี่ยวกับบัญชีผู้ใช้งาน ทำให้*ผู้ใช้งาน*ต้องใช้บัญชีผู้ใช้งานร่วมกันและถือ*รหัสผ่าน*ร่วมกัน ให้*เจ้าของระบบสารสนเทศ*เป็นผู้มอบหมายให้*ผู้ใช้งาน*ถือ*รหัสผ่าน*ร่วมกัน

(๑๐) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องไม่อนุญาตให้ผู้ร้องขอใช้*ระบบสารสนเทศ*เข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

(๑๑) *ผู้ใช้งาน*ต้องรับทราบและยอมรับสิทธิและหน้าที่เกี่ยวกับการใช้งาน*ระบบสารสนเทศ* รวมทั้งต้องปฏิบัติตามอย่างเคร่งครัด

๒.๓ การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of Privileged Access Right)

(๑) บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึง*ระบบสารสนเทศ*ในระดับสูง เช่น Root หรือ Administrator หรือเทียบเท่า ต้องได้รับการพิจารณามอบหมายแก่*ผู้ปฏิบัติการ*ตามความจำเป็น และมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

(๒) กรณีมีความจำเป็นต้องให้สิทธิในระดับสูงแก่*ผู้ปฏิบัติการ*หรือ*บุคคลภายนอก* ต้องมีการพิจารณาการควบคุมอย่างรัดกุม โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๑) ต้องได้รับความเห็นชอบและอนุมัติจาก*เจ้าของระบบสารสนเทศ*นั้น ๆ

๒) ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๓) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔) ต้องมีการเปลี่ยน*รหัสผ่าน*หลังเสร็จสิ้นการใช้งาน

๒.๔ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของ*ผู้ใช้งาน* (Management of Secret Authentication Information of Users)

(๑) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องเก็บรักษา*รหัสผ่าน*ของ*ผู้ใช้งาน*ให้เป็นความลับ

(๒) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*กำหนดรูปแบบ*รหัสผ่าน* ให้ต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยต้องมีการผสมกันระหว่างอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข อักขระพิเศษเข้าด้วยกันเพื่อให้ยากต่อการเดา และกำหนดชื่อบัญชีผู้ใช้งานหรือ*รหัสผ่าน*ต้องไม่ซ้ำกัน

(๓) การกำหนด*รหัสผ่าน*ให้กับ*ผู้ใช้งาน*ครั้งแรก ให้*ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*กำหนด*รหัสผ่าน*ชั่วคราวจากการสุ่ม

(๔) การส่งมอบ*รหัสผ่าน*ให้กับ*ผู้ใช้งาน*ในครั้งแรก ให้ใช้วิธีการใส่ซองปิดผนึกหรือกระดาษสลิปคาร์บอนก่อนส่งมอบให้กับ*ผู้ใช้งาน*

(๕) *ผู้ใช้งาน*ต้องตอบยืนยันการได้รับ*รหัสผ่าน*มายัง*ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*

(๖) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*จัดทำระบบที่สามารถให้*ผู้ใช้งาน*เปลี่ยน*รหัสผ่าน*ของตนเองได้ และกำหนดให้เปลี่ยน*รหัสผ่าน*ทุก ๙๐ วัน

(๗) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องกำหนดจำนวนครั้งที่ยอมให้*ผู้ใช้งาน*ใส่*รหัสผ่าน*ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๘) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องกำหนดจำนวนครั้งของการใช้งาน*รหัสผ่าน*ห้ามซ้ำกับ*รหัสผ่าน*เดิมอย่างน้อยจำนวน ๕ ครั้ง

(๙) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องแจ้งเตือนให้*ผู้ใช้งาน*ทราบล่วงหน้าเป็นเวลา ๒ สัปดาห์ก่อนที่*รหัสผ่าน*จะหมดอายุ

๒.๕ การทบทวนสิทธิการเข้าถึงของ*ผู้ใช้งาน* (Review of User Access Rights)

(๑) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ทบทวนสิทธิการเข้าถึงของ*ผู้ใช้งาน*ทุก ๆ ๑ ปี หรือเมื่อเกิดการว่าจ้างงาน การเปลี่ยนแปลงหน้าที่รับผิดชอบ การโยกย้าย*หน่วยงานภายใน* การเกษียณ และการลาออกจากงาน

(๒) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*จัดทำรายการชื่อ*ผู้ใช้งาน*ที่มีสิทธิการเข้าถึง*ระบบสารสนเทศ*แยกตาม*หน่วยงานภายใน* และส่งให้*เจ้าของระบบสารสนเทศ* เพื่อทบทวนสิทธิการเข้าถึงของ*ผู้ใช้งาน*ให้เหมาะสมกับหน้าที่รับผิดชอบ

(๓) *เจ้าของระบบสารสนเทศ*แจ้งรายชื่อ*ผู้ใช้งาน*และสิทธิที่ได้รับจากการทบทวนสิทธิการเข้าถึงแล้วให้กับ*ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*

๒.๖ การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal and Adjustment of Access Rights)

(๑) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องยกเลิก*สิทธิของผู้ใช้งาน*ในการเข้าใช้งาน*ระบบสารสนเทศ*โดยทันที เมื่อสิ้นสุดสภาพการเป็นพนักงาน เกษียณอายุ สิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน หรือเมื่อไม่มีหน้าที่รับผิดชอบใน*ระบบสารสนเทศ*ที่ได้รับสิทธิในการใช้งาน

(๒) *ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน*ต้องปรับเปลี่ยนสิทธิในการเข้าใช้งาน*ระบบสารสนเทศ*ให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ ของ*ผู้ใช้งาน*ที่เกิดขึ้น หรือตามที่ได้รับแจ้งจาก*เจ้าของระบบสารสนเทศ* พร้อมทั้งแจ้ง*ผู้ใช้งาน*ให้ทราบถึงการปรับเปลี่ยนดังกล่าว

๓. หน้าที่ความรับผิดชอบของ*ผู้ปฏิบัติการ*และผู้ใช้งาน (User Responsibilities)

๓.๑ การใช้งาน*รหัสผ่าน*ของ*ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*

(๑) เมื่อ*ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ได้รับ*รหัสผ่าน*ครั้งแรกจาก*ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน* ให้เปลี่ยน*รหัสผ่าน*ของตนเองใหม่ โดยต้องมีความยาวมากกว่าหรือเท่ากับ ๘ ตัวอักษร มีการผสมกันระหว่างอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข อักขระพิเศษเข้าด้วยกันเพื่อให้ยากต่อการเดา

(๒) *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ต้องเปลี่ยน*รหัสผ่าน*ของตนเองทุก ๙๐ วัน และ*รหัสผ่าน*ต้องไม่ถูกใช้งานซ้ำกับ*รหัสผ่าน*เดิมอย่างน้อยจำนวน ๕ ครั้ง

(๓) *รหัสผ่าน*ต้องถูกป้องกันเสมือนเป็นข้อมูลลับ โดยห้าม*ผู้ใช้งาน*เปิดเผยหรือบอกต่อบุคคลอื่น

(๔) *รหัสผ่าน*ต้องไม่ถูกเขียนบนกระดาษ หรือบันทึกในไฟล์อิเล็กทรอนิกส์โดยไม่ได้รับการปกป้องโดยเด็ดขาด หากมีความจำเป็น กระดาษนั้นต้องถูกจัดเก็บในสถานที่ที่ได้รับการควบคุมการเข้าถึง หรือไฟล์นั้นจะต้องได้รับการเข้ารหัสอย่างเหมาะสม

(๕) ห้ามใช้งานคำสั่งช่วยจดจำ*รหัสผ่าน*ของแอพพลิเคชั่นใด ๆ

(๖) *รหัสผ่าน*ที่ใช้ในการเข้าถึงระบบของ*บริษัท* จะต้องแตกต่างจาก*รหัสผ่าน*ที่ใช้เพื่อกิจธุระส่วนตัว

(๗) หากสงสัยว่ามีผู้อื่นล่วงรู้*รหัสผ่าน* หรือ*รหัสผ่าน*ถูกล่วงละเมิด *ผู้ใช้งาน*ต้องแจ้งเหตุไปยัง*ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน* และทำการเปลี่ยน*รหัสผ่าน*ทั้งหมดทันที

๓.๒ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ที่เป็นเจ้าของบัญชีผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Account) ของ*เครื่องคอมพิวเตอร์*และ*ระบบเครือข่าย* เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๓ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนเข้าใช้งาน*ทรัพย์สินสารสนเทศ*หรือ*ระบบสารสนเทศ*ของ*บริษัท* ดังนี้

(๑) *เครื่องคอมพิวเตอร์*ทุกประเภทต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนเข้าถึงระบบปฏิบัติการ

(๒) การใช้งานอินเทอร์เน็ตต้องทำการพิสูจน์ตัวตนทุกครั้ง หรือทำการพิสูจน์ตัวตนเพียงครั้งเดียว จากการเข้าถึง*ทรัพย์สินสารสนเทศ*หรือ*ระบบสารสนเทศ*อื่น ๆ ของ*บริษัท*ก่อนหน้าได้

(๓) *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ต้องทำการล็อคหน้าจอทุกครั้งเมื่อไม่อยู่หน้า*เครื่องคอมพิวเตอร์*

๓.๔ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ต้องตระหนักและระมัดระวังในการใช้งานข้อมูล

๓.๕ ข้อมูลที่เป็นชั้นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของ*หน่วยงานภายใน* ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจาก*เจ้าของข้อมูล*

๓.๖ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*มีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของ*บริษัท* โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต *ผู้ใช้งาน*ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๓.๗ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ต้องป้องกัน ดูแลรักษาไว้ซึ่งความลับความถูกต้อง และความพร้อมใช้งานของข้อมูลที่อยู่ในความรับผิดชอบของตน ตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ

๓.๘ ห้าม*ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*กระทำการ ดังนี้

(๑) ใช้*สินทรัพย์*ของ*บริษัท*เพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของ*บริษัท*

(๒) ใช้*สินทรัพย์*ของ*บริษัท*เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของ*บริษัท*

(๓) ใช้*สินทรัพย์*ของ*บริษัท*เพื่อประโยชน์การประกอบธุรกิจส่วนบุคคล

(๔) กระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดใน*ระบบเครือข่าย*ของ*บริษัท*

(๕) กระทำการรบกวน ทำลาย หรือทำให้*ระบบสารสนเทศ*ของ*บริษัท*หยุดชะงัก

(๖) กระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อใช้ทรัพยากรก็ตาม

(๗) ติดตั้งหรือเชื่อมต่ออุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึง*ระบบสารสนเทศ*ของ*บริษัท* โดยไม่ได้รับอนุญาตจาก*ผู้ดูแลระบบฯ*

(๘) เข้าไปยังศูนย์ข้อมูล (Data Center) โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบฯ

๓.๙ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต และ*ผู้ใช้งาน*ต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น

๓.๑๐ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*ต้องรับผิดชอบดูแลอุปกรณ์หรือ*สินทรัพย์*ของ*บริษัท* เสมือนเป็น*สินทรัพย์*ของตนเอง

๓.๑๑ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*มีหน้าที่รับผิดชอบที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของ*ผู้ใช้งาน*และ*ผู้ปฏิบัติการ*

๓.๑๒ *ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*มีสิทธิในการใช้งาน*สินทรัพย์*และ*ระบบสารสนเทศ*ต่าง ๆ ที่*บริษัท* จัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของ*บริษัท*เท่านั้น ห้ามไม่ให้*ผู้ปฏิบัติการ*และ*ผู้ใช้งาน*นำ*สินทรัพย์*และ*ระบบสารสนเทศ*ต่าง ๆ ของ*บริษัท*ไปใช้ในกิจกรรมที่*บริษัท*ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อ*บริษัท*

๓.๑๓ *ผู้ใช้งาน*พาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) หรือการทำธุรกรรมทางออนไลน์ (Online transaction) ให้ตรวจสอบการใช้งานผ่านช่องทางที่ปลอดภัยและมีการเข้ารหัสตามนโยบายและแนวปฏิบัติฯ ส่วนที่ ๕ การเข้ารหัสข้อมูล ข้อ ๑ การควบคุมการเข้ารหัส (Cryptography Control)

๔. การควบคุมการเข้าถึงระบบ (System and Application Access Control)

๔.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

(๑) สิทธิการเข้าถึงไฟล์ข้อมูลต้องได้รับการควบคุม

(๒) *เจ้าของข้อมูล*ต้องพิจารณาอนุมัติให้สิทธิการเข้าถึงข้อมูลแก่*ผู้ใช้งาน*เท่าที่จำเป็นเท่านั้น

๔.๒ ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความปลอดภัย (Secure Log-on Procedures)

(๑) กำหนดให้มีการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบปฏิบัติการและ*ระบบสารสนเทศ*

(๒) ไม่แสดงข้อมูลของระบบใด ๆ จนกว่าจะทำการเข้าสู่ระบบสำเร็จ

(๓) ไม่แสดงข้อความช่วยเหลือในระหว่างขั้นตอนการเข้าสู่ระบบ

(๔) แสดงข้อความแจ้งเตือนให้ทราบว่า*ระบบสารสนเทศ*สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๕) ตรวจสอบข้อมูลการเข้าสู่ระบบของ*ผู้ใช้งาน*เมื่อเสร็จสิ้นการป้อนข้อมูลทั้งหมดเท่านั้น หากมีข้อผิดพลาดเกิดขึ้น ระบบต้องไม่แสดงข้อมูลการเข้าสู่ระบบทั้งที่ถูกต้องและไม่ถูกต้อง

(๖) จำกัดจำนวนครั้งของการเข้าสู่ระบบไม่สำเร็จให้ไม่เกิน ๓ ครั้ง เพื่อป้องกันการคาดเดาบัญชีผู้ใช้งานและ*รหัสผ่าน*เพื่อเข้าสู่ระบบ

๔.๓ ระบบบริหารจัดการ*รหัสผ่าน* (Password Management System)

ต้องมีระบบบริหารจัดการ*รหัสผ่าน*ที่สามารถให้บริการ*ผู้ใช้งาน*ดำเนินการจัดการด้วยตัวเอง (Self Service) เพื่อให้*รหัสผ่าน*มีคุณภาพ รวมทั้งในกรณีที่*ผู้ใช้งาน*กำหนด*รหัสผ่าน*ไม่เป็นไปตามข้อกำหนดดังกล่าวระบบต้องไม่อนุญาตการใช้*รหัสผ่าน*นั้น พร้อมแจ้งให้*ผู้ใช้งาน*เปลี่ยน*รหัสผ่าน*ใหม่จนกว่าการกำหนด*รหัสผ่าน*จะเป็นไปตามข้อกำหนด

๔.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

(๑) โปรแกรมอรรถประโยชน์สำหรับระบบปฏิบัติการ (OS Utilities Programs) ซึ่งติดตั้งมาพร้อมกับระบบปฏิบัติการอยู่แล้ว ได้แก่ โปรแกรมจัดการไฟล์ (File Explorer) โปรแกรมยกเลิกการติดตั้งโปรแกรม (Uninstaller) โปรแกรมสแกนดิสก์ (Disk scanner) โปรแกรมจัดเรียงพื้นที่จัดเก็บข้อมูลบนฮาร์ดไดรฟ์ (Hard Drive) โปรแกรมรักษาหน้าจอ (Screen saver) เป็นโปรแกรมที่อนุญาตให้*ผู้ใช้งาน*ใช้งานได้

(๒) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องควบคุมการติดตั้งและใช้งานโปรแกรมอรรถประโยชน์อื่น ๆ ซึ่งเป็นโปรแกรมที่ช่วยให้*เครื่องคอมพิวเตอร์*ทำงานได้อย่างมีประสิทธิภาพ เช่น โปรแกรมบีบอัดไฟล์ (File Compression) โปรแกรมไฟร์วอลล์ (Firewall) โปรแกรมป้องกันไวรัส (Antivirus Program) เป็นต้น

๔.๕ การควบคุมการเข้าถึงรหัสต้นฉบับของโปรแกรม (Access Control to Program Source Code)

(๑) *ผู้พัฒนาระบบสารสนเทศ*ต้องจัดเก็บรหัสต้นฉบับ (Source Code) และคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๒) *ผู้พัฒนาระบบสารสนเทศ*ต้องไม่เก็บรหัสต้นฉบับ (Source Code) ของโปรแกรมที่อยู่ระหว่างการทดสอบไว้รวมกับรหัสต้นฉบับ (Source Code) ที่ใช้งานจริง

๔.๖ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลและการควบคุมการติดตั้งซอฟต์แวร์ลงไปยัง*ระบบคอมพิวเตอร์แม่ข่าย*ที่ให้บริการ

(๑) *ผู้ดูแลระบบคอมพิวเตอร์*เป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อ*ระบบคอมพิวเตอร์แม่ข่าย* (Server) ในการแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software)

(๒) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องจัดทำคู่มือปฏิบัติในการตรวจสอบ*ระบบคอมพิวเตอร์แม่ข่าย* และในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานให้*เจ้าของระบบสารสนเทศ*ทราบโดยทันที

(๓) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องเปิดใช้บริการเท่าที่จำเป็นเท่านั้น

(๔) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของ*เครื่องคอมพิวเตอร์แม่ข่าย* ต้องมีการขออนุมัติจาก*เจ้าของระบบสารสนเทศ*ก่อนการดำเนินการ

(๕) ในการทดสอบ*ระบบสารสนเทศ*ก่อนการใช้งานจริง *ผู้พัฒนาระบบสารสนเทศ*

ต้องทำการทดสอบโปรแกรมบน*เครื่องคอมพิวเตอร์แม่ข่าย* ที่*ผู้ดูแลระบบคอมพิวเตอร์*จัดไว้สำหรับการทดสอบเท่านั้น

(๖) ให้*ผู้ดูแลระบบคอมพิวเตอร์*เป็นผู้ติดตั้ง*ระบบสารสนเทศ*ที่ได้จากการพัฒนาลงบน*เครื่องคอมพิวเตอร์แม่ข่าย*เพื่อเปิดให้บริการแก่*ผู้ใช้งาน*

(๗) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับ*ระบบสารสนเทศ*เดิม และขั้นตอนปฏิบัติที่เกี่ยวข้องของ*ระบบสารสนเทศ*ในกรณีที่จำเป็นต้องกลับไปใช้ซอฟต์แวร์เวอร์ชันเก่าเหล่านั้น

(๘) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องเปิดเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

๔.๗ การควบคุมระบบซึ่งไวต่อการรบกวน

(๑) *ผู้ดูแลระบบฯ* ต้องระบุระดับความสำคัญของ*ระบบสารสนเทศ*ซึ่งไวต่อการรบกวนหรือมีผลกระทบสูงต่อ*บริษัท*

(๒) *ผู้ดูแลระบบฯ* ต้องแยกระบบซึ่งไวต่อการรบกวนออกจาก*ระบบสารสนเทศ*อื่น ๆ

(๓) *ผู้ดูแลระบบฯ* ต้องคอยตรวจสอบและป้องกันการมีทรัพยากรที่ไม่เพียงพอของ*ระบบสารสนเทศ*ซึ่งไวต่อการรบกวน

(๔) *ผู้ดูแลระบบฯ* ต้องจัดให้มีระบบเฝ้าระวังการเข้าถึง*ระบบสารสนเทศ*ที่สำคัญโดยผู้ไม่ได้รับอนุญาต

๔.๘ การจำกัดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) เพื่อให้มีความมั่นคงปลอดภัยมากขึ้น สำหรับ*ระบบสารสนเทศ*ที่มีความสำคัญ หรือมีความเสี่ยงสูง ให้ปฏิบัติดังนี้

(๑) *ผู้ดูแลจัดการระบบงาน*ต้องกำหนดให้มีการยุติการใช้งาน*ระบบสารสนเทศ* (Session Time-out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งอย่างน้อย ๑๕ นาที หรือตามความเหมาะสมแก่*ระบบสารสนเทศ*นั้น ๆ

(๒) *ผู้ดูแลจัดการระบบงาน*ต้องจำกัดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งาน*ระบบสารสนเทศ*ที่มีความเหมาะสมแก่*ระบบสารสนเทศ*นั้น

๔.๙ ช่องทางการเข้าถึง*ระบบสารสนเทศ*และข้อมูล

(๑) *ระบบสารสนเทศ*บริการข้อมูลสำหรับประชาชน สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง โดยผ่านอินเทอร์เน็ต

(๒) *ระบบสารสนเทศ*บริการพนักงาน สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง โดยผ่านอินทราเน็ต

(๓) *ระบบสารสนเทศ*สนับสนุนการปฏิบัติงาน (Back office) สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง โดยผ่านอินทราเน็ต

(๔) *ระบบสารสนเทศ*สนับสนุนการเดินอากาศ สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง โดยผ่านเครือข่ายสื่อสารการบินตามที่*บริษัท*กำหนด

ส่วนที่ ๕
การเข้ารหัสข้อมูล

วัตถุประสงค์

๑. เพื่อให้มีการใช้การเข้ารหัสข้อมูลสำหรับรับ–ส่งและจัดเก็บข้อมูลที่เป็นความลับ

๒. เพื่อป้องกันการปลอมแปลง หรือยืนยันความถูกต้องของข้อมูล

ผู้รับผิดชอบ

๑. *ผู้ดูแลระบบฯ*

๒. *ผู้ใช้งาน*

อ้างอิงมาตรฐาน

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. การควบคุมการเข้ารหัส (Cryptography Control)

๑.๑ การใช้งานการเข้ารหัส

(๑) การรับ–ส่งข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่าง*หน่วยงานภายใน*หรือภายนอกสำหรับข้อมูลที่มีระดับชั้นความลับ ได้แก่ ลับที่สุด (Top Secret) ลับมาก (Secret) และลับ (Confidential) ให้ใช้เทคโนโลยีในการเข้ารหัสข้อมูลอิเล็กทรอนิกส์ ได้แก่ Public Key Infrastructure (PKI) และ Secure Socket Layer/Transport Layer Security

(๒) การเก็บข้อมูลหรือไฟล์อิเล็กทรอนิกส์บนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์มีระดับชั้นความลับ ได้แก่ ลับที่สุด (Top Secret) ลับมาก (Secret) และลับ (Confidential) ให้ใช้มาตรฐาน Advance Encryption Standard (AES), Triple DES (3DES) หรือ Blowfish ในการเข้ารหัสข้อมูลอิเล็กทรอนิกส์

๑.๒ การบริหารจัดการกุญแจในการเข้ารหัส (Key Management)

(๑) ต้องมีกระบวนการในการควบคุมเพื่อให้การเข้าถึงกุญแจที่ใช้ในการเข้ารหัสข้อมูลถูกเข้าถึงได้เฉพาะบุคคลที่จำเป็นเท่านั้น และต้องมีการแบ่งแยกหน้าที่การทำงานของบุคคลที่มีสิทธิในการเข้าถึงกุญแจที่ใช้ในการเข้ารหัสข้อมูล โดยการควบคุมนี้จะใช้กับบุคคลใดก็ตามที่มีหน้าที่เกี่ยวข้องกับการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสข้อมูล หรือบุคคลที่มีสิทธิในการเข้าถึงพื้นที่ที่ใช้ในการประมวลผลที่เกี่ยวข้องกับการเข้ารหัสข้อมูล รวมไปถึง Certificate Authority (CA) และ Registration Authority (RA) และผู้ให้บริการอื่น ๆ

(๒) ต้องมีการสำรองข้อมูลของกุญแจที่ใช้ในการเข้ารหัสข้อมูล ไฟล์ และการสำรองข้อมูลการกำหนดค่าของระบบ (Configuration) เพื่อป้องกันการสูญหายของข้อมูลกุญแจที่ใช้ในการเข้ารหัสและ/หรือถอดรหัส

(๓) กุญแจที่ใช้ในการเข้ารหัสข้อมูลที่ถูกจัดเก็บในอุปกรณ์ที่ใช้ในการจัดเก็บใด ๆ หรือ

ในระหว่างการส่งผ่านจะต้องได้รับการเข้ารหัสเสมอ

(๔) กุญแจส่วนตัวที่ใช้ในการเข้ารหัสข้อมูลต้องถูกจัดเก็บให้เป็นความลับและจัดเก็บอย่างมั่นคงปลอดภัยเสมอ

(๕) กุญแจที่ใช้ในการเข้ารหัสกุญแจ (Key-encrypting Key) ต้องเป็นคนละกุญแจกับกุญแจที่ใช้ในการเข้ารหัสข้อมูล (Data-encrypting Key)

(๖) การใช้กุญแจที่มีอายุ (Key Life) ยาวกว่า ๕ ปี ต้องใช้ในเฉพาะกรณีที่จำเป็นเท่านั้น และจะต้องได้รับการอนุมัติจากผู้บริหารระดับสูงที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัยของ*ข้อมูลสารสนเทศ*ก่อน

(๗) การส่งกุญแจถึงผู้รับกุญแจต้องส่งผ่านในช่องทางที่มีความมั่นคงปลอดภัยเสมอ

(๘) อุปกรณ์ที่ใช้ในการสร้างกุญแจต้องได้รับการปกป้องอย่างมั่นคงปลอดภัย ทั้งทางด้านกายภาพและการเข้าถึงอุปกรณ์ดังกล่าว

(๙) กุญแจต้องได้รับการเพิกถอนทันทีเมื่อทราบว่ากุญแจมีความเสี่ยงที่จะก่อให้เกิดการล่วงละเมิดทางด้านความมั่นคงปลอดภัย เช่น เมื่อกุญแจส่วนตัว (Private Key) รั่วไหลไปยังบุคคลอื่น

(๑๐) การเพิกถอนการใช้งานกุญแจต้องมีการแจ้งให้ผู้เกี่ยวข้องกับกุญแจหรือผู้ที่ใช้งานกุญแจทราบ รวมถึงรหัสกุญแจ เหตุผลของการเพิกถอน วันที่และเวลาที่กุญแจถูกเพิกถอน ทั้งนี้การเพิกถอนกุญแจอาจทำโดยการใช้ช่องทางอัตโนมัติ เช่น Online Certificate Revocation List (CRL) เป็นต้น

(๑๑) การกระทำใดๆ ที่เกี่ยวข้องกับกุญแจต้องได้รับการจัดเก็บอย่างมั่นคงปลอดภัยเสมอเพื่อให้สามารถตรวจสอบได้ในภายหลัง

(๑๒) การทำ Archive กุญแจเมื่อไม่มีการใช้งานกุญแจเป็นระยะเวลานาน ต้องใช้วิธีการ Archive ที่มีความมั่นคงปลอดภัยโดยต้องมีการเข้ารหัสกุญแจที่ถูก Archive ด้วยเสมอ

(๑๓) ต้องกำหนดให้มีการทดสอบการเรียกคืนกุญแจที่ถูก Archive (Key Recovery) ไว้ในแผนการทดสอบบริหารความต่อเนื่องทางธุรกิจ

(๑๔) การทำลายกุญแจต้องทำด้วยความระมัดระวังเป็นพิเศษ โดยต้องทำลายด้วยวิธีการทำลายกุญแจแบบมั่นคงปลอดภัย (Secure Deletion) และต้องแน่ใจว่ากุญแจนั้นจะไม่มีความต้องการในการใช้งานถอดรหัสข้อมูลอีกในอนาคต

๑.๓ การใช้งานลายมือชื่ออิเล็กทรอนิกส์แบบเชื่อถือได้

(๑) เจ้าของลายมือชื่อต้องใช้ความระมัดระวังตามสมควรเพื่อมิให้มีการใช้ข้อมูลสำหรับสร้างลายชื่อของตนโดยปราศจากอำนาจหรือไม่ได้รับอนุญาต

(๒) เจ้าของลายมือชื่อต้องรีบแจ้งให้บุคคลที่ตนรู้ว่าจะต้องกระทำการโดยอาศัยลายมือชื่อนั้นโดยเร็ว หากรู้หรือควรรู้ว่าข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสูญหาย ถูกทำลาย ถูกแก้ไข หรือถูกเปิดเผยโดยมิชอบหรือมีความเสี่ยงว่าอาจเกิดเหตุเช่นนั้น

(๓) กรณีมีการออกใบรับรองเพื่อสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์ต้องใช้

ความระมัดระวังตามสมควรในการยืนยันว่าใบรับรองนั้นแสดงรายละเอียดต่าง ๆ ของผู้สร้างลายมือชื่อได้อย่างถูกต้องและครบถ้วนนับตั้งแต่เวลามีการยื่นคำขอใช้บริการเกี่ยวกับใบรับรองจนถึงวันที่ใบรับรองนั้นหมดอายุ

(๔) ผู้ซึ่งอาจกระทำการใด ๆ ซึ่งเชื่อถือใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ ทั้งที่มีหรือไม่มีความผูกพันตามสัญญากับเจ้าของลายมือชื่อหรือผู้ให้บริการใบรับรอง ต้องใช้ความระมัดระวังตามสมควรในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์นั้นหรือในกรณีที่ลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวมีใบรับรองจะต้องตรวจสอบถึงความสมบูรณ์ การพักใช้หรือการเพิกถอนใบรับรอง รวมทั้งตรวจสอบข้อจำกัดใด ๆ ที่เกี่ยวกับใบรับรองดังกล่าวด้วย

ส่วนที่ ๖
การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

วัตถุประสงค์

๑. เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีผลต่อข้อมูลและอุปกรณ์ประมวลผลสารสนเทศของ*บริษัท*

๒. เพื่อป้องกันการสูญหาย ความเสียหาย การขโมย หรือภาวะเป็นอันตรายต่อ*ทรัพย์สินสารสนเทศ*และป้องกันการหยุดชะงักต่อการดำเนินงานของ*บริษัท*

ผู้รับผิดชอบ

๑. *ผู้ดูแลงานอาคารและสถานที่*

๒. *ผู้ดูแลระบบฯ*

๓. *ผู้ใช้งาน*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

๓. ประกาศ*บริษัท* เรื่อง แนวปฏิบัติการรักษาความปลอดภัยด้านกายภาพ (Standard Operating Procedures of Physical Security)

แนวปฏิบัติ

๑. ความมั่นคงปลอดภัยของพื้นที่ปฏิบัติงาน (Secure Areas)

๑.๑ การกำหนดบริเวณหรือพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยทางกายภาพ

(๑) กำหนดให้พื้นที่ศูนย์ข้อมูล พื้นที่จัดเก็บข้อมูล พื้นที่ทำงานของ*ผู้ดูแลระบบฯ* พื้นที่ติดตั้งอุปกรณ์เครือข่าย และพื้นที่ติดตั้ง*อุปกรณ์คอมพิวเตอร์สำหรับผู้ใช้งาน* เป็น*พื้นที่ควบคุมเฉพาะ*

(๒) พื้นที่ขนส่งและส่งมอบ เป็น*พื้นที่ควบคุม*

๑.๒ การควบคุมการเข้า–ออกทางกายภาพ (Physical Entry Controls)

(๑) มาตรการรักษาความปลอดภัยทางกายภาพและมาตรการควบคุมบุคคลผ่านเข้า–ออกของ *พื้นที่ควบคุม* และ*พื้นที่ควบคุมเฉพาะ*ให้เป็นไปตามประกาศ*บริษัท* เรื่อง แนวปฏิบัติการรักษาความปลอดภัยด้านกายภาพ (Standard Operating Procedures of Physical Security)

(๒) กำหนดมาตรการรักษาความปลอดภัยทางกายภาพและมาตรการควบคุมบุคคลผ่านเข้า–ออก พื้นที่ศูนย์ข้อมูล (Data Center) เพิ่มเติมดังนี้

๑) พื้นที่ศูนย์ข้อมูล (Data Center) ต้องมีระบบควบคุมการเข้า–ออก เพื่อพิสูจน์ตัวตนของผู้ใช้พื้นที่ศูนย์ข้อมูล (Data center)

๒) มีระบบบันทึกการเข้า–ออกพื้นที่ศูนย์ข้อมูล (Data Center) และต้องบันทึกเหตุผลและความจำเป็นของการเข้าใช้งาน

๓) กรณี*บุคคลภายนอก*มีความจำเป็นต้องเข้า–ออกพื้นที่ศูนย์ข้อมูล (Data Center) ต้องได้รับอนุญาตจาก*ผู้บังคับบัญชาของผู้ดูแลระบบคอมพิวเตอร์* และ*ผู้ดูแลระบบคอมพิวเตอร์*ต้องอยู่กับ*บุคคลภายนอก*ตลอดระยะเวลาการปฏิบัติงานของ*บุคคลภายนอก*

๔) ห้ามถ่ายภาพ สูบบุหรี่ นำอาหารและเครื่องดื่มเข้ามาในบริเวณศูนย์ข้อมูล (Data Center)

(๓) กำหนดมาตรการการควบคุมการเข้า–ออกทางกายภาพเพิ่มเติมของ*พื้นที่ควบคุม*เฉพาะในส่วนของพื้นที่ติดตั้ง*อุปกรณ์คอมพิวเตอร์*สำหรับ*ผู้ใช้งาน* ดังนี้

๑) *ผู้ใช้งาน*ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาดเว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และ*พื้นที่ควบคุม*ความมั่นคงปลอดภัยโดยบุคคลที่ได้รับอนุญาตไม่สามารถโอนกรรมสิทธิ์หรือหยิบยืมใช้งานแทนกันได้

๒) *ผู้ใช้งาน*ต้องปิดล็อคตู้เซฟ ตู้เอกสาร ลิ้นชัก และตู้อุปกรณ์ต่าง ๆ อย่างเหมาะสม โดยกุญแจที่ปิดล็อคดังกล่าวจะต้องถูกเก็บรักษาไว้อย่างปลอดภัย

๓) *ผู้ใช้งาน*ต้องไม่ทิ้งข้อมูล สื่อบันทึก และอุปกรณ์ที่จัดเก็บข้อมูลลับไว้บนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๔) *ผู้ใช้งาน*ต้องไม่ทิ้งข้อมูล สื่อบันทึก และอุปกรณ์ที่จัดเก็บข้อมูลลับลงในถังขยะโดยไม่ได้รับการทำลายตามส่วนที่ ๓ การบริหารจัดการ*ทรัพย์สินสารสนเทศ* แนวปฏิบัติข้อ ๓.๒ การทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

(๔) กำหนดมาตรการการควบคุมการเข้า–ออกทางกายภาพของ*พื้นที่ควบคุม*ที่เป็นพื้นที่ขนส่งและส่งมอบเพิ่มเติมดังนี้

๑) ผู้ดูแลอาคารและสถานที่ต้องจำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒) จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ *ภายในบริษัท*

๓) ตรวจนับและลงทะเบียนหรือขึ้นบัญชีคุมอุปกรณ์ที่ส่งมอบโดยผู้ถูกจ้าง ผู้ขายหรือผู้ให้บริการภายนอก

๑.๓ การป้องกันภัยพิบัติและภัยคุกคามจากภายนอก (Protecting Against External and Environment) เพื่อประโยชน์ในการรักษาความปลอดภัยสถานที่ติดตั้งและเก็บรักษา*ทรัพย์สินสารสนเทศ* ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ พร้อมทั้งให้ทดสอบระบบรักษาความปลอดภัยภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๑.๔ ต้องจัดให้มีการอบรมแก่บุคลากรที่ปฏิบัติงานภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาอันสมควร เพื่อให้สามารถใช้งานอุปกรณ์รักษาความปลอดภัยได้อย่างถูกต้องและเหมาะสม

๒. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)

๒.๑ การจัดวางและการป้องกันอุปกรณ์ (Equipment Sitting and Protection)

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อให้เกิดความเป็นระเบียบเรียบร้อย และไม่ให้เกิดความเสี่ยงจากความร้อน แสงแดด ฝุ่นละอองและความชื้น

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย

(๓) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มี*ระบบสารสนเทศ*อยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติหรือไม่ เป็นต้น

(๔) ไม่นำอุปกรณ์สารสนเทศ *ข้อมูลสารสนเทศ* หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของ*บริษัท*โดยมิได้รับอนุญาต

๒.๒ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของ*ระบบสารสนเทศ*ที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบ ดังต่อไปนี้

๑) ระบบสำรองกระแสไฟฟ้า (UPS)

๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

๓) ระบบระบายอากาศ

๔) ระบบปรับอากาศ และควบคุมความชื้น

๕) ระบบดับเพลิง

๖) ระบบกล้องวงจรปิด

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือนในพื้นที่สำคัญ เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานมีความผิดปกติหรือหยุดการทำงาน

๒.๓ ความมั่นคงปลอดภัยของสายสื่อสาร (Cabling Security)

(๑) สายเคเบิ้ลที่ต้องวางผ่านเข้าไปในบริเวณที่มี*บุคคลภายนอก*เข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณและป้องกันสัตว์ต่าง ๆ กัดแทะสาย

(๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน

(๓) ทำป้ายชื่อสำหรับสายสัญญาณหัวท้ายและบนอุปกรณ์

(๔) จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๕) ปิดตู้ Rack ให้สนิทอยู่เสมอ

๒.๔ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนดและต้องปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๒) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจสอบในภายหลัง

(๓) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๔) ควบคุมและสอดส่องดูแลการปฏิบัติงานของ*บริษัท*ผู้รับจ้างเหมาบำรุงรักษา*ระบบคอมพิวเตอร์*ที่มาทำการบำรุงรักษาอุปกรณ์ภายใน*บริษัท*

(๕) ควบคุมการส่งอุปกรณ์ที่นำออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือส่งอุปกรณ์ดังกล่าวไปซ่อมบำรุง ทั้งนี้เพื่อเป็นการป้องกันการรั่วไหลของข้อมูล

๒.๕ การนำ*ทรัพย์สินสารสนเทศ*ออกนอกสำนักงาน (Removal of Assets)

(๑) ห้ามนำ*ทรัพย์สินสารสนเทศ*ออกนอกสำนักงาน โดยไม่ได้รับอนุญาต

(๒) ให้มีบันทึกการนำ*ทรัพย์สินสารสนเทศ*ก่อนนำออกนอกสำนักงานและบันทึกการส่งคืน เพื่อเก็บเป็นหลักฐานป้องกันการสูญหาย

๒.๖ ความมั่นคงปลอดภัยของ*ทรัพย์สินสารสนเทศ*นอกสำนักงาน (Security of Equipment and Assets Off-premises)

(๑) ไม่ทิ้งอุปกรณ์หรือ*ทรัพย์สินสารสนเทศ*ของ*บริษัท*ไว้นอกพื้นที่สำนักงานโดยไม่มีผู้ดูแล

(๒) *ผู้ใช้งาน*ต้องรับผิดชอบดูแลอุปกรณ์หรือ*สินทรัพย์*ของ*บริษัท*เสมือนเป็น*สินทรัพย์*ของตนเอง

๒.๗ ความมั่นคงปลอดภัยในการกำจัดหรือนำอุปกรณ์สารสนเทศมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

ผู้ดูแลระบบฯ หรือ*ผู้ใช้งาน*ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ ทั้งนี้เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลดังกล่าว

๒.๘ การป้องกันอุปกรณ์ขณะที่ไม่มี*ผู้ใช้งาน*ที่อุปกรณ์ (Unattended User Equipment)

(๑) *ผู้ใช้งาน*ต้องออกจาก*ระบบสารสนเทศ*โดยทันทีเมื่อเสร็จสิ้นการปฏิบัติงาน และปิด*เครื่องคอมพิวเตอร์*ทุกครั้งเมื่อเสร็จสิ้นการปฏิบัติงานประจำวัน หรือเมื่อไม่มีการใช้งานเกิน ๑ ชั่วโมง

(๒) *ผู้ใช้งาน*ต้องล็อคอุปกรณ์เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

(๓) *ผู้ใช้งาน*ต้องปิดล็อคพื้นที่เพื่อจัดเก็บอุปกรณ์ในสถานที่ปลอดภัยเมื่อไม่มีการใช้งาน

(๔) *ผู้ดูแลระบบคอมพิวเตอร์*และ*ผู้ใช้งาน*ต้องกำหนดให้*เครื่องคอมพิวเตอร์*พักหน้าจอเมื่อไม่มี*ผู้ใช้งาน*นานเกินกว่า ๑๕ นาที และมีการใช้*รหัสผ่าน*ในการเข้าถึงใหม่อีกครั้ง

๒.๙ นโยบายในการจัดระเบียบโต๊ะและหน้าจออุปกรณ์สารสนเทศ (Clear Desk and Clear Screen Policy) *ผู้ใช้งาน*ต้องจัดระเบียบโต๊ะทำงานและหน้าจอ*เครื่องคอมพิวเตอร์*เพื่อลดความเสี่ยงของการเปิดเผยข้อมูลความลับ ดังนี้

(๑) ข้อมูลความลับหรือข้อมูลที่มีความสำคัญที่บันทึกอยู่ในเอกสารในรูปแบบกระดาษหรือที่จัดเก็บในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์ ต้องมีการจัดเก็บอย่างปลอดภัยเมื่อไม่มีความจำเป็นต้องใช้งาน

(๒) ต้องล็อคหน้าจอ*เครื่องคอมพิวเตอร์*ด้วย*รหัสผ่าน* หรือระบบการยืนยันตัวตนอื่นเมื่อไม่ได้ใช้งาน

(๓) ไม่วางเอกสารที่มีชั้นความลับหรือเอกสารสำคัญ ซึ่งสั่งพิมพ์ผ่านเครื่องพิมพ์ทิ้งไว้

ส่วนที่ ๗
ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

วัตถุประสงค์

๑. เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

๒. เพื่อให้ข้อมูลและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

๓. เพื่อป้องกันการสูญหายของข้อมูล

๔. เพื่อให้มีการบันทึกเหตุการณ์และการจัดทำหลักฐาน

๕. เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

๖. เพื่อให้ทราบถึงระดับความเสี่ยงที่อาจเกิดขึ้นกับ*ระบบสารสนเทศ* และระดับความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งจะนำไปสู่การปรับปรุงแก้ไข

ผู้รับผิดชอบ

๑. *เจ้าของระบบสารสนเทศ*

๒. *เจ้าของข้อมูล*

๓. *ผู้ดูแลระบบฯ*

๔. ผู้ตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๕. *ผู้ใช้งาน*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๓. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

๑.๑ ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)

(๑) *ผู้ดูแลระบบฯ* ต้องจัดทำเอกสารวิธีปฏิบัติที่เหมาะสมสำหรับแต่ละ*ระบบสารสนเทศ*ที่อยู่ในความรับผิดชอบของตนและประกาศให้ผู้ปฏิบัติงานทราบ

(๒) *ผู้ดูแลระบบฯ* ต้องปรับปรุงเอกสารวิธีปฏิบัติตามความเหมาะสมต่อสภาวะแวดล้อมการปฏิบัติงาน

(๓) *ผู้ดูแลระบบฯ* มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับ*ระบบสารสนเทศ*ถูกเข้าถึงโดยมิได้รับอนุญาต

๑.๒ การบริหารการเปลี่ยนแปลง (Change Management)

(๑) ก่อนทำการเปลี่ยนแปลงกับ*ระบบสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์* ซอฟต์แวร์ หรือฐานข้อมูล โดย*ผู้ดูแลระบบฯ* หรือผู้ให้บริการภายนอกต้องดำเนินการขออนุมัติการดำเนินการเปลี่ยนแปลงจาก*เจ้าของระบบสารสนเทศ*อย่างเป็นลายลักษณ์อักษร

(๒) การเปลี่ยนแปลงกับ*ระบบเครือข่าย ระบบคอมพิวเตอร์* ซอฟต์แวร์ หรือฐานข้อมูล โดยผู้ให้บริการภายนอกต้องได้รับการควบคุมดูแลจาก*ผู้ดูแลระบบฯ*

(๓) *ผู้ดูแลระบบฯ* ต้องแจ้งให้*ผู้ใช้งาน*ทราบก่อนทุกครั้ง ก่อนทำการเปลี่ยนแปลงระบบ

(๔) *ผู้ดูแลระบบฯ* หรือผู้ให้บริการภายนอกต้องมีการประเมินผลกระทบของการเปลี่ยนแปลงระบบ ก่อนที่จะทำการเปลี่ยนแปลงนั้น เพื่อป้องกันผลกระทบกับการทำงานของระบบที่ใช้ดำเนินงานอยู่ในปัจจุบัน

(๕) *ผู้ดูแลระบบฯ* ต้องบันทึกรายละเอียดการเปลี่ยนแปลง*ระบบสารสนเทศ*

(๖) *ผู้ดูแลระบบฯ* หรือผู้ให้บริการภายนอกต้องมีการทดสอบการเปลี่ยนแปลงนั้นก่อนเสมอ โดยเฉพาะอย่างยิ่งในกรณีเป็น*ระบบสารสนเทศ*ที่สำคัญ

(๗) *ผู้ดูแลระบบฯ* หรือผู้ให้บริการภายนอกต้องกำหนดแผนย้อนคืน (Fallback Plan) เพื่อรองรับหากการเปลี่ยนแปลงไม่เป็นไปตามที่คาดคิด

(๘) *ผู้ดูแลระบบฯ* หรือผู้ให้บริการจากภายนอกต้องกำหนดระยะเวลาในการติดตามการเปลี่ยนแปลงนั้น เพื่อตรวจสอบผลกระทบที่อาจเกิดขึ้นกับระบบหลังจากการเปลี่ยนแปลง

๑.๓ การบริหารจัดการขีดความสามารถของทรัพยากรสารสนเทศ (Capacity Management)

ผู้ดูแลระบบฯ ต้องเฝ้าติดตามสังเกตการใช้งานทรัพยากรสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ เพื่อวางแผนบริหารทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม

๑.๔ การแบ่งแยกสภาพแวดล้อมในการพัฒนา ทดสอบ และปฏิบัติงานจริง (Separation of Development, Testing and Operational Environments)

กำหนดให้มีการแยก*ระบบสารสนเทศ*สำหรับการทดสอบ (Development: DEV) (Quality: QAS) และใช้งานจริง (Production: PRD) ออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลง*ระบบสารสนเทศ*โดยมิได้รับอนุญาต

๒. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection From Malware)

๒.๑ มาตรการป้องกันโปรแกรมไม่พึงประสงค์ (Controls Against Malware)

(๑) *เครื่องคอมพิวเตอร์*ลูกข่าย และ*เครื่องคอมพิวเตอร์*แบบพกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่ได้รับการอัพเดทข้อมูลจาก*เครื่องคอมพิวเตอร์แม่ข่าย*ที่ให้บริการป้องกันไวรัส และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

(๒) *เครื่องคอมพิวเตอร์แม่ข่าย*ที่ให้บริการป้องกันไวรัส ต้องมีการอัพเดทข้อมูลล่าสุดอยู่เสมอ

(๓) *ผู้ใช้งาน*ต้องตรวจสอบไฟล์แนบที่มากับจดหมายอิเล็กทรอนิกส์ (E-mail) หรือไฟล์ที่ได้รับมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๔) ห้าม*ผู้ใช้งาน*สร้าง เก็บ หรือเผยแพร่โปรแกรมไม่ประสงค์ดีเข้าสู่*ระบบคอมพิวเตอร์*ของ*บริษัท*

๓. การสำรองข้อมูล (Backup)

๓.๑ แนวทางปฏิบัติในการคัดเลือกและสำรองข้อมูล

(๑) *เจ้าของระบบสารสนเทศ*และ*เจ้าของข้อมูล*ทำบัญชีรายชื่อของข้อมูลที่มีความสำคัญและปรับปรุงบัญชีรายชื่อให้มีความทันสมัยอยู่เสมอ

(๒) *เจ้าของระบบสารสนเทศ*และ*เจ้าของข้อมูล*กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลไว้อย่างน้อยต้องประกอบด้วยข้อมูลในฐานข้อมูลของ*ระบบสารสนเทศ*หรือไฟล์ข้อมูลที่เกี่ยวข้อง

(๓) *เจ้าของระบบสารสนเทศ*และ*เจ้าของข้อมูล*กำหนดความถี่ในการสำรองข้อมูล

(๔) *ผู้ดูแลระบบฯ* เป็นผู้รับผิดชอบในการสำรองข้อมูลบน*ระบบสารสนเทศ*ตามความถี่ที่กำหนดไว้ และข้อมูลสำหรับตัว*ระบบสารสนเทศ* เช่น ค่า Configuration ของ*ระบบสารสนเทศ* ระบบปฏิบัติการ ซอฟต์แวร์ที่เกี่ยวข้อง เป็นต้น รวมทั้งต้องตรวจสอบความสำเร็จครบถ้วน

๓.๒ แนวปฏิบัติการสำรองข้อมูล

(๑) *ผู้ดูแลระบบฯ* ต้องจัดให้มีการสำรองและทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

(๒) *ผู้ดูแลระบบฯ* ต้องจัดทำบันทึกการสำรองข้อมูล (Operation Logs)

(๓) *ผู้ดูแลระบบฯ* ต้องจัดทำรายงานข้อผิดพลาด (Fault Logging) ที่เกิดจากการสำรองข้อมูล รวมทั้งวิธีการแก้ไข

(๔) กำหนดชนิดและช่วงเวลาของการสำรองข้อมูล พร้อมทั้งสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี ๒ ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Back up) และการสำรองข้อมูลแบบเพิ่มส่วนต่าง (Incremental Backup)

(๕) ในกรณีพบปัญหาทำให้ไม่สามารถสำรองข้อมูลได้อย่างครบถ้วนสมบูรณ์ให้*ผู้ดูแลจัดการระบบงาน*ดำเนินการแก้ไขปัญหา และสรุปผลให้*ผู้บังคับบัญชา*ทราบ

(๖) *ผู้ดูแลระบบฯ* ต้องสำรองข้อมูลตามความถี่ที่*เจ้าของระบบสารสนเทศ*และ*เจ้าของข้อมูล*กำหนดไว้ หรือดังนี้เป็นอย่างน้อย

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูลแบบเต็ม
ระบบ E-mail	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ข้อมูลในส่วน Mail box	๑ ครั้งต่อสัปดาห์
ระบบ Web server	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ข้อมูลบนเว็บที่เผยแพร่	๑ ครั้งต่อเดือน

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูลแบบเต็ม
ระบบ Database server	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ฐานข้อมูลที่มีความสำคัญ	๑ ครั้งต่อวัน
อุปกรณ์ Firewall	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
อุปกรณ์ IPS/IDS	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ข้อมูล Rule ของอุปกรณ์	๑ ครั้งต่อเดือน
อุปกรณ์ Server อื่น ๆ	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ข้อมูลที่มีความสำคัญต่อระบบสารสนเทศนั้น ๆ	๑ ครั้งต่อสัปดาห์

(๗) *ผู้ใช้งานเครื่องคอมพิวเตอร์*ต้องสำรองข้อมูลตามความจำเป็นและเหมาะสมไว้บนสื่อบันทึกอื่น ๆ เป็นประจำทุกเดือน เช่น CD, DVD, External hard drive เป็นต้น

(๘) *ผู้ใช้งานเครื่องคอมพิวเตอร์*ต้องรักษาสื่อบันทึกข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๓.๓ แนวปฏิบัติการกู้คืนระบบ

(๑) ในกรณีพบปัญหาที่อาจสร้างความเสียหายต่อ*ระบบคอมพิวเตอร์*หรือ*ระบบเครือข่าย*จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้*ผู้ดูแลระบบฯ* ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อ*ผู้บังคับบัญชา*หรือผู้ที่ได้รับมอบหมาย

(๒) ให้ใช้ข้อมูลที่ทันสมัยที่สุดที่ได้สำรองไว้ หรือตามความเหมาะสมเพื่อกู้คืนระบบ

(๓) หากความเสียหายที่เกิดขึ้นกับ*ระบบคอมพิวเตอร์*หรือ*ระบบเครือข่าย*กระทบต่อการให้บริการแก่*ผู้ใช้งาน* ให้แจ้ง*ผู้ใช้งาน*ทราบทันทีพร้อมทั้งรายงานความคืบหน้าในการกู้คืนระบบเป็นระยะจนกว่าการดำเนินการจะเสร็จสมบูรณ์

๔. การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

๔.๑ การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)

(๑) *ระบบคอมพิวเตอร์*หรือ*ระบบเครือข่าย*ต้องมีการเก็บบันทึกข้อมูลล็อก ต้องบันทึกข้อมูลกิจกรรมการใช้งานของ*ผู้ใช้งานระบบสารสนเทศ*และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง รวมทั้งให้มีการวิเคราะห์ข้อมูลล็อกดังกล่าวอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดอย่างเหมาะสม

(๒) *ผู้ดูแลระบบฯ* ต้องจัดให้มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งาน*ระบบสารสนเทศ*และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ

(๓) *ผู้ดูแลระบบฯ* ต้องจัดเก็บ*ข้อมูลจราจรทางคอมพิวเตอร์*เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน

๔.๒ การป้องกันข้อมูลล็อก (Protection of Log Information)

*ระบบสารสนเทศ*ที่จัดเก็บข้อมูลล็อก และข้อมูล Log ต้องได้รับการปกป้องเพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต

๔.๓ ข้อมูลล็อกกิจกรรมของ*ผู้ดูแลระบบฯ* (Administrator and Operation Log)

กำหนดให้มีการจัดเก็บข้อมูลล็อกที่เกี่ยวข้องกับการดูแลระบบโดย*ผู้ดูแลระบบฯ*

๔.๔ การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

ผู้ดูแลระบบฯ ตั้งเวลาของ*เครื่องคอมพิวเตอร์*และ*ระบบเครือข่าย*ให้มีเวลาตรงกันทั้งหมด โดยให้อ้างอิงเวลาสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๕. การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)

ผู้ดูแลระบบฯ ต้องควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี ซอฟต์แวร์อุดช่องโหว่ลงใน*เครื่องคอมพิวเตอร์แม่ข่าย*ที่ให้บริการอยู่ โดยต้องมีการทดสอบซอฟต์แวร์เหล่านั้นก่อน เพื่อให้มั่นใจว่าจะไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

๖. การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

๖.๑ *ผู้ดูแลระบบฯ* ต้องอัพเดทระบบซอฟต์แวร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ อย่างสม่ำเสมอ

๖.๒ *ผู้ดูแลระบบฯ* ต้องประเมินความเสี่ยงของช่องโหว่ทางเทคนิค และกำหนดมาตรการเพื่อลดความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๖.๓ *ผู้ดูแลระบบคอมพิวเตอร์*ต้องกำหนดและจำกัดรายการของซอฟต์แวร์ที่ติดตั้งบน*เครื่องคอมพิวเตอร์*ลูกข่าย

๗. การควบคุมกิจกรรมในการตรวจสอบระบบสารสนเทศ (Information Systems Audit Controls)

๗.๑ ผู้ตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศตามแนวทาง ดังนี้

(๑) ให้มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศโดย*เจ้าของระบบสารสนเทศ*

(๒) ให้มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๓) ให้มีการตรวจสอบและประเมินความเสี่ยงของ*ระบบสารสนเทศ*ที่ให้บริการ

(๔) ให้มีการตรวจสอบและประเมินความเสี่ยงอย่างน้อย ๑ ครั้งต่อปี

(๕) ภายหลังการตรวจสอบให้รายงานผลการตรวจสอบและประเมินความเสี่ยงของ*ระบบสารสนเทศ* ต่อ*เจ้าของระบบสารสนเทศ*ทราบต่อไป

(๖) *เจ้าของระบบสารสนเทศ*ที่ได้รับการตรวจสอบและประเมินความเสี่ยง ต้องจัดทำแผนดำเนินการเพื่อบริหารจัดการความเสี่ยงที่ตรวจพบเหล่านั้น

๗.๒ แนวทางในการตรวจสอบและประเมินความเสี่ยงของ*ระบบสารสนเทศ*

(๑) ผู้ตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูล เพื่อให้ผู้ตรวจสอบใช้งาน ซึ่งในระหว่างการใช้งานต้องจัดเก็บสำเนาของข้อมูลนั้นแบบมีการป้องกัน และทำลายสำเนาของข้อมูลนั้นทันทีที่ตรวจสอบเสร็จ

(๓) ต้องมีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(๔) ต้องมีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลแสดงการเข้าถึงนั้น

(๕) ในกรณีที่มีการใช้เครื่องมือสำหรับการตรวจประเมิน*ระบบสารสนเทศ* ต้องแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจาก*ระบบสารสนเทศ*ที่ให้บริการ และต้องมีการป้องกันเครื่องมือตรวจสอบจากการเข้าถึงโดยไม่ได้รับอนุญาต

(๖) ให้มีการป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise)

(๗) กำหนดรายการที่ต้องมีการตรวจประเมินอย่างน้อย ดังนี้

- การป้องกันการบุกรุก*ระบบสารสนเทศ*
- การสำรองข้อมูล
- การควบคุมการเข้าถึงพื้นที่ศูนย์ข้อมูล (Data Center)
- การควบคุมการเข้า–ออกอาคาร
- การเตรียมความพร้อมรับสถานการณ์ฉุกเฉิน
- การเข้าถึง*ระบบสารสนเทศ*
- การกำหนดการใช้งานตามภารกิจ

๗.๓ กำหนดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้การพิจารณาทบทวนดังกล่าวควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

๗.๔ กำหนดให้มีการทบทวนตรวจสอบ*ระบบสารสนเทศ*ในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๘. ข้อตกลงระดับการให้บริการ

๘.๑ *เจ้าของระบบสารสนเทศ*ต้องจัดทำข้อตกลงระดับการให้บริการที่*ผู้ใช้งาน*ยอมรับได้

๘.๒ ข้อตกลงระดับการให้บริการต้องครอบคลุมรายละเอียดดังนี้เป็นอย่างน้อย

(๑) ขอบเขตการให้บริการ

- งานที่ให้บริการ

– สถานที่หรือช่องทางการให้บริการ

– ระยะเวลาที่เปิดให้บริการ

(๒) ข้อกำหนดการให้บริการ

– เอกสารหรือหลักฐานที่ใช้ประกอบการรับบริการ

– ข้อกำหนดอื่น ๆ

(๓) ระดับการให้บริการ

– ด้านระยะเวลา

– ด้านคุณภาพ

(๔) ขั้นตอนการให้บริการ

– ระบุขั้นตอนการให้บริการเรียงตามลำดับก่อนหลัง

(๕) การรับเรื่องร้องเรียน

– ระบุรายละเอียดเกี่ยวกับช่องทางและวิธีการรับเรื่องร้องเรียนจาก*ผู้ใช้งาน*

ส่วนที่ ๘
ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

วัตถุประสงค์

๑. เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ

๒. เพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีการถ่ายโอนกับ*หน่วยงานภายใน*ของ*บริษัท*และถ่ายโอนกับหน่วยงานภายนอก

ผู้รับผิดชอบ

๑. *เจ้าของระบบสารสนเทศ*

๒. *ผู้ดูแลระบบฯ*

๓. *ผู้ดูแลระบบเครือข่าย*

๔. *ผู้ใช้งาน*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๓. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. การบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

๑.๑ การใช้งาน*ระบบเครือข่าย*

(๑) *ผู้ใช้งาน*ต้องใช้บริการ*ระบบเครือข่าย*ตามที่*ผู้ดูแลระบบเครือข่าย*อนุญาตเท่านั้น

(๒) *ผู้ใช้งาน*ต้องใช้*ระบบเครือข่าย*ที่ไม่กระทบต่อประสิทธิภาพการใช้งานเครือข่ายโดยรวม เช่น การรับ-ส่งไฟล์ขนาดใหญ่ การดาวน์โหลดหรืออัพโหลดไฟล์ที่มีขนาดใหญ่ ฟังเพลงออนไลน์ ดูทีวีหรือวีดีโอออนไลน์ เล่นเกมออนไลน์ ในระหว่างเวลาปฏิบัติงาน เป็นต้น

(๓) ห้าม*ผู้ใช้งาน*นำอุปกรณ์เครือข่ายเชื่อมต่อกับ*ระบบเครือข่าย*ของ*บริษัท*ก่อนได้รับอนุญาตจาก*ผู้ดูแลระบบเครือข่าย*

(๔) ห้ามใช้เครือข่ายเพื่อกระทำสิ่งที่ผิดกฎหมาย

(๕) *ผู้ใช้งาน*ต้องเข้าใช้*ระบบเครือข่าย*ด้วยบัญชีผู้ใช้งานของตนเองเท่านั้น

(๖) ห้ามเผยแพร่ข้อมูลของผู้อื่นหรือของ*หน่วยงานภายใน* โดยไม่ได้รับอนุญาต

๑.๒ การควบคุม*ระบบเครือข่าย* (Network Controls)

(๑) *ผู้ดูแลระบบเครือข่าย*ต้องจำกัดการเข้าถึง*ระบบเครือข่าย*และ*ระบบสารสนเทศ*ที่เชื่อมต่ออยู่กับ*ระบบเครือข่าย* โดยกำหนดให้*ผู้ใช้งาน*ในเครือข่ายสามารถเข้าถึง*ระบบสารสนเทศ*ผ่านทาง

*ระบบเครือข่าย*ได้แต่เพียงบริการที่อนุญาตให้เข้าถึงเท่านั้น

(๒) *ผู้ดูแลระบบเครือข่าย*ต้องทดสอบความปลอดภัยทุกครั้งที่จะเชื่อมต่อกับ*ระบบเครือข่าย*ของ*บุคคลภายนอก* เพื่อให้มั่นใจว่าไม่มีการเข้าถึงทรัพยากรที่ไม่ได้รับอนุญาต

(๓) *ผู้ดูแลระบบเครือข่าย*ต้องควบคุมไม่ให้มีการเปิดให้บริการบน*ระบบเครือข่าย*โดยไม่ได้รับอนุญาต

(๔) การเข้าถึงอุปกรณ์เครือข่ายเพื่อการตรวจสอบและปรับแต่งระบบทั้งทางกายภาพและการเข้าถึงจากระยะไกลต้องมีการควบคุม และทำได้เพียงแต่เฉพาะ*ผู้ดูแลระบบเครือข่าย*ที่ได้รับอนุญาตเท่านั้น

(๕) ในกรณีที่ต้องกำหนดสิทธิการเข้าถึงแบบชั่วคราวแก่*บุคคลภายนอก ผู้ดูแลระบบเครือข่าย*ต้องให้มีผู้ควบคุม ตรวจสอบและยกเลิกสิทธิการเข้าถึงทันทีที่ปฏิบัติงานเสร็จ

(๖) *ผู้ดูแลระบบเครือข่าย*ต้องกำหนดค่าเริ่มต้นพื้นฐานของทุก*ระบบเครือข่าย*ต้องเป็นอนุญาตบางส่วนและปฏิเสธทั้งหมด (Permit any & Deny all)

(๗) *ผู้ดูแลระบบเครือข่าย*ต้องตรวจสอบและปิดพอร์ตของอุปกรณ์เครือข่ายที่ไม่ใช้งาน

(๘) การให้บริการทางเครือข่ายสำหรับ*เครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบเครือข่าย*ต้องอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

(๙) *เครื่องคอมพิวเตอร์แม่ข่าย*ที่ให้บริการ*ระบบสารสนเทศ*ต่าง ๆ ต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

(๑๐) *ผู้ดูแลระบบเครือข่าย*ต้องตรวจสอบ Security Log เพื่อค้นหา Invalid Attempt Access ของผู้บุกรุกและตรวจสอบ Fault Alarm Log เพื่อการตรวจสอบปัญหาที่เกิดขึ้นประจำวัน

(๑๑) *ผู้ดูแลระบบเครือข่าย*ต้อง Update Security Patch ของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ

(๑๒) *ผู้ดูแลระบบเครือข่าย*ต้องจัดทำบันทึกสรุปการเกิดปัญหากับ*ระบบเครือข่าย*และแนวทางแก้ไข

(๑๓) *ผู้ดูแลระบบเครือข่าย*ต้องสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์เครือข่ายเป็นประจำหรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

(๑๔) *ผู้ดูแลระบบเครือข่าย*ต้องจัดทำแผนผังเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของ*ระบบเครือข่าย*ภายใน*บริษัท* พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๕) *ผู้ดูแลระบบเครือข่าย*ต้องตั้งชื่ออุปกรณ์เครือข่ายให้เป็นไปตามมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนด

(๑๖) *ผู้ดูแลระบบเครือข่าย*ต้องจัดเก็บ*ข้อมูลจราจรทางคอมพิวเตอร์*ให้สอดคล้องกับกฎหมาย

(๑๗) ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับ*ระบบสารสนเทศ*โดยอัตโนมัติ (Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริง

หรือจากสถานที่ที่กำหนดไว้เท่านั้น ทั้งนี้ จำเป็นสำหรับการที่*ระบบสารสนเทศ*จะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ที่ได้รับอนุญาตหรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาต

๑.๓ การแบ่งแยก*ระบบเครือข่าย* (Segregation in Networks) กำหนดให้มีการแบ่งแยก*ระบบเครือข่าย*ตามกลุ่มบริการสารสนเทศ *ผู้ใช้งาน* และระบบ ดังนี้เป็นอย่างน้อย

(๑) กลุ่มที่ให้บริการสารสนเทศ เป็น*ระบบเครือข่าย*ที่สามารถเข้าถึงและใช้งานโดย*ผู้ใช้งาน* เช่น ระบบอินทราเน็ต ระบบจดหมายอิเล็กทรอนิกส์ เป็นต้น

(๒) กลุ่มที่ให้บริการ*ระบบสารสนเทศ* เป็น*ระบบเครือข่าย*ที่เข้าถึงและใช้งานโดย*ระบบสารสนเทศ* ซึ่งต้องไม่ถูกเข้าถึงจาก*ผู้ใช้งาน*โดยตรง เช่น ระบบฐานข้อมูล ระบบ Directory Service ระบบ Domain Name System (DNS) ระบบ Printer Service เป็นต้น

(๓) กลุ่มที่ให้บริการ*ผู้ใช้งาน* เป็นเครือข่ายที่สามารถเข้าถึงและใช้งานโดย*เครื่องคอมพิวเตอร์*ของ*ผู้ใช้งาน*

(๔) กลุ่มที่ให้บริการ*ผู้ใช้งาน*แบบไร้สาย เป็นเครือข่ายสามารถเข้าถึงและใช้งานโดย*เครื่องคอมพิวเตอร์*พกพา แท็บเล็ต และสมาร์ทโฟนของ*ผู้ใช้งาน*

๑.๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(๑) วิธีการใด ๆ ที่สามารถเข้าถึงข้อมูลหรือ*ระบบสารสนเทศ*ได้จากระยะไกลต้องกำหนดให้มีการพิสูจน์ตัวตน*ผู้ใช้งาน*ก่อนเข้าใช้งาน

(๒) *เจ้าของระบบสารสนเทศ*เป็นผู้ให้สิทธิให้*ผู้ใช้งาน*เข้าสู่ระบบจากระยะไกลตามความจำเป็นเท่านั้น

(๓) *ผู้ดูแลระบบฯ* ต้องควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๔) *ผู้ดูแลระบบฯ* ต้องตรวจสอบความมั่นคงปลอดภัยการเข้าใช้งานระบบจากระยะไกลอย่างสม่ำเสมอ

๑.๕ การตรวจสอบการโจมตีระบบ (Detection of attacks of system)

(๑) *ผู้ดูแลระบบฯ* ต้องจัดให้มีการใช้งานซอฟต์แวร์สำหรับการตรวจสอบการโจมตี*ระบบสารสนเทศ* (Intrusion Prevention/Detection System)

(๒) *ผู้ดูแลระบบฯ* ต้องจัดให้มีการเฝ้าระวังการโจมตีการทำงานของ*ระบบสารสนเทศ*อย่างต่อเนื่อง

๒. การถ่ายโอนข้อมูลสารสนเทศ (Information Transfer)

๒.๑ นโยบายและขั้นตอนปฏิบัติสำหรับการโอนถ่ายข้อมูล (Information Transfer Policies and Procedures)

(๑) การรับ–ส่งข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่าง*หน่วยงานภายใน*หรือภายนอก*บริษัท*ต้องได้รับการเข้ารหัสข้อมูลตามนโยบายและแนวปฏิบัติฯ ส่วนที่ ๕ การเข้ารหัสข้อมูล ข้อ ๑ การควบคุมการเข้ารหัส (Cryptography Control)

(๒) กำหนดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลหรือไฟล์อิเล็กทรอนิกส์ระหว่าง*หน่วยงานภายใน*กับบุคคลหรือหน่วยงานภายนอก

(๓) กำหนดให้มีข้อตกลงในการรักษาความลับหรือไม่เปิดเผยความลับอย่างเป็นลายลักษณ์อักษร กับผู้ให้บริการภายนอก

ส่วนที่ ๙

การจัดหา การพัฒนา และการบำรุงรักษาระบบ

วัตถุประสงค์

๑. เพื่อให้เป็นความมั่นคงปลอดภัยด้านสารสนเทศเป็นข้อกำหนดสำคัญในการจัดหา การพัฒนาและการบำรุงรักษา*ระบบสารสนเทศ*

๒. เพื่อให้มีการทดสอบ*ระบบสารสนเทศ*ตามข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑. *เจ้าของระบบสารสนเทศ*

๒. *ผู้ดูแลระบบคอมพิวเตอร์*

๓. *ผู้พัฒนาระบบสารสนเทศ*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. ความต้องการด้านความมั่นคงปลอดภัยระบบสารสนเทศ (Security Requirements of Information Systems)

๑.๑ กำหนดให้มีเกณฑ์การตรวจรับ*ระบบสารสนเทศ*ที่มีการปรับปรุง หรือที่มีเวอร์ชันใหม่ และควรมีการทดสอบ*ระบบสารสนเทศ*ทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ

๑.๒ กำหนดให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยของ*ระบบสารสนเทศ*ในการจัดทำข้อกำหนดขั้นต่ำของ*ระบบสารสนเทศ*ใหม่ หรือการปรับปรุง*ระบบสารสนเทศ*เดิม

๑.๓ *ข้อมูลสารสนเทศ*ที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของ*ข้อมูลสารสนเทศ*

๑.๔ กำหนดให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

๑.๕ ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์

๒. กระบวนการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย (Security in Information System Development)

๒.๑ มีการแยก*ระบบสารสนเทศ*สำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลง*ระบบสารสนเทศ*โดยมิได้รับอนุญาต

๒.๒ การทบทวนการทำงานของ*ระบบสารสนเทศ*ภายหลังจากปรับปรุงหรือเปลี่ยนแปลงระบบปฏิบัติการของ*เครื่องคอมพิวเตอร์แม่ข่าย*ที่ให้บริการ

(๑) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องแจ้งให้ผู้ที่เกี่ยวข้องกับ*ระบบสารสนเทศ*รับทราบเกี่ยวกับการปรับปรุงหรือเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการปรับปรุงหรือเปลี่ยนแปลงระบบปฏิบัติการ

(๒) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องวางแผนดำเนินการปรับปรุงหรือเปลี่ยนแปลงระบบปฏิบัติการของ*ระบบสารสนเทศ*ก่อนเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

(๓) *ผู้ดูแลระบบคอมพิวเตอร์*ต้องทดสอบโปรแกรมระบบ (System Software) ที่มีความสำคัญ และประสิทธิภาพการใช้งานโดยทั่วไป หลังจากการแก้ไข หรือบำรุงรักษาระบบด้วย

๒.๓ จำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software Package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด

๒.๔ เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ *ผู้ดูแลระบบคอมพิวเตอร์*และ*ผู้พัฒนาระบบสารสนเทศ*จะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

๒.๕ ในการทำสัญญาว่าจ้างการพัฒนา*ระบบสารสนเทศ* ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้งานระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนา*ระบบสารสนเทศ*

๒.๖ การทดสอบด้านความมั่นคงปลอดภัยของ*ระบบสารสนเทศ* (System Security Testing)

(๑) *ผู้พัฒนาระบบสารสนเทศ*ต้องมีการตรวจสอบข้อมูลนำเข้า*ระบบสารสนเทศ*

(๒) *ผู้พัฒนาระบบสารสนเทศ*ต้องมีวิธีการตรวจสอบการประมวลผล*ข้อมูลสารสนเทศ* (Checks and Controls) ว่ามีข้อผิดพลาดหรือไม่

(๓) *ผู้พัฒนาระบบสารสนเทศ*ต้องมีวิธีการตรวจสอบการส่งข้อมูลใน*ระบบสารสนเทศ*เพื่อให้แน่ใจว่าข้อมูลใน*ระบบสารสนเทศ*มีความปลอดภัยและมีความถูกต้องสมบูรณ์

๒.๗ การทดสอบระบบเพื่อรับรอง*ระบบสารสนเทศ* *ผู้พัฒนาระบบสารสนเทศ*ต้องมีขั้นตอนการตรวจสอบ ทดสอบและประมวลผล เพื่อให้มั่นใจว่าระบบสามารถใช้ได้จริงและมีผลลัพธ์ที่ถูกต้อง

๒.๘ ห้ามมิให้ใช้ข้อมูลในระบบที่ใช้ปฏิบัติงานจริงที่ประกอบด้วย ข้อมูลส่วนบุคคลหรือข้อมูลที่มีชั้นความลับ ในการทดสอบระบบใด ๆ ทั้งนี้ หากมีความจำเป็นต้องใช้ข้อมูลเหล่านี้ จะต้องได้รับอนุญาตจาก*เจ้าของข้อมูล*ก่อน และต้องมีมาตรการในการป้องกันการทำสำเนาข้อมูลโดยไม่ได้รับอนุญาต รวมถึงมีขั้นตอนในการยืนยันตัวตนและทำการบันทึกไว้เป็นหลักฐานนำข้อมูลที่ใช้ปฏิบัติงานจริงไปใช้ในการทดสอบ

๒.๙ การพัฒนา*ระบบสารสนเทศ*ที่มีการใช้งาน Mobile Code ต้องมีการตั้งค่าการทำงานเพื่อให้มั่นใจได้ว่าการทำงานของ Mobile code นั้นมีความมั่นคงปลอดภัยด้านสารสนเทศที่เพียงพอ หาก*ระบบสารสนเทศ*ดังกล่าวไม่มีการใช้งาน Mobile Code ต้องการตั้งค่าการทำงาน (Configuration) โดยห้ามมิให้ Mobile code สามารถทำงานได้โดยอัตโนมัติ

ส่วนที่ ๑๐
ความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอก

วัตถุประสงค์

๑. เพื่อให้มีการป้องกัน*ทรัพย์สินสารสนเทศ*ของ*บริษัท*ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

๒. เพื่อกำหนดแนวทางการคัดเลือกผู้ให้บริการภายนอกอย่างเหมาะสม

ผู้รับผิดชอบ

๑. *เจ้าของระบบสารสนเทศ*

๒. *ผู้ดูแลระบบคอมพิวเตอร์*

๓. *ผู้พัฒนาระบบสารสนเทศ*

อ้างอิงมาตรฐาน

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. ความมั่นคงปลอดภัยของการทำงานร่วมกับผู้ให้บริการภายนอก

๑.๑ กำหนดให้มีเจ้าหน้าที่ผู้ควบคุมงานเพื่อคอยกำกับดูแลการดำเนินงานต่าง ๆ ของผู้ให้บริการภายนอก ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

๑.๒ กำหนดให้ผู้ให้บริการภายนอกต้องรับทราบและปฏิบัติตามระเบียบ นโยบาย แนวปฏิบัติ ขั้นตอนการปฏิบัติงานและวิธีการปฏิบัติงานต่าง ๆ ของ*บริษัท*อย่างเคร่งครัด

๑.๓ ผู้ให้บริการภายนอกต้องติดบัตรผู้มาติดต่อตลอดเวลาที่ปฏิบัติงานในพื้นที่

๑.๔ ผู้ให้บริการภายนอกทุกคน ต้องรักษาข้อมูลต่าง ๆ ที่ได้รับทราบระหว่างการปฏิบัติงานให้แก่*บริษัท*ไว้เป็นความลับ และอนุญาตให้ใช้ข้อมูลเพื่อการปฏิบัติงานให้กับทาง*บริษัท*เท่านั้น ห้ามมิให้ทำการเปิดเผยต่อบุคคลอื่นก่อนได้รับอนุญาตจากทาง*บริษัท*อย่างเป็นลายลักษณ์อักษร

๑.๕ กรณีที่ผู้ให้บริการภายนอกมีความจำเป็นต้องขอใช้งานข้อมูลสำคัญของ*บริษัท* ให้ทำการแจ้งต่อพนักงานที่เป็นผู้ติดต่อประสานงานเพื่อขออนุญาตใช้งานข้อมูลจาก*เจ้าของข้อมูล*หรือผู้มีอำนาจ โดยผู้ให้บริการภายนอกได้รับอนุญาตให้ใช้งานข้อมูลเท่าที่จำเป็นต้องรับรู้หรือใช้เพื่อการปฏิบัติงานเท่านั้น

๑.๖ ผู้ให้บริการภายนอกต้องแจ้งรายชื่อของเจ้าหน้าที่ที่จะเข้าปฏิบัติงานต่อ*บริษัท*ก่อนเริ่มการปฏิบัติงาน และหากมีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน หรือมีการเปลี่ยนแปลงตำแหน่งหน้าที่ที่อาจส่งผลกระทบต่อ*บริษัท* ต้องแจ้งให้ทาง*บริษัท*ทราบล่วงหน้าทุกครั้ง

๑.๗ ผู้ให้บริการภายนอกสามารถนำอุปกรณ์สารสนเทศส่วนบุคคล เช่น คอมพิวเตอร์พกพา เข้าใช้งานในพื้นที่สำนักงานของ*บริษัท*ได้โดยห้ามเชื่อมต่อกับ*ระบบเครือข่าย*หรือ*ระบบคอมพิวเตอร์*ภายในของ*บริษัท* กรณีที่มีความจำเป็นต้องเชื่อมต่อเพื่อการปฏิบัติงานต้องแจ้งความจำนงต่อพนักงานที่เป็นผู้ติดต่อประสานงาน เพื่อดำเนินการขออนุมัติจากตามขั้นตอนของ*บริษัท*

๑.๘ ห้ามผู้ให้บริการภายนอกนำสื่อบันทึกข้อมูลใด ๆ มาเชื่อมต่อกับอุปกรณ์สารสนเทศภายในพื้นที่สำนักงานของ*บริษัท*ด้วยตนเอง หากมีความจำเป็นต้องถ่ายโอนข้อมูลให้ดำเนินการโดยพนักงานที่เป็นผู้ติดต่อประสานงานเท่านั้น

๑.๙ หากผู้ให้บริการภายนอกมีความจำเป็นต้อง เข้าใช้งาน*ระบบสารสนเทศ*ของ*บริษัท*เข้าปฏิบัติงานใน*พื้นที่ควบคุม*เฉพาะ ต้องแจ้งความจำนงต่อพนักงานที่เป็นผู้ติดต่อประสานงาน เพื่อดำเนินการขออนุมัติตามความเหมาะสม โดย*บริษัท*จะอนุญาตให้สามารถเข้าใช้งานได้ตามความจำเป็นเท่านั้น ทั้งนี้ เจ้าหน้าที่จากผู้ให้บริการภายนอกต้องให้ความร่วมมือกับ*บริษัท*ในการตรวจสอบอุปกรณ์ที่นำเข้าใช้งานอย่างเหมาะสม

๑.๑๐ ผู้ให้บริการภายนอกต้องไม่นำเอกสารหรือซอฟต์แวร์ที่มีลิขสิทธิ์ของ*บริษัท* ไปใช้งานส่วนตัวหรือใช้งานในทางที่ผิด และห้ามมิให้นำเอกสารหรือซอฟต์แวร์ที่ไม่มีลิขสิทธิ์มาใช้งานใน*บริษัท*

๑.๑๑ ในการปฏิบัติงาน หากผู้ให้บริการภายนอกต้องการติดตั้งโปรแกรมปรับแต่ง*ระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย* หรือกระทำการใด ๆ ที่ก่อให้เกิดความเปลี่ยนแปลงต่อ*ระบบสารสนเทศ*ของ*บริษัท* ต้องแจ้งต่อพนักงานผู้ติดต่อประสานงานเพื่อดำเนินการขออนุมัติ*ผู้ดูแลระบบฯ* ก่อนดำเนินการทุกครั้ง

๑.๑๒ ห้ามผู้ให้บริการภายนอกทำการสแกน*ระบบเครือข่าย*ดักฟังข้อมูลบน*ระบบเครือข่าย*หรือพยายามเข้าถึง*ระบบสารสนเทศ*ของ*บริษัท*โดยไม่ได้รับอนุญาต

๑.๑๓ ผู้ให้บริการภายนอกที่มีการจ้างช่วงงานต่อให้ Subcontractor ต้องแจ้งให้ทาง*บริษัท*ทราบทุกครั้ง และต้องดำเนินการให้ Subcontractor ลงนามใน “ข้อตกลงการไม่เปิดเผยข้อมูล Non Discloser Agreement (NDA)” และปฏิบัติตามสัญญาที่ผู้ให้บริการภายนอกได้ทำไว้กับ*บริษัท*

๑.๑๔ ผู้ให้บริการภายนอกต้องไม่นำบุคคลอื่นที่ไม่เกี่ยวข้อง เข้ามาในพื้นที่*บริษัท*โดยไม่ได้รับอนุญาต

๑.๑๕ ห้ามผู้ให้บริการภายนอกทำการถ่ายรูป หรือ บันทึกเสียง ภายในพื้นที่*บริษัท*ก่อนได้รับอนุญาต

๑.๑๖ ขณะปฏิบัติงานหากพบว่ามีสิ่งผิดปกติใด ๆ เกิดขึ้น ผู้ให้บริการภายนอกต้องรายงานให้พนักงานที่เป็นผู้ติดต่อประสานงานทราบทันที

๑.๑๗ *บริษัท*สงวนสิทธิ์ในการตรวจสอบการทำงานของผู้ให้บริการภายนอกรวมถึงการเพิกถอนสิทธิต่าง ๆ ในการเข้าใช้ข้อมูลและ*ระบบสารสนเทศ* เมื่อพบสิ่งผิดปกติหรือมีเหตุกระทบด้านความมั่นคง (Security Violation) โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

๑.๑๘ ผู้ให้บริการภายนอกต้องปฏิบัติงานตามขอบเขตและหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย หรือที่ระบุไว้ในสัญญาเท่านั้น

๑.๑๙ ผู้ให้บริการภายนอกต้องปฏิบัติงานด้วยความระมัดระวัง เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อ*บริษัท*

๑.๒๐ การกระทำใด ๆ ของผู้ให้บริการภายนอกที่ก่อให้เกิดความเสียหายหรือละเมิดข้อตกลง

หรือสัญญาต่าง ๆ ที่ได้ทำไว้กับ*บริษัท* ผู้ให้บริการภายนอกต้องรับผิดชอบต่อความเสียหายทั้งหมด

๑.๒๑ ในวันสุดท้ายของการปฏิบัติงานตามข้อตกลงหรือสัญญา ผู้ให้บริการภายนอกต้องทำการส่งคืนทรัพย์สินต่าง ๆ เช่น กุญแจ อุปกรณ์ต่าง ๆ และรหัสเข้าระบบ ให้แก่พนักงาน ผู้ติดต่อประสานงานอย่างครบถ้วน

๑.๒๒ กรณีที่ผู้ให้บริการภายนอกมีการดำเนินการเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อการให้บริการตามข้อตกลงหรือสัญญา ผู้ให้บริการภายนอก ต้องแจ้งต่อทาง*บริษัท*อย่างเป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย ๗ วัน เพื่อให้*บริษัท*ทำการพิจารณา วิเคราะห์ผลกระทบและหาวิธีในการแก้ไขควบคุมความเสี่ยงได้อย่างเหมาะสม

๒. การคัดเลือกผู้ให้บริการภายนอก

๒.๑ การคัดเลือกผู้ให้บริการภายนอกอย่างเหมาะสมก่อนที่จะทำสัญญาใหม่หรือทบทวนเพื่อต่ออายุสัญญาการใช้บริการจากผู้ให้บริการภายนอก จะพิจารณาให้ครอบคลุมประเด็นสำคัญอย่างน้อย ดังต่อไปนี้

(๑) ความสามารถทางด้านเทคนิค ความเชี่ยวชาญ และประสบการณ์ในการดำเนินงาน

(๒) สถานะความมั่นคงทางการเงิน

(๓) ชื่อเสียงทางธุรกิจ ประวัติการถูกร้องเรียน หรือถูกฟ้องร้องดำเนินคดี

(๔) วัฒนธรรมองค์กรและนโยบายการให้บริการที่มีความเหมาะสมกับ*บริษัท*

(๕) ความสามารถในการปรับตัวตอบสนองพัฒนาการใหม่ ๆ

(๖) ความเสี่ยงในกรณีที่ผู้ให้บริการภายนอกไม่สามารถให้บริการได้

๒.๒ สัญญาและข้อตกลง *บริษัท*กำหนดให้การทำสัญญาและข้อตกลงระหว่าง*บริษัท*กับผู้ให้บริการภายนอกเป็นลายลักษณ์อักษรโดยต้องพิจารณาให้ครอบคลุมประเด็นดังต่อไปนี้เป็นอย่างน้อย

(๑) กำหนดรายละเอียดและประเภทของการใช้บริการ ขอบเขตความรับผิดชอบการบริหารความเสี่ยง ระบบควบคุมภายใน ระบบรักษาความปลอดภัยในการเก็บรักษาข้อมูล และทรัพย์สินของ*บริษัท*

(๒) ข้อตกลงการให้บริการ (Service Level Agreement) เพื่อกำหนดเป็นมาตรฐานการให้บริการขั้นต่ำที่ผู้ให้บริการภายนอกต้องปฏิบัติ ทั้งภายใต้สถานการณ์ปกติและไม่ปกติ

(๓) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ของผู้ให้บริการภายนอก เพื่อรองรับกรณีงานที่ใช้บริการจากผู้ให้บริการภายนอกมีปัญหาหยุดชะงักลงและไม่สามารถให้บริการได้อย่างต่อเนื่อง

(๔) ขั้นตอนการติดตาม ตรวจสอบ และประเมินประสิทธิภาพการปฏิบัติงานของผู้ให้บริการภายนอก (Outsource)

(๕) การกำหนดค่าบริการระหว่างคู่สัญญา ต้องมีความสมเหตุสมผลอ้างอิงจากต้นทุนหรืออัตราที่เรียกเก็บกันในตลาดทั่วไป โดยต้องไม่เป็นการเอื้อประโยชน์จนเกินสมควรแก่เหตุให้แก่บุคคล

หรือนิติบุคคลอื่นทั้งในและนอกกลุ่มธุรกิจ

(๖) อายุสัญญา ข้อกำหนด และเงื่อนไขการยกเลิกสัญญา ซึ่งรวมถึงสิทธิของ*บริษัท*ในการเปลี่ยนแปลงแก้ไขและต่ออายุสัญญา ทั้งนี้ เพื่อให้มีความคล่องตัวในการปรับปรุงการให้บริการหากจำเป็น รวมทั้งเพื่อไม่ให้เป็นอุปสรรคต่อการดำเนินงานของ*บริษัท*ในอนาคต

(๗) ขอบเขตความรับผิดชอบของคู่สัญญาในกรณีการให้บริการเกิดปัญหาขัดข้อง เช่น การบริการล่าช้า และความผิดพลาดในการให้บริการ เป็นต้น ตลอดจนแนวทางแก้ไขปัญหาต่าง ๆ หรือการชดใช้ค่าเสียหายที่เกิดขึ้น

(๘) การรักษาความปลอดภัยของข้อมูล การรักษาความลับ และความเป็นส่วนตัวของข้อมูลของ*บริษัท*รวมถึงสิทธิในการเข้าถึง และความเป็น*เจ้าของข้อมูล* บทลงโทษอย่างชัดเจน หากมีการเปิดเผยข้อมูลสำคัญของ*บริษัท*ตลอดจนความต้องการด้านความมั่นคงปลอดภัยอื่น ๆ

(๙) เงื่อนไขในการอนุญาตให้ผู้ให้บริการภายนอกจะมอบหมายหรือว่าจ้างผู้ให้บริการภายนอกรายอื่นรับจ้างช่วงงานต่อ (Subcontract) ในบางส่วนหรือทั้งหมดของงานที่รับว่าจ้าง โดยผู้ให้บริการภายนอกที่รับช่วงต่อมานั้น ยังคงต้องถือปฏิบัติตามหลักเกณฑ์เงื่อนไขต่าง ๆ ที่ได้ตกลงกับ*บริษัท*ไว้

(๑๐) ต้องปฏิบัติตามกฎเกณฑ์ของรัฐที่เกี่ยวข้อง

(๑๑) กำหนดสิทธิให้*บริษัท*ในการเข้าตรวจสอบการดำเนินงาน ระบบควบคุมภายในต่าง ๆ รวมทั้งการเรียกดูข้อมูลที่เกี่ยวข้องจากผู้ให้บริการภายนอกหรือผู้รับจ้างช่วงงานต่อ (ถ้ามี) ในเรื่องที่เกี่ยวข้องกับงานที่ให้บริการนั้น ๆ ทั้งนี้ หากการเข้าตรวจสอบต้องได้รับความยินยอมจากหน่วยงานที่กำกับดูแลของผู้ให้บริการภายนอกนั้นผู้ให้บริการภายนอกต้องดำเนินการให้สามารถเข้าตรวจสอบได้อย่างถูกต้อง

ส่วนที่ ๑๑
การบริหารจัดการสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยด้านสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยด้านสารสนเทศให้ได้รับทราบ

ผู้รับผิดชอบ

๑. *ผู้ดูแลระบบฯ*

๒. ผู้ใช้งาน

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. การแก้ไขปัญหา บันทึกเหตุการณ์ และการรายงาน กรณีระบบสารสนเทศได้รับความเสียหาย

๑.๑ *ผู้ใช้งาน*ระบบสารสนเทศของ*บริษัท*มีหน้าที่ในการรายงานเหตุละเมิดหรือจุดอ่อนด้านความมั่นคงใด ๆ ที่พบเห็น หรือที่ต้องสงสัยต่อ*ผู้บังคับบัญชา*และ/หรือผู้ดูและระบบฯ โดยทันที เพื่อให้สามารถแก้ไขปัญหาได้อย่างรวดเร็ว ตัวอย่างของเหตุละเมิดความมั่นคงที่ต้องรายงาน ได้แก่

(๑) การตรวจพบไวรัส หรือโปรแกรมไม่ประสงค์ดีต่าง ๆ

(๒) การตรวจพบความพยายามเจาะระบบ หรือเครื่องมือเจาะระบบ

(๓) การใช้งานข้อมูลหรือ*ระบบสารสนเทศ*อย่างไม่เหมาะสม

(๔) การเข้าถึงข้อมูลหรือ*ระบบสารสนเทศ*โดยไม่ได้รับอนุญาต

(๕) ช่องโหว่หรือจุดอ่อนของซอฟต์แวร์

(๖) การละเมิดนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย

(๗) การกระทำที่ผิดกฎหมาย หรือข้อบังคับของ*บริษัท*

๑.๒ *ผู้ใช้งานระบบสารสนเทศ*ของ*บริษัท*ซึ่งพบเห็นเหตุละเมิด หรือจุดอ่อนด้านความมั่นคงต้องไม่บอกเล่าถึงเหตุที่ตนพบเห็นนั้นกับบุคคลอื่นใด ยกเว้น*ผู้บังคับบัญชา*และ*ผู้ดูแลระบบฯ* ทั้งนี้ *ผู้ใช้งาน*ต้องหลีกเลี่ยงการพิสูจน์จุดอ่อนด้านความมั่นคงที่ต้องสงสัยด้วยตนเอง

๑.๓ *ผู้ดูแลระบบฯ* ที่มีหน้าที่รับผิดชอบต่อการรับมือเหตุละเมิดความมั่นคงปลอดภัยต้องดำเนินการตอบสนองต่อเหตุด้วยความรวดเร็ว มีสติรอบคอบ และต้องติดต่อประสานงานกับ

หน่วยงานต่าง ๆ ที่เกี่ยวข้องอย่างเหมาะสม รวมถึง บันทึกข้อมูล และจัดทำเอกสารเกี่ยวกับเหตุละเมิดความมั่นคงปลอดภัยโดยละเอียด

๑.๔ ข้อมูลและหลักฐานที่เกี่ยวข้องกับเหตุละเมิดความมั่นคงที่เกิดขึ้นทั้งหมด ต้องได้รับการบันทึกและจัดเก็บอย่างปลอดภัยโดย*ผู้ดูแลระบบฯ* เพื่อนำมาศึกษาและป้องกันไม่ให้เกิดเหตุซ้ำในอนาคต

๑.๕ บท.สท. ร่วมกับ สอ.สส. จัดทำสื่อเพื่อเสริมสร้างการตระหนักรู้ และความเข้าใจเกี่ยวกับเหตุละเมิดความมั่นคง วิธีการรายงานเหตุ วิธีการรวบรวมข้อมูลที่เป็นประโยชน์ต่อการสืบสวนและการเก็บรักษาหลักฐานให้แก่*ผู้ดูแลระบบฯ*

๑.๖ บท.สท. ต้องจัดฝึกอบรมในหัวข้อที่เกี่ยวข้องกับการตอบสนอง/รับมือต่อเหตุละเมิดความมั่นคงโดยผู้เชี่ยวชาญจากหน่วยงานภายนอก ให้แก่*ผู้ดูแลระบบฯ* ที่มีหน้าที่รับผิดชอบในการรับมือเหตุละเมิดความมั่นคง

๑.๗ *เครื่องคอมพิวเตอร์*ของ*ผู้ใช้งาน*ที่ถูกปลดออก โอนย้าย และลดตำแหน่งจากการกระทำผิดที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ต้องถูกแยกออกจากเครือข่ายทั้งภายในและภายนอกโดยทันที และก่อนที่จะนำกลับมาใช้ใหม่ ต้องมีการสำรองข้อมูลจากฮาร์ดไดรฟ์เสียก่อน แล้วจึงทำการฟอร์แมต*เครื่องคอมพิวเตอร์*นั้น เพื่อป้องกันการแพร่กระจายของซอฟต์แวร์มุ่งร้าย เช่น back-door ไวรัส โทรจัน ฯลฯ หรือเพื่อกำจัดซอฟต์แวร์ที่ไม่ได้รับอนุญาตซึ่งอาจถูกติดตั้งไว้ใน*ระบบเครือข่าย*

๑.๘ กระบวนการที่ใช้คอมพิวเตอร์ในการประมวลผลข้อมูลสำคัญ ต้องได้รับการควบคุมด้วยมาตรการต่าง ๆ ได้แก่ การตรวจสอบภูมิหลังของ*ผู้ใช้งาน* การแบ่งแยกอำนาจหน้าที่ของ*ผู้ใช้งาน*การบังคับให้*ผู้ใช้งาน*หยุดพักร้อนหรือหมุนเวียนตำแหน่งงานเพื่อทำการตรวจสอบ หรือมาตรการอื่น ๆ เพื่อให้แน่ใจว่าไม่มีผู้ใดมีสิทธิขาดในการควบคุมข้อมูลสำคัญเพียงลำพัง ทั้งนี้ เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล

ส่วนที่ ๑๒
การบริหารจัดการด้านการบริการ
หรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

วัตถุประสงค์

๑. เพื่อป้องกันการหยุดชะงักในการดำเนินงานของ*บริษัท*ที่เป็นผลมาจากภัยพิบัติหนึ่ง

๒. เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

ผู้รับผิดชอบ

๑. *ผู้ดูแลระบบฯ*

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. การบริหารจัดการความต่อเนื่องของความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๑ การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน

(๑) *ผู้ดูแลระบบฯ* ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Contingency Plan) เพื่อรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นได้ ทั้งวิธีการทางอิเล็กทรอนิกส์และทางกายภาพโดยแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องมีรายละเอียดอย่างน้อย ดังนี้

๑) การกำหนดหน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้อง

๒) การกำหนดขั้นตอนการปฏิบัติในการกู้คืน*ระบบสารสนเทศ*

๓) การกำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้

๔) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก

๑.๒ ให้ปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยมุ่งเน้นที่*ระบบสารสนเทศ*ที่มีความสำคัญสูง

๑.๓ ให้ทำการทดสอบแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง หากมีปัญหาเกิดขึ้นในระหว่างการกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหาเหล่านั้น พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

๒. ระบบปฏิบัติงานสำรอง

๒.๑ กำหนดให้*ผู้ดูแลระบบฯ* ประเมินและกำหนด*ระบบสารสนเทศ*สำหรับระบบสำคัญรวมไปถึงจัดเตรียมอุปกรณ์ที่สามารถทำงานทดแทนได้อย่างเหมาะสม

๒.๒ กำหนดให้*ผู้ดูแลระบบฯ* กำหนดสถานที่และเตรียมพื้นที่ให้อยู่ในสภาพพร้อมใช้งานสำหรับระบบทำงานทดแทน

๒.๓ กำหนดให้*ผู้ดูแลระบบฯ* ทดสอบระบบปฏิบัติงานสำรองอย่างสม่ำเสมอเพื่อมั่นใจได้ว่าจะสามารถทำงานทดแทนระบบหลักได้ เมื่อมีความจำเป็นต้องใช้งาน

ส่วนที่ ๑๓
การปฏิบัติตามข้อกำหนด

วัตถุประสงค์

๑. เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

๒. เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ*บริษัท*

ผู้รับผิดชอบ

๑. *ผู้ดูแลงานนิติการ*

๒. *ผู้ดูแลระบบฯ*

๓. ผู้ใช้งาน

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

แนวปฏิบัติ

๑. การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและสัญญา (Compliance With Legal and Contractual Requirements)

๑.๑ การระบุกฎหมายและสัญญาที่ต้องปฏิบัติตาม (Identification of Applicable Legislation and Contractual Requirement)

(๑) *ผู้ใช้งาน*ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งาน*ระบบสารสนเทศ*ที่กำหนดขึ้นอย่างเคร่งครัด โดยมีรายการดังต่อไปนี้เป็นอย่างน้อย

๑) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๒) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๓) พระราชบัญญัติลิขสิทธิ์

๔) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

๕) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

๖) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ*บริษัท*

๑.๒ ทรัพย์สินทางปัญญา (Intellectual Property Rights)

(๑) *ผู้ใช้งาน*ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่*บริษัท*จัดหามาให้ใช้งาน

(๒) *ผู้ดูแลระบบฯ* ต้องมีการบริหารจัดการและควบคุมดูแลการใช้งานซอฟต์แวร์ให้เป็นไปตามลิขสิทธิ์ที่ได้รับ

(๓) ห้าม*ผู้ใช้งาน*ทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บน*เครื่องคอมพิวเตอร์* แท็บแล็ต หรือสมาร์ทโฟนของ*บริษัท*โดยเด็ดขาด

๑.๓ การป้องกันข้อมูล (Protection of Records)

ผู้ดูแลระบบฯ ต้องป้องกันมิให้ข้อมูลที่สำคัญเกิดความเสียหายสูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของ*บริษัท*และข้อกำหนดการให้บริการ

๑.๔ การคุ้มครองข้อมูลส่วนบุคคล (Privacy and Protection of Personally Identifiable Information)

กำหนดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของ*บริษัท*

๒. การทบทวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Reviews)

๒.๑ กำหนดให้มีการทบทวนวัตถุประสงค์ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงของสภาวะแวดล้อมของ*บริษัท*

๒.๒ กำหนดให้มีการทบทวนขั้นตอนการปฏิบัติงานโดยเทียบกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ*บริษัท*

๒.๓ กำหนดให้มีการทบทวนความสอดคล้องของ*ระบบสารสนเทศ*เทียบกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และดำเนินการแก้ไขความไม่สอดคล้องที่ตรวจสอบของ*บริษัท*

๓. การกำกับ ดูแลการปฏิบัติงานให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ*บริษัท*

๓.๑ ให้*ผู้บังคับบัญชา*เป็นผู้กำกับ ดูแล ให้ผู้ใต้บังคับบัญชาปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ*บริษัท*อย่างเคร่งครัด

๓.๒ ในกรณีที่มีการฝ่าฝืนหรือละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ*บริษัท* ให้*ผู้บังคับบัญชา*ดำเนินการเพื่อยับยั้งเหตุการณ์ฝ่าฝืนหรือละเลยการปฏิบัติดังกล่าวตามสมควร และรายงานตามสายบังคับบัญชาไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) เพื่อพิจารณาดำเนินการต่อไป

๓.๓ หากบุคคลใดจงใจฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ*บริษัท* ฉบับนี้ จะถือว่าเป็นความผิดทางวินัยและให้ดำเนินการตาม ข้อบังคับเกี่ยวกับพนักงาน ทั้งนี้ หากการกระทำนั้นเป็นเหตุให้*บริษัท*ได้รับความเสียหาย *บริษัท*จะพิจารณาดำเนินคดีตามกฎหมายอีกทางหนึ่งด้วย