ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. 21-2562

ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์

INFORMATION SECURITY FOR DATA MESSAGE GENERATION, TRANSFER AND STORAGE SERVICE PROVIDERS

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับ ผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์

ขมธอ. 21-2562

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 11 มกราคม พ.ศ. 2562

คณะทำงานจัดทำร่างข้อเสนอแนะเกี่ยวกับการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ประธานคณะทำงาน

นางสาวอุรัชฎา เกตุพรหม	ผู้อำนวยการสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงาน

นายกำชัย จัตตานนท์	ผู้แทนกรมศุลกากร
นางสาวขนิษฐา สหเมธาพัฒน์	ผู้แทนกรมสรรพากร
นายธานินทร์ ตันกิติบุตร	ผู้แทนบริษัท ไทยเทรดเน็ท จำกัด
นางสาวพัชราภรณ์ ลี้ธนะรุ่ง	ผู้แทนสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
นางสาวขนิษฐ์ ผาทอง	ผู้แทนสำนักพัฒนาดิจิทัลเพื่อธุรกิจ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายนิธิ อมรพิพิธกุล	ผู้แทนสำนักบริการโครงสร้างพื้นฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงานและเลขานุการ

นายสมบัติ ชั้นอินทร์งาม	สำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับ ผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ ฉบับนี้จัดทำขึ้นเพื่ออธิบายแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์ และใบรับอิเล็กทรอนิกส์ หรือหน่วยงานอื่น ๆ ที่ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนำไปใช้เป็นแนวปฏิบัติเพื่อช่วยให้บริการมีความมั่นคงปลอดภัยและสร้างความน่าเชื่อถือให้กับผู้ให้บริการ โดยข้อเสนอแนะมาตรฐานฉบับนี้ได้พัฒนาตามแนวมาตรฐานของ

1. European Union Agency for Network and Information Security (ENISA) , Technical guidelines for the implementation of minimum security measures for Digital Service providers, December, 2016.
2. ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems - Requirements, 2013.
3. ISO/IEC 27002:2013, Information technology - Security techniques – Code of practice for Information security Controls, 2013.
4. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ.2555

และได้มีการนำเสนอเพื่อรับฟังความคิดเห็นเป็นการทั่วไป เพื่อนำข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับ ผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ ฉบับนี้จัดทำขึ้นโดยสำนักมาตรฐาน ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

คำนำ

ปัจจุบันธุรกรรมทางอิเล็กทรอนิกส์มีบทบาทสำคัญในการดำเนินธุรกิจในระบบเศรษฐกิจยุคใหม่ ทำให้ผู้ประกอบการต่าง ๆ ต้องพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความสะดวก รวดเร็ว และมีประสิทธิภาพ แต่เนื่องจากในการพัฒนานั้นมีระยะเวลาและต้นทุนที่สูง ผู้ประกอบการหลายแห่งจึงมีแนวคิดที่จะลดระยะเวลาและต้นทุนในการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ จึงหันมาใช้บริการจาก “ผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์” หรือ “ผู้ให้บริการ” ที่ทำหน้าที่เสมือนเป็นตัวกลางทำธุรกรรมทางอิเล็กทรอนิกส์แทนผู้ประกอบการกับภาครัฐ หรือผู้ประกอบการรายอื่น ในการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ ผู้ให้บริการดังกล่าวจึงมีบทบาทสำคัญต่อการสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ให้มีการเชื่อมโยงเครือข่ายเข้าด้วยกัน มีการใช้ทรัพยากรร่วมกัน มีการประมวลผลและกระจายข้อมูลไปตามหน่วยงานต่าง ๆ ทำให้ต้องมีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและข้อมูลอิเล็กทรอนิกส์ให้มีความถูกต้องครบถ้วน พร้อมใช้งาน และน่าเชื่อถือ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงได้จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ ฉบับนี้ขึ้นเพื่อกำหนดวัตถุประสงค์ ข้อกำหนด และแนวทางปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้บริการของผู้ให้บริการมีความมั่นคงปลอดภัย สอดคล้องกับมาตรฐานสากล และสร้างความน่าเชื่อถือให้กับผู้ให้บริการ

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับ ผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์

โดยที่เป็นการสมควรกำหนดแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ ให้มีแนวทางในการรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๗ (๔) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ เลขที่ ขมธอ. ๒๑-๒๕๖๒ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๑๗ มกราคม พ.ศ. ๒๕๖๒

(นางสุรางคณา วายุภาพ)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับ ผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฯ ฉบับนี้ เป็นข้อกำหนดและแนวทางปฏิบัติสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ โดยครอบคลุมการพิจารณาระดับความมั่นคงปลอดภัยของผู้ให้บริการ ตามวัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัย เพื่อให้ผู้ให้บริการมีแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานเดียวกัน

ในข้อเสนอแนะมาตรฐานฯ ฉบับนี้ มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) มีดังต่อไปนี้

- “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ซึ่งต้องปฏิบัติตาม
- “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
- “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 ผู้ให้บริการ (service providers) หมายถึง บุคคลที่ทำหน้าที่เป็นผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์แทนหน่วยธุรกิจ บุคคล ตลอดจนองค์กรเอกชนหรือองค์กรของรัฐใด ๆ

2.2 ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

2.3 บุคลากรหลัก (key personnel) หมายถึง บุคคลที่มีบทบาทสำคัญเกี่ยวกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยที่อยู่ภายใต้ขอบเขตการให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ เช่น ผู้บริหารระดับสูง (CEO CIO หรือ CISO) ผู้จัดการความต่อเนื่องทางธุรกิจ ผู้ดูแลระบบของระบบสารสนเทศที่สำคัญ หรือบุคคลที่สามที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศที่สำคัญ เป็นต้น

2.4 บุคลากรที่เกี่ยวข้อง หมายถึง บุคคลที่เกี่ยวกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยในองค์กรทุกคน และบุคคลที่สามที่อยู่ภายใต้ขอบเขตการให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์

2.5 บุคคลที่สาม (third party) หมายถึง บุคคลที่ทำงานร่วมกับผู้ให้บริการ เช่น ผู้ขาย ผู้ผลิตซอฟต์แวร์ ผู้ผลิตฮาร์ดแวร์ ที่ปรึกษา ผู้ตรวจสอบบัญชี บริษัทผู้ให้บริการภายนอก และอื่น ๆ เป็นต้น ซึ่งคำว่า บุคคลที่สามในเอกสารนี้ไม่ได้หมายถึงผู้ใช้บริการ หรือ รัฐบาล หรือหน่วยงานกำกับดูแล

2.6 ผู้ใช้บริการ หมายถึง บุคคลที่ได้รับบริการจากผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์

2.7 สินทรัพย์ (asset) หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

2.8 ทรัพย์สินสารสนเทศ หมายถึง

(1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

2.9 เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

2.10 สถานการณ์ด้านความมั่นคงปลอดภัย (security incident) หมายถึง เหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

3. การพิจารณาระดับความมั่นคงปลอดภัย

ระดับความมั่นคงปลอดภัยสามารถพิจารณาได้จากการประเมินระดับผลกระทบที่อาจเกิดขึ้นจากการให้บริการ โดยมีรายละเอียดดังนี้

3.1 ระดับความมั่นคงปลอดภัย

ระดับความมั่นคงปลอดภัยสำหรับผู้ให้บริการ แบ่งออกเป็น 2 ระดับ ได้แก่ **ระดับพื้นฐาน** และ**ระดับสูง** (รายละเอียดดังตารางที่ 1) โดยแต่ละระดับมีข้อกำหนดและแนวทาง (clauses and guidelines) รวมถึงหลักฐานที่ใช้แสดงถึงการปฏิบัติตามข้อกำหนดและแนวทางปฏิบัติดังกล่าว

ตารางที่ 1 ระดับความมั่นคงปลอดภัย

ระดับ	คำอธิบาย
ระดับพื้นฐาน (Basic)	ข้อกำหนดด้านความมั่นคงปลอดภัยขั้นพื้นฐานที่สามารถนำมาใช้เพื่อบรรลุวัตถุประสงค์การรักษาความมั่นคงปลอดภัยที่กำหนดไว้
ระดับสูง (Advanced)	ข้อกำหนดด้านความมั่นคงปลอดภัยที่มีการตรวจสอบและทบทวนการดำเนินงานอย่างต่อเนื่อง โดยคำนึงถึงการเปลี่ยนแปลง สถานการณ์ด้านความมั่นคงปลอดภัย และการทดสอบ เพื่อเพิ่มประสิทธิภาพของการรักษาความมั่นคงปลอดภัยในเชิงรุก

ผู้ให้บริการสามารถพิจารณาระดับความมั่นคงปลอดภัยที่เหมาะสมกับการให้บริการของตนจากการประเมินระดับผลกระทบที่อาจเกิดขึ้นจากการให้บริการ โดยรายละเอียดการประเมินระดับผลกระทบจะกล่าวถึงในหัวข้อ 3.2

3.2 การประเมินระดับผลกระทบ

ข้อเสนอแนะมาตรฐานฯ ฉบับนี้ กำหนดให้ผู้ให้บริการใช้แนวทางการประเมินระดับผลกระทบที่อาจเกิดขึ้นตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555 ข้อ 4 ถึง ข้อ 8 โดยการประเมินระดับผลกระทบที่อาจเกิดขึ้นจากการให้บริการจะต้องประเมินผลกระทบในด้านต่อไปนี้

(1) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน
(2) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกาย หรืออนามัย
(3) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก จากข้อ (2)
(4) ผลกระทบด้านความมั่นคงของรัฐ (การประเมินโดยมุ่งเฉพาะปัจจัยที่สำคัญเป็นหลักและเน้นไปที่ปัจจัยภายในประเทศเป็นส่วนใหญ่ เช่น ด้านการเมือง เศรษฐกิจ สังคม การทหาร และด้านอื่น ๆ)

ในการประเมินระดับผลกระทบที่อาจเกิดขึ้นจากการให้บริการ ให้หน่วยงานหรือองค์กรยึดหลักการประเมินความเสี่ยงตามเกณฑ์ประเมินระดับผลกระทบดังตารางที่ 2

ตารางที่ 2 เกณฑ์ประเมินระดับผลกระทบ

ด้านของผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
ด้านมูลค่าความเสียหายทางการเงิน	ความเสียหายไม่เกิน 1 ล้านบาท	ความเสียหายเกิน 1 ล้านบาทแต่ไม่เกิน 100 ล้านบาท	ความเสียหายเกินกว่า 100 ล้านบาท
จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต	ไม่ได้รับผลกระทบต่อชีวิตร่างกายหรืออนามัย	ได้รับผลกระทบต่อชีวิตร่างกายหรืออนามัยตั้งแต่ 1 คน แต่ไม่เกิน 1,000 คน	ได้รับผลกระทบต่อร่างกายหรืออนามัยเกินกว่า 1,000 คน หรือต่อชีวิตตั้งแต่ 1 คน
จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่น ๆ	ได้รับผลกระทบไม่เกิน 10,000 คน	ได้รับผลกระทบเกิน 10,000 คน แต่ไม่เกิน 100,000 คน	ได้รับผลกระทบเกินกว่า 100,000 คน
ผลกระทบด้านความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	-	มีผลกระทบต่อความมั่นคงของรัฐ

3.3 การพิจารณาผลการประเมินระดับผลกระทบกับระดับความมั่นคงปลอดภัย

ผลลัพธ์ที่ได้จากการประเมินระดับผลกระทบแต่ละด้านในหัวข้อ 3.2 จะถูกนำมาใช้พิจารณาระดับความมั่นคงปลอดภัย ดังนี้

(1) ผลลัพธ์ที่ได้จากการประเมินระดับผลกระทบเป็นระดับสูงด้านหนึ่งด้านใด หรือระดับกลางอย่างน้อย 2 ด้านขึ้นไป ผู้ให้บริการจะต้องปฏิบัติตามระดับความมั่นคงปลอดภัยใน**ระดับสูง**

(2) หากผลลัพธ์ที่ได้จากการประเมินระดับผลกระทบในกรณีอื่น ผู้ให้บริการจะต้องปฏิบัติตามระดับความมั่นคงปลอดภัยใน **<u>ระดับพื้นฐานขึ้นไป</u>**

<u>ตัวอย่างที่ 1</u>

ด้านของผลกระทบ	ระดับ ผลกระทบ	ระดับ ความมั่นคงปลอดภัย
มูลค่าความเสียหายทางการเงิน	สูง	ระดับสูง
จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต	ต่ำ	
จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่น ๆ	กลาง	
ความมั่นคงของรัฐ	ต่ำ	

จะเห็นได้ว่า ผลลัพธ์ที่ได้จากการประเมินระดับผลกระทบ อยู่ในระดับสูง 1 ด้าน ระดับกลาง 1 ด้าน และระดับต่ำ 2 ด้าน ดังนั้นผู้ให้บริการจะต้องปฏิบัติตามระดับความมั่นคงปลอดภัยในระดับสูง

<u>ตัวอย่างที่ 2</u>

ด้านของผลกระทบ	ระดับ ผลกระทบ	ระดับ ความมั่นคงปลอดภัย
มูลค่าความเสียหายทางการเงิน	กลาง	ระดับพื้นฐาน
จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต	ต่ำ	
จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่น ๆ	ต่ำ	
ความมั่นคงของรัฐ	ต่ำ	

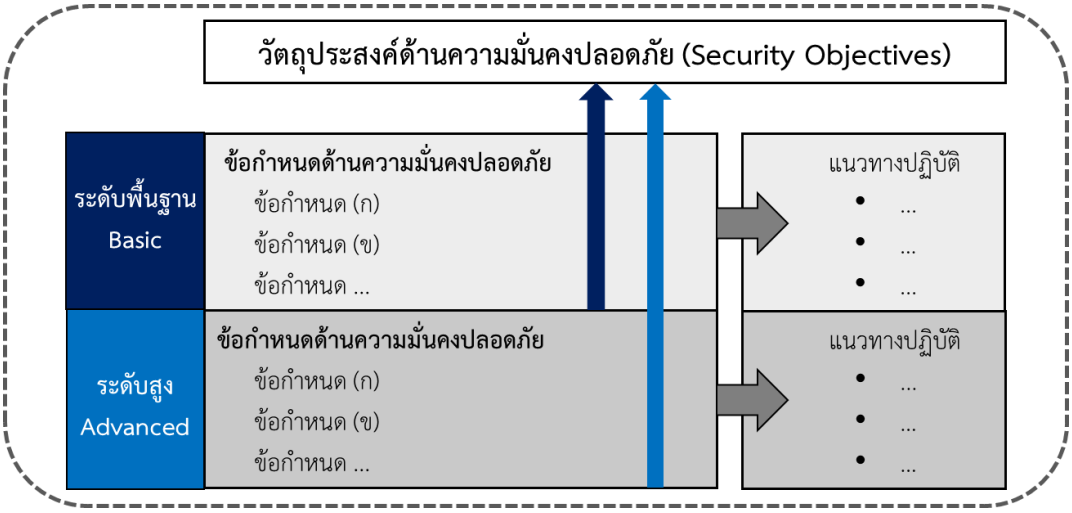
จะเห็นได้ว่า ผลลัพธ์ที่ได้จากการประเมินระดับผลกระทบ อยู่ในระดับกลาง 1 ด้าน และระดับต่ำ 3 ด้าน ดังนั้นผู้ให้บริการจะต้องปฏิบัติตามระดับความมั่นคงปลอดภัยในระดับพื้นฐาน

ผู้ให้บริการสามารถนำระดับความมั่นคงปลอดภัยที่ได้จากการประเมินระดับผลกระทบไปประยุกต์ใช้กับการให้บริการ โดยปฏิบัติตามวัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการ หัวข้อ 5 ซึ่ง**ผู้ให้บริการที่มีระดับความมั่นคงปลอดภัยอยู่ในระดับสูงจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยระดับพื้นฐาน** เพื่อแสดงให้ผู้ใช้บริการและผู้มีส่วนได้เสียเห็นถึงการปฏิบัติที่มีการรักษาความมั่นคงปลอดภัยในระดับสูง

ทั้งนี้ ระดับความมั่นคงปลอดภัยของผู้ให้บริการอาจขึ้นอยู่กับการประเมินระดับผลกระทบของหน่วยงานหรือองค์กรที่นำข้อเสนอแนะมาตรฐานฯ ฉบับนี้ไปเป็นข้อกำหนดและแนวทางปฏิบัติกับผู้ให้บริการ

4. โครงสร้างของวัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อเสนอแนะมาตรฐานฯ ฉบับนี้ กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการ ซึ่งภายใต้วัตถุประสงค์สามารถแบ่งระดับความมั่นคงปลอดภัยออกเป็น 2 ระดับ ตามการพิจารณาระดับความมั่นคงปลอดภัยในหัวข้อ 3 แต่ละระดับจะแสดงรายการข้อกำหนดด้านความมั่นคงปลอดภัย และแนวทางปฏิบัติที่มีความเข้มงวดต่างกัน โดยผู้ให้บริการที่มีระดับความมั่นคงปลอดภัยอยู่ในระดับสูงจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยในระดับพื้นฐานด้วย รายละเอียดตามรูปที่ 1



รูปที่ 1 โครงสร้างของวัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัย

4.1 วัตถุประสงค์ด้านความมั่นคงปลอดภัย (security objectives)

วัตถุประสงค์ด้านความมั่นคงปลอดภัยประกอบด้วย 26 วัตถุประสงค์ และ 129 ข้อกำหนด ซึ่งแบ่งเป็นข้อกำหนดด้านความมั่นคงปลอดภัยระดับพื้นฐาน 58 ข้อ และระดับสูง 71 ข้อ รายละเอียดดังตารางที่ 3

ตารางที่ 3 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการ

วัตถุประสงค์ด้านความมั่นคงปลอดภัย	จำนวนข้อกำหนดด้านความมั่นคงปลอดภัย	
	ระดับพื้นฐาน	ระดับสูง
1. การกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (information security policy)	2	2
2. การบริหารจัดการความเสี่ยง (risk management)	3	3
3. การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (security roles)	1	3
4. การบริหารจัดการบุคคลที่สาม (third party management)	4	5
5. การตรวจสอบประวัติบุคลากร (background checks)	1	3
6. การสร้างความตระหนักด้านความมั่นคงปลอดภัย (security awareness)	2	2
7. การเปลี่ยนแปลงบุคลากร (personnel changes)	2	3
8. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)	4	7
9. การรักษาความมั่นคงปลอดภัยของระบบสนับสนุนการดำเนินงาน (security of supporting utilities)	1	2
10. การควบคุมการเข้าถึงระบบเครือข่าย และระบบสารสนเทศ (access control to network and information system)	2	6

วัตถุประสงค์ด้านความมั่นคงปลอดภัย	จำนวนข้อกำหนดด้านความมั่นคงปลอดภัย	
	ระดับพื้นฐาน	ระดับสูง
11. การควบคุมความถูกต้องขององค์ประกอบระบบเครือข่ายและระบบสารสนเทศ (integrity of network components and information system)	3	4
12. การกำหนดขั้นตอนการปฏิบัติงาน (operating procedures)	1	2
13. การบริหารจัดการการเปลี่ยนแปลง (change management)	2	3
14. การบริหารจัดการสินทรัพย์ (asset management)	2	1
15. การตรวจพบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย (security incident detection and response)	2	2
16. การรายงานสถานการณ์ด้านความมั่นคงปลอดภัย (security incident reporting)	1	1
17. การดำเนินธุรกิจอย่างต่อเนื่อง (business continuity)	3	2
18. การกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery capabilities)	2	2
19. การเฝ้าติดตามและการบันทึกเหตุการณ์ (monitoring and logging)	3	2
20. การทดสอบระบบ (system test)	2	1
21. การประเมินการรักษาความมั่นคงปลอดภัย (security assessments)	2	2
22. การปฏิบัติตามข้อกำหนด (compliance)	1	2
23. การรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บ (security of data at rest)	5	6
24. การรักษาความมั่นคงปลอดภัยของส่วนเชื่อมต่อบริการ (interface security)	3	2
25. การรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ (software security)	1	2
26. การทำงานร่วมกันและการโอนย้ายบริการ (interoperability and portability)	3	1
รวม	**58**	**71**

ลำดับของวัตถุประสงค์ด้านความมั่นคงปลอดภัยข้างต้นไม่มีจุดประสงค์เพื่อแสดงความสำคัญใด ๆ ผู้ให้บริการต้องปฏิบัติตามข้อกำหนดในแต่ละวัตถุประสงค์ตามระดับความมั่นคงปลอดภัยของตน

4.2 ข้อกำหนดด้านความมั่นคงปลอดภัย (security requirements)

ข้อกำหนดด้านความมั่นคงปลอดภัยที่อยู่ภายใต้วัตถุประสงค์ด้านความมั่นคงปลอดภัยแต่ละวัตถุประสงค์ที่ผู้ให้บริการควรนำมาปฏิบัติเพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้ ซึ่งแต่ละข้อกำหนดมีโครงสร้างการอธิบายดังนี้

ข้อกำหนด

อธิบายสิ่งที่ต้องปฏิบัติตามเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยที่กำหนดไว้

แนวทางปฏิบัติ

อธิบายสิ่งที่ควรปฏิบัติเพื่อให้สอดคล้องกับวัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้

5. วัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการ

5.1 วัตถุประสงค์ที่ 1: การกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (information security policy)

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรให้สอดคล้องกับวัตถุประสงค์ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อกำหนด	แนวทางปฏิบัติ
5.1.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศให้มีความสอดคล้องกับวัตถุประสงค์ขององค์กร กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง	ควรจัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศที่ได้รับการอนุมัติจากผู้บริหารระดับสูงก่อนนำไปใช้งานและเผยแพร่ให้บุคลากรที่เกี่ยวข้องรับทราบ ซึ่งนโยบาย ฯ ควรอธิบายภาพรวมของหัวข้อดังนี้ – การบริหารจัดการบุคคลที่สาม – การเปลี่ยนแปลงบุคลากร – ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม – ความมั่นคงปลอดภัยของระบบสนับสนุนการดำเนินงาน – การควบคุมการเข้าถึง – การบริหารจัดการระบบเครือข่าย – การบริหารจัดการสินทรัพย์ – การตรวจพบและการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย – การเฝ้าติดตามและบันทึกเหตุการณ์ – การทดสอบระบบ – การประเมินผลและการทดสอบความมั่นคงปลอดภัย – การปฏิบัติตามข้อกำหนด – การเข้ารหัสลับ – การบริหารจัดการข้อมูลที่จัดเก็บ – ความมั่นคงปลอดภัยของส่วนเชื่อมต่อบริการ – ความมั่นคงปลอดภัยของการพัฒนาซอฟต์แวร์

ข้อกำหนด	แนวทางปฏิบัติ
(ข) ผู้ให้บริการต้องสร้างความตระหนักให้แก่บุคลากรหลักทราบถึงนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ	ควรสร้างความตระหนักให้แก่บุคลากรหลักทราบถึงหน้าที่ความรับผิดชอบของตนเอง และนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ
5.1.2 ระดับสูง	
(ก) ผู้ให้บริการต้องสร้างความตระหนักให้แก่บุคลากรที่เกี่ยวข้องทราบถึงความสำคัญของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ	ควรสร้างความตระหนักให้แก่บุคลากรที่เกี่ยวข้องทราบถึงนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและความสำคัญของหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย
(ข) ผู้ให้บริการต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ	ควรทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและดำเนินการทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงการดำเนินงานใด ๆ ภายในองค์กร

5.2 วัตถุประสงค์ที่ 2: การบริหารจัดการความเสี่ยง (risk management)

เพื่อกำหนดกรอบการบริหารจัดการความเสี่ยงและการกำกับดูแล (governance) ที่เหมาะสม รวมถึงขั้นตอนการบริหารจัดการความเสี่ยง เช่น การระบุความเสี่ยง การประเมินความเสี่ยง และการใช้เครื่องมือช่วยในการประเมินความเสี่ยง เป็นต้น

ข้อกำหนด	แนวทางปฏิบัติ
5.2.1 ระดับพื้นฐาน	
(ก) ให้บริการต้องประเมินความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่ายและระบบสารสนเทศรวมถึงสินทรัพย์ที่สำคัญ (critical asset) ในการให้บริการ	ควรมีวิธีการประเมินความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสินทรัพย์ที่สำคัญ ซึ่งประกอบด้วยประเด็นสำคัญดังนี้ – การกำหนดเกณฑ์การประเมินความเสี่ยงที่รวมถึงเกณฑ์การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัย – การระบุความเสี่ยงด้านความมั่นคงปลอดภัยที่เกี่ยวกับการถูกเปิดเผยข้อมูล ความถูกต้องครบถ้วน และความพร้อมใช้งานของระบบสารสนเทศ และระบุผู้เป็นเจ้าของความเสี่ยง – การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยโดยการประเมินผลกระทบและโอกาสที่จะเกิดขึ้น รวมถึงการกำหนดระดับค่าความเสี่ยง
(ข) ผู้ให้บริการต้องกำหนดแผนจัดการความเสี่ยง (risk treatment plan) เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ	ควรจัดทำแผนจัดการความเสี่ยงที่ประกอบด้วยประเด็นสำคัญดังนี้ – การเลือกวิธีจัดการความเสี่ยง และประโยชน์ที่คาดว่าจะได้รับ – การระบุผู้รับผิดชอบและผู้อนุมัติแผนในการนำแผน

