Information Security Policy

นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

บริษัท โอสถสภา จำกัด (มหาชน) และบริษัทในเครือฯ

บังคับใช้ตั้งแต่วันที่ 1 พฤษภาคม 2568 เป็นต้นไป

Document Control

Approved by (Wannipa Bhakdibutr) Chief Executive Officer	
Reviewed by (Pajaree Saengcum) Head of Digital Technology	**Prepared by** (Anupas Siriwej) Head of Digital Service Excellence

Revision History

ทบทวนครั้งล่าสุด: เมษายน 2568
ทบทวนครั้งถัดไป: เมษายน 2569

แก้ไขครั้งที่	วันที่เริ่มใช้	รายละเอียดการแก้ไข
00	13 พฤษภาคม 2559	ฉบับเริ่มต้น
01	1 มีนาคม 2563	- เปลี่ยนชื่อนโยบายภาษาไทย - ปรับปรุงเนื้อหาทั้งฉบับ
02	1 มกราคม 2567	- ปรับระยะเวลาการจัดเก็บ Log - แก้ไขชื่อหน่วยงาน
03	1 เมษายน 2567	- เปลี่ยนชื่อนโยบายภาษาอังกฤษ
04	1 พฤษภาคม 2568	- เพิ่มหมวดการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) - ปรับปรุงเนื้อหาการควบคุมการเข้ารหัสข้อมูล (Cryptographic Control) - ปรับความถี่ของการทดสอบการเจาะระบบ

OSOTSPA	**หน่วยงาน (Unit / Division) :** Digital Technology
	ประเภทเอกสาร (Document Type) : นโยบาย (Policy)
	หมายเลขเอกสาร (Document Number) : M-HM-ITD-001 **แก้ไขครั้งที่ (Revision) : 4**
	Effective Date : 1 พฤษภาคม 2568 **หน้า/จำนวนหน้า (Page No.) : 3** of **29**

เรื่อง (Subject) : นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

บทนำ

บริษัท โอสถสภา จำกัด (มหาชน) กำหนดให้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศฉบับนี้ เพื่อกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยต้องดำเนินการควบคุมดูแล ติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบายฯ และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตลอดจนการทำให้ระบบคอมพิวเตอร์ และระบบเครือข่ายต่างๆ ทำงานอย่างมีประสิทธิภาพ และเกิดประสิทธิผลสูงสุดในการดำเนินการธุรกิจของบริษัท โอสถสภา จำกัด (มหาชน) และบริษัทในเครือฯ ทั้งในประเทศ และต่างประเทศ ให้มีมาตรฐานในระดับเดียวกัน โดยพนักงานและผู้ใช้งานทุกคนต้องปฏิบัติตามนโยบายฯ ฉบับนี้

วัตถุประสงค์

1. เพื่อกำหนดมาตรฐานในการปฏิบัติงาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้มีความปลอดภัยในการใช้งานระบบสารสนเทศให้กับผู้ใช้งาน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และตรงตามวัตถุประสงค์ที่กำหนดไว้ รวมถึงให้ผู้ใช้งานตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ
2. เพื่อป้องกันไม่ให้ระบบสารสนเทศ และข้อมูลสารสนเทศถูกบุกรุก โจมตี เปลี่ยนแปลงแก้ไข ทำลาย หรือการกระทำอื่นๆ ที่อาจสร้างความเสียหาย ต่อการดำเนินการธุรกิจ
3. เพื่อกำหนดมาตรฐานหรือแนวปฏิบัติงานการบริหารงานระบบสารสนเทศ และงานข้อมูลสารสนเทศ ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายหรือระเบียบข้อบังคับที่เกี่ยวข้อง รวมทั้งกฎหมายการปกป้องข้อมูลส่วนบุคคล
4. เพื่อเผยแพร่นโยบายฯ ให้กับผู้ใช้งาน และบุคคลภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงข้อมูล หรือระบบสารสนเทศได้รับทราบ และปฏิบัติอย่างเคร่งครัด

ขอบเขตหน้าที่ความรับผิดชอบ

บริษัท โอสถสภา จำกัด (มหาชน) กำหนดให้มีนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร และทบทวน หรือปรับปรุงนโยบายฯ โดยหน่วยงาน Digital Technology อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมต่างๆ เช่น ธุรกิจ กฎเกณฑ์ กฎหมาย หรือเทคโนโลยี เป็นต้น นอกจากนี้กำหนดให้เผยแพร่นโยบายฯ ในลักษณะที่ผู้ใช้งานสามารถเข้าถึงได้ เพื่อให้พนักงาน และผู้ใช้งานที่เกี่ยวข้องรับทราบ และปฏิบัติตามที่นโยบายฯ กำหนด

พนักงาน และผู้ใช้งานทุกคนมีหน้าที่ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเคร่งครัด และให้ความร่วมมืออย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศ ตลอดจนหมั่นตรวจสอบ สอดส่องดูแล ปกป้องข้อมูล และระบบสารสนเทศให้มีความปลอดภัย

บทลงโทษ

นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศฉบับนี้ ถือเป็นส่วนหนึ่งของข้อกำหนด ในการปฏิบัติงานของพนักงานและผู้ใช้งานทุกคน หากพบผู้ใดฝ่าฝืน ไม่ปฏิบัติตามข้อกำหนด หรือละเมิดนโยบายอาจถูกพิจารณาลงโทษทางวินัยตามระเบียบข้อบังคับของบริษัท โอสถสภา จำกัด (มหาชน) รวมถึงการดำเนินคดีตามกฎหมายหากการละเมิดนั้นผิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ฉบับที่ประกาศบังคับใช้ในช่วงเวลานั้นๆ และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง

หมวดที่ 1 : การกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี (Governance of Enterprise IT)

บทนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจ และถือเป็นหนึ่งในระบบงานหลักที่หากเกิดเหตุขัดข้องขึ้นอาจส่งผลกระทบต่อการดำเนินงานทางธุรกิจ ดังนั้นผู้บริหารระดับสูงจึงต้องมีบทบาทสำคัญในการบริหารจัดการ การนำระบบเทคโนโลยีสารสนเทศมาใช้ในการประกอบธุรกิจ รวมถึงมีหน้าที่ในการส่งต่อเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนงานระดับองค์กรสู่เป้าหมายที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศภายใต้การกำกับดูแลของคณะกรรมการบริษัทฯ

วัตถุประสงค์

เพื่อให้มั่นใจว่าการนำระบบเทคโนโลยีสารสนเทศ มาใช้ในการประกอบธุรกิจนั้น สามารถบรรลุเป้าหมายตามที่กำหนดไว้ โดยมีการใช้ทรัพยากรอย่างเหมาะสม และมีการบริหารจัดการความเสี่ยงอย่างเหมาะสมสอดคล้องกับการกำกับดูแลกิจการที่ดี เป็นไปตามมาตรฐาน (Corporate Governance)

ข้อกำหนด

1. กำหนดให้มีนโยบายเป็นลายลักษณ์อักษรในการกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศ โดยให้มีเนื้อหาที่ครอบคลุมหัวข้อดังต่อไปนี้
   1) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถยอมรับได้
   2) การจัดสรร และบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้
   3) การจัดให้มีนโยบาย และมาตรการรักษาความปลอดภัยของระบบสารสนเทศ เพื่อให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ
2. กำหนดให้มีการกำกับดูแล และบริหารจัดการด้านเทคโนโลยีสารสนเทศ โดยให้มีเนื้อหาที่ครอบคลุมหัวข้อดังต่อไปนี้
   1) สื่อสารนโยบายการกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศให้แก่บุคคลากร อย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลากรเข้าใจ และสามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง
   2) กำหนดขั้นตอน และวิธีปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศ
   3) ทบทวน หรือปรับปรุงนโยบายการกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยให้ทบทวนทันทีเมื่อมีเหตุการณ์ใดๆ หรือการเปลี่ยนแปลงของกฎหมายและระเบียบข้อบังคับ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศ ตลอดจนต้องปรับปรุงขั้นตอน และวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

หมวดที่ 2 : การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (IT Security)

1. แนวทางปฏิบัติเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

กำหนดให้มีนโยบายเป็นลายลักษณ์อักษรในการกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศ

1. การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ
    1) การควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศ (Access Control)
    2) การสร้างความปลอดภัยด้านกายภาพ และสภาพแวดล้อม (Physical and Environmental Security)
2. การจัดการข้อมูลสารสนเทศและการรักษาความลับ
    1) การจำแนกประเภททรัพย์สินสารสนเทศ (IT Asset Classification) เพื่อกำหนดมาตรการรักษาความปลอดภัย
    2) การสำรองข้อมูล (Data Backup)
    3) การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)
3. การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน
    1) การควบคุมการใช้งานของผู้ใช้งาน (End User) เช่น
        - การป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน (Protection of Unattended User Equipment)
        - การใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอก (Mobile Device and Teleworking)
        - การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน (Installation of Software on Operational Systems)
    2) การควบคุมดูแลผู้รับดำเนินการด้านระบบสารสนเทศ (IT Outsourcing)
4. การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับ-ส่งข้อมูลสารสนเทศ
    1) การรักษาความปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)
    2) การควบคุมการรับ-ส่งข้อมูลสารสนเทศ (Information Transfer)
5. การป้องกันภัยคุกคามต่อระบบสารสนเทศ
    1) การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (Protection From Malware)
    2) การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)
6. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

2. การจัดโครงสร้างความปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

วัตุประสงค์

1. เพื่อควบคุมการปฏิบัติหน้าที่ด้านการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ สำหรับส่วนงานต่าง ๆ ให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
2. เพื่อกำหนดมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก รวมทั้งการใช้งานอุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบงานภายใน

ข้อกำหนด

1. การจัดโครงสร้างภายใน (Internal Organization)
   1) กำหนดหน้าที่ความรับผิดชอบด้านการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยระบุรายละเอียดหน้าที่ความรับผิดชอบ เพื่อให้เป็นแนวทางปฏิบัติสำหรับผู้ที่เกี่ยวข้องในทุกส่วนงาน
   2) แบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties) ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศออกจากกันอย่างชัดเจน เพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกัน
   3) แบ่งแยกบุคคลากรและสิทธิในการปฏิบัติหน้าที่ของส่วนงานพัฒนาระบบ (System Development) ออกจากบุคคลากรที่ทำหน้าที่บริหารจัดการดูแลระบบ (System Administration) ซึ่งปฏิบัติงานในระบบงานจริง (Production Environment)
   4) มีบุคลากรสำรอง (Delegates) ในการปฏิบัติงาน เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีที่จำเป็น และเร่งด่วน
   5) หน่วยงาน Digital Technology กำหนดให้มีผู้ทำหน้าที่สำหรับการติดต่อของหน่วยงานที่ปฏิบัติงานระบบสารสนเทศ เพื่อให้สามารถติดต่อประสานงานในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ และทบทวน ปรับปรุงรายชื่อ สำหรับการติดต่อให้เป็นปัจจุบันอย่างสม่ำเสมอ
2. การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (Moveable Device: Computer Notebook, Mobile Device)
   1) กำหนดให้ลงทะเบียนอุปกรณ์เคลื่อนที่ (Moveable Device) เช่นยี่ห้อ รุ่น ระบบปฏิบัติการ รหัสประจำเครื่อง (Serial Number) และหมายเลขอ้างอิงอุปกรณ์เครือข่าย (IP Address / MAC Address) เป็นต้น ก่อนการใช้งานรวมถึงการทบทวนทะเบียนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม
   2) มีการป้องกันข้อมูลที่เป็นความลับ หรือมีความสำคัญ (Sensitive Data) กรณีที่อุปกรณ์เคลื่อนที่สูญหาย เช่นกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (Lock Screen) หรือการลบข้อมูลจากระยะไกล (Remove Wipe-out) เป็นต้น
   3) กำหนดประเภทการใช้งานแอปพลิเคชัน (Application Service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์เคลื่อนที่ และควบคุมจำกัดการเข้าถึง เพื่อคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่นจำกัดให้เข้าถึงการใช้งานบางประเภทหากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น
   4) จัดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญทั้งที่จัดเก็บในอุปกรณ์เคลื่อนที่ และที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์
   5) จัดให้มีการสื่อสารให้ผู้ใช้งานลงนามรับทราบ เพื่อสร้างความตระหนัก และทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงที่อาจเกิดขึ้นได้
   6) ควบคุมการติดตั้งซอฟต์แวร์ และโปรแกรมที่ถูกต้องตามลิขสิทธิ์ เพื่อปิดช่องโหว่ (Patch) ป้องกันโปรแกรมไม่ประสงค์ดี (Malware) ทั้งนี้เพื่อป้องกันการบุกรุก หรือก่อให้เกิดความเสียหายต่อข้อมูลสารสนเทศที่จัดเก็บในอุปกรณ์เคลื่อนที่
   7) จัดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความปลอดภัยของข้อมูลสารสนเทศ เช่นการตัดสิทธิการใช้งาน หรือตัดการเชื่อมต่อ โดยทันทีที่ทราบเหตุ เป็นต้น
3. การปฏิบัติงานจากเครือข่ายภายนอก (Teleworking)
   1) กำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสมเพียงพอกับขอบเขตการปฏิบัติงาน สำหรับพื้นที่ปฏิบัติงานภายนอก
   2) การควบคุมสิทธิการเข้าใช้งาน การเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสมตามหน้าที่ความรับผิดชอบ
   3) การรักษาความมั่นคงปลอดภัยของระบบงานภายในที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์ กรณีการเชื่อมต่อ หรือรับส่งข้อมูลที่เป็นความลับ หรือมีความสำคัญจากภายนอก (Remote Access) มีการติดตั้ง Firewall การ Update โปรแกรม

ป้องกัน Malware การกำหนดสิทธิการเข้าถึง และการเข้ารหัสข้อมูล (Data Encryption) หรือการเข้ารหัสระบบเครือข่าย (Network Encryption) เป็นต้น

4) มีระบบป้องกันการรั่วไหลของข้อมูลสารสนเทศ (Data Leak Prevention)

5) กำหนดรหัสผู้ใช้งาน และการใช้รหัสผ่านยืนยันตัวบุคคล เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งาน เช่นญาติพี่น้อง และเพื่อน เป็นต้น

6) ตรวจสอบสิทธิการเข้าถึงของพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานจากเครือข่ายภายนอก

7) มีการป้องกันโปรแกรมไม่ประสงค์ดี เช่น Malware และ Virus เป็นต้น

4. การใช้บริการ Cloud Computing

1) กำหนดนโยบายการใช้งาน Cloud Computing โดยอย่างน้อยมีเนื้อหาดังนี้

- ประเมินความเสี่ยงเกี่ยวกับการใช้บริการ
- กำหนดประเภทงาน และรูปแบบของการใช้บริการ เช่น Software as a Service (SaaS), Platform as a Service (PaaS) และ Infrastructure as a Service (IaaS)
- กำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ (Due Diligence) โดยให้ความสำคัญเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (Availability)
- กำหนดการทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอ เช่น ความเพียงพอของการให้บริการ (Capacity Planning) เพื่อให้มั่นใจว่าผู้ให้บริการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการทางธุรกิจอย่างต่อเนื่อง
- จัดให้มีการเผยแพร่นโยบายเกี่ยวกับการใช้บริการ และสื่อสารให้พนักงานที่เกี่ยวข้องพร้อมทั้งลงนามรับทราบ เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ Cloud Computing
- กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน เช่น การสำรองข้อมูล เป็นต้น
- การรับเรื่องแก้ไขปัญหา ขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อ เป็นต้น
- กำหนดความปลอดภัยของข้อมูลแต่ละประเภทที่ใช้ใน Cloud โดยกำหนดระดับชั้นของข้อมูลตาม Information Safeguarding Guideline
- กำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภท เพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- กำหนดใช้วิธีพิสูจน์ตัวตนแบบ Multi-Factor Authentication สำหรับการเข้าถึงหน้าผู้ดูแลระบบ (Administrator Page) สำหรับระบบสารสนเทศที่มีความสำคัญ
- กำหนดให้มีการตรวจสอบบันทึกหลักฐานต่างๆ และติดตามปัญหาที่อาจส่งผลต่อการใช้บริการ

2) กำหนดข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ โดยมีลักษณะดังนี้

- ผู้ใช้บริการถือเป็นเจ้าของข้อมูลสารสนเทศ
- กำหนดประเภทบริการที่จะใช้ Cloud Computing
- กำหนดมาตรฐานความปลอดภัยด้านเครือข่าย เช่นการเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีในลักษณะ Distributed Denial of Service : DDoS การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์

ดี การป้องกันภัยคุกคามในรูปแบบใหม่ (Advanced Persistent Threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอปพลิเคชัน (Application) การป้องกันการบุกรุกแบบลำดับชั้น (Defense-in-Depth) และการสร้างความปลอดภัยให้กับระบบสารสนเทศ (Hardening) เป็นต้น

- ระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพ และสภาพโดยรวมของระบบ อย่างชัดเจน
- กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล กระบวนการแก้ไขปัญหา ระดับการให้บริการ (Service Level Agreement) ระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (Recovery Time Objectives : RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective : RPO) อย่างชัดเจน
- กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามที่กำหนดในข้อตกลง
- กำหนดให้เนื้อหา หรือเอกสารที่เกี่ยวข้องกับข้อตกลงมีการระบุรายละเอียดที่เกี่ยวข้องกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ
- ผู้ให้บริการไม่มีสิทธิเข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการ หรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล (Cloud Server Hosting Country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (Origin Country)
- ผู้ให้บริการควรปรับปรุงการปฏิบัติงานให้เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากลฉบับปัจจุบันโดยทันที เช่น ISO27001 เป็นต้น หากมาตรฐานดังกล่าวไม่ถูกปรับปรุงให้เป็นปัจจุบัน (Update)
- มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (Exit Plan) เช่น กำหนดระยะเวลารักษาข้อมูล และวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้
- มีข้อกำหนดในการใช้บริการ Cloud Computing ต่อจากผู้ให้บริการรายอื่น (Subcontract) อย่างชัดเจน โดยอย่างน้อยควรมีเงื่อนไขกำหนดให้บริการดังกล่าวเป็นส่วนหนึ่งของผู้ให้บริการ และผู้ให้บริการควรรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการกระทำหรือการดำเนินการใดๆ ของผู้ให้บริการรายอื่น

3) การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการควรดำเนินการเพิ่มเติม ดังนี้

- ติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่างๆ หรือข้อตกลงในการให้บริการ
- ประเมินความเพียงพอของระบบงานของผู้ให้บริการ (Capacity Planning) อย่างสม่ำเสมอ
- ทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
- ทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่นการตรวจสอบกระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

3. การสร้างความปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อให้พนักงาน และบุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูล หรือระบบงานภายในมีความรู้ ความเข้าใจ ตระหนัก และปฏิบัติงานโดยคำนึงถึงการรักษาความปลอดภัยของระบบสารสนเทศ

ข้อกำหนด

1. ให้ความรู้เกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่พนักงาน และบุคคลภายนอกที่ปฏิบัติงาน
2. มีการสื่อสารให้บุคลากร และบุคคลภายนอกที่ปฏิบัติงานดังกล่าว มีความระมัดระวัง และงดเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายต่อการดำเนินการธุรกิจ และต้องรายงานผู้มีหน้าที่รับผิดชอบ ในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศโดยทันที เมื่อพบความผิดปกติใดๆ อย่างมีนัยสำคัญ

   ตัวอย่าง ความเสียหายต่อการดำเนินการธุรกิจ เช่นการหมิ่นประมาท ข่มขู่ ปลอมแปลงเป็นบุคคลอื่น การส่งจดหมายอิเล็กทรอนิกส์แบบลูกโซ่ และเปิดเผยข้อมูลที่เป็นความลับ เป็นต้น
3. กำหนดมาตรการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืน หรือไม่ปฏิบัติตามนโยบายฯ หรือหลักเกณฑ์เกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

4. การบริหารจัดการทรัพย์สินสารสนเทศ (IT Asset Management)

วัตุประสงค์

1. เพื่อควบคุมทรัพย์สินสารสนเทศ และโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศ ระบบการเชื่อมต่อเครือข่ายให้มีความปลอดภัย
2. เพื่อให้ทรัพย์สินสารสนเทศได้รับการป้องกัน และปกป้องดูแลรักษาอย่างเหมาะสม รวมทั้งลดความเสี่ยงต่อการถูกเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศที่ถูกจัดเก็บในสื่อบันทึกข้อมูล

ข้อกำหนด

1. หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (Responsibility for Assets)
   1) กำหนดให้หน่วยงาน Digital Technology มีหน้าที่ดูแลรับผิดชอบทรัพย์สินสารสนเทศประเภท Hardware และ Software ตลอดอายุการใช้งานของทรัพย์สินดังกล่าว
   2) กำหนดให้พนักงานทุกคนมีหน้าที่ในการรับผิดชอบคอมพิวเตอร์ที่ถือครอง เช่นคอมพิวเตอร์ Desktop และ Notebook เพื่อใช้ในการทำงานตลอดอายุการใช้งานของทรัพย์สินดังกล่าว
   3) มีการทบทวนหน้าที่ความรับผิดชอบที่มีต่อทรัพย์สินสารสนเทศให้สอดคล้องกับหน้าที่ของผู้ปฏิบัติงาน เมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ
   4) หน่วยงาน Digital Technology มีหน้าที่รับผิดชอบดูแลบริหารจัดการทรัพย์สินสารสนเทศประเภทระบบ หรืออุปกรณ์ต้องมีการจัดทำ และจัดเก็บทะเบียนทรัพย์สิน ตลอดจนมีการทบทวนอย่างน้อยทุก 3 ปี หรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินสารสนเทศ

2. การจำแนกประเภททรัพย์สินสารสนเทศ (IT Asset Classification)
    1) กำหนดมาตรฐานการดูแลรักษาความมั่นคงปลอดภัยโดยมีการจำแนกประเภทของข้อมูล และจัดประเภททรัพย์สินสารสนเทศตามลำดับความสำคัญ เป็นต้น
    2) การบริหารจัดการสื่อบันทึกข้อมูล มีแนวทางปฏิบัติ ดังนี้
        - มีกระบวนการทำลายข้อมูลตามมาตรฐานเพื่อป้องกันการรั่วไหล และไม่ให้สามารถกู้คืนข้อมูลได้ ในกรณีที่ไม่จำเป็นต้องใช้ข้อมูล
        - มีกระบวนการทำลายสื่อบันทึกข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับ หรือมีความสำคัญ
        - กำหนดอายุการใช้งานสื่อบันทึกข้อมูลรวมทั้งวิธีการนำข้อมูลกลับมาใช้ใหม่ เช่น Server, Switch, Media Tape Backup เป็นต้น ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน
        - จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต
        - จัดให้มีกระบวนการดูแลรักษาความปลอดภัยกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกนอกพื้นที่

5. การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

วัตถุประสงค์

1. เพื่อให้ข้อมูลมีความถูกต้องครบถ้วนและมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม
2. ให้ครอบคลุมตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน ไปจนถึงการทำลายข้อมูล รวมทั้งระบุชั้นความลับของข้อมูล (Labeling) อย่างชัดเจน

ข้อกำหนด

1. หน้าที่ความรับผิดชอบต่อข้อมูลบริษัท
    1) พนักงานทุกคนมีหน้าที่ในการปกป้องข้อมูลของบริษัท และไม่เปิดเผยแก่บุคคลภายนอกหรือสาธารณะหากไม่ใช่การปฏิบัติตามหน้าที่ความรับผิดชอบของตนเอง เพื่อให้การรักษาความลับและการจัดการข้อมูลเป็นไปอย่างเหมาะสม โดยกำหนดให้
        - เจ้าของข้อมูล คือ ผู้สร้างข้อมูล มีหน้าที่จัดชั้นความลับของข้อมูล ทำป้ายชื่อระบุชั้นความลับ และกำหนดสิทธิ์การเข้าถึงให้กับผู้ใช้ข้อมูล โดยมีมาตรการในการจัดการข้อมูลให้มีความมั่นคงปลอดภัย
        - ผู้ใช้ข้อมูล คือ ผู้ที่ได้รับอนุญาตจากเจ้าของข้อมูลให้เข้าถึงข้อมูลได้ มีหน้าที่ปฏิบัติและจัดการข้อมูลตามชั้นความลับที่เจ้าของข้อมูลกำหนดไว้

2. เกณฑ์การจัดชั้นความลับของข้อมูล (Data Classification)

1) เจ้าของข้อมูลต้องมีการจัดชั้นความลับของข้อมูล ไม่ว่าจะจัดเก็บในรูปแบบเอกสารหรืออิเล็กทรอนิกส์ ด้วยการพิจารณาถึงผลกระทบต่อบริษัทฯ ที่อาจเกิดขึ้นเมื่อข้อมูลถูกเปิดเผย โดยใช้เกณฑ์การจัดชั้นความลับของข้อมูลดังนี้

ระดับชั้นความลับ (Sensitivity Level)	คำจำกัดความ	ตัวอย่างข้อมูล
For Public Use	ข้อมูลที่ได้รับอนุมัติให้เปิดเผยหรือเผยแพร่ต่อสาธารณะ โดยไม่จำกัดการเข้าถึง ไม่มีเนื้อหาที่เป็นความลับ เป็นทรัพย์สินทางธุรกิจ หรือมีความอ่อนไหว	สื่อการตลาด ข่าวประชาสัมพันธ์ ประกาศรับสมัครงาน ประกาศและรายงานที่เผยแพร่ต่อสาธารณะ
Confidential (Internal and OSP Partner Use)	ข้อมูลที่ใช้ภายในบริษัทและเข้าถึงได้โดยบุคคลภายนอกที่ได้รับอนุญาต มีเนื้อหาที่เป็นความลับซึ่งไม่ควรเปิดเผยหรือเผยแพร่ต่อสาธารณะ กรณีเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ให้พิจารณาปิดบังข้อมูลบางส่วน (Masking) หรือเข้ารหัสก่อนส่งออก	ข้อตกลงกับซัพพลายเออร์ ใบเสนอราคา ใบสั่งซื้อ เอกสารโครงการที่ทำงานร่วมกับผู้รับจ้าง ข้อมูลด้านทรัพยากรบุคคลที่ต้องส่งให้บุคคลภายนอกตามระเบียบข้อบังคับหรือเพื่อสวัสดิการของพนักงาน
Confidential (Internal Use Only)	ข้อมูลสำหรับใช้ภายในบริษัทเท่านั้น มีเนื้อหาที่เป็นความลับ ห้ามเปิดเผยหรือเผยแพร่ออกนอกบริษัท กรณีมีความจำเป็นต้องอนุญาตให้บุคคลภายนอกเข้าถึงได้ ให้พิจารณาปิดบังข้อมูลความลับ (Masking) ก่อนปรับลดระดับชั้นความลับเพื่อส่งออก	นโยบายและขั้นตอนปฏิบัติงานภายในประกาศภายในของบริษัท เอกสารการประเมินผลงานของพนักงาน ข้อมูลด้านทรัพยากรบุคคลที่ไม่จำเป็นต้องส่งให้บุคคลภายนอก เป้ายอดขาย รายงานตรวจสอบภายใน
Highly Confidential (Restricted Distribution)	ข้อมูลที่มีความลับสูงสุด เข้าถึงได้เฉพาะบุคคลที่มีความจำเป็นและได้รับอนุญาตเท่านั้น การเปิดเผยโดยไม่ได้รับอนุญาตอาจก่อให้เกิดความเสียหายทางการเงิน ทางกฎหมายหรือกฎระเบียบ หรือมีผลกระทบต่อชื่อเสียงของบริษัท	แผนธุรกิจระดับผู้บริหาร แผนการควบรวมและเข้าซื้อกิจการ ความลับทางการค้า เช่น สูตรการผลิต

3. การจัดการทำป้ายชื่อและการจัดการข้อมูลตามชั้นความลับ (Data Labeling and Handling)

1) สำหรับข้อมูลในรูปแบบอิเล็กทรอนิกส์ ให้ดำเนินการอย่างน้อยดังนี้

การจัดการข้อมูล	ระดับชั้นความลับ			
	For Public Use	**Confidential (Internal and OSP Partner Use)**	**Confidential (Internal Use Only)**	**Highly Confidential (Restricted Distribution)**
การจัดทำป้ายชื่อ	-	แสดงให้เห็นอย่างชัดเจนในหน้าจอแสดงผล สื่อบันทึกข้อมูล และข้อความทางอิเล็กทรอนิกส์	แสดงให้เห็นอย่างชัดเจนในหน้าจอแสดงผล สื่อบันทึกข้อมูล และข้อความทางอิเล็กทรอนิกส์	แสดงให้เห็นอย่างชัดเจนในหน้าจอแสดงผล สื่อบันทึกข้อมูล และข้อความทางอิเล็กทรอนิกส์
การพิสูจน์ตัวตน	-	มีการพิสูจน์ตัวตน	มีการพิสูจน์ตัวตน	มีการพิสูจน์ตัวตนแบบ Multi-Factor Authentication
การควบคุมการเข้าถึง	-	เข้าถึงได้เฉพาะพนักงานและบุคคลภายนอกที่เกี่ยวข้อง	เข้าถึงได้เฉพาะพนักงานเท่านั้น	เข้าถึงได้เฉพาะพนักงานและบุคคลภายนอกมีความจำเป็นเท่านั้น
การรับส่งข้อมูลผ่านเครือข่าย (Data in Transit)	-	มีการเข้ารหัส	มีการเข้ารหัส	มีการเข้ารหัส
การจัดเก็บข้อมูลบนสื่อบันทึกข้อมูล (Data at Rest)	-	มีการเข้ารหัส	มีการเข้ารหัส	มีการเข้ารหัส
การทำลายข้อมูลในสื่อบันทึกข้อมูล	-	ทำลายข้อมูลเพื่อให้มั่นใจว่าจะไม่สามารถนำกลับมาได้อีก	ทำลายข้อมูลเพื่อให้มั่นใจว่าจะไม่สามารถนำกลับมาได้อีก	ทำลายข้อมูลเพื่อให้มั่นใจว่าจะไม่สามารถนำกลับมาได้อีก

2) สำหรับข้อมูลในรูปแบบเอกสาร ให้ปฏิบัติตามนโยบายการจัดการบริหารเอกสารของบริษัทฯ

6. การควบคุมการใช้งานระบบคอมพิวเตอร์ และระบบเครือข่าย (Access Control and Network Security)

วัตุประสงค์

1. เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงข้อมูล และอำนวยความสะดวกในการประมวลผลข้อมูลของระบบ
2. เพื่อควบคุมสิทธิการเข้าใช้งานระบบสารสนเทศอย่างเหมาะสม ตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน
3. เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ สามารถเข้าถึงระบบสารสนเทศได้
4. เพื่อป้องกันการเข้าถึงระบบสารสนเทศ และแอปพลิเคชันโดยไม่ได้รับอนุญาต และสร้างความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อกำหนด

1. การควบคุมการเข้าถึงตามข้อกำหนดทางธุรกิจ (Business Requirement of Access Control)
   1) การกำหนดสิทธิการเข้าถึงข้อมูล และระบบสารสนเทศตามความเหมาะสมกับการใช้งานตามหน้าที่ความรับผิดชอบของผู้ใช้งาน มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิของบุคคลที่ไม่มีความจำเป็นในการเข้าถึงอย่างทันเวลา
   2) การแบ่งแยกบทบาทหน้าที่ความรับผิดชอบ (Segregation of Duties) ของบุคคลที่เกี่ยวข้อง เช่น บุคคลผู้ร้องขอ (Access Request) บุคคลผู้มีอำนาจอนุมัติ (Access Authorization) และบุคคลผู้บริหารสิทธิการเข้าถึง (Access Administration) เป็นต้น ในกรณีที่ไม่สามารถดำเนินการได้ ต้องมีการพิจารณาการควบคุมในด้านอื่น เช่น การเฝ้าระวังการปฏิบัติงาน และการสอบทานหลักฐานการตรวจสอบ โดยหัวหน้างานหรือบุคคลอื่นซึ่งไม่มีความเกี่ยวข้องโดยตรงกับการปฏิบัติงานนั้นๆ
   3) รายละเอียดส่วนที่เกี่ยวกับการควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ เช่นระบุประเภท หรือบริการทางเครือข่าย (Network Services) และบุคคลที่ได้รับอนุญาตให้เข้าถึง กระบวนการควบคุมและป้องกันการเข้าถึง วิธีการเข้าถึงแบบปลอดภัย เทคนิคการระบุตัวตน และการติดตามการใช้งานของบุคคลที่ได้รับอนุญาตให้เข้าถึง
   4) มีระบบที่ระบุผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ได้อย่างชัดเจน โดยเฉพาะกรณีที่ใช้หมายเลขประจำเครื่องแบบ Dynamic IP Address เพื่อให้มีข้อมูลที่สามารถระบุผู้ใช้งานหมายเลข IP Address ในช่วงเวลาที่ใช้งานได้
2. การบริหารจัดการบัญชีผู้ใช้งาน (User Access Management)

   มีการบริหารจัดการบัญชีผู้ใช้งานโดยจำกัดการเข้าถึงข้อมูลสารสนเทศให้สามารถเข้าถึงได้ เฉพาะบุคคลที่ได้รับสิทธิการเข้าถึงดังนี้
   1) ทำการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศตามสิทธิและหน้าที่ในการทำงานที่ได้รับอนุมัติเท่านั้น
   2) จัดสรรสิทธิการเข้าถึงระดับสูงอย่างจำกัดและมีการควบคุมการเข้าถึงสิทธิดังกล่าว
   3) มีขั้นตอนการบริหารจัดการในการกำหนดรหัสผ่านตามมาตรฐานสากล
   4) มีการติดตาม และทบทวนระดับสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
   1) กำหนดสิทธิ์การเข้าใช้งานระบบตาม User ID โดยผู้ใช้งานทุกคนมีหน้าที่ต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดขึ้นภายใต้ User ID ของผู้ใช้งาน
   2) มีข้อกำหนดให้ผู้ใช้งานปฏิบัติตามขั้นตอนการใช้งาน และดูแลรับผิดชอบรหัสผ่านอย่างปลอดภัย
   3) ผู้ใช้งานเป็นผู้ดูแลรับผิดชอบบัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) รวมทั้งข้อมูลส่วนบุคคลที่นำมาใช้เพื่อเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ (Accountable for Safeguard)
4. การควบคุมการเข้าถึงระบบสารสนเทศ และแอปพลิเคชัน (System and Application Access Control) มีการป้องกันมิให้มีการเข้าถึงระบบสารสนเทศและแอปพลิเคชันโดยไม่ได้รับอนุญาต ดังนี้
   1) ควบคุมการเข้าถึง และการใช้งานข้อมูลสารสนเทศและฟังก์ชันต่างๆ ในแอปพลิเคชันของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ ให้สอดคล้องกับสิทธิที่ได้รับ
   2) จัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีความปลอดภัย และจำกัดการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ และจำกัดการเข้าถึงชุดคำสั่งควบคุมการทำงานของโปรแกรม
   3) มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม และมีการจัดเก็บและตรวจสอบ Log-in Attempt Log อย่างสม่ำเสมอ
   4) แนวทางปฏิบัติให้เป็นไปตามข้อกำหนด ดังนี้
      - กำหนดให้ผู้ใช้งานทุกคนต้องรับผิดชอบบัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ของตนเอง
      - กำหนดให้ผู้ใช้งานแต่ละรายมีชื่อผู้ใช้งาน (User ID) และรหัสผ่าน (Password) เป็นของตนเองเพื่อยืนยันตัวบุคคล
      - กำหนดให้เปลี่ยนรหัสผ่านของตนเองทันที หลังจากได้รับรหัสผ่านจากผู้ดูแลระบบสารสนเทศ โดยรหัสผ่านใหม่ต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร ต้องประกอบด้วยตัวอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ หรือขึ้นอยู่กับระบบงานนั้นๆ
      - กำหนดให้ผู้ใช้งานสามารถตั้งค่า หรือเปลี่ยนแปลงรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนให้ยืนยันความถูกต้อง
      - กำหนดให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสผ่านครั้งแรก และควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน หรือขึ้นอยู่กับระบบงานนั้นๆ
      - ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำกับรหัสที่ใช้งานครั้งล่าสุด 6 ครั้ง หรือขึ้นอยู่กับระบบงานนั้นๆ
      - กำหนดให้ระบบไม่ควรแสดงให้เห็นค่ารหัสผ่านบนหน้าจอระหว่างที่ผู้ใช้งานระบุรหัสผ่าน
      - มีระบบการเข้ารหัส (Encryption) ข้อมูลรหัสผ่าน เพื่อป้องกันการล่วงรู้ หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน Folder เดียวกันกับ Folder ที่จัดเก็บข้อมูลของแอปพลิเคชัน
      - หากมีการเข้าสู่ระบบผิดพลาดมากกว่า 6 ครั้ง หรือขึ้นอยู่กับระบบงานนั้นๆ ชื่อผู้ใช้งานต้องถูกล็อค และการปลดล็อคให้ดำเนินการโดยผู้ดูแลระบบสารสนเทศ หรือโดยระบบเมื่อได้รับอนุมัติจากหัวหน้างานของผู้ใช้งาน
      - มีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่นการใส่ซองปิดผนึก เป็นต้น

7. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

วัตุประสงค์

เพื่อให้การใช้งานระบบต่างๆ มีการเข้ารหัสข้อมูล (Cryptographic) และการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management) เป็นไปตามมาตรฐานสากล และมีความเหมาะสม มีประสิทธิภาพ ตลอดจนสามารถป้องกันการเข้าถึง หรือเปลี่ยนแปลง แก้ไขข้อมูลที่เป็นความลับ หรือมีความสำคัญต่อการดำเนินธุรกิจ

ข้อกำหนด

1. การใช้มาตรการการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)
   1) หน่วยงาน Digital Technology ต้องจัดให้มีการเข้ารหัสข้อมูลให้สอดคล้อง และเหมาะสมกับระดับชั้นความลับของข้อมูล
   2) มาตรฐานวิธีการเข้ารหัสข้อมูล (Cryptographic Algorithm) ต้องเป็นไปตามมาตรฐานสากล เช่น การใช้อัลกอริทึมขั้นต่ำ AES-128 สำหรับกุญแจแบบสมมาตร (Symmetric Key) และ RSA 2048 สำหรับกุญแจแบบอสมมาตร (Asymmetric Key)
   3) มีการทบทวนมาตรฐานวิธีการเข้ารหัสข้อมูลอยู่เสมออย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานอยู่ยังมีความมั่นคงเพียงพอในการรักษาความปลอดภัยของข้อมูล
2. การบริหารจัดการกุญแจ (Key Management)
   1) การสร้างและติดตั้งกุญแจเข้ารหัส ควรดำเนินการอย่างน้อยดังนี้
      - ควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสที่รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (Certification Authority) ที่น่าเชื่อถือและมีการทำลายข้อมูลที่อาจหลงเหลือภายหลังการสร้างกุญแจเข้ารหัสแล้วเสร็จ เพื่อป้องกันการเข้าถึงหรือกู้คืนกุญแจเข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น
      - กำหนดสิทธิการเข้าถึงกุญแจเข้ารหัสให้สามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น
      - กำหนดความยาวของกุญแจเข้ารหัสที่เพียงพอในการป้องกันการถูกถอดรหัส (Decrypt) โดยผู้ไม่หวังดี เช่น การโจมตีแบบ Brute Force เป็นต้น
      - แลกเปลี่ยนกุญแจเข้ารหัส (Key Exchange) ผ่านกระบวนการและช่องทางที่ปลอดภัย
   2) การจัดเก็บและการสำรองกุญแจเข้ารหัส ควรดำเนินการอย่างน้อยดังนี้
      - มีการรักษาความปลอดภัยในการจัดเก็บกุญแจเข้ารหัสทั้งด้านกายภาพ (Physical) และการควบคุมการเข้าถึง (Access Control) อย่างเหมาะสม
      - มีการสำรองข้อมูลกุญแจเข้ารหัสโดยวิธีการเก็บรักษาข้อมูลกุญแจเข้ารหัสชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสชุดหลัก
   3) การเพิกถอนหรือทำลายกุญแจเข้ารหัส ควรดำเนินการอย่างน้อยดังนี้
      - กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัส เช่น กรณีกุญแจเข้ารหัสหมดอายุการใช้งานหรือไม่ปลอดภัย เป็นต้น
      - กำหนดกระบวนการทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก
   4) ควรจัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมสำคัญที่เกี่ยวกับกุญแจเข้ารหัส เช่น การสร้างกุญแจ การสำรองกุญแจ การเข้าถึงหรือใช้งานกุญแจ และการเพิกถอนกุญแจ เป็นต้น

8. การสร้างความมั่นคงปลอดภัยด้านกายภาพ และสภาพแวดล้อม (Physical Security of Data Center Management)

วัตุประสงค์

1. เพื่อป้องกันไม่ให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้าม (Secure Areas) เช่นศูนย์คอมพิวเตอร์ (Data Center) ศูนย์คอมพิวเตอร์สำรอง (Backup Site) และพื้นที่ติดตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ ได้แก่ Floor Switch หรือ Router ซึ่งอาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศ หรือมีผลกระทบต่อข้อมูลที่เป็นความลับ หรือมีความสำคัญ
2. เพื่อป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ไม่ให้สูญหาย หรือเกิดความเสียหาย จากการเข้าถึง หรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง รวมทั้งเพื่อให้ทรัพย์สินสารสนเทศสามารถทำงานได้อย่างต่อเนื่อง

ข้อกำหนด

1. พื้นที่หวงห้าม (Restricted Areas)
   1) กำหนดให้พื้นที่ศูนย์คอมพิวเตอร์ พื้นที่ติดตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ และพื้นที่จัดเก็บทรัพย์สินสารสนเทศเป็นพื้นที่หวงห้าม (Restricted Areas)
   2) ออกแบบพื้นที่หวงห้ามโดยคำนึงถึงความปลอดภัยจากภัยธรรมชาติ ภัยคุกคามจากมนุษย์ และให้มีความมิดชิด รวมทั้งป้องกันไม่ให้มีการเปิดเผยข้อมูลรายละเอียดของพื้นที่หวงห้ามต่อสาธารณะ
   3) กำหนดสิทธิการเข้า-ออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง รวมถึงจัดให้มีระบบการควบคุมการเข้า-ออกอย่างรัดกุม และทบทวนสิทธิอย่างสม่ำเสมอ
   4) จัดให้มีระบบการรักษาความปลอดภัยภายในพื้นที่ศูนย์คอมพิวเตอร์ (Data Center) เช่นระบบกล้องวงจรปิด อุปกรณ์แจ้งเตือนสัญญาณไฟไหม้ ถังดับเพลิง หรือระบบดับเพลิงอัตโนมัติ ระบบไฟฟ้าสำรอง (UPS) หรือเครื่องกำเนิดไฟฟ้าสำรอง (Generator) และระบบควบคุมอุณหภูมิและความชื้นที่เหมาะสม เป็นต้น พร้อมทั้งดูแลบำรุงรักษาอย่างสม่ำเสมอ
   5) ควบคุม และติดตามบุคคลภายนอก หรือผู้ที่ไม่มีส่วนเกี่ยวข้องที่เข้าปฏิบัติงานในพื้นที่หวงห้ามอย่างใกล้ชิด
   6) แยกพื้นที่จุดรับ-ส่งของ ออกจากศูนย์คอมพิวเตอร์
   7) จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่นอุปกรณ์ Server และอุปกรณ์ Network ไว้ในพื้นที่หวงห้ามอย่างปลอดภัย
2. ทรัพย์สินสารสนเทศประเภทอุปกรณ์ (Equipment)
   1) จัดให้มีการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ที่อาจหยุดชะงักจากการทำงานผิดพลาดของระบบโครงสร้างพื้นฐาน เช่นระบบไฟฟ้า ระบบโทรคมนาคม ระบบระบายอากาศ และระบบปรับอากาศ เป็นต้น
   2) จัดให้มีมาตรการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร สายไฟ และอุปกรณ์ที่เกี่ยวข้อง เช่น Floor Switch ท่อเดินสายเคเบิล และสายไฟอย่างรัดกุม ตลอดจนการบำรุงดูแลรักษาอย่างสม่ำเสมอเพื่อไม่ให้เกิดความเสียหาย
   3) กำหนดให้มีการติดป้าย (Labelling) สำหรับอุปกรณ์ทั้งหมดภายในตู้จัดเก็บอุปกรณ์สื่อสาร (Rack Server)
   4) ควบคุมไม่ให้มีการนำทรัพย์สินสารสนเทศประเภทอุปกรณ์ออกนอกพื้นที่โดยไม่ได้รับอนุญาต และในกรณีที่ได้รับอนุญาตควรจัดให้มีการทำทะเบียนคุม และการรักษาความปลอดภัยโดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำใช้งานในสถานที่ต่างๆ
   5) ควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน เช่นการ Lock Screen หน้าจออัตโนมัติ หรือการกำหนด Session Time Out เป็นต้น

6) จัดให้ควบคุมป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งานให้มีความปลอดภัย รวมถึงการควบคุมเอกสารข้อมูล หรือสื่อบันทึกข้อมูลต่างๆ เช่น Thumb Drive และ External Hard Disk ที่มีข้อมูลสารสนเทศจัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือสถานที่ที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน

7) จัดให้มีการดูแลบำรุงรักษาทรัพย์สินสารสนเทศประเภทอุปกรณ์อย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วน และอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

8) กรณีที่ยกเลิกการใช้งาน หรือจำหน่ายทรัพย์สินสารสนเทศประเภทอุปกรณ์ด้านเครือข่าย เช่นอุปกรณ์ Switch, Firewall และ Router เป็นต้น ควรตรวจสอบทรัพย์สินว่ามีการลบ ย้าย หรือทำลายข้อมูล Configuration ที่สำคัญ หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (Reset to Factory Default) ด้วยวิธีการตามมาตรฐานเพื่อให้มั่นใจว่าไม่สามารถกู้คืนค่าได้อีก

9. การรักษาความปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

วัตุประสงค์

1. เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย
2. เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี หรือภัยคุกคามจากช่องโหว่ทางเทคนิค รวมถึงการป้องกันการสูญหายของข้อมูล
3. เพื่อบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศอย่างครบถ้วน และเพียงพอสำหรับการตรวจสอบ การสอบทานการใช้งานข้อมูล และระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย ตลอดจนการตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง การตรวจสอบและการป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติ หรือไม่เป็นไปตามกฎหมาย เพื่อให้มีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บ
4. เพื่อควบคุมให้ระบบทำงานโดยมีความถูกต้องครบถ้วน และมีความน่าเชื่อถือ (Integrity of Operational System)

ข้อกำหนด

1. กำหนดหน้าที่ความรับผิดชอบ และขั้นตอนการปฏิบัติงาน (Operational Procedures and Responsibilities)
   1) กำหนดให้มีคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ เพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์สามารถปฏิบัติงานได้อย่างถูกต้อง เช่นขั้นตอนในการเปิด-ปิดระบบ การประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และทบทวนขั้นตอนการปฏิบัติงานดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้อยู่ในสภาพที่พร้อมใช้งาน และเข้าถึงได้อยู่เสมอ
   2) ควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างระบบงาน ขั้นตอนการปฏิบัติงาน หรือการทำงานของระบบงานต่างๆ ซึ่งอาจกระทบต่อความปลอดภัยของระบบสารสนเทศ เช่น
      - กำหนดขั้นตอน หรือวิธีปฏิบัติที่เป็นลายลักษณ์อักษร ในกรณีที่มีการเปลี่ยนแปลง มีแผนรองรับ และดำเนินการทดสอบภายหลังการเปลี่ยนแปลง
      - มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง และมีขั้นตอนการขออนุมัติจากผู้มีอำนาจ
      - มีขั้นตอนการตรวจสอบเพื่อให้มั่นใจว่ากระบวนการเปลี่ยนแปลงดังกล่าวเป็นไปตามนโยบายด้านความปลอดภัยของระบบสารสนเทศ
      - มีการสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง
      - มีกระบวนการถอยกลับสู่สภาพเดิม (Fall-Back) ของระบบงาน หากเกิดข้อผิดพลาดระหว่างการเปลี่ยนแปลง

3) ติดตามประสิทธิภาพการทำงานของระบบสารสนเทศ และทรัพย์สินสารสนเทศประเภทอุปกรณ์ที่สำคัญ ให้ทำงานต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ และความเพียงพอ (Capacity) ของระบบสารสนเทศ รวมถึงเพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพด้วย

4) แบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) และใช้งานจริง (Production Environment) ออกจากกัน และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้อง ในแต่ละส่วนเท่านั้น

2. การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (Protection From Malware)

1) กำหนดการห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต

2) ติดตั้ง Firewall เพื่อป้องกัน และตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ที่ไม่ปลอดภัยอาจมีโปรแกรมไม่ประสงค์ดี

3) ติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงาน และแก้ไขปัญหากรณีพบภัยคุกคาม

4) ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้ง หรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาตให้ดำเนินการตรวจสอบทันที

5) ติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

3. การสำรองข้อมูล (Backup Data)

1) กำหนดขั้นตอน หรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อป้องกันการสูญหายของข้อมูล และเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยให้มีรายละเอียดข้อมูล ดังนี้

- ข้อมูลที่ต้องสำรองข้อมูล
- ความถี่ที่ต้องสำรองข้อมูล
- จำนวนที่ต้องสำรองข้อมูล
- ประเภทสื่อบันทึกข้อมูล สถานที่ และวิธีการเก็บรักษาสื่อบันทึกข้อมูล
- ขั้นตอน และวิธีการสำรองโดยละเอียด
- กระบวนการกู้คืนข้อมูลในกรณีที่สูญหาย

2) จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอน หรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวควรจัดให้มีระบบควบคุมการเข้า-ออก และระบบป้องกันความเสียหาย

3) กำหนดเป้าหมายในการกู้คืนข้อมูล เช่นกำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective : RPO)

4) กรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ให้คำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานด้วย เช่นการจัดเก็บข้อมูลในสื่อบันทึกประเภทใด มีการเก็บอุปกรณ์ และโปรแกรมที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วย

4. การบันทึก การจัดเก็บหลักฐาน และการติดตาม (Logging and Monitoring)

   1) กำหนดให้มีระบบบันทึก และจัดเก็บหลักฐาน (Log) การใช้งานเกี่ยวกับระบบสารสนเทศจากการสร้าง การถูกเปลี่ยนแปลง แก้ไขต่างๆ ให้ครบถ้วน และเพียงพอกับการตรวจสอบเพื่อป้องกันการทำความเสียหายของข้อมูล หรือเข้าถึงโดยไม่ได้รับอนุญาต

   2) กำหนดให้มีการป้องกันข้อมูล และระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับผู้ใช้งานทั่วไปรวมถึง System Administrator Log และ System Operator Log จากการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงแก้ไข

   3) กำหนดให้ตั้งค่านาฬิกาเวลา (Clock Synchronization) โดยกำหนดระบบเวลาของอุปกรณ์ และระบบสารสนเทศที่มีความสำคัญให้ตรงกับเวลาอ้างอิงตามมาตรฐานสากล

   4) กำหนดให้เก็บบันทึกข้อมูล (Log) แสดงเหตุการณ์ ของระบบงานที่มีความสำคัญต่างๆ เป็นหลักฐาน ดังนี้

ลำดับ	ประเภทการจัดเก็บหลักฐาน	รายละเอียดการจัดเก็บหลักฐาน	ระยะเวลาที่จัดเก็บ
1	หลักฐานการเข้าถึงพื้นที่หวงห้าม (Physical Access Log)	บุคคลที่เข้าถึง / วันเวลาที่ผ่านเข้า-ออก / ความพยายามในการเข้าถึง (ถ้ามี)	ไม่น้อยกว่า 90 วัน
2	หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์ (Authentication Log)	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / ความพยายามในการเข้าใช้งาน	ไม่น้อยกว่า 90 วัน
3	หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ (Application Log)	บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP Address) / วันเวลาที่มีการใช้งาน ต้องสามารถระบุตัวตนผู้ใช้งาน และ Local IP Address ในช่วงเวลาที่ใช้งานได้ (เฉพาะการใช้งานผ่านอุปกรณ์ของบริษัท) ทั้งนี้ขึ้นอยู่กับระบบ หรือเงื่อนไขของแอปพลิเคชันนั้นๆ	ไม่น้อยกว่า 90 วัน
4	หลักฐานการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายใน (Internet Access Log)	บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP Address) / หมายเลขอินเทอร์เน็ต (Organization IP Address) / วันเวลาที่มีการใช้งาน / ที่อยู่ของเว็บไซต์ปลายทาง (Full URL) ต้องสามารถระบุตัวตนผู้ใช้งานและ IP Address ในช่วงเวลาที่ใช้งานได้	ไม่น้อยกว่า 90 วัน
5	หลักฐานการใช้งานแฟ้มข้อมูล (Audit Log)	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / บันทึกการเรียกดูและการแก้ไขข้อมูล	ไม่น้อยกว่า 90 วัน
6	หลักฐานการบริหาร (Event Log) ระบบปฏิบัติการ และ Network Firewall	วันและเวลาที่เกิดเหตุการณ์ / เหตุการณ์ที่เกิดขึ้นกับ OS (Event Services) เช่น สถานะการให้บริการของ Service / เหตุการณ์ที่เกิดขึ้นกับ Network Firewall เช่น การปรับปรุง หรือแก้ไข Firewall Rules	ไม่น้อยกว่า 90 วัน
7	หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ของ Network Firewall (Network Firewall Log)	วันและเวลา / IP address ต้นทาง (Source) และปลายทาง (Destination) / Firewall Action / Port ที่ใช้ติดต่อ	ไม่น้อยกว่า 90 วัน

ลำดับ	ประเภทการจัดเก็บหลักฐาน	รายละเอียดการจัดเก็บหลักฐาน	ระยะเวลาที่จัดเก็บ
8	หลักฐานการจัดการบริหารข้อมูล (Database Log)	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน	ไม่น้อยกว่า 90 วัน
9	หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (Electronic Messaging)	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / ข้อมูลการติดต่อตลอดระยะเวลาการสนทนา	ไม่น้อยกว่า 90 วัน

5. การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน (Installation of Software on Operational Systems) โดยควบคุมการติดตั้ง และจำกัดสิทธิการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน เพื่อให้ระบบปฏิบัติงานต่างๆ มีความถูกต้องครบถ้วน และน่าเชื่อถือ (Integrity of Operational System)
6. การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)
    1) ทดสอบการเจาะระบบกับระบบงานที่มีความสำคัญ โดยโดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยง และผลกระทบทางธุรกิจ
        - ระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูงและมีช่องทางเชื่อมต่อกับเครือข่ายสาธารณะ (Internet Facing) ต้องทดสอบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ
        - ระบบงานอื่นๆ ที่มีความสำคัญให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบการเจาะระบบตามความเหมาะสม
    2) มีการประเมินช่องโหว่ของระบบกับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลง
    3) ดำเนินการปิดช่องโหว่ที่พบทันที โดยประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ก่อนการติดตั้งโปรแกรม ทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว
    4) มีกระบวนการจัดการช่องโหว่ด้านเทคนิคที่สอดคล้องกับกระบวนการจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (Incident Management) เพื่อเตรียมความพร้อมรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่
    5) มีการบันทึกและจัดเก็บหลักฐานเพื่อตรวจสอบการดำเนินการต่างๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค
7. การตรวจสอบระบบสารสนเทศ (Information System Audit)
    1) วางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้
    2) กำหนดขอบเขตในการตรวจสอบระบบสารสนเทศทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญ โดยการตรวจสอบดังกล่าวต้องไม่กระทบต่อการปฏิบัติงาน
    3) ตรวจสอบระบบสารสนเทศนอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบ

10. การจัดการความปลอดภัยด้านการสื่อสารผ่านระบบเครือข่าย (Communications Technology Security)

วัตุประสงค์

1. เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศของระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนการทำงานระบบเครือข่ายคอมพิวเตอร์
2. เพื่อรักษาความปลอดภัยในการรับ-ส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายใน และระหว่างระบบเครือข่ายภายในกับระบบเครือข่ายภายนอก

ข้อกำหนด

1. การบริการจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)
   1) มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัย โดยสามารถป้องกันไม่ให้เกิดการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์
   2) กำหนดการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ โดยระบุขอบเขตของระบบเครือข่ายย่อยอย่างชัดเจน และมีการควบคุมการเข้าถึงอย่างเหมาะสมให้สอดคล้องกับการรักษาความปลอดภัยของแต่ละขอบเขตตามที่ถูกจัดแบ่งไว้
   3) กำหนดการแบ่งแยกหน้าที่ความรับผิดชอบระหว่าง Network Administrator, Server Administrator และ Computer Administrator ออกจากกัน โดยกำหนดสิทธิการเข้าใช้งานตามหน้าที่และความรับผิดชอบ และขั้นตอนในการบริหารจัดการระบบและอุปกรณ์เครือข่ายให้ชัดเจน
   4) มีการควบคุมการเชื่อมต่อระบบเครือข่ายสาธารณะ (Public Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยผู้ใช้งานทุกคนต้องพิสูจน์ตัวตนด้วย User Login ผ่านระบบ Active Directory (AD) Authentication เพื่อป้องกันการรั่วไหลหรือเปลี่ยนแปลงแก้ไขข้อมูลที่ส่งผ่านระบบเครือข่ายดังกล่าว
   5) มีระบบ Firewall เพื่อป้องกันระบบที่เชื่อมต่อและแอปพลิเคชัน โดยแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ออกจากกัน
   6) จำกัดการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างเครือข่าย เช่นจำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (Port Outlet) ระหว่าง Server และ Client โดยเปิดใช้งาน Service Port ที่เชื่อมต่อตามความจำเป็นพร้อมทั้งมีวิธีการระบุถึงอุปกรณ์ที่เชื่อมต่อ (Authenticate) อย่างชัดเจน เช่น IP Address และประเภทของอุปกรณ์ เป็นต้น
   7) จัดให้มีระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานทดแทนกันได้ (Network Load Balance) เพื่อให้ระบบเครือข่ายคอมพิวเตอร์มีสภาพพร้อมใช้งาน และลดผลกระทบต่อการดำเนินธุรกิจ
   8) กำหนดการเชื่อมต่อเครือข่ายจากภายนอก โดยผู้ใช้งานเครือข่ายจากภายนอก หรือจากการเชื่อมต่อผ่านอุปกรณ์เคลื่อนที่ เช่น Notebook หรือ Mobile Device ต้องระบุตัวตน หรือยืนยันตัวตนผ่านช่องทางที่กำหนดในการเข้าใช้งาน
   9) จัดเก็บบันทึกหลักฐาน (Logs) ที่ใช้งานระบบเครือข่าย เพื่อเฝ้าระวังและติดตามเหตุการณ์ที่ผิดปกติของการใช้งาน และเพื่อตรวจสอบการทำงานที่เกี่ยวข้องที่อาจส่งผลกระทบต่อความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์
   10) จัดทำข้อตกลงการใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์กับผู้ให้บริการภายนอก เพื่อให้มีความปลอดภัยต่อระบบเครือข่ายคอมพิวเตอร์
2. การควบคุมการรับ-ส่งข้อมูลสารสนเทศ (Information Transfer)
   1) กำหนดแนวทางปฏิบัติการรับ-ส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างเครือข่ายภายในองค์กรกับเครือข่ายภายนอกให้มีความปลอดภัย
      - จัดให้มีแนวทางปฏิบัติการรับ-ส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่างๆ
      - มีกระบวนการป้องกันการรับ-ส่งข้อมูลสารสนเทศออกนอกเส้นทางที่กำหนดไว้ การดักรับสัญญาณ การเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดี (Malware) ที่ถูกส่งผ่านช่องทางการสื่อสาร
      - มีกระบวนการป้องกันข้อมูลที่เป็นความลับ หรือมีความสำคัญ ที่รับ-ส่งในรูปแบบไฟล์แนบ (Attached Files) และส่งต่อ e-Mail แบบอัตโนมัติออกสู่ภายนอก (Data Leak Prevention)
      - การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับ-ส่งข้อมูลสารสนเทศที่เป็นความลับ และมีความสำคัญผ่านช่องทางการสื่อสารบางประเภทที่ต้องการรักษาความปลอดภัย เช่นการใช้งานระบบ Cloud Computing เป็นต้น

2) กำหนดมาตรการรักษาความปลอดภัยของข้อมูลสารสนเทศที่มีการรับ-ส่งผ่านระบบเครือข่ายคอมพิวเตอร์
   - จัดให้มีการป้องกันการเปลี่ยนแปลงแก้ไข หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
   - มีการจัดการ และควบคุมให้ระบบทำงานรับ-ส่งข้อมูลได้อย่างถูกต้อง และพร้อมใช้งานอยู่เสมอ
   - การส่งข้อมูล หรือข้อความทาง e-Mail ในการรับ-ส่งข้อมูล หรือทางสื่ออิเล็กทรอนิกส์ ต้องคำนึงถึงความปลอดภัยของข้อมูล
   - มีการขออนุมัติการใช้งานระบบรับ-ส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ที่ให้บริการโดยบุคคลภายนอก
3) การใช้งานระบบรับ-ส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Electronic Messaging)
   - กำหนดมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
   - กำหนดให้มีกระบวนการตรวจสอบผู้ใช้งานโดยต้องระบุตัวตนทุกครั้งเมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
   - มีการควบคุมการใช้งานระบบรับ-ส่งข้อมูลข่าวสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้บริการโดยบุคคลภายนอก
     - โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (Instant Messaging) ระบบเครือข่ายสังคมออนไลน์ (Social Network) เช่น LINE, Facebook, Instagram, WhatsApp เป็นต้น
     - โปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (File Sharing) on Cloud เช่น OneDrive, GoogleDoc, Dropbox เป็นต้น

     โดยการขอใช้งาน Application เหล่านี้ต้องได้รับอนุมัติโดยผู้บริหารสูงสุดของหน่วยงานเท่านั้น และหน่วยงาน Digital Technology มีหน้าที่ควบคุม (Control List) อย่างเคร่งครัด
   - กำหนดให้ผู้ใช้งานต้องปฏิบัติตามกฎหมาย (พรบ.) และหลักเกณฑ์อย่างเคร่งครัด
4) กำหนดให้มีการทำข้อตกลงการรักษาความลับ หรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements) โดยผู้ใช้งานภายใน และผู้รับดำเนินการ ต้องทำสัญญารักษาความลับ หรือไม่เปิดเผยข้อมูลที่มีความสำคัญต่อความปลอดภัยด้านเทคโนโลยีสารสนเทศ
   - การระบุความเป็นเจ้าของข้อมูลที่สำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีการป้องกันการรั่วไหลของข้อมูล
   - การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ต้องจัดให้มีการลงนามโดยผู้รับผิดชอบ
   - กำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูล หรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม
   - กำหนดสิทธิการเข้าถึงข้อมูลเพื่อเฝ้าระวัง ติดตาม และตรวจสอบการใช้งานข้อมูลที่มีความสำคัญ
   - กำหนดให้มีการแจ้งเตือนและรายงานต่อที่ผู้เกี่ยวข้องหากพบว่ามีการรั่วไหล หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
   - กำหนดมาตรการดำเนินการ กรณีละเมิด หรือยกเลิกสัญญารวมถึงข้อกำหนดการส่งคืน หรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดสัญญา

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

วัตุประสงค์

1. เพื่อให้กระบวนการ ขั้นตอนในการปฏิบัติงานด้านระบบสารสนเทศ มีรูปแบบมาตรฐานการทำงานที่ชัดเจน และมีความปลอดภัยต่อการดำเนินธุรกิจ ตั้งแต่กระบวนการจัดหา กระบวนการพัฒนาระบบ การใช้งาน และการดูแลรักษา
2. เพื่อให้การพัฒนา หรือเปลี่ยนแปลงแก้ไขระบบสารสนเทศประมวลผลได้อย่างถูกต้องครบถ้วน มีประสิทธิภาพ และเป็นไปตามความต้องการของผู้ใช้งาน (Change Management)
3. เพื่อลดข้อผิดพลาด และป้องกันการสูญหาย ตลอดจนการแก้ไขอย่างไม่ถูกต้องที่อาจเกิดขึ้นต่อระบบสารสนเทศ
4. เพื่อการรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบงานสารสนเทศ (System Development Life Cycle : SDLC)

ข้อกำหนด

1. การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Security Requirements of Information Systems)
   1) มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศให้มีความปลอดภัย เมื่อมีระบบสารสนเทศใหม่ หรือมีการปรับปรุงระบบเดิม
   2) มีการรักษาความปลอดภัยของข้อมูลสารสนเทศ ในกรณีที่มีการเข้าถึงระบบการให้บริการ (Application Services)
2. การรักษาความปลอดภัยของกระบวนการพัฒนาระบบสารสนเทศ (Security in Development and Support Process)
   1) กำหนดให้ควบคุมการพัฒนา หรือเปลี่ยนแปลงแก้ไขระบบสารสนเทศในทุกขั้นตอนให้เป็นไปตามข้อกำหนด
      - มีการทำคำขอโดยหน่วยงานหรือผู้ใช้งาน เมื่อต้องการให้พัฒนา หรือเปลี่ยนแปลงแก้ไขระบบสารสนเทศ โดยจัดทำเป็นลายลักษณ์อักษร และอนุมัติคำขอโดยผู้มีอำนาจเพื่อควบคุมผลข้างเคียงที่อาจเกิดขึ้นจากการแก้ไขระบบ เช่น Business Process Owner : BPO เป็นต้น
      - ทำการประเมินความเสี่ยง หรือผลกระทบที่อาจจะเกิดขึ้นต่อการพัฒนาเปลี่ยนแปลงแก้ไขระบบงาน
      - มีการควบคุมบุคลากร ขั้นตอน และเทคโนโลยีสารสนเทศสำหรับการพัฒนาระบบสารสนเทศตลอดการพัฒนาระบบ
      - มีการควบคุมติดตามการพัฒนาระบบสารสนเทศของผู้รับดำเนินการให้เป็นไปตามข้อตกลงการใช้บริการ เช่นการรักษาความลับของข้อมูลที่นำมาประมวลผล การควบคุมการนำข้อมูลเข้า และออกจากระบบที่อยู่ระหว่างการพัฒนา การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบอย่างรัดกุมเหมาะสม มีการติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบ เป็นต้น
      - กรณีที่มีการจ้างหน่วยงาน หรือบุคคลจากภายนอก เข้ามาพัฒนาระบบ กำหนดให้มีการกำกับดูแล เฝ้าระวัง และติดตามกระบวนการพัฒนาระบบที่จ้างหน่วยงานภายนอกดำเนินการ ให้มีการดำเนินการตามนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
   2) กำหนดขั้นตอนวิธีปฏิบัติในการพัฒนาเปลี่ยนแปลง แก้ไขระบบงานเป็นลายลักษณ์อักษร โดยมีข้อกำหนดเกี่ยวกับการร้องขอ การพัฒนาเปลี่ยนแปลง แก้ไข และการทดสอบ ตลอดจนกระบวนการโอนย้ายระบบงานเพื่อใช้งานจริง
      - มีการแบ่งแยกส่วนคอมพิวเตอร์ หรือแอปพลิเคชันสำหรับการพัฒนาระบบงาน (Development Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) โดยกำหนดสิทธิ และควบคุมการเข้าถึงเฉพาะผู้ที่ได้รับมอบหมายหรือมีเกี่ยวข้องในแต่ละส่วนงานเท่านั้น

3) กำหนดขั้นตอนวิธีปฏิบัติกรณีที่มีการเปลี่ยนแปลง แก้ไขระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) สำหรับการขออนุมัติจากผู้มีอำนาจทุกครั้ง

4) กำหนดให้มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาเปลี่ยนแปลงแก้ไขโดยผู้ใช้งาน หรือผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบ เพื่อให้มั่นใจว่าระบบสารสนเทศดังกล่าวทำงานได้อย่างมีประสิทธิภาพ สามารถประมวลผลได้ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

5) กำหนดให้ปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับการพัฒนาเปลี่ยนแปลงแก้ไขระบบสารสนเทศ

6) กำหนดให้จัดเก็บเวอร์ชันของโปรแกรมที่ได้รับการพัฒนา และจัดทำเอกสารประกอบการพัฒนาระบบ

- จัดเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน โดยมีรายละเอียดการพัฒนาเปลี่ยนแปลงแก้ไข
- ปรับปรุงเอกสารประกอบระบบงานหลังจากที่ได้พัฒนาเปลี่ยนแปลงแก้ไข เพื่อให้ทันสมัยอยู่เสมอ และจัดเก็บเอกสารในที่ปลอดภัย มีความสะดวกต่อการใช้งาน
- จัดเก็บโปรแกรมเวอร์ชันก่อนการเปลี่ยนแปลงแก้ไขไว้ใช้งานเมื่อมีความจำเป็นต้องถอยกลับสู่สภาพเดิม (Fall-Back) ของระบบในกรณีที่ระบบงานผิดพลาด หรือไม่สามารถใช้งานได้

7) กำหนดให้มีการสื่อสารถึงการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

8) กำหนดให้บันทึก และจัดเก็บหลักฐานทั้งหมดที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

12. การบริการระบบสารสนเทศจากผู้รับดำเนินการ (IT Outsourcing)

วัตุประสงค์

1. เพื่อจัดทำข้อกำหนดต่างๆ และหลักเกณฑ์การปฏิบัติงาน สำหรับการรับบริการ หรือการใช้บริการให้สอดคล้องตามวัตถุประสงค์ มีประสิทธิภาพ และมีความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)
2. เพื่อป้องกันทรัพย์สินสารสนเทศ จากการเข้าถึงโดยผู้รับดำเนินการอย่างไม่เหมาะสม
3. เพื่อควบคุมผู้รับดำเนินการ ให้ส่งมอบงานถูกต้องครบถ้วน และเป็นไปตามข้อตกลงที่ได้จัดทำไว้

ข้อกำหนด

1. การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศจากผู้รับดำเนินการ (Information Security in IT Outsourcing)

   1) กำหนดให้มีการแบ่งแยกประเภทของผู้ให้บริการ (IT Outsourcing Classification) และประเมินความเสี่ยงของผู้ให้บริการ (IT Outsourcing Risk Assessment) เพื่อให้มีแนวทางการบริหารจัดการผู้ให้บริการแต่ละประเภท และลดความเสี่ยงที่อาจจะเกิดขึ้นภายหลัง

   2) กำหนดวิธีการคัดเลือก และประเมินผู้รับดำเนินการ (Due Diligence) โดยให้ความสำคัญเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) ตลอดจนความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (Available)

   3) กำหนดให้มีแนวทางการควบคุมดูแลผู้รับดำเนินการเป็นลายลักษณ์อักษร เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม และทบทวนคุณสมบัติของผู้รับดำเนินการอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้รับดำเนินการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการในการดำเนินธุรกิจอย่างต่อเนื่อง

4) กำหนดให้ทำสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) หรือสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) โดยระบุขอบเขตงาน และเงื่อนไขการให้บริการ (Services Level Agreement : SLA) อย่างชัดเจน ทั้งนี้ให้ลงนามร่วมกันระหว่างผู้มีอำนาจหน้าที่ลงนาม และผู้ให้บริการ
5) กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการ และระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้รับดำเนินการเข้าถึงได้ โดยจัดให้มีขั้นตอน กระบวนการควบคุม และติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสม ภายใต้หลักความจำเป็นในการเข้าถึงข้อมูล
6) มีการรักษาความปลอดภัย กรณีที่มีการถ่ายโอนข้อมูลสารสนเทศ และควบคุมความครบถ้วนถูกต้องของข้อมูล และการประมวลผลที่ได้รับจากผู้รับดำเนินการ
7) กำหนดกระบวนการควบคุมอย่างเป็นมาตรฐานเพื่อติดตามการทำงานของผู้รับดำเนินการ
8) กำหนดให้มีการติดตาม ทบทวน และตรวจสอบผู้รับดำเนินการอย่างสม่ำเสมอ ทั้งในด้านกระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการ
9) กรณีที่ผู้รับดำเนินการมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน ในการรักษาความปลอดภัยของการปฏิบัติงาน กำหนดให้ประเมินความเสี่ยงจากการเปลี่ยนแปลง และกระบวนการจัดการความเสี่ยงให้สอดคล้องเหมาะสม
10) การเปลี่ยนแปลงผู้รับดำเนินการกำหนดให้พิจารณาผลการปฏิบัติงาน ตามความเหมาะสมในการเปลี่ยนแปลงเท่าที่จำเป็น รวมถึงการพิจารณาความเสี่ยงที่อาจกระทบต่อการดำเนินการทางธุรกิจระหว่างการเปลี่ยนแปลง
11) ข้อตกลงเกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ มีดังนี้
    - รายละเอียดของข้อมูลที่จำเป็นในการเข้าถึงข้อมูลโดยผู้รับดำเนินการ รวมทั้งวิธีการเข้าถึงข้อมูล
    - การจัดแบ่งประเภทข้อมูลตามระดับชั้นของข้อมูล ให้สอดคล้องกับข้อกำหนดตาม Information Safeguarding Guideline
    - กำหนดมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับ หรือมีความสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมาย
    - กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการในการปฏิบัติงานภายใต้การควบคุมต่างๆ เช่นการกำหนดเงื่อนไขการเข้าถึงข้อมูล การติดตามตรวจสอบการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลง และกำหนดให้ผู้รับดำเนินการรายงานผลการปฏิบัติงาน การแก้ไขปัญหาต่างๆ ภายในระยะเวลาที่กำหนด เป็นต้น
    - แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม
    - แผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ
    - รายชื่อ และช่องทางสำหรับติดต่อบุคคล หรือหน่วยงานอื่นๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งบุคคล หรือหน่วยงานที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
    - ข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรณีที่ผู้รับดำเนินการมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ (Sub-Contracting to Another Supplier)

2. การควบคุมการส่งมอบงานของผู้รับดำเนินการ (Supplier Services Delivery Management)

1) มีการติดตาม ประเมิน ทบทวน และตรวจสอบผู้รับดำเนินการอย่างสม่ำเสมอ ตลอดจนการประเมินความเสี่ยง และกำหนดกระบวนการบริหารจัดการความเสี่ยงในกรณีที่ผู้รับดำเนินการเปลี่ยนแปลงกระบวนการขั้นตอน หรือวิธีการปฏิบัติงาน
2) กรณีที่ใช้บริการด้านการพัฒนาระบบ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมี

การติดตาม ควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่ควบคุม ดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิด

3) กรณีที่ผู้รับดำเนินการเข้ามาปฏิบัติหน้าที่ภายในหน่วยงาน (Onsite Service) กำหนดให้เจ้าหน้าที่ผู้มีอำนาจหน้าที่ตรวจสอบการทำงานของผู้รับดำเนินการอย่างละเอียด

4) กรณีที่เป็นการให้บริการในลักษณะ Remote Access กำหนดให้ระบุระยะเวลาการเข้าใช้งานชัดเจน และดำเนินการปิดการใช้งานทันทีที่ให้บริการเสร็จสิ้น

5) กำหนดให้ผู้รับดำเนินการต้องจัดทำคู่มือปฏิบัติงาน และเอกสารที่เกี่ยวข้องก่อนการส่งมอบงาน

6) กำหนดให้ผู้รับดำเนินการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข เมื่อพบเจอปัญหา

7) กำหนดให้มีขั้นตอนในการตรวจรับงานของผู้รับดำเนินการให้มีความถูกต้องเป็นไปตามเงื่อนไข และข้อตกลง

13. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

วัตุประสงค์

1. เพื่อบริหารจัดการเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการตรวจสอบและแก้ไขอย่างถูกต้อง รวดเร็ว และมีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม
2. เพื่อให้ผู้ที่เกี่ยวข้องเกิดการเรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้น และปรับปรุงแก้ไข ซึ่งเป็นการป้องกันการเกิดเหตุการณ์ทางด้านความปลอดภัยในครั้งต่อไป

ข้อกำหนด

1. กำหนดให้มีขั้นตอน และกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ
   1) กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร
   2) ประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
   3) จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (Point of Contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (Escalation)
   4) ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลาย หรือกลับสู่ภาวะปกติอย่างรวดเร็ว
   5) รวบรวมและจัดเก็บหลักฐานโดยทันทีเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ เช่นความเสียหายกับข้อมูลหรือทรัพย์สินของลูกค้าโดยคำนึงถึงประเด็นสำคัญต่างๆ มีกระบวนการการจัดเก็บอย่างมั่นคงปลอดภัย การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง เพื่อวิเคราะห์ตรวจสอบและจัดทำเอกสารสรุปนำเสนอต่อบุคคลที่มีหน้าที่รับผิดชอบ
   6) บันทึกและจัดเก็บหลักฐานการบริหารจัดการตามความจำเป็นและเหมาะสม
   7) ตรวจหา ติดตาม วิเคราะห์ และรายงานเหตุการณ์ ทั้งนี้ ให้รวมถึงการวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

2. กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ
3. กำหนดให้มีการรายงานต่อผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
4. พิจารณาทบทวน ทดสอบ ขั้นตอน และกระบวนการในการบริหารจัดการที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ โดยให้ครอบคลุมการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill) อย่างน้อยปีละ 1 ครั้ง

   คำอธิบายเพิ่มเติม ความเสี่ยงไซเบอร์ (Cyber Security Drill) คือ ภัยคุกคามที่ส่งผลกระทบ หรือสร้างความเสียหาย หรือก่อให้เกิดความเสี่ยงต่อการดำเนินการธุรกิจ ซึ่งเกิดจากการใช้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม เป็นต้น

5. กำหนดให้มีการประเมินผลการทดสอบ และประเมินผลพิจารณาทบทวน โดยต้องรายงานผลต่อผู้บริหาร ทั้งนี้การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
6. กำหนดให้จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการในการบริหารจัดการเหตุการณ์ เป็นระยะเวลาไม่น้อยกว่า 2 ปี นับแต่วันที่จัดทำเอกสาร โดยต้องเก็บรักษาไว้ในลักษณะที่สามารถเรียกดู และพร้อมให้ตรวจสอบได้โดยทันที

14. การบริหารจัดการความต่อเนื่องทางธุรกิจด้านความปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

วัตุประสงค์

1. เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) และระบบสารสนเทศอยู่ในสภาที่พร้อมใช้งานอยู่เสมอ
2. เพื่อรองรับการดำเนินการทางธุรกิจได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุฉุกเฉิน สถานการณ์ความเสียหายที่มีต่อระบบสารสนเทศ
3. เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญ อันเป็นผลมาจากการล้มเหลว ติดขัด หยุดชะงัก หรือเกิดเหตุการณ์ฉุกเฉินที่มีผลกระทบต่อการทำงานของระบบสารสนเทศ ให้สามารถทำงานได้อย่างต่อเนื่อง
4. เพื่อให้สามารถกู้คืนระบบสารสนเทศกลับมาสู่สภาพการทำงานตามปกติ ได้ในระยะเวลาที่รวดเร็ว และไม่ส่งผลกระทบต่อการดำเนินธุรกิจ

ข้อกำหนด

1. กำหนดมาตรการรองรับกรณีที่เกิดเหตุการณ์ฉุกเฉินของระบบสารสนเทศ
   1) กำหนดความต้องการด้านความปลอดภัยของระบบสารสนเทศ และสถานการณ์ความเสียหายที่เกิดขึ้น เช่นการเกิดภัยพิบัติทางธรรมชาติ หรือการเกิดวิกฤตทางการเมือง เป็นต้น
   2) ระบุข้อมูลระบบ หรือแอปพลิเคชัน และกระบวนการที่มีความสำคัญต่อการดำเนินธุรกิจ
   3) สำรองข้อมูลเพื่อรักษาความถูกต้องสมบูรณ์ และมีความพร้อมใช้งานของข้อมูลสารสนเทศ รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ โดยรูปแบบและความถี่ในการสำรองข้อมูลให้พิจารณาตามความจำเป็น
   4) จัดทำแผนการรองรับกรณีเกิดเหตุฉุกเฉินเป็นลายลักษณ์อักษร เกี่ยวกับแผนการปฏิบัติงาน กระบวนการ ขั้นตอนปฏิบัติงาน การติดต่อประสานงานผู้ที่เกี่ยวข้อง หรือสภาพแวดล้อมการปฏิบัติงานเปลี่ยนแปลง

5) จัดทำแผนการรองรับกรณีเกิดเหตุฉุกเฉินที่สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ การทดสอบแผน และการรายงานผลการทดสอบให้ผู้ที่เกี่ยวข้องรับทราบ โดยจัดให้มีการทดสอบอย่างน้อยปีละ 1 ครั้ง

2. กำหนดขั้นตอน กระบวนการดำเนินการ และควบคุมเกี่ยวกับความปลอดภัยของระบบสารสนเทศให้สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ

1) กำหนดผู้เข้าร่วมทดสอบ แผนการรองรับกรณีเกิดเหตุฉุกเฉิน (DRP: Disaster Recovery Plan) ที่เกี่ยวข้องทั้งภายใน และภายนอก โดยพิจารณาตามเหตุการณ์ที่ซักซ้อมของแต่ละครั้งเมื่อเกิดเหตุภัยพิบัติ เพื่อเชิญเข้าร่วมทดสอบแผนการรองรับกรณีเกิดเหตุฉุกเฉิน

2) มีการตรวจสอบ ทบทวน ปรับปรุงแผนการปฏิบัติงาน กระบวนการ และขั้นตอนการปฏิบัติงานของแผนการรองรับกรณีเกิดเหตุฉุกเฉินให้มีความทันสมัยอยู่เสมออย่างน้อยปีละ 1 ครั้งเพื่อให้มีแนวทาง และมาตรฐานระดับความต่อเนื่องด้านความปลอดภัยของระบบสารสนเทศตามที่กำหนดไว้ และเพื่อให้มั่นใจว่ามาตรการที่กำหนดไว้นั้นยังถูกต้อง และได้ผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น

3. กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินการปกติของระบบสารสนเทศ และจัดลำดับความสำคัญของการกู้คืนระบบสารสนเทศให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น

1) กำหนดให้มีการตรวจสอบสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

2) กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานตามปกติของระบบสารสนเทศ

3) จัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญทุกระบบงาน ให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น

4) จัดให้มีการสำรองระบบสารสนเทศ เพื่อให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

4. มีระบบสารสนเทศสำรองที่อยู่ในสภาพพร้อมใช้งานให้สอดคล้องกับระยะเวลาในการกลับคืนสู่สภาพการดำเนินการปกติของระบบสารสนเทศ

1) กำหนดให้มีศูนย์คอมพิวเตอร์สำรอง และระบบสารสนเทศสำรอง โดยให้ระบุรายละเอียดของสถานที่สำรอง หรือแผนที่ เป็นต้น เพื่อรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุฉุกเฉิน

2) กำหนดรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของคอมพิวเตอร์, คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) รวมถึง Configuration และอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นต้น

3) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการสนับสนุนการปฏิบัติตามแผนการรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan) และเงื่อนไขการเรียกใช้แผน

4) กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานตามปกติของระบบสารสนเทศ และลำดับการกู้คืนของระบบงานสารสนเทศที่มีความสำคัญทุกระบบ ให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น