PPS

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(IT Security Policy)

บริษัท โปรเจค แพลนนิ่ง เซอร์วิส จำกัด (มหาชน)

และบริษัทในเครือ

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เป็นฉบับทบทวนครั้งที่ 3 ทบทวนโดยฝ่ายวิจัยและพัฒนานวัตกรรม มีผลบังคับใช้ตั้งแต่วันที่ 1 มีนาคม 2567 เป็นต้นไป

บันทึกการปรับปรุง

ทบทวนครั้งที่	วันที่บังคับใช้	รายละเอียด	หมายเหตุ
00	27 กุมภาพันธ์ 2563	จัดทำ IT Policy ฉบับแรก	-
01	4 มกราคม 2565	เพิ่มเติมนโยบาย - การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล - การใช้งานจดหมายอิเล็กทรอนิกส์	-
02	15 พฤศจิกายน 2565	ปรับปรุงรายละเอียดในนโยบาย ให้สอดคล้องกับการดำเนินงานในปัจจุบัน	-
03	1 มีนาคม 2567	- แก้ไขชื่อเอกสารเป็น “นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)” - ปรับปรุงให้สอดคล้องกับข้อกำหนดของระบบมาตรฐาน ISO 27001:2022	-

ผู้จัดทำ	ผู้ทบทวน	ผู้อนุมัติ
(นางสาวศิวพร สุวรรณศรี) เจ้าหน้าที่เทคโนโลยีสารสนเทศอาวุโส	(นายชาญชัย ริ้วกุลประเสริฐ) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ	(นายประสงค์ ธาราไชย) ประธานบริษัท

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

(IT Security Policy)

วัตถุประสงค์ของนโยบาย

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท โปรเจค แพลนนิ่ง เซอร์วิส จำกัด (มหาชน) และบริษัทในเครือ หรือต่อไปนี้เรียกว่า "องค์กร" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ องค์กรจึงเห็นสมควรกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และป้องกันภัยคุกคามต่างๆ สอดคล้องกับข้อกำหนดของระบบ **มาตรฐาน ISO 27001:2022 การจัดการความมั่นคงปลอดภัยสารสนเทศ** โดยมีวัตถุประสงค์ดังต่อไปนี้

1. การจัดทำนโยบายด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
2. นโยบายนี้จะต้องทำการเผยแพร่ให้ผู้บริหารและพนักงานทุกระดับในองค์กรได้รับทราบ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

หลักการในการจัดทำนโยบาย

1. มุ่งเน้นการกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศ ให้มีการรักษาความลับ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีสภาพพร้อมใช้งานอยู่เสมอ (Availability) โดยกำหนดเป็นแนวปฏิบัติดังนี้

1) **ในด้านการรักษาความลับ (Confidentiality)** เพื่อป้องกันการเข้าถึงข้อมูลในระบบสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต จึงต้องมีการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) ระบบปฏิบัติการ (Operating System Access Control) แอพพลิเคชั่นหรือโปรแกรมประยุกต์ (Application and Information Access Control) การควบคุมทางกายภาพ (Physical Security) และการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

2) **ในด้านการรักษาความถูกต้องครบถ้วน (Integrity)** เพื่อให้ข้อมูลสารสนเทศมีความถูกต้อง ครบถ้วน ไม่ถูกเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหายหรือถูกทำลายโดยไม่ได้รับอนุญาต จึงต้องมีการกำหนดการเข้าถึงและควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control) และการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3) **ในด้านการรักษาสภาพพร้อมใช้งาน (Availability)** เพื่อให้ระบบสารสนเทศสามารถเข้าถึงหรือใช้งานได้ในเวลาที่ต้องการ จึงต้องมีระบบสำรองข้อมูล เพื่อเตรียมความพร้อมในกรณีฉุกเฉิน

2. การสร้างความเข้าใจให้กับผู้ใช้งานระบบ เพื่อให้เกิดความตระหนักถึงผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

3. ทบทวนนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร ให้สอดคล้องกับสภาพแวดล้อมและกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง

องค์ประกอบของนโยบาย

นโยบายนี้จัดทำขึ้นให้มีความสอดคล้องกับมาตรฐานสากลด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 รวมทั้งข้อกำหนดและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาสินทรัพย์ด้านสารสนเทศขององค์กร จากภาวะคุกคามที่อาจจะเกิดขึ้นจากภายในและภายนอก ซึ่งเป็นแนวนโยบายในภาพรวมเพื่อบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยสาระสำคัญประกอบด้วย

1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)
2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)
3 การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)
4 การบริหารจัดการทรัพย์สิน (Asset Management)
5 การควบคุมการเข้าถึง (Access Control)
6 การเข้ารหัสข้อมูล (Cryptography)
7 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)
8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)
9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)
10 การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)
11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)
12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
13 การบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Management)
14 การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษของการละเมิดนโยบายฯ (Compliance)

ผู้รับผิดชอบตามนโยบายขององค์กร

เพื่อให้การดำเนินตามนโยบายด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มีการกำหนดหน้าที่รับผิดชอบให้แก่ผู้ที่เกี่ยวข้อง เพื่อดูแล ควบคุมให้เป็นไปตามที่กำหนด ดังนี้

- ผู้จัดการฝ่ายวิจัยและพัฒนานวัตกรรม หรือ ผู้จัดการฝ่ายไอที

รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางการแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงาน และตรวจสอบระบบความปลอดภัยของระบบสารสนเทศ พร้อมรายงานผลการดำเนินงาน รวมทั้งรับผิดชอบ ดังนี้

1) ควบคุมการเข้า-ออกห้องแม่ข่าย ตามการกำหนดสิทธิการเข้าถึง
2) กำกับดูแล ติดตาม ตรวจสอบ การเข้าใช้งาน และการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์เครื่อง Server และอุปกรณ์เครือข่าย (Network) ให้สามารถ ใช้งานได้ตามปกติตลอดเวลา

3) กำกับดูแล การติดตั้ง รื้อถอน ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายระบบ LAN, Internet, Intranet ที่ให้บริการภายในองค์กร
4) กำกับ ดูแล รักษา ตรวจสอบ การทำงานของระบบแจ้งเตือนภัยภายในห้องแม่ข่าย ให้มีการทำงานเป็นปกติอยู่ตลอดเวลา
5) แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยง และความเสียหายที่เกิดขึ้นกับระบบสารสนเทศขององค์กร
6) กำกับ ดูแล การป้องกันการถูกคุกคามทางระบบสารสนเทศ และแก้ไขปัญหาการถูกบุกรุกจากบุคคลภายนอกที่ไม่ได้รับอนุญาต (Hacker)
7) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกบุกรุกจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ภายใน Server ให้สามารถใช้งานได้ปกติตลอดเวลา
8) กำกับดูแล ตรวจสอบ การกำหนดหรือแก้ไขเปลี่ยนแปลงค่าพารามิเตอร์ต่างๆของระบบ
9) รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบ

- เจ้าหน้าที่ดูแลระบบสารสนเทศ (System Administrator) หรือ เจ้าหน้าที่ไอที รับผิดชอบดังนี้
  1) ทำการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery) ตามระยะเวลาที่กำหนด
  2) บริหารจัดการสิทธิการเข้าถึงเครื่องแม่ข่าย (Server) เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
  3) บำรุงรักษาอุปกรณ์แม่ข่าย (Server) ให้สามารถใช้งานได้เป็นปกติตลอดเวลา
  4) แก้ไขปัญหา อุปสรรค หรือความเสี่ยงต่างๆที่เกิดขึ้นกับระบบงานเครื่องแม่ข่าย
  5) กำหนด แก้ไข หรือเปลี่ยนแปลงค่าพารามิเตอร์ของระบบต่างๆ
  6) บริหารจัดการสิทธิการเข้าถึงข้อมูลของระบบสารสนเทศต่างๆ (User Access Management) ตามอำนาจหน้าที่และความจำเป็น และตรวจสอบสิทธิผู้ใช้งานตามรอบระยะเวลาที่กำหนด
  7) แก้ไขปัญหา อุปสรรคต่างๆ ในการใช้งานระบบสารสนเทศ
  8) ควบคุมการใช้ทรัพยากร ทั้งฮาร์ดแวร์และซอฟต์แวร์ ให้เป็นไปตามนโยบายที่กำหนด
  9) อื่นๆตามที่ได้รับมอบหมาย
- เจ้าหน้าที่อื่นๆ ที่เกี่ยวข้อง ตามอำนาจหน้าที่ที่ได้รับมอบหมาย ให้เป็นผู้ปฏิบัติและมีหน้าที่รับผิดชอบเกี่ยวกับระบบสารสนเทศขององค์กร

การบังคับใช้นโยบาย

นโยบายฉบับนี้มีผลบังคับนับแต่วันที่ประกาศใช้

สารบัญ

หน้า

-1-

นโยบายความมั่นคงปลอดภัยสารสนเทศ

(Information Security Policy)

1.1 วัตถุประสงค์

เพื่อกำหนดกรอบและแนวทางการดำเนินการด้านความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เพื่อให้เกิดการดำเนินการตามมาตรฐานสากล และสอดคล้องกับข้อกำหนดและระเบียบปฏิบัติที่เกี่ยวข้อง