ข้อกำหนด	แนวทางปฏิบัติ
	จัดการความเสี่ยงไปใช้ – การระบุกิจกรรมที่จะดำเนินการ – การระบุทรัพยากรที่ต้องการรวมถึงทรัพยากรสำรองที่ใช้ – การวัดผลการปฏิบัติงานและข้อจำกัด – การรายงานผลและการติดตามตรวจสอบ – การระบุระยะเวลาและกำหนดการ
(ค) ผู้ให้บริการต้องสร้างความตระหนักให้บุคลากรหลักทราบถึงการบริหารจัดการความเสี่ยง	ควรสร้างความตระหนักให้กับบุคลากรหลักทราบถึงความเสี่ยงที่สำคัญ และวิธีการจัดการความเสี่ยงขององค์กรและสามารถนำไปปฏิบัติได้อย่างถูกต้อง
5.2.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดวิธีการบริหารจัดการความเสี่ยงตามมาตรฐานสากลหรือตามความเหมาะสมขององค์กร	ควรกำหนดวิธีการบริหารจัดการความเสี่ยง ที่ประกอบด้วยหัวข้ออย่างน้อยดังนี้ – วัตถุประสงค์ บทบาทและหน้าที่ – ขอบเขตของวิธีการบริหารจัดการความเสี่ยง – ขั้นตอนการประเมินความเสี่ยง – การประเมินผลกระทบ และโอกาสที่จะเกิดขึ้น รวมถึงผลกระทบที่อาจส่งผลต่อการให้บริการ **หมายเหตุ** : ผู้ให้บริการอาจนำวิธีการบริหารจัดการความเสี่ยงตามมาตรฐานสากลมาประยุกต์ใช้ตามความเหมาะสมขององค์กร เช่น มาตรฐาน ISO 31000 หรือมาตรฐาน ISO/IEC 27005
(ข) ผู้ให้บริการต้องสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทราบถึงความเสี่ยงในการปฏิบัติงาน	ควรสร้างความตระหนักให้แก่บุคลากรที่เกี่ยวข้องทราบเกี่ยวกับความเสี่ยงขององค์กร และสามารถปฏิบัติได้อย่างถูกต้อง
(ค) ผู้ให้บริการต้องทบทวนวิธีการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ	ควรกำหนดระยะเวลาทบทวนวิธีการบริหารจัดการความเสี่ยงและวิธีการประเมินความเสี่ยงขององค์กรพร้อมดำเนินการทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงการดำเนินงานใด ๆ ภายในองค์กร

5.3 วัตถุประสงค์ที่ 3: การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (security roles)

เพื่อกำหนดบทบาทและหน้าที่ความรับผิดชอบให้แก่บุคลากรที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัยขององค์กร

ข้อกำหนด	แนวทางปฏิบัติ
5.3.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยให้กับบุคลากรที่เกี่ยวข้องโดยมั่นใจได้ว่าบทบาทและหน้าที่ดังกล่าวสามารถเข้าถึงได้เมื่อเกิดสถานการณ์ด้านความมั่นคงปลอดภัย	ควรกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยโดยจัดทำรายการหน้าที่ความรับผิดชอบของแต่ละหน้าที่ และข้อมูลการติดต่อให้กับบุคลากรที่เกี่ยวข้อง เช่น ผู้บริหารระดับสูงด้านความมั่นคงปลอดภัย (CISO) ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) ผู้จัดการความต่อเนื่องทางธุรกิจ
5.3.2 ระดับสูง	
(ก) ผู้ให้บริการต้องประกาศอย่างเป็นทางการให้บุคลากรที่เกี่ยวข้องทราบถึงบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย	ควรจัดทำรายชื่อบุคลากรที่เกี่ยวข้องที่ได้รับการแต่งตั้งและอธิบายรายละเอียดเกี่ยวกับบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย เช่น ผู้บริหารระดับสูงด้านความมั่นคงปลอดภัย (CISO) ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) ผู้จัดการความต่อเนื่องทางธุรกิจ
(ข) ผู้ให้บริการต้องสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องรับทราบถึงบทบาทและหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย	ควรสร้างความตระหนักถึงบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย และช่องทางการติดต่อบุคคลหรือหน่วยงานที่เกี่ยวกับด้านความมั่นคงปลอดภัยให้แก่บุคลากรที่เกี่ยวข้องทราบ
(ค) ผู้ให้บริการต้องทบทวนบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ	ควรทบทวนบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงใด ๆ ต่อการดำเนินงานภายในองค์กร

5.4 วัตถุประสงค์ที่ 4: การบริหารจัดการบุคคลที่สาม (third party management)

เพื่อกำหนดนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยในการทำสัญญากับบุคคลที่สาม ตัวอย่างเช่น ระบุข้อตกลงระดับการให้บริการ (SLAs) ระบุข้อกำหนดด้านความมั่นคงปลอดภัยภายในสัญญา และจัดทำสัญญาเมื่อจ้างงานกับบุคคลที่สาม เพื่อให้มั่นใจว่าการใช้บริการจากบุคคลที่สามและความเสี่ยงที่เหลือ (residual risks) จะไม่ส่งผลกระทบหรือส่งผลเสียต่อการให้บริการขององค์กร

ข้อกำหนด	แนวทางปฏิบัติ
5.4.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดข้อตกลงร่วมกันกับบุคคลที่สามเมื่อมีการตกลงติดต่อซื้อขายสินค้า และ/หรือ บริการ	1. ควรจัดทำข้อตกลงกับบุคคลที่สามอย่างเป็นทางการโดยมีรายละเอียดชัดเจน 2. ควรมีรายการข้อตกลงของบุคคลที่สามที่เกี่ยวข้องกับการให้บริการ

ข้อกำหนด	แนวทางปฏิบัติ
(ข) ผู้ให้บริการต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยและข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการให้บริการภายในข้อตกลงที่ได้จัดทำขึ้นกับบุคคลที่สาม	ควรมีข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการให้บริการ ระบุไว้ภายในข้อตกลงที่จัดทำขึ้นกับบุคคลที่สาม ซึ่งควรประกอบด้วยหัวข้อดังนี้ – รายละเอียดของการให้บริการ – ข้อกำหนดด้านความมั่นคงปลอดภัย เช่น ระบบพิสูจน์ตัวตนที่นำมาใช้ในการปฏิบัติงาน การพัฒนาซอฟต์แวร์ และขั้นตอนการปฏิบัติงานต่าง ๆ ของบริการที่มีให้แก่องค์กร – ข้อตกลงการไม่เปิดเผยข้อมูลหรือความลับขององค์กร (non-disclosure agreement: NDA) – บทบาท และหน้าที่ความรับผิดชอบ – ข้อตกลงระดับการให้บริการ (service level agreement) – ช่องทางการติดต่อประสานงานและรายงานผลการดำเนินงาน – ข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง
(ค) ผู้ให้บริการต้องกำหนดสิทธิในการตรวจสอบไว้ในข้อตกลงกับบุคคลที่สาม	ควรกำหนดสิทธิไว้ในข้อตกลงกับบุคคลที่สามเพื่อให้ผู้ตรวจสอบสามารถเข้าดำเนินการตรวจสอบในกรณีที่พบประเด็นหรือข้อสงสัยที่มีนัยสำคัญ
(ง) ผู้ให้บริการต้องกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการบำรุงรักษาอุปกรณ์ การปฏิบัติงาน และความเป็นเจ้าของทรัพย์สินสารสนเทศไว้ในข้อตกลงกับบุคคลที่สาม	ควรกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการบำรุงรักษาอุปกรณ์ การปฏิบัติงาน และความเป็นเจ้าของทรัพย์สินสารสนเทศที่ระบุในข้อตกลง เช่น การจัดหาอุปกรณ์สารสนเทศ การให้บริการด้านเทคโนโลยีสารสนเทศ การมอบหมายงานขององค์กรให้บุคคลที่สามรับผิดชอบ การให้คำแนะนำหรือความช่วยเหลือในการปฏิบัติงาน (help desk) ศูนย์กลางการให้บริการข้อมูล (call center) การเชื่อมต่อระบบเครือข่ายเข้าด้วยกัน การใช้สิ่งอำนวยความสะดวกร่วมกัน (shared facilities) และอื่น ๆ เป็นต้น
5.4.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายสำหรับการบริหารจัดการกับบุคคลที่สาม	ควรจัดทำนโยบายสำหรับการบริหารจัดการบุคคลที่สามที่ประกอบด้วยประเด็นสำคัญ ดังนี้ – การระบุประเภทของบุคคลที่สามที่ให้บริการแก่องค์กร เช่น ผู้ให้บริการทางด้านเทคโนโลยีสารสนเทศ (IT service) ผู้ให้บริการทางด้านโครงสร้างพื้นฐานของระบบสารสนเทศ (IT infrastructure) หรือผู้ให้บริการด้านการเงิน (financial service) เป็นต้น

ข้อกำหนด	แนวทางปฏิบัติ
	– การระบุชนิดข้อมูลที่อนุญาตให้บุคคลที่สามสามารถเข้าถึงได้ รวมถึงการเฝ้าติดตามและการควบคุมการเข้าถึง – การระบุข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับข้อมูลแต่ละประเภทโดยขึ้นอยู่กับความต้องการทางธุรกิจขององค์กรและความเสี่ยงที่มีอยู่ – การกำหนดกระบวนการและขั้นตอนการตรวจสอบการปฏิบัติงานให้เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูลในแต่ละชนิด – การควบคุมความถูกต้องและครบถ้วนของข้อมูลเพื่อให้มั่นใจว่าข้อมูลที่จัดทำขึ้นมีความถูกต้อง – การระบุข้อตกลงที่บังคับใช้กับบุคคลที่สามเพื่อปกป้องข้อมูลขององค์กร – การจัดการสถานการณ์ด้านความมั่นคงปลอดภัยและหน้าที่ของบุคคลที่สามรวมถึงหน้าที่ความรับผิดชอบขององค์กร – การสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทราบถึงนโยบายและขั้นตอนการปฏิบัติงานที่บังคับใช้พร้อมระดับการเข้าถึงระบบหรือข้อมูล – เงื่อนไขที่อยู่ภายใต้ข้อกำหนดและการควบคุมความมั่นคงปลอดภัยของข้อมูลควรได้รับการระบุไว้ในข้อตกลงที่ได้รับการลงนามร่วมกัน – การบริหารจัดการการเปลี่ยนแปลงข้อมูลที่จำเป็นและสิ่งอำนวยความสะดวกสำหรับการประมวลผลข้อมูลที่ต้องใช้เมื่อเกิดสถานการณ์ด้านความมั่นคงปลอดภัย
(ข) ผู้ให้บริการต้องมีกระบวนการติดตามตรวจสอบการดำเนินงานเพื่อให้มั่นใจว่าบุคคลที่สามสามารถดำเนินงานให้เป็นไปตามข้อตกลง และนโยบายที่กำหนดไว้	1. ควรกำหนดให้บุคคลที่สามรายงานสถานการณ์ด้านความมั่นคงปลอดภัยให้กับองค์กรทุกครั้งที่ตรวจพบ 2. ควรกำหนดให้บุคคลที่สามต้องจัดทำรายงานการดำเนินการอย่างสม่ำเสมอ 3. ควรกำหนดให้บุคคลที่สามต้องรายงานการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นต่อระบบสารสนเทศ 4. ควรมีข้อกำหนดเกี่ยวกับสถานการณ์ด้านความมั่นคงปลอดภัยระบุไว้ในข้อตกลงกับบุคคลที่สามในกรณีเกิดเหตุการณ์ เช่น – กระแสไฟฟ้าดับ

ข้อกำหนด	แนวทางปฏิบัติ
	– ความต้านทานของกระแสไฟฟ้าไม่เท่ากัน – ภัยพิบัติทางธรรมชาติ – อุบัติเหตุ หรือเหตุฉุกเฉินอื่น ๆ ที่สามารถเกิดขึ้นได้
(ค) ผู้ให้บริการต้องวิเคราะห์ความเสี่ยงก่อนการทำข้อตกลงกับบุคคลที่สาม	ควรจัดทำรายงานผลการวิเคราะห์ความเสี่ยงของการใช้บริการบุคคลที่สามก่อนมีการจัดทำข้อตกลงร่วมกัน
(ง) ผู้ให้บริการต้องติดตามและลดความเสี่ยงจากการใช้บริการบุคคลที่สามให้อยู่ในระดับที่ยอมรับได้	ควรระบุความเสี่ยงที่เหลืออยู่จากการใช้บริการบุคคลที่สาม และความเสี่ยงที่เหลืออยู่นั้นองค์กรต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่องค์กรยอมรับได้
(จ) ผู้ให้บริการต้องทบทวนนโยบายสำหรับการบริหารจัดการกับบุคคลที่สามอย่างสม่ำเสมอ หรือเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่คาดคิดหรือมีการเปลี่ยนแปลงเกิดขึ้น	ควรทบทวนนโยบายการบริหารจัดการบุคคลที่สามโดยคำนึงถึงสถานการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือเมื่อมีการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานภายในองค์กร

5.5 วัตถุประสงค์ที่ 5: การตรวจสอบประวัติบุคลากร (background checks)

เพื่อกำหนดขั้นตอนและนโยบายการตรวจสอบประวัติบุคลากร เช่น ลูกจ้าง พนักงานสัญญาจ้าง และบุคคลที่สามซึ่งเกี่ยวข้องกับการปฏิบัติงานภายในองค์กรก่อนการจ้างงาน เพื่อให้เป็นไปตามข้อกำหนดหรือ กฎหมายที่ได้กำหนดไว้ การตรวจสอบประวัติบุคลากรอาจรวมถึงการตรวจสอบการปฏิบัติงานที่ผ่านมา การตรวจสอบเอกสารที่ใช้อ้างอิงทางวิชาชีพ และการตรวจสอบอื่น ๆ ที่มีความเหมาะสมไม่ขัดต่อกฎหมาย หรือละเมิดสิทธิส่วนบุคคล

ข้อกำหนด	แนวทางปฏิบัติ
5.5.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องตรวจสอบประวัติบุคลากรหลักให้สอดคล้องกับข้อกฎหมาย ระเบียบ ข้อบังคับที่องค์กรต้องปฏิบัติตาม	ควรตรวจสอบประวัติบุคลากรหลักโดยไม่ละเมิดต่อข้อกฎหมาย ระเบียบ หรือละเมิดข้อมูลส่วนบุคคล
5.5.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายและขั้นตอนการปฏิบัติงานสำหรับการตรวจสอบประวัติบุคลากรหลัก	ควรจัดทำนโยบายและขั้นตอนการปฏิบัติงานสำหรับการตรวจสอบประวัติบุคลากรหลัก โดยคำนึงถึงระดับชั้นความลับของข้อมูลที่เข้าถึง รวมถึงระบุข้อกฎหมาย ระเบียบที่เกี่ยวกับการตรวจสอบประวัติบุคลากร
(ข) ผู้ให้บริการต้องกำหนดเกณฑ์สำหรับการตรวจสอบประวัติบุคลากรหลัก	ควรกำหนดเกณฑ์สำหรับตรวจสอบประวัติบุคลากรหลักเพื่อเป็นการยืนยันความถูกต้องของเอกสาร ข้อมูลหรือบุคคลที่ใช้อ้างอิง ซึ่งประกอบด้วยเอกสารหรือข้อมูลที่สำคัญอย่างน้อยดังนี้ – ประสบการณ์ทำงาน

ข้อกำหนด	แนวทางปฏิบัติ
	– เอกสารรับรองทางการศึกษา – ใบรับรองหรือประกาศนียบัตรทางด้านวิชาชีพต่าง ๆ – ข้อมูลหรือหลักฐานประกอบการแสดงตน เช่น บัตรประชาชน ใบอนุญาตขับขี่ ทะเบียนบ้าน – ประวัติอาชญากรรม
(ค) ผู้ให้บริการต้องทบทวนนโยบายและขั้นตอนการปฏิบัติงานการตรวจสอบประวัติบุคลากรหลักอย่างสม่ำเสมอ	ควรทบทวนนโยบายและขั้นตอนการปฏิบัติงานการตรวจสอบประวัติบุคลากรหลักอย่างสม่ำเสมอหรือเมื่อเกิดการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานภายในองค์กร

5.6 วัตถุประสงค์ที่ 6: การสร้างความตระหนักด้านความมั่นคงปลอดภัย (security awareness)

เพื่อกำหนดให้บุคลากรที่เกี่ยวข้องมีความตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวกับความมั่นคงปลอดภัย และเข้าใจหน้าที่ความรับผิดชอบของตนเองเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง และลดความเสี่ยงจากความผิดพลาดในการปฏิบัติงาน

ข้อกำหนด	แนวทางปฏิบัติ
5.6.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องสร้างความตระหนักแก่บุคลากรหลักทราบถึงความมั่นคงปลอดภัย ภัยคุกคามและปัญหาอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ	ควรสร้างความตระหนักแก่บุคลากรหลักทราบและทำความเข้าใจนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ภัยคุกคาม รวมถึงบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยให้ครอบคลุมประเด็นสำคัญดังนี้ – การระบุความมุ่งมั่นของผู้บริหารในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ – การปฏิบัติตามกฎระเบียบที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ – การรับผิดชอบต่อการกระทำของตนเองเมื่อไม่ปฏิบัติตามข้อกำหนดหรือระเบียบขององค์กร – ขั้นตอนการรักษาความมั่นคงปลอดภัยของข้อมูลขั้นพื้นฐาน เช่น การรายงานสถานการณ์ด้านความมั่นคงปลอดภัย รวมถึงการควบคุมขั้นพื้นฐาน เช่น การควบคุมความมั่นคงปลอดภัยของรหัสผ่าน – ช่องทางติดต่อสำหรับรับทราบข้อมูลและคำแนะนำเกี่ยวกับความมั่นคงปลอดภัย
(ข) ผู้ให้บริการต้องตรวจสอบบุคคลที่สามที่ปฏิบัติงานภายในองค์กรเพื่อให้มั่นใจ	ควรตรวจสอบบุคคลที่สามที่ปฏิบัติงานภายในองค์กรว่าได้รับการสร้างความตระหนักด้านความมั่นคงปลอดภัย

ข้อกำหนด	แนวทางปฏิบัติ
ว่าได้รับการให้ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัย	
5.6.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดแผนการให้ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัยแก่บุคลากรที่เกี่ยวข้อง	ควรจัดทำแผนการให้ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัยแก่บุคลากรที่เกี่ยวข้อง ซึ่งควรสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร และได้รับการอนุมัติจากผู้บริหารระดับสูง
(ข) ผู้ให้บริการต้องสร้างความตระหนักให้แก่บุคลากรที่เกี่ยวข้องทราบถึงความมั่นคงปลอดภัย ภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย	1. ควรสร้างความตระหนักด้านความมั่นคงปลอดภัยให้แก่บุคลากรที่เกี่ยวข้องมีความตระหนักถึงการรักษาความมั่นคงปลอดภัย 2. ควรรวบรวมหลักฐาน หรือบันทึกข้อมูลของบุคลากรที่เกี่ยวข้องซึ่งได้รับการสร้างความตระหนักด้านความมั่นคงปลอดภัย

5.7 วัตถุประสงค์ที่ 7: การเปลี่ยนแปลงบุคลากร (personnel changes)

เพื่อกำหนดกระบวนการและขั้นตอนการบริหารจัดการการเปลี่ยนแปลงบุคลากรเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน การเปลี่ยนแปลงบทบาทและหน้าที่ปฏิบัติงาน การกำหนดสิทธิและการเพิกถอนสิทธิให้มีความเหมาะสม

ข้อกำหนด	แนวทางปฏิบัติ
5.7.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องเพิกถอนสิทธิการเข้าใช้งานอุปกรณ์ บัตรที่ใช้ระบุสิทธิการเข้าถึง และอุปกรณ์อื่น ๆ หลังจากการเปลี่ยนแปลงบุคลากรหรือเมื่อบุคลากรพ้นสภาพจากการเป็นพนักงานขององค์กรแล้ว	1. ควรมีขั้นตอนการเพิกถอนสิทธิการเข้าใช้งานอุปกรณ์ เช่น บัตรผ่านประตู หรืออุปกรณ์ที่ใช้กำหนดสิทธิการเข้าถึงต่าง ๆ ทันทีเมื่อพนักงานหรือบุคคลที่สามสิ้นสุดการจ้างหรือเปลี่ยนแปลงหน้าที่ในการปฏิบัติงาน 2. ควรมีขั้นตอนเรียกคืนสินทรัพย์เมื่อบุคลากรที่เกี่ยวข้องสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาข้อตกลง 3. ควรรวบรวมหลักฐานในกรณีที่มีการเปลี่ยนแปลงบุคลากร และมีการเพิกถอนสิทธิอุปกรณ์ที่ใช้ปฏิบัติงานและอุปกรณ์อื่น ๆ ที่บุคลากรเคยได้สิทธิในการเข้าใช้งาน
(ข) ผู้ให้บริการต้องให้ความรู้เกี่ยวกับการปฏิบัติงานเบื้องต้นแก่บุคลากรใหม่เพื่อให้รับทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและขั้นตอนการปฏิบัติงานขององค์กร	ควรรวบรวมหลักฐานเพื่อยืนยันว่าบุคลากรใหม่ได้รับการให้ความรู้เกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และขั้นตอนในการปฏิบัติงานเบื้องต้น

ข้อกำหนด	แนวทางปฏิบัติ
5.7.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับกระบวนการเปลี่ยนแปลงบุคลากรและกระบวนการเพิกถอนสิทธิการเข้าใช้งานอุปกรณ์สารสนเทศและอุปกรณ์อื่น ๆ ที่กำหนดสิทธิการเข้าใช้งานให้แก่บุคลากร	ควรจัดทำนโยบายหรือขั้นตอนการปฏิบัติงานการเปลี่ยนแปลงบุคลากรควรประกอบด้วยประเด็นสำคัญดังนี้ – หน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน – การบริหารจัดการทรัพย์สินสารสนเทศ – การเพิกถอนสิทธิการเข้าถึง – ข้อตกลงการรักษาความลับ
(ข) ผู้ให้บริการต้องจัดทำนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการอบรมให้ความรู้บุคลากรที่ได้รับบทบาทหน้าที่ใหม่	ควรจัดทำนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการอบรมให้ความรู้บุคลากรที่ได้รับบทบาทหน้าที่ใหม่ประกอบด้วยหัวข้อดังนี้ – การสร้างความตระหนักและการอบรมให้ความรู้ – สัญญาและเงื่อนไขการจ้างงาน – การป้องกันสิทธิและทรัพย์สินทางปัญญา – การป้องกันข้อมูลส่วนบุคคล – การลงโทษทางวินัย
(ค) ผู้ให้บริการต้องทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานการเปลี่ยนแปลงบุคลากรอย่างสม่ำเสมอ	ควรพิจารณาทบทวนนโยบายและขั้นตอนการปฏิบัติงานการเปลี่ยนแปลงบุคลากร และการเพิกถอนสิทธิการเข้าใช้งานอุปกรณ์สารสนเทศอย่างสม่ำเสมอตามระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ต่อการดำเนินงานภายในองค์กร

5.8 วัตถุประสงค์ที่ 8: การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

เพื่อกำหนดนโยบาย และข้อกำหนดสำหรับการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของศูนย์คอมพิวเตอร์ เช่น มีการควบคุมการเข้าถึงทางกายภาพ ระบบแจ้งเตือน การควบคุมด้านสภาพแวดล้อม ระบบดับเพลิงแบบอัตโนมัติ และระบบอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์คอมพิวเตอร์

ข้อกำหนด	แนวทางปฏิบัติ
5.8.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องป้องกันการเข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย, โครงสร้างพื้นฐานระบบบริหารจัดการศูนย์คอมพิวเตอร์	ควรมีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมขั้นพื้นฐาน เช่น ระบบล็อคประตู ระบบสัญญาณกันขโมย สัญญาณแจ้งเตือนเมื่อเกิดเหตุเพลิงไหม้

ข้อกำหนด	แนวทางปฏิบัติ
(infrastructure) และติดตั้งระบบควบคุมสภาพแวดล้อม	ถังดับเพลิงแบบพกพา ระบบกล้องวงจรปิด ระบบป้องกันน้ำท่วม และอื่น ๆ เป็นต้น
(ข) ผู้ให้บริการต้องกำหนดรายชื่อบุคคลที่มีสิทธิเข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย และกำหนดสิ่งที่ใช้ยืนยันตัวตนสำหรับเข้าถึง	1. ควรจัดทำทะเบียนรายชื่อบุคคลที่ได้รับสิทธิเข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย 2. ควรกำหนดสิ่งที่ใช้ยืนยันตัวตนสำหรับเข้าถึง เช่น ป้ายบัตรประจำตัวพนักงาน ซึ่งองค์กรเป็นผู้เก็บรักษาและทบทวนสิทธิผู้ใช้งานอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงบทบาทและหน้าที่การปฏิบัติงาน
(ค) ผู้ให้บริการต้องตรวจสอบสิทธิของผู้เข้าเยี่ยมชม (visitors) ก่อนอนุญาตให้เข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย	1. ควรจัดทำทะเบียนรายชื่อผู้เข้าเยี่ยมชมