ประกาศ

ที่ ITG 001/2567

เรื่อง นโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ

(Information Technology Management and Security Policy)

บริษัทได้จัดทำนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Technology Management and Security Policy) และแนวปฏิบัติที่เกี่ยวข้อง เพื่อเป็นมาตรฐานและแนวปฏิบัติให้ระบบเทคโนโลยีสารสนเทศของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ทั้งจากภายในและภายนอก ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจก็ตาม อันเป็นการลดความเสียหายต่าง ๆ และรักษาไว้ซึ่งความสามารถในการดำเนินงานได้อย่างมีประสิทธิภาพ และเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายอื่นๆ ที่เกี่ยวข้อง โดยที่การดำเนินการดังกล่าว จะเป็นมาตรการที่ช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 27001, ISO/IEC 27701 และใช้แนวทางจากนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศเครือเจริญโภคภัณฑ์

1. ขอบเขตของประกาศ

ให้ประกาศฉบับนี้มีผลบังคับใช้กับ บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย (ยกเว้น บมจ. ซีพี แอ็กซ์ตร้า และบริษัทในกลุ่มบมจ.ซีพี แอ็กซ์ตร้า)

2. คำนิยาม	**ความหมาย**
“ บริษัท ”	บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย
“ บริษัทย่อย ”	บริษัทในกลุ่มธุรกิจการตลาดและการจัดจำหน่าย เครือเจริญโภคภัณฑ์ (ยกเว้น บมจ. ซีพี แอ็กซ์ตร้า และบริษัทในกลุ่มบมจ.ซีพี แอ็กซ์ตร้า)
“ คณะทำงานเทคโนโลยีสารสนเทศ ” (IT Task Group)	คณะทำงานฯ มีหน้าที่กำหนดกรอบนโยบายด้านเทคโนโลยีสารสนเทศ และนำเสนอต่อคณะกรรมการเทคโนโลยีสารสนเทศกลุ่มฯ (EX-O+)

“ พนักงาน ” **(Employee)**	พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ รวมถึงพนักงานสัญญาจ้างให้ปฏิบัติงานเป็นการชั่วคราวและ/หรือมีกำหนดระยะเวลาและสิ้นสุดที่แน่นอน และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท
“ ผู้ใช้งาน ” **(User)**	คณะกรรมการ ผู้บริหาร ผู้จัดการฝ่าย พนักงาน ลูกจ้าง บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหาร หรือดูแล รักษาระบบสารสนเทศของบริษัทตามสิทธิและหน้าที่ความรับผิดชอบ
“ หน่วยงานเจ้าของข้อมูล ” **(Information Owner)**	หน่วยงานที่รับผิดชอบข้อมูลของบริษัท รวมถึงผู้บังคับบัญชาของหน่วยงานนั้นด้วย โดยหน่วยงานเป็นผู้ที่รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
“ เจ้าของข้อมูลส่วนบุคคล ” **(Data Subject)**	ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น ซึ่งหมายรวมถึง ลูกค้า พนักงาน คู่ค้า และอื่น ๆ ที่ให้ข้อมูลส่วนบุคคลกับบริษัท
“ หน่วยงานเจ้าของกิจกรรม ” **(Business Owner)**	หน่วยงานที่ได้รับมอบหมายให้ดูแลรับผิดชอบกิจกรรมทางธุรกิจนั้น ๆ
ผู้ดูแลระบบ (Infrastructure)	ผู้ที่มีหน้าที่ในการดูแล Infrastructure ของระบบ เพื่อให้ระบบทำงานได้อย่างต่อเนื่องตามข้อตกลง โดยดูแลในส่วนของ Machine , Operating System , Platform , Network ทั้ง On-Premise/Cloud
“ หน่วยงานรับเรื่องเกี่ยวกับ IT ”	หน่วยงานที่รับเรื่องปัญหาทางด้าน IT เช่น Hotline 1500 , Helpdesk
“ หน่วยงานที่ดูแลระบบ IT ”	หน่วยงานที่ได้รับมอบหมายให้ดูแลรับผิดชอบระบบ IT เช่น บริษัท โกซอฟท์ (ประเทศไทย) จำกัด และสำนัก Information System & Service (ISS)
“ หน่วยงานภายนอก/ **ผู้ให้บริการภายนอก/** **บุคคลภายนอก ”**	ผู้ให้บริการภายนอก (Third Party) หรือบุคคลภายนอกที่ใช้งานระบบสารสนเทศของบริษัท ได้เป็นครั้งคราวหรือตามสัญญา

“ ระบบภายในบริษัท ”	กิจกรรมการทำงานของบริษัท ซึ่งรวมถึง กิจกรรมทางธุรกิจ และระบบ IT
“ ระบบสารสนเทศ ” **(Information System)**	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วย เทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น
“ ข้อมูล ” **(Data)**	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของซีดี (CD) ดีวีดี (DVD) Hard Disk Thumb drive เอกสาร แฟ้มรายงาน หนังสือ แผนที่ แผนผัง ภาพวาด ภาพถ่าย การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
“ พื้นที่ใช้งานระบบสารสนเทศ ” **(Information System Workspaces)**	พื้นที่ที่บริษัทอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น 1. พื้นที่มั่นคงปลอดภัย (Secure Area) คือ พื้นที่ที่มีการควบคุมการเข้าถึง และมีระบบการป้องกันจากภัยคุกคามต่างๆ 2. ห้องปฏิบัติงานทั่วไป (Working Area) ห้องประชุม เช่น พื้นที่ปฏิบัติงานทั่วไปของพนักงานของบริษัท 3. พื้นที่ทั่วไป (General Area) คือ พื้นที่สำหรับใช้รับรองบุคคลที่มาติดต่อบริษัท
“ ระบบเครือข่าย ” **(Network System)**	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูลระหว่างระบบคอมพิวเตอร์ได้แก่ ระบบ LAN (Local Area Network) ระบบ WLAN (Wireless LAN) ระบบ Intranet และระบบ เป็นต้น

3. บทบาทหน้าที่

3.1. หน้าที่ของกรรมการผู้จัดการและประธานเจ้าหน้าที่บริหาร (MD&CEO)

3.1.1. กำหนดวิสัยทัศน์ อนุมัติแผนการดำเนินงานของบริษัท และขับเคลื่อนการดำเนินการตามแผนดังกล่าว รวมถึงการให้ข้อเสนอแนะแนวทางในการดำเนินงานและการลงทุนต่าง ๆ เพื่อสนับสนุนการดำเนินงานของบริษัท ให้เป็นไปตามนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ

3.1.2. จัดให้มีการกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม เพื่อให้เป็นไปตามกฎ ระเบียบ ข้อบังคับ นโยบาย แผนกลยุทธ์ และแผนการดำเนินงานต่าง ๆ ของบริษัท

3.1.3 พิจารณาอนุมัตินโยบายความมั่นคงปลอดภัยสารสนเทศ

3.2. หน้าที่ของ Chief Information Officer (CIO)

3.2.1. กำหนดเป้าหมาย นโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศโดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท

3.2.2. จัดการ พัฒนานโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ Policy, Standard, Procedure และ Guideline เพื่อให้บริษัทได้มาซึ่งการรักษา ความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)

3.2.3. ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และ พัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท

3.2.4. ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

3.3. หน้าที่ของ Cyber Security Officer (CSO)

3.3.1. ร่วมกำหนดเป้าหมาย นโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท

3.3.2. จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน

3.3.3. มีการบริหารความเสี่ยงและการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจของบริษัท

3.3.4. นำเสนอผู้บริหารระดับสูง เช่น กรรมการผู้จัดการและประธานเจ้าหน้าที่บริหาร (MD&CEO) Chief Information Officer (CIO) เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง

3.3.5. เตรียมพร้อมรับสถานการณ์ และเรียนรู้เทคนิคใหม่ ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ

3.4. หน้าที่ของ Data Protection Officer (DPO)

3.4.1. ร่วมกำหนดเป้าหมาย นโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทโดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท

3.4.2. กำกับหน่วยงานให้มีการบริหารความเสี่ยงและการวิเคราะห์ความเสี่ยงด้านข้อมูลส่วนบุคคลที่อาจทำให้กระทบกับเจ้าของข้อมูลและการดำเนินธุรกิจของบริษัท

3.4.3. กำกับหน่วยงานให้มีการเตรียมความพร้อมในการบริหารจัดการสถานการณ์ข้อมูลส่วนบุคคลถูกละเมิดหรือรั่วไหล

3.5. หน้าที่ของผู้บังคับบัญชา

3.5.1. ชี้แจง และส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

3.6. หน้าที่ของผู้ใช้งาน

3.6.1. ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทโดยเคร่งครัด

3.6.2. ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทให้มีความปลอดภัย

3.6.3. รายงานต่อบริษัททันที เมื่อพบว่าอุปกรณ์ หรือข้อมูลสารสนเทศสำคัญสูญหาย หรือพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึงการสร้างความเสียหายต่อบริษัท

3.7. หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

3.7.1. จัดให้มีการจัดทำเอกสาร มาตรการ และขั้นตอนควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท

3.7.2. ดูแลให้พนักงานปฏิบัติตามนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท

3.7.3. ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ

3.7.4. รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ

3.7.5. แจ้งหน่วยงานเทคโนโลยีสารสนเทศที่รับผิดชอบด้านการบริหารบัญชีผู้ใช้งาน และสิทธิ์ในการใช้ระบบสารสนเทศเพื่อลบ/เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงาน / อำนาจหน้าที่ / โอนย้าย

3.8. หน้าที่ของหน่วยงานตรวจสอบภายใน (Internal Audit)

3.8.1. ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่ เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศตามความจำเป็น

4. บริษัทกำหนดนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศในประเด็นสำคัญ ซึ่งประกอบด้วย

4.1. แนวนโยบายโครงสร้างความมั่นคงปลอดภัยสารสนเทศและการจัดการข้อมูลส่วนบุคคล (Organization of information security and privacy controls)

4.1.1. การจัดการข่าวกรองด้านภัยคุกคามสารสนเทศ (Threat intelligence management)

4.1.2. ความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการ (Information security in project management)

4.1.3. บัญชีทรัพย์สินสารสนเทศและทรัพย์สินอื่นๆ ที่เกี่ยวข้อง (Inventory of information and other associated assets)

4.1.4. การบริหารจัดการชั้นความลับของข้อมูล (Information classification and labelling)

4.1.5. การถ่ายโอนข้อมูล (Information transfer)

4.1.6. การบริหารจัดการการเข้าถึงและการพิสูจน์ตัวตน (Access and authentication management)

4.1.7. การบริหารจัดการผู้ให้บริการภายนอก (Supplier management)

4.1.8. การรักษาความปลอดภัยของข้อมูลสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)

4.1.9. การบริหารจัดการ Incident ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล (Information security incident management)

4.1.10. การบริหารจัดการเพื่อความต่อเนื่องทางธุรกิจ (Business continuity management)

4.1.11. ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญา (Legal, statutory, regulatory and contractual requirements)

4.1.12. การป้องกันข้อมูล (Protection of records)

4.1.13. ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of PII)

4.1.14. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

4.1.15 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

4.2. แนวนโยบายความปลอดภัยด้านทรัพยากรบุคคล (Human resource security)

4.2.1. ความปลอดภัยด้านทรัพยากรบุคคล (Human resource security)

4.2.2. การปฏิบัติงานจากระยะไกล (Remote working)

4.2.3. การรายงานเหตุการณ์การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

4.3. แนวนโยบายความมั่นคงปลอดภัยทางกายภาพ (Physical controls)

4.3.1. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

4.3.2. การจัดโต๊ะทำงานให้เป็นระเบียบเรียบร้อยและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen)

4.3.3. สื่อจัดเก็บข้อมูล (Storage media)

4.3.4. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure disposal or re-use of equipment)

4.4. แนวนโยบายมาตรการควบคุมด้านเทคโนโลยี (Technological controls)

4.4.1. อุปกรณ์ปลายทางผู้ใช้งาน (User endpoint devices)

4.4.2. การยืนยันตัวตนและการควบคุมการเข้าถึง (Secure authentication and access control)

4.4.3. การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

4.4.4. มาตรการป้องกันโปรแกรมมัลแวร์ (Protection against malware)

4.4.5. การบริหารจัดการของช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

4.4.6. การบริหารจัดการการกำหนดค่า (Configuration management)

4.4.7. การลบสารสนเทศ (Information deletion)

4.4.8. การปิดบังข้อมูลบางส่วน (Data masking)

4.4.9. การป้องกันข้อมูลรั่วไหล (Data leakage prevention)

4.4.10. การสำรองข้อมูล (Information backup)

4.4.11. ความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศแบบ Redundancy (Redundancy of information processing facilities)

4.4.12. การบันทึกข้อมูลเหตุการณ์ (Logging)

4.4.13. กิจกรรมการเฝ้าระวังติดตาม (Monitoring activities)

4.4.14. การตั้งค่าเวลามาตรฐาน (Clock synchronization)

4.4.15. การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

4.4.16. การบริหารจัดการความปลอดภัยด้านเครือข่าย (Networks security management)

4.4.17. การเข้ารหัสข้อมูล (Use of cryptography)

4.4.18. การพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development)

4.4.19. การทดสอบสารสนเทศ (Testing Information)

4.4.20. การป้องกันระบบสารสนเทศระหว่างที่ทดสอบการตรวจประเมิน (Protection of information systems during audit testing)

หมายเหตุ : นโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ รายละเอียดตามเอกสารแนบท้าย 1

5. การทบทวนนโยบาย

ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำอย่างน้อยปีละ 1 ครั้งหรือกรณีที่มีความจำเป็นต้องปรับปรุงเปลี่ยนแปลงและต้องเสนอประธานกรรมการบริหารอนุมัติหากมีการเปลี่ยนแปลง

6. การฝ่าฝืนและบทลงโทษ

พนักงานทุกคนต้องปฏิบัติตามนโยบายฉบับนี้ กรณีที่เกิดการสอบสวน ต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอก อย่างเต็มที่ ทั้งนี้หากกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายฉบับนี้ ไม่ว่าทางตรงหรือทางอ้อม จะถูกพิจารณาโทษทางวินัยตามระเบียบข้อบังคับการทำงานของบริษัท และหากเป็นเหตุที่ผิดกฎหมาย และ/หรือเกิดความเสียหายขึ้น ผู้นั้นจะต้องรับโทษทางกฎหมายตามความผิดที่เกิดขึ้น ทั้งนี้ หากเหตุดังกล่าวก่อให้เกิดความเสียหายแก่บริษัท และ/หรือบุคคลอื่นใด บริษัทอาจพิจารณาดำเนินคดีตามกฎหมายเพิ่มเติม และต้องรับผิดในความเสียหายที่เกิดขึ้นกับบริษัท และบริษัทอาจเรียกร้องความเสียหายทั้งหมด

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 15 ตุลาคม พ.ศ. 2567 เป็นต้นไป

ประกาศ ณ วันที่ 15 ตุลาคม พ.ศ. 2567

(นายก่อศักดิ์ ไชยรัศมีศักดิ์)

ประธานกรรมการบริหาร

เอกสารแนบท้าย 1

ประกาศ ที่ ITG 001/2567

เรื่อง นโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ

(Information Technology Management and Security Policy)

สารบัญ

1. หลักการและเหตุผล

บริษัท ซีพีออลล์ จำกัด (มหาชน) และบริษัทย่อย หรือต่อไปนี้เรียกว่า “บริษัท” ได้จัดทำนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Policy) และแนวปฏิบัติที่เกี่ยวข้อง เพื่อเป็นมาตรฐานและแนวปฏิบัติให้ระบบเทคโนโลยีสารสนเทศของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ทั้งจากภายในและภายนอก ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจก็ตาม อันเป็นการลดความเสียหายต่าง ๆ และรักษาไว้ซึ่งความสามารถในการดำเนินงานได้อย่างมีประสิทธิภาพ และเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายอื่นๆ ที่เกี่ยวข้อง โดยที่การดำเนินการดังกล่าว จะเป็นมาตรการที่ช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 27001, ISO/IEC 27701 และใช้แนวทางจากนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศเครือเจริญโภคภัณฑ์

2. วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ บริษัทจึงเห็นสมควรกำหนดนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติ (Procedure) วิธีการปฏิบัติ (Work Instruction) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังนี้

1. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของบริษัท
2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน แนวปฏิบัติ ขั้นตอนการปฏิบัติ วิธีการปฏิบัติ รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อให้พนักงาน และผู้ใช้งาน หรือผู้ที่เชื่อมต่อระบบคอมพิวเตอร์ของบริษัท สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท ถูกบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท
5. เพื่อให้กระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศมีความชัดเจน สามารถตรวจสอบ และพัฒนาปรับปรุงได้อย่างต่อเนื่อง

3. ขอบเขตการใช้งาน

นโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Policy) และแนวปฏิบัติที่เกี่ยวข้องฉบับนี้มีผลบังคับใช้กับสารสนเทศของบริษัท ผู้ทำหน้าที่ดูแลทรัพย์สิน ผู้ใช้ทรัพย์สิน คณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง และผู้ที่สามารถเข้าถึงสารสนเทศของบริษัท โดยมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการ และปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้งานอื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลทรัพย์สินจะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของบริษัท

4. บริษัทกำหนดนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยสารสนเทศในประเด็นสำคัญประกอบด้วย

4.1. แนวนโยบายโครงสร้างความมั่นคงปลอดภัยสารสนเทศและการจัดการข้อมูลส่วนบุคคล (Organization of information security and privacy controls)

4.1.1. การจัดการข่าวกรองด้านภัยคุกคามสารสนเทศ (Threat intelligence management)

วัตถุประสงค์

1. เพื่อให้ตระหนักถึงการบริหารจัดการภัยคุกคามที่อาจมีผลต่อองค์กร รวมถึงดำเนินการป้องกันและบรรเทาภัยคุกคามได้อย่างเหมาะสม

เอกสารที่เกี่ยวข้อง

1. SCM-PRC-Threat intelligence management

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการรวบรวม วิเคราะห์ ข้อมูลข่าวกรองด้านภัยคุกคามต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อดำเนินการบรรเทาผลกระทบจากภัยคุกคามที่เกิดขึ้น

4.1.2. ความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการ (Information security in project management)

วัตถุประสงค์

1. เพื่อให้แน่ใจว่ามีการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศที่เกี่ยวข้องกับโครงการและสิ่งที่ส่งมอบอย่างมีประสิทธิภาพ

เอกสารที่เกี่ยวข้อง

1. PMP-PRC-Project Management

แนวทางการปฏิบัติ

1. การบริหารจัดการโครงการจะต้องมีการผสานรวมการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงต้องบริหารจัดการความเสี่ยง ตั้งแต่ เริ่มดำเนินโครงการ จนถึง สิ้นสุดโครงการ

4.1.3. บัญชีทรัพย์สินสารสนเทศและทรัพย์สินอื่นๆ ที่เกี่ยวข้อง (Inventory of information and other associated assets)

วัตถุประสงค์

1. เพื่อระบุสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับองค์กร ตามที่เจ้าของทรัพย์สินได้รับมอบหมายให้แน่ใจว่ามีการควบคุมการใช้งาน เปลี่ยนแปลง ยกเลิกสารสนเทศ และสินทรัพย์ที่เกี่ยวข้องอย่างเหมาะสม

เอกสารที่เกี่ยวข้อง

1. PAM-PRC-Asset Management Procedure
2. ISM-PRC-Acceptable Use of Assets Procedure
3. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)
4. RSM-PRC-Risk Management Methodology

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการบริหารจัดการทรัพย์สิน ตั้งแต่ การลงทะเบียน การใช้งาน และการส่งคืนทรัพย์สิน
2. ต้องมีการทบทวนบัญชีทรัพย์สินเป็นประจำ เพื่อตรวจสอบความถูกต้องครบถ้วนของบัญชีทรัพย์สินของบริษัท
3. ข้อมูลส่วนบุคคลต้องมีการจัดทำบันทึกกิจกรรมการประมวลผล (PI Inventory) รวมถึงการทำ Data Flow ของข้อมูลส่วนบุคคล
4. ต้องมีการประเมินความเสี่ยงการใช้งานทรัพย์สินสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลให้เหมาะสม

4.1.4. การบริหารจัดการชั้นความลับของข้อมูล (Information classification and labelling)

วัตถุประสงค์

1. เพื่อเป็นหลักการและแนวทางปฏิบัติให้มั่นใจว่าข้อมูลของบริษัทจะได้รับการจัดการ และการปกป้องที่เหมาะสมในแง่ของภัยคุกคามที่มีต่อข้อมูล โดยคำนึงถึงความสำคัญของข้อมูลที่มีต่อธุรกิจ

เอกสารที่เกี่ยวข้อง

1. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)

แนวทางการปฏิบัติ

1. ปฏิบัติตามนโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices) ที่ประกาศจาก Data Governance

4.1.5. การถ่ายโอนข้อมูล (Information transfer)

วัตถุประสงค์

1. เพื่อให้มีการแลกเปลี่ยนข้อมูลต่าง ๆ กับหน่วยงานภายในและภายนอกอย่างมั่นคงปลอดภัย

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Information Exchange Procedure
2. ISM-PRC-Acceptable Use of Assets Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการแลกเปลี่ยนข้อมูลโดยผ่านช่องทางอิเล็กทรอนิกส์ สื่อจัดเก็บ
2. ต้องมีการกำหนดแนวปฏิบัติสำหรับผู้ใช้งานในเรื่องการเปิดเผยข้อมูลช่องทางต่างๆ เช่น การสื่อสารด้วยวาจา การใช้งานจดหมายอิเล็กทรอนิกส์
3. ต้องมีการจัดทำข้อตกลงการรักษาความลับหรือไม่เปิดเผยข้อมูล
4. กรณีที่มีการแลกเปลี่ยนข้อมูลส่วนบุคคลต้องมีการจัดทำข้อตกลงการประมวลผลข้อมูล (Data processing agreement) หรือข้อตกลงของผู้ควบคุมข้อมูลร่วมกัน (Data sharing agreement)

4.1.6. การบริหารจัดการการเข้าถึงและการพิสูจน์ตัวตน (Access and authentication management)

วัตถุประสงค์

1. เพื่อกำหนดกฎเกณฑ์ และควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงาน อันรวมถึงระบบสารสนเทศที่ใช้สนับสนุนการทำงานของบริการ
2. เพื่อปกป้องข้อมูล และระบบเทคโนโลยีสารสนเทศของหน่วยงาน จากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
3. เพื่อกำหนดกระบวนการในการบริหารจัดการ อนุมัติ/อนุญาต สร้าง เปลี่ยนแปลง ถอดถอน และยกเลิกบัญชีผู้ใช้ สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศที่สำคัญของหน่วยงาน

4. เพื่อให้สามารถระบุตัวตนที่เป็นลักษณะเฉพาะของแต่ละบุคคลและระบบต่าง ๆ ที่เข้าถึงสารสนเทศและทรัพย์สินที่ขององค์กรและเพื่อให้สามารถกำหนดสิทธิ์การเข้าถึงได้อย่างเหมาะสม
5. เพื่อให้แน่ใจว่าข้อมูลเกี่ยวกับการยืนยันตัวตนมีความปลอดภัย

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-User Access Management Procedure
2. ISM-PRC-System and Application Access Control Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศและสินทรัพย์ให้มีความมั่นคงปลอดภัย
2. ต้องมีการบริหารจัดการการยืนยันตัวตน โดยเริ่มตั้งแต่การจัดสรร การเก็บรักษา และการยกเลิก บัญชีผู้ใช้งาน
3. ต้องมีการกำหนดแนวปฏิบัติการจัดการสิทธิ์การเข้าถึงสารสนเทศและสินทรัพย์ให้ครอบคลุมวงจรชีวิตของผู้ใช้งานในทุกขั้นตอน ตั้งแต่การลงทะเบียนผู้ใช้งานใหม่ การเปลี่ยนแปลงสถานภาพต่าง ๆ ไปจนถึงการเพิกถอนสิทธิ์ของผู้ใช้งาน

4.1.7. การบริหารจัดการการผู้ให้บริการภายนอก (Supplier management)

วัตถุประสงค์

1. เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกมีมาตรฐานการดูแลรักษาความปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคลสอดคล้องตามกฎหมาย นโยบายของบริษัท และข้อตกลงทางธุรกิจ

เอกสารที่เกี่ยวข้อง

1. SUM-PRC-Supplier Relationship Management
2. SUM-GUI-Third Party IT Practical Guideline
3. RSM-PRC-Risk Management Methodology
4. SUM-PRC-Supplier Relationships Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอกเกี่ยวกับการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล การจัดการความเสี่ยง ที่เกี่ยวข้องกับผลิตภัณฑ์และบริการทางด้านสารสนเทศ
2. บริษัทต้องมีการสื่อสารแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลให้กับผู้ให้บริการภายนอก

3. ต้องมีการตรวจสอบเป็นประจำสม่ำเสมอให้มั่นใจว่าผู้ให้บริการภายนอกมีการปฏิบัติสอดคล้องกับข้อกำหนดและเงื่อนไขของบริษัท
4. ในกรณีที่มีการว่าจ้างบุคคลภายนอกในการพัฒนาระบบ ต้องมีการสื่อสารข้อตกลงด้านการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล รวมถึงเฝ้าติดตามการดำเนินงานอย่างต่อเนื่อง

4.1.8. การรักษาความปลอดภัยของข้อมูลสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)

วัตถุประสงค์

1. เพื่อบริหารจัดการการรักษาความมั่นคงปลอดภัยสำหรับการใช้บริการคลาวด์

เอกสารที่เกี่ยวข้อง

1. RDM-PRC-Security Controls for Cloud Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติและสื่อสารนโยบายเกี่ยวกับการใช้บริการคลาวด์ให้กับผู้ที่เกี่ยวข้อง

4.1.9. การบริหารจัดการ Incident ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล (Information security incident management)

วัตถุประสงค์

1. เพื่อให้สามารถรับมือกับเหตุการณ์ละเมิดความมั่นคงปลอดภัย การรั่วไหลของข้อมูล ได้อย่างรวดเร็วมีประสิทธิภาพ และวิเคราะห์ปรับปรุงเพื่อลดโอกาสหรือผลสืบเนื่องในอนาคต
2. เพื่อตรวจสอบให้แน่ใจว่ามีการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัย การรั่วไหลของข้อมูล สอดคล้องตามที่กฎหมายกำหนด

เอกสารที่เกี่ยวข้อง

1. ICM-PRC-Incident Management
2. PDA-PRC-Data Incident and Breach Management Procedure
3. Data Breach & Cyber Security Incident Response Plan
4. นโยบายการละเมิดและข้อมูลรั่วไหล (Data Breach Handling Policy)

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัย การรั่วไหลของข้อมูล โดยต้องประกอบด้วยการกำหนดบทบาทหน้าที่ ขั้นตอนการปฏิบัติที่รวมถึงการรายงานให้กับผู้ที่เกี่ยวข้อง
2. ต้องมีการกำหนดเกณฑ์ระดับความรุนแรง (Severity level) และการตอบสนองของเหตุการณ์ละเมิดความมั่นคงปลอดภัย การรั่วไหลของข้อมูล
3. ต้องนำผลการวิเคราะห์เหตุการณ์ละเมิดความมั่นคงปลอดภัย การรั่วไหลของข้อมูลมาปรับปรุงเพื่อลดโอกาสหรือผลสืบเนื่องในอนาคต
4. กรณีที่เกิดเหตุการณ์ละเมิดความปลอดภัยและข้อมูลรั่วไหลให้ปฏิบัติตามแผนตอบสนองเหตุการณ์ละเมิดความปลอดภัยไซเบอร์และข้อมูลรั่วไหล (Data Breach & Cyber Security Incident Response Plan)
5. กรณีที่เกิดการละเมิดข้อมูลส่วนบุคคลจะต้องพิจารณาการแจ้งเหตุการณ์ให้กับสำนักงานคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลให้สอดคล้องกฎหมายตามระยะเวลาที่กำหนด อ้างอิงประกาศนโยบายการละเมิดและข้อมูลรั่วไหล (Data Breach Handling Policy)

4.1.10. การบริหารจัดการเพื่อความต่อเนื่องทางธุรกิจ (Business continuity management)

วัตถุประสงค์

1. เพื่อให้มีแนวทางการบริหารจัดการความต่อเนื่องของธุรกิจ หน่วยงานสามารถดำเนินกิจกรรมการให้บริการที่สำคัญ (Critical Business Process) และ/หรือการให้บริการที่สำคัญ (Key Services) ต่อผู้ใช้บริการ เมื่อเกิดเหตุฉุกเฉิน หรือภัยพิบัติขึ้น สามารถบริหารจัดการให้กลับเข้าสู่สถานการณ์ปกติ (Normal Operation) ได้อย่างมีประสิทธิภาพ

เอกสารที่เกี่ยวข้อง

1. SCM-PRC-Business Continuity Management
2. SCM-PRC-Service Continuity Management

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการบริหารจัดการความต่อเนื่องทางธุรกิจเมื่อเกิดเหตุการณ์ที่ทำให้ธุรกิจหยุดชะงัก
2. ต้องมีการจัดทำแผน ดูแลรักษาและทดสอบ เมื่อเกิดเหตุการณ์ที่ทำให้ธุรกิจหยุดชะงัก

4.1.11. ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญา (Legal, statutory, regulatory and contractual requirements)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่าการดำเนินงานสอดคล้องกับข้อกำหนดทางกฎหมาย ภาคบังคับ ระเบียบข้อบังคับ สัญญาและมาตรฐานที่บริษัทนำมาประยุกต์ใช้ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Acceptable Use of Assets Procedure
2. SUM-CPA-Checklist Legal

แนวทางการปฏิบัติ

1. ต้องมีการระบุข้อกำหนดทางกฎหมาย ภาคบังคับ ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลและวิธีการที่บริษัทจะปฏิบัติตามข้อกำหนดเหล่านี้
2. ต้องมีการติดตามกฎหมาย มาตรฐานอย่างสม่ำเสมอเพื่อนำมาวิเคราะห์และวางแผนปรับปรุงให้สอดคล้องโดยใช้กระบวนการการบริหารจัดการการเปลี่ยนแปลง

4.1.12. การป้องกันข้อมูล (Protection of records)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่าการบริหารจัดการ Record สอดคล้องกับข้อกำหนดทางกฎหมาย ภาคบังคับ ระเบียบข้อบังคับ และสัญญา (Record คือที่จัดเก็บข้อมูลหรือเหตุการณ์ต่างๆ ที่เกิดขึ้นจากกระบวนการทำงานทั้งในรูปแบบของอิเล็กทรอนิกส์ กระดาษ เช่น บันทึกข้อมูล รายการธุรกรรมทางการขาย Application Log เป็นต้น)

เอกสารที่เกี่ยวข้อง

1. AVM-PRC-Record Control Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการบริหารจัดการ Record ตั้งแต่การรวบรวม จัดเก็บ เผยแพร่ ทำลาย รวมถึงกำหนดระยะเวลาในการจัดเก็บ

4.1.13. ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of PII)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่าสอดคล้องกับข้อกำหนดทางกฎหมาย ภาคบังคับ ระเบียบข้อบังคับ และสัญญาเกี่ยวกับด้านการรักษาความปลอดภัยของข้อมูลในการปกป้องข้อมูลส่วนบุคคล

เอกสารที่เกี่ยวข้อง

1. นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Policy)
2. แนวทางปฏิบัติการจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (Personal Information Inventory)
3. แนวทางปฏิบัติผู้ควบคุมข้อมูลและผู้ประมวลผล (Data Controller and Data Processor Management)
4. แนวทางปฏิบัติผู้การประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

แนวทางการปฏิบัติ

1. ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Policy) และแนวปฏิบัติที่ประกาศจากหน่วยงาน Data Protection Office
2. ต้องมีการกำหนดแนวทางปฏิบัติในการบันทึกกิจกรรมประมวลผลข้อมูลบุคคล
3. ต้องมีการกำหนดแนวทางปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
4. ต้องมีการกำหนดแนวทางปฏิบัติการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

4.1.14. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

วัตถุประสงค์

1. เพื่อตรวจสอบให้มั่นใจว่าการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ มีความเหมาะสม เพียงพอ และมีประสิทธิภาพอย่างต่อเนื่อง

เอกสารที่เกี่ยวข้อง

1. PQA-PRC-Internal Audit Procedure
2. PQA-PRC-Corrective and Preventive Action Procedure

แนวทางการปฏิบัติ

1. ควรมีการดำเนินการตรวจสอบการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศจากผู้ที่ไม่มีส่วนได้ส่วนเสียของหน่วยงาน
2. ควรมีการบันทึกผลการตรวจสอบและรายงานให้ต่อผู้บริหาร

4.1.15. เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

วัตถุประสงค์

1. เพื่อให้มั่นใจว่าการปฏิบัติงานด้านการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศดำเนินงานอย่างถูกต้อง

เอกสารที่เกี่ยวข้อง

-

แนวทางการปฏิบัติ

1. ต้องมีการจัดทำเอกสารขั้นตอนการปฏิบัติงาน
   1.1. เมื่อกิจกรรมจำเป็นต้องมีผู้ดำเนินการหลายคน
   1.2. เมื่อเป็นกิจกรรมที่ไม่ได้ปฏิบัติเป็นประจำ
   1.3. เมื่อเป็นกิจกรรมใหม่หรือก่อให้เกิดความเสี่ยงหากดำเนินการไม่ถูกต้อง
   1.4. เมื่อเป็นกิจกรรมที่สำคัญมีผลกระทบต่อองค์กรหากเกิดข้อผิดพลาด
2. ต้องมีการกำหนดกระบวนการในการบริหารจัดการเอกสาร

4.2. แนวนโยบายความปลอดภัยด้านทรัพยากรบุคคล (Human resource security)

4.2.1. ความปลอดภัยด้านทรัพยากรบุคคล (Human resource security)

วัตถุประสงค์

1. เพื่อกำหนดบทบาทและหน้าที่ความรับผิดชอบของระบบการบริหารทรัพยากรบุคคลในองค์กร ตั้งแต่การวางแผนโครงสร้างองค์กร การวางแผนอัตรากำลัง การสรรหา การคัดเลือก การประเมินผล การฝึกอบรมและพัฒนา กระบวนการทางวินัย และการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน

เอกสารที่เกี่ยวข้อง

1. OPD-PRC-Disciplinary Action Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดกระบวนการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ด้านทรัพยากรบุคคลตั้งแต่การวางแผนโครงสร้าง

องค์กร การวางแผนอัตรากำลัง การสรรหา การคัดเลือก การประเมินผล การฝึกอบรมและพัฒนา กระบวนการทางวินัย และการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน

4.2.2. การปฏิบัติงานจากระยะไกล (Remote working)

วัตถุประสงค์

1. เพื่อตรวจสอบให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลเมื่อปฏิบัติงานจากระยะไกล

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Mobile Computing and Teleworking Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดกระบวนการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลด้านเกี่ยวกับการใช้งานอุปกรณ์เคลื่อนที่ อุปกรณ์ประมวลผล และการปฏิบัติงานจากระยะไกล

4.2.3. การรายงานเหตุการณ์การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

วัตถุประสงค์

1. เพื่อสนับสนุนการรายงานเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ การละเมิดและรั่วไหลของข้อมูล อย่างมีประสิทธิภาพ

เอกสารที่เกี่ยวข้อง

1. ICM-PRC-Incident Management
2. PDA-PRC-Data Incident and Breach Management Procedure
3. นโยบายการละเมิดและข้อมูลรั่วไหล (Data Breach Handling Policy)

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการแจ้งรายงานเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ การละเมิดและรั่วไหลของข้อมูล

4.3. แนวนโยบายความมั่นคงปลอดภัยทางกายภาพ (Physical controls)

4.3.1. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

วัตถุประสงค์

1. เพื่อป้องกันและรักษาความมั่นคงปลอดภัย การเข้าถึงโดยไม่ได้รับอนุญาต, ความเสียหายทางกายภาพ ซึ่งรวมถึงสำนักงานห้องและสิ่งอำนวยความสะดวกต่างๆ

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Physical and Environment Procedure
2. ISM-POL-Data Center Policy
3. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดอาณาเขตที่มีการรักษาความมั่นคงปลอดภัยและใช้เพื่อป้องกันพื้นที่ที่มีสารสนเทศและ สินทรัพย์ที่เกี่ยวข้องอื่น ๆ
2. ต้องมีการควบคุมการเข้าถึงพื้นที่ต่างๆ เช่น พื้นที่ขนส่งและพื้นที่ขนถ่าย และจุดอื่นๆ ที่มีบุคคลไม่ได้รับ อนุญาตสามารถเข้าในบริเวณสถานที่
3. ต้องออกแบบและดำเนินการการรักษาความมั่นคงปลอดภัยทางกายภาพให้กับสำนักงาน ห้อง และสิ่งอำนวยความสะดวกต่าง ๆ ให้สอดคล้องกับลำดับชั้นความลับของข้อมูลสารสนเทศ
4. ต้องมีการตรวจสอบความมั่นคงปลอดภัยการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต
5. ต้องมีการออกแบบและดำเนินการการป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม เช่น ภัยธรรมชาติและภัยคุกคามทางกายภาพโดยเจตนาหรือโดยไม่เจตนาอื่นๆ ที่มีต่อโครงสร้างพื้นฐาน
6. ต้องมีการกำหนดแนวทางปฏิบัติงานสำหรับการทำงานในพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยให้กับบุคลากรที่เกี่ยวข้อง โดยให้ครอบคลุมทุกกิจกรรมที่เกิดขึ้นในพื้นที่
7. ต้องมีการจัดวางอุปกรณ์อย่างปลอดภัยและมีการป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม
8. ต้องมีการกำหนดแนวทางปฏิบัติงานในการรักษาความมั่นคงปลอดภัยของทรัพย์สินที่ถูกนำไปใช้นอกสถานที่
9. ต้องมีการป้องกันสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศไม่ให้เกิดไฟฟ้าขัดข้อง และการหยุดชะงักอื่น ๆ รวมถึงระบบสาธารณูปโภคที่สนับสนุน
10. ต้องมีการกำหนดแนวปฏิบัติในการบริหารความปลอดภัยของ สายไฟ สายสื่อสาร และสายอื่นๆ ที่สนับสนุนการให้บริหารสารสนเทศ ไม่ให้เกิดการสูญเสีย ความเสียหาย การโจรกรรม หรืออยู่ในภาวะเสี่ยง และไม่ให้การดำเนินงานขององค์กรหยุดชะงัก
11. ต้องมีการกำหนดแนวปฏิบัติในการดูแลรักษาอุปกรณ์เพื่อทำให้แน่ใจว่าพร้อมใช้งาน มีความสมบูรณ์ และรักษาความลับของสารสนเทศ

4.3.2. การจัดโต๊ะทำงานให้เป็นระเบียบเรียบร้อยและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen)

วัตถุประสงค์

1. เพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย และความเสียหายต่อสารสนเทศบนโต๊ะ หน้าจอแสดงผล และในสถานที่อื่นๆ ที่สามารถเข้าถึงได้ทั้งในและนอกเวลาทำงานปกติ

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Acceptable Use of Assets Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวทางปฏิบัติงานเกี่ยวกับการจัดบริเวณพื้นที่ทำงาน (Clear desk and clear screen) ให้เป็นระเบียบเรียบร้อยและการป้องกันหน้าจอให้มีความมั่นคงปลอดภัย

4.3.3. สื่อจัดเก็บข้อมูล (Storage media)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่ามีการเปิดเผย ดัดแปลง ลบ หรือทำลายข้อมูลบนสื่อจัดเก็บสารสนเทศที่ได้รับอนุญาต เท่านั้น

เอกสารที่เกี่ยวข้อง

1. AVM-PRC-Disposal of Media Procedure
2. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)

แนวทางการปฏิบัติ

1. ต้องมีการจัดการสื่อจัดเก็บข้อมูลตั้งแต่การจัดหา การใช้ การขนส่ง และการกำจัดตามการจัดหมวดหมู่ขององค์กรและข้อกำหนดของบริษัท

4.3.4. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure disposal or re-use of equipment)

วัตถุประสงค์

1. เพื่อป้องกันสารสนเทศรั่วไหลออกจากอุปกรณ์ที่จะทิ้งหรือนำกลับมาใช้ใหม่

เอกสารที่เกี่ยวข้อง

1. AVM-PRC-Disposal of Media Procedure
2. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติเพื่อให้มั่นใจว่าอุปกรณ์ที่มีการจัดเก็บข้อมูลจะถูกลบหรือทำลายข้อมูลอย่างปลอดภัยก่อนอุปกรณ์นั้นจะถูกทิ้งหรือนำกลับมาใช้ใหม่

4.4. แนวนโยบายมาตรการควบคุมด้านเทคโนโลยี (Technological controls)

4.4.1. อุปกรณ์ปลายทางผู้ใช้งาน (User endpoint devices)

วัตถุประสงค์

1. เพื่อป้องกันสารสนเทศไม่ให้เกิดความเสี่ยงจากการใช้งานอุปกรณ์ปลายทางของผู้ใช้

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Acceptable Use of Assets Procedure
2. PAM-PRC-Asset Management Procedure

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติและกำหนดความรับผิดชอบของผู้ใช้เกี่ยวกับการใช้อุปกรณ์ปลายทาง การใช้อุปกรณ์ส่วนตัว การเชื่อมต่อแบบไร้สาย ให้มีความมั่นคงปลอดภัย

4.4.2. การยืนยันตัวตนและการควบคุมการเข้าถึง (Secure authentication and access control)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่ามีเพียงผู้ใช้งานที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงสารสนเทศและทรัพย์สินได้
2. เพื่อป้องกันการเปลี่ยนแปลงสารสนเทศที่ไม่ได้ตั้งใจหรือมุ่งร้าย และรักษาความลับของทรัพย์สินทางปัญญา
3. เพื่อให้มั่นใจว่ากระบวนการยืนยันตัวตนถูกต้องและปลอดภัย เมื่อให้สิทธิ์ เข้าถึงระบบ แอปพลิเคชัน และบริการต่าง ๆ

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-User Access Management Procedure
2. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการจัดสรรสิทธิ์ในการเข้าถึงสำหรับสิทธิ์ขั้นสูง (Privileged access) ให้มีความเข้มงวดกว่าการบริหารจัดการสิทธิ์ทั่วไป
2. ต้องมีแนวปฏิบัติในการจำกัดสิทธิ์การเข้าถึงสารสนเทศและทรัพย์สินที่เกี่ยวข้องตามลำดับชั้นความลับ

3. ต้องควบคุมการเข้าถึงและแก้ไขซอร์สโค้ดและรายการที่เกี่ยวข้อง (เช่น designs, specifications, test plans and UAT plans) และเครื่องมือพัฒนา (เช่น Compilers, builders, integration tools, test platforms and environments) อย่างเข้มงวด
4. ต้องกำหนดเทคโนโลยีและขั้นตอนการตรวจสอบตัวตนให้เหมาะสมและมีความรัดกุม เพื่อลดความเสี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

4.4.3. การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

วัตถุประสงค์

1. เพื่อตรวจสอบให้มั่นใจว่าทรัพยากรต่างๆ (เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ทรัพยากรบุคคล สำนักงาน และสิ่งอำนวยความสะดวกอื่น ๆ) มีขีดความสามารถที่เพียงพอต่อความจำเป็นทางธุรกิจ

เอกสารที่เกี่ยวข้อง

1. CPM-PRC-Capacity Management

แนวทางการปฏิบัติ

1. ต้องกำหนดแนวทางปฏิบัติในการเฝ้าติดตามการใช้ทรัพยากรและปรับเปลี่ยนให้สอดคล้องกับขีดความสามารถในปัจจุบันและตามความจำเป็นทางธุรกิจ

4.4.4. มาตรการป้องกันโปรแกรมมัลแวร์ (Protection against malware)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่ามีการคุ้มครองสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่นๆ จากมัลแวร์ อย่างปลอดภัย

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Acceptable Use of Assets Procedure

แนวทางการปฏิบัติ

1. ต้องจัดให้มีแนวปฏิบัติและซอฟต์แวร์ในการป้องกันมัลแวร์
2. เตรียมแผนความต่อเนื่องของธุรกิจที่เหมาะสมสำหรับการกู้คืนจากการโจมตีของมัลแวร์
3. สร้างความตระหนักรู้เกี่ยวกับการป้องกันมัลแวร์อย่างเหมาะสมและสม่ำเสมอ

4.4.5. การบริหารจัดการของช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

วัตถุประสงค์

1. เพื่อป้องกันภัยคุกคามที่เกิดจากการใช้ประโยชน์จากช่องโหว่ทางเทคนิคของระบบสารสนเทศ ทำให้ระบบสารสนเทศได้รับความเสียหาย ซึ่งอาจทำให้การดำเนินงานทางธุรกิจขององค์กรหยุดชะงักได้

เอกสารที่เกี่ยวข้อง

1. ISM-POL-Vulnerability Management Policy
2. ISM-PRC-Patch Management Procedure

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการตรวจสอบ ประเมินและจัดการช่องโหว่ด้านความปลอดภัยของระบบอย่างเหมาะสม
2. การสแกนหาช่องโหว่ (Vulnerability Assessment) ต้องมีการดำเนินการอย่างน้อยปีละ 1 ครั้ง
3. ระบบที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet facing) ต้องทำการทดสอบการเจาะระบบ (Penetration Test) ก่อนขึ้นระบบ (Production) หรือเมื่อมีการเปลี่ยนแปลงระบบที่มีความเสี่ยงต่อความมั่นคงปลอดภัย เช่น เมื่อมีการเปลี่ยนแปลง Architecture หรือ Servers เมื่อมีการเพิ่มฟังก์ชั่นการทำงานที่มีการติดต่อกับภายนอก เมื่อมีการทำโปรแกรมเชื่อมต่อกับระบบใหม่อื่นๆ
4. ผู้ดูแลระบบต้องมีหน้าในการบริหารจัดการ ตรวจสอบ เฝ้าระวัง และปรับปรุง Patch โดยเฉพาะ Security Patch ให้เป็นปัจจุบันในทุกระบบ (ไม่ว่าระบบนั้นจะอยู่ On-Cloud หรือ On-Premise)

4.4.6. การบริหารจัดการการกำหนดค่า (Configuration management)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่า ฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่ายทำงานอย่างถูกต้องด้วยการกำหนดค่าการรักษาความมั่นคงปลอดภัยที่จำเป็น และไม่เปลี่ยนแปลงการกำหนดค่าโดยไม่ได้รับอนุญาตหรือไม่ถูกต้อง

เอกสารที่เกี่ยวข้อง

1. CFM-PRC-Configuration Management

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการบริการจัดการ Configurations ด้านการรักษาความมั่นคงปลอดภัยของ ฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่าย และจัดทำเป็นเอกสาร นำไปปฏิบัติ เฝ้าติดตามและทบทวน

2. ต้องมีการกำหนดเทมเพลตมาตรฐานสำหรับการกำหนดค่าฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายที่ปลอดภัย
3. ต้องมีการเฝ้าระวังติดตามการ Configurations ให้ถูกต้องเป็นไปตามที่กำหนดไว้

4.4.7. การลบสารสนเทศ (Information deletion)

วัตถุประสงค์

1. เพื่อป้องกันการเปิดเผยสารสนเทศโดยไม่จำเป็น และสอดคล้องตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญา สำหรับการลบสารสนเทศ

เอกสารที่เกี่ยวข้อง

1. AVM-PRC-Record Control Procedure
2. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)
3. AVM-PRC-Disposal of Media Procedure
4. แนวทางปฏิบัติผู้ควบคุมข้อมูลและผู้ประมวลผล (Data Controller and Data Processor Management)

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการลบหรือทำลายข้อมูลสารสนเทศที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือสื่อจัดเก็บข้อมูลอื่น ๆ ตามลำดับชั้นความลับ
2. ต้องมีการกำหนดระยะเวลาในการลบเมื่อสิ้นสุดวัตถุประสงค์ในการใช้ข้อมูล
3. กรณีที่เป็นข้อมูลส่วนบุคคลต้องปฏิบัติตามกฎหมายที่ว่าด้วยเรื่องของการลบข้อมูล

4.4.8. การปิดบังข้อมูลบางส่วน (Data masking)

วัตถุประสงค์

1. เพื่อจำกัดการเปิดเผยข้อมูลสำคัญรวมถึงข้อมูลส่วนบุคคล และเพื่อให้เป็นไปตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญา

เอกสารที่เกี่ยวข้อง

1. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)
2. แนวทางปฏิบัติผู้ควบคุมข้อมูลและผู้ประมวลผล (Data Controller and Data Processor Management)

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการปกปิดข้อมูลตามลำดับชั้นความลับ รวมถึงข้อมูลส่วนบุคคล

4.4.9. การป้องกันข้อมูลรั่วไหล (Data leakage prevention)

วัตถุประสงค์

1. เพื่อตรวจจับและป้องกันการเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาตโดยบุคคลหรือระบบต่าง ๆ

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Information Exchange Procedure
2. นโยบายการละเมิดและข้อมูลรั่วไหล (Data Breach Handling Policy)

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการป้องกันและเฝ้าระวังทรัพย์สินต่างๆ จากความเสี่ยงข้อมูลรั่วไหล

4.4.10. การสำรองข้อมูล (Information backup)

วัตถุประสงค์

1. เพื่อทำให้สามารถกู้คืนข้อมูลได้จากการที่ระบบหรือข้อมูลสูญหาย

เอกสารที่เกี่ยวข้อง

1. AVM-PRC-Information Backup and Restore Procedure
2. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการสำรองข้อมูล กู้คืนข้อมูล รวมถึงมีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

4.4.11. ความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศแบบ Redundancy (Redundancy of information processing facilities)

วัตถุประสงค์

1. เพื่อให้แน่ใจว่าระบบและโครงสร้างพื้นฐานรองรับการดำเนินงานได้อย่างต่อเนื่องตามความต้องการของธุรกิจ

เอกสารที่เกี่ยวข้อง

1. SCM-PRC-Business Continuity Management
2. SCM-PRC-Service Continuity Management

แนวทางการปฏิบัติ

1. บริษัทต้องมีการออกแบบสถาปัตยกรรมและโครงสร้างพื้นฐานของระบบ เพื่อรองรับความต้องการความต่อเนื่องทางธุรกิจ โดยออกแบบตามเกณฑ์ ICT readiness for business

4.4.12. การบันทึกข้อมูลเหตุการณ์ (Logging)

วัตถุประสงค์

1. เพื่อบันทึกเหตุการณ์ สร้างหลักฐาน ตรวจสอบให้แน่ใจว่าข้อมูลบันทึกมีความสมบูรณ์ ป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต เพื่อใช้สำหรับระบุเหตุการณ์ด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลรวมถึงเป็นหลักฐานในการสนับสนุนการตรวจสอบ

เอกสารที่เกี่ยวข้อง

1. AVM-PRC-Logging and Monitoring System Use Procedure
2. PDA-PRC-Data Incident and Breach Management Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวทางในการบันทึกเหตุการณ์ เช่น Event Log, Access Log, User Activity Log, Authentication Log, Transaction Log
2. ต้องมีการกำหนดแนวทางในการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลของบันทึกเหตุการณ์
3. ต้องมีแนวทางในการตรวจสอบและวิเคราะห์ความผิดปกติจากข้อมูลบันทึกเหตุการณ์อย่างสม่ำเสมอ เพื่อนำไปบริหารจัดการด้านความปลอดภัย ตาม Incident Management

4.4.13. กิจกรรมการเฝ้าระวังติดตาม (Monitoring activities)

วัตถุประสงค์

1. เพื่อตรวจจับพฤติกรรมที่ผิดปกติและเหตุการณ์ด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลของสารสนเทศที่อาจเกิดขึ้น

เอกสารที่เกี่ยวข้อง

1. AVM-PRC-Logging and Monitoring System Use Procedure
2. ICM-PRC-Incident Management
3. PDA-PRC-Data Incident and Breach Management Procedure

แนวทางการปฏิบัติ

1. ต้องกำหนดขอบเขตและระดับการเฝ้าระวังติดตามของ เครือข่าย ระบบ และแอพพลิเคชั่น ให้เป็นไปตามความต้องการทางธุรกิจ การรักษาความปลอดภัย กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง
2. ต้องมีการบันทึกการเฝ้าระวังติดตาม
3. ต้องกำหนด Threshold และ Alerts เพื่อใช้ในการเฝ้าระวังพฤติกรรมที่ผิดปกติ

4.4.14. การตั้งค่าเวลามาตรฐาน (Clock synchronization)

วัตถุประสงค์

1. เพื่อให้เกิดความสัมพันธ์และวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยและข้อมูลที่บันทึกไว้อื่นๆ รวมถึงสนับสนุนการสอบสวนเหตุการณ์ด้านการรักษาความปลอดภัยของสารสนเทศ

เอกสารที่เกี่ยวข้อง

-

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดการตั้งค่าเวลามาตรฐานของเครื่องคอมพิวเตอร์ทุกเครื่องในบริษัทไปยังเครื่องแม่ข่ายที่ให้บริการข้อมูลเวลาและเครื่องคอมพิวเตอร์ทุกเครื่องในบริษัทด้วย Network Time Protocol (NTP) ไปยังเครื่องแม่ข่าย โดยอ้างอิงเวลามาตรฐานจาก กรมอุทกศาสตร์ กองทัพเรือ ที่ให้บริการข้อมูลเวลาอย่างน้อยที่เป็น Stratum 1 คือ time.navy.mi.th.or.th หรือ time2.navy.mi.th หรือ ตาม Active Directory
2. ทุกอุปกรณ์จะต้องมีการกำหนดเวลาให้ตรงกับเวลามาตรฐาน

4.4.15. การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

วัตถุประสงค์

1. เพื่อตรวจสอบให้มั่นใจว่า ระบบปฏิบัติการมีความสมบูรณ์และป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค
2. เพื่อตรวจสอบให้แน่ใจว่าการใช้โปรแกรมอรรถประโยชน์จะไม่เป็นอันตรายต่อการควบคุมระบบและแอปพลิเคชันสำหรับการรักษาความปลอดภัยของสารสนเทศ

เอกสารที่เกี่ยวข้อง

1. IT-STD-มาตรฐานโปรแกรมเพื่อใช้ในการปฏิบัติงานของบริษัท
2. ISM-PRC-User Access Management Procedure
3. ISM-PRC-Acceptable Use of Assets Procedure

แนวทางการปฏิบัติ

1. ต้องมีแนวปฏิบัติในการบริหารการเปลี่ยนแปลงและการติดตั้งซอฟต์แวร์ ไลบรารี่บนระบบปฏิบัติการอย่างปลอดภัยรวมถึง ต้องไม่ End of Support
2. กรณีที่ต้องใช้โปรแกรมที่สามารถควบคุมระบบหรือแอพพลิเคชั่น (Privileged utility programs) จะต้องมีการตรวจสอบว่าโปรแกรมเหล่านั้นไม่เป็นอันตรายและไม่มีผลกระทบต่อระบบปฏิบัติการและแอพพลิเคชั่น
3. ต้องมีการควบคุมการกำหนดสิทธิ์และบันทึกการใช้งานของผู้ใช้งานโปรแกรมที่สามารถควบคุมระบบหรือแอพพลิเคชั่น (Privileged utility programs)

4.4.16. การบริหารจัดการความปลอดภัยด้านเครือข่าย (Networks security management)

วัตถุประสงค์

1. เพื่อให้มั่นใจว่าสารสนเทศ ทรัพยากร และการดำเนินกิจกรรมในเครือข่าย มีความปลอดภัย ไม่ให้ถูกโจมตีและป้องกันไม่ให้เข้าถึงทรัพยากรโดยไม่ได้รับอนุญาต

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Network Security Procedure
2. ISM-PRC-User Access Management Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของเครือข่าย
2. ต้องมีการกำหนดขอบเขตของแต่ละประเภทของเครือข่าย
3. ต้องมีการกำหนดแนวทางในการกรองการเข้าถึงเว็บไซต์ (Web filtering) ที่เหมาะสม

4.4.17. การเข้ารหัสข้อมูล (Use of cryptography)

วัตถุประสงค์

1. เพื่อตรวจสอบให้แน่ใจว่ามีการใช้ การเข้ารหัสอย่างเหมาะสมและมีประสิทธิภาพปกป้องการรักษาความลับ ความถูกต้องหรือความสมบูรณ์ของสารสนเทศ ตามข้อกำหนดทางธุรกิจ และคำนึงถึงข้อกำหนดทางกฎหมาย ภาคบังคับ ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้องกับการเข้ารหัส

เอกสารที่เกี่ยวข้อง

1. ISM-PRC-Cryptography Control Procedure
2. นโยบายการจัดลำดับชั้นข้อมูลและแนวทางการปฏิบัติ (Data Classification Policy and Practices)

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดเกณฑ์มาตรฐานการเข้ารหัสตามลำดับชั้นความลับ
2. ต้องมีการกำหนดมาตรฐานในการบริหารจัดการคีย์ (Key management)

4.4.18. การพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development)

วัตถุประสงค์

1. เพื่อควบคุมการพัฒนาและเปลี่ยนแปลงระบบสารสนเทศและซอฟต์แวร์ ให้มีประสิทธิภาพ และมีความมั่นคงปลอดภัย ตั้งแต่กระบวนการออกแบบ การพัฒนา การทดสอบ และวางแผนการดำเนินการซึ่งนำไปสู่กระบวนการติดตั้งเพื่อใช้งานอย่างมีประสิทธิภาพ และลดความเสี่ยงที่อาจเกิดความเสียหายขึ้นบนระบบสารสนเทศหลัก

เอกสารที่เกี่ยวข้อง

1. RDM-PRC-Information System and Software Development
2. TSM-FRM-Privacy by Design Guideline for IT
3. CHM-PRC-Change Management Procedure
4. SUM-GUI-Third Party IT Practical Guideline

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติในการพัฒนาระบบให้มีความมั่นคงปลอดภัยและคุ้มครองข้อมูลบุคคล
2. กรณีที่ระบบมีการประมวลผลข้อมูลส่วนบุคคลจะต้องปฏิบัติตาม Privacy by Design Guideline for IT ที่บริษัทกำหนด
3. ต้องมีการกำหนดความต้องการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบ (Security requirements)
4. ต้องมีการกำหนดหลักการทางวิศวกรรมด้านความมั่นคงปลอดภัย และนำไปใช้กับการออกแบบและพัฒนาระบบ
5. ต้องมีกระบวนการเพื่อให้มั่นใจว่ามีการ Coding โปรแกรมอย่างปลอดภัย ตั้งแต่ก่อน ระหว่าง และหลัง Coding โปรแกรม
6. ต้องมีกระบวนการทดสอบด้านความมั่นคงปลอดภัย สำหรับระบบใหม่หรือระบบที่มีการปรับปรุง
7. ในกรณีที่มีการว่าจ้างบุคคลภายนอกในการพัฒนาระบบ ต้องมีการสื่อสารข้อตกลงด้านความมั่นคงปลอดภัย และเฝ้าติดตามการดำเนินงานอย่างต่อเนื่อง
8. ต้องแยกสภาพแวดล้อมของการพัฒนา (Development) การทดสอบ (Test) และการใช้งานระบบจริง (Production)
9. ต้องมีการกำหนดกระบวนการการบริหารจัดการการเปลี่ยนแปลง

4.4.19. การทดสอบสารสนเทศ (Testing information)

วัตถุประสงค์

1. เพื่อตรวจสอบให้มั่นใจว่ากระบวนการทดสอบได้รับการป้องกันอย่างเหมาะสม

เอกสารที่เกี่ยวข้อง

1. RDM-PRC-Information System and Software Development

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยระหว่างการทดสอบ
2. ผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริง กรณีที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลที่เป็นข้อมูลจริงจะต้องมีการประเมินความเสี่ยงและหาแนวทางปกป้องเพื่อไม่ให้ข้อมูลรั่วไหล

ออกไป และต้องใช้ในช่วงเวลาที่สั้นที่สุดที่เป็นไปได้ โดยหลังจากดำเนินการ Test เสร็จสิ้นต้องทำการลบข้อมูลทันที

4.4.20. การป้องกันระบบสารสนเทศระหว่างที่ทดสอบการตรวจประเมิน (Protection of information systems during audit testing)

วัตถุประสงค์

1. เพื่อตรวจสอบให้มั่นใจว่ามีการป้องกันข้อมูลและระบบสารสนเทศระหว่างการตรวจประเมินอย่างเหมาะสม

เอกสารที่เกี่ยวข้อง

1. PQA-PRC-Internal Audit Procedure

แนวทางการปฏิบัติ

1. ต้องมีการกำหนดกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยในระหว่างการตรวจประเมิน