1.2 ผู้ที่เกี่ยวข้องกับนโยบาย

นโยบายฯ นี้มีผลบังคับใช้กับบุคลากรของบริษัท โปรเจค แพลนนิ่ง เซอร์วิส จำกัด (มหาชน) และบริษัทในเครือ รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

1.3 การใช้งาน

การใช้งานสารสนเทศรวมถึงระบบเทคโนโลยีสารสนเทศ ต้องเป็นไปอย่างเหมาะสม และปฏิบัติอย่างถูกต้องตามกฎหมายและระเบียบปฏิบัติต่างๆ ที่เกี่ยวข้อง

1.4 ขอบข่ายที่มีผลบังคับใช้

นโยบายนี้มีผลบังคับใช้กับพื้นที่ที่สามารถเข้าถึงระบบสารสนเทศขององค์กร รวมถึงการเรียกใช้งานจากระยะไกลและการเชื่อมโยงจากองค์กรภายนอก การอนุญาตและมอบสิทธิในการเข้าถึงทุกระบบฯ ต้องดำเนินการตามนโยบายฯ และได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจเกิดขึ้น

1.5 การตรวจสอบและทบทวน

ต้องกำหนดให้มีผู้ทำหน้าที่กำกับดูแลนโยบายฯ และรับผิดชอบตรวจสอบการดำเนินงานตามนโยบายฯ อย่างสม่ำเสมอ โดยให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์เปลี่ยนแปลงที่สำคัญ

-2-

โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ

(Organizational of Information Security)

2.1 โครงสร้างภายในด้านความมั่นคงปลอดภัยสารสนเทศ (Internal Organization)

วัตถุประสงค์

เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร และการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย

นโยบาย

2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ผู้บริหารระดับสูง เป็นผู้รับผิดชอบการบริหารจัดการและกำกับดูแลภาพรวมของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร โดยมอบหมายให้ฝ่ายไอทีทำหน้าที่รับผิดชอบในส่วนของนโยบายการรักษาความมั่นคงปลอดภัย ทั้งนี้ให้หน่วยงานที่เป็นเจ้าของข้อมูลที่อยู่ในระบบส่วนกลาง รับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติขององค์กร

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

ต้องมีการแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน เพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงทรัพย์สินสารสนเทศ หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม

2.1.3 ข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with Authorities)

ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider), ผู้ให้บริการ Cloud Service เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

2.1.4 การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)

ต้องมีการกำหนดระเบียบ ข้อบังคับ กฎเกณฑ์ต่าง ๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูลเพื่อให้มีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานจากภายนอก และการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

นโยบาย

ต้องมีการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานด้วยอุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล โดยต้องมีการกำหนดมาตรการบริหารจัดการและแนวปฏิบัติ

การรักษาความปลอดภัยด้านทรัพยากรมนุษย์

(Human resource security)

3.1 การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงาน

นโยบาย

ต้องกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นลายลักษณ์อักษร และต้องมีการตรวจสอบคุณสมบัติของผู้สมัครตามระเบียบที่เกี่ยวข้อง

3.2 การสร้างความความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During employment)

วัตถุประสงค์

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบาย

บุคลากรขององค์กร หรือผู้ได้รับจ้าง ต้องปฏิบัติตามนโยบายฯ และแนวปฏิบัติขององค์กร โดยต้องมีการให้ความรู้และฝึกอบรมด้านความมั่นคงปลอดภัยแก่บุคลากร

ในกรณีที่มีผู้กระทำความผิดต้องมีกระบวนการสอบสวนและลงโทษตามระเบียบขององค์กรด้วย

3.3 การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

วัตถุประสงค์

เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

นโยบาย

เมื่อสิ้นสุดการเป็นบุคลากร หรือมีการโยกย้าย เปลี่ยนหน้าที่ความรับผิดชอบ หรือการเปลี่ยนสัญญาการจ้างงาน ต้องมีการคืนทรัพย์สินขององค์กร และเพิกถอนหรือมอบสิทธิที่เหมาะสมในการเข้าถึงระบบสารสนเทศของบุคลากรนั้น

- 4-

การบริหารจัดการทรัพย์สิน
(Asset Management)

4.1 การบริหารจัดการทรัพย์สินสารสนเทศ (IT Assets Management)

วัตถุประสงค์

เพื่อให้ทรัพย์สินขององค์กรได้รับการปกป้อง ดูแล อย่างเหมาะสม

นโยบาย

4.1.1 นโยบายการควบคุม ดูแล จัดการทรัพย์สินสารสนเทศให้ปลอดภัย

1) มีการจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ (Information Classification) จัดทำทะเบียนทรัพย์สิน (Inventory of Assets) และกำหนดหน้าที่และความรับผิดชอบต่อทรัพย์สินอย่างเหมาะสม

2) มีการควบคุมการอนุญาตให้ใช้ทรัพย์สินสารสนเทศและอุปกรณ์ที่เกี่ยวข้อง เพื่อให้แน่ใจว่าทรัพย์สินสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม

3) มีการจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

-5-

การควบคุมการเข้าถึง
(Access Control)

5.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย

นโยบาย

ต้องมีนโยบายควบคุมการเข้าถึงเครือข่ายและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรและทบทวนตามระยะเวลาที่กำหนดไว้ โดยพิจารณาให้สอดคล้องกับบทบาทหน้าที่ และความมั่นคงปลอดภัยในการเข้าถึงสินทรัพย์สารสนเทศ

5.2 การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

นโยบาย

ต้องมีการกำหนดมาตรการและแนวปฏิบัติเพื่อใช้ในการกำหนดรหัสบัญชีผู้ใช้, การจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ, การจัดการรหัสผ่าน รวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์ตัวตน

นโยบาย

ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามมาตรการด้านการรักษาความปลอดภัยในการเข้าถึงอย่างเคร่งครัด เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

5.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

นโยบาย

การเข้าถึงระบบจากภายในองค์กรหรือการเชื่อมต่อจากภายนอกต้องมีมาตรการควบคุมที่ชัดเจน ต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิตามขั้นตอน โดยระบบต้องยอมให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตผ่านเข้าสู่เครือข่าย และใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

-6-

การเข้ารหัสข้อมูล

(Cryptography)

6.1 การกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

วัตถุประสงค์

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องการความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

นโยบาย

ต้องมีวิธีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง อย่างเหมาะสม

-7-

ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร
(Physical and Environmental Security)

7.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สินขององค์กร

นโยบาย

กำหนดรายละเอียดของสถานที่และอุปกรณ์ที่จำเป็นต้องมี ระบบป้องกันการเสียหายและการควบคุมการเข้าออก ในการรักษาความมั่นคงปลอดภัย เช่น ห้องแม่ข่าย (ห้อง Server) ต้องมีระบบรักษาความปลอดภัยและมีการควบคุมการเข้าถึงอย่างเข้มงวด

7.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)

วัตถุประสงค์

เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่นๆ

นโยบาย

อุปกรณ์สำคัญที่ถูกจัดเก็บในห้องแม่ข่าย (ห้อง Server) ต้องมีการจัดวางอย่างถูกต้อง มีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่ออุปกรณ์ และมีการกำหนดแผนการบำรุงรักษาอุปกรณ์

-8-

ความมั่นคงปลอดภัยสำหรับการดำเนินงาน
(Operation Security)

8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

นโยบาย

โครงสร้างพื้นฐานและสารสนเทศทุกระบบต้องมีผู้รับผิดชอบมีเอกสารขั้นตอนการปฏิบัติงานที่ได้บันทึกไว้เป็นลายลักษณ์อักษร ในกรณีที่มีการเปลี่ยนแปลงข้อมูล หรือการปรับเปลี่ยนเวอร์ชันของระบบ หรือโปรแกรมภายใน ต้องมีการบันทึกการจัดการกับปัญหาที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นได้ และสามารถกลับคืนสู่สถานะเดิมได้หากแก้ไขไม่สำเร็จ มีการบริหารขีดความสามารถของโครงสร้างพื้นฐานและระบบสารสนเทศ

8.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

นโยบาย

จัดให้มีการติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งโปรแกรมเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงานหรืออุปกรณ์ที่ใช้ดำเนินงานขององค์กร

8.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์

เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัยธรรมชาติระบบเสียหาย ฯลฯ

นโยบาย

ต้องจัดให้มีการสำรองข้อมูลที่สำคัญ โดยต้องกำหนดรูปแบบและวิธีปฏิบัติ รวมทั้งแผนการสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของหน่วยงานภายในองค์กร เพื่อป้องกันการสูญหายทั้งจากภาวะคุกคามหรือจากภัยพิบัติ โดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบและแผนการดำเนินการที่กำหนดไว้

8.4 การบันทึกข้อมูล Log และการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์

เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

นโยบาย

ต้องจัดให้มีการเฝ้าระวังระบบที่มีความสำคัญเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต, การปฏิเสธการให้บริการของระบบหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

ต้องให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ และต้องกำหนดวิธีปฏิบัติในการตั้งเวลาของเครื่องแม่ข่ายให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องที่ช่วยในการตรวจสอบช่วงเวลาในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ขององค์กรได้

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)

วัตถุประสงค์

เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

นโยบาย

ต้องมีมาตรการในการรักษาความสมบูรณ์ของระบบปฏิบัติงานโดยมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบรารี ซอฟต์แวร์อุดช่องโหว่ โดยก่อนการติดตั้งในระบบต้องผ่านการทดสอบการใช้งานก่อนแล้วจึงติดตั้งลงในเครื่องที่ใช้งาน

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

นโยบาย

ต้องดูแลฮาร์ดแวร์และซอฟต์แวร์ที่ใช้งานอย่างสม่ำเสมอ เพื่อให้สามารถทำงานได้เป็นปกติ ต้องปรับปรุงช่องโหว่ในระบบต่างๆ มีการประเมินความเสี่ยงของช่องโหว่เหล่านั้นตามระยะเวลาที่กำหนด และมีการกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

8.7 การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

วัตถุประสงค์

เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

นโยบาย

ต้องวางแผนการตรวจสอบระบบ โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

-9-

ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล
(Communications Security)

9.1 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์

เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายขององค์กร

นโยบาย

จัดให้มีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถตรวจจับทรัพยากรสารสนเทศตามหลักเกณฑ์ที่ประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งานได้ตามข้อกำหนด และมีการบำรุงรักษาระบบให้ใช้งานได้ดีอยู่เสมอ

9.2 การถ่ายโอนข้อมูล (Information Transfer)

วัตถุประสงค์

เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กร และถ่ายโอนข้อมูลกับภายนอกหน่วยงาน

นโยบาย

ในการถ่ายโอนหรือแลกเปลี่ยนสารสนเทศจากหน่วยงานภายนอก ต้องมีการตรวจสอบและบันทึกการปฏิบัติงาน มีการเฝ้าระวังรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอ รวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อองค์กร

-10-

การจัดหา พัฒนา และดูแลระบบสารสนเทศ
(Systems Acquisition, Development and Maintenance)

10.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

วัตถุประสงค์

เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

นโยบาย

ในการจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบงานที่เดิม ต้องมีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศบนเครือข่ายสาธารณะ

10.2 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

วัตถุประสงค์

เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ (development lifecycle)

นโยบาย

ในการพัฒนาระบบสารสนเทศต้องมีความมั่นคงปลอดภัยมีตลอดวงจรของการพัฒนา มีการกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการ เพื่อใช้ควบคุมการเปลี่ยนแปลงหรือแก้ไข และต้องมีการตรวจสอบการทำงานหลังการเปลี่ยนแปลงนั้นๆ

10.3 ข้อมูลสำหรับการทดสอบ (Test data)

วัตถุประสงค์

เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

นโยบาย

ต้องมีมาตรการควบคุมการใช้ข้อมูลสำหรับการทดสอบระบบและการป้องกันข้อมูลรั่วไหล

-11-

ความสัมพันธ์กับผู้ให้บริการภายนอก
(Supplier relationships)

11.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

วัตถุประสงค์

เพื่อให้มีการป้องกันทรัพย์สินขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบาย

การรับบริการจากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงาน มีการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอ รวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อการดำเนินงานขององค์กร

11.2 การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ ของผู้ให้บริการภายนอก

นโยบาย

ต้องติดตามทบทวนบริการของผู้ให้บริการภายนอก มีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถตรวจรับทรัพยากรสารสนเทศตามหลักเกณฑ์ที่ประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

-12-

การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security Incident Management)

12.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสำนักงาน ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

นโยบาย

ต้องมีวิธีการสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องและได้ผล รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ จุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศให้รับทราบ

-13-

การบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ
(Business Continuity Management)

13.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

วัตถุประสงค์

เพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือระบบหยุดทำงาน

นโยบาย

มีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุงกระบวนการ ขั้นตอนปฏิบัติ รวมถึงมีมาตรการสร้างความต่อเนื่องที่ได้เตรียมการไว้ตามรอบระยะเวลาที่กำหนด

13.2 การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์

เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

นโยบาย

จัดเตรียมความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

-14-

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
(Compliance)

14.1 การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ

นโยบาย

ต้องมีการศึกษากฎ ระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศขององค์กร เพื่อให้บุคลากรได้รับทราบ ทำความเข้าใจ และปฏิบัติตามได้อย่างเคร่งครัด

14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

นโยบาย

จัดให้มีการทบทวนมาตรการ นโยบาย กระบวนการ ขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัยสารสนเทศ ตามรอบระยะเวลาที่กำหนดไว้ โดยอ้างอิงกับข้อกำหนดมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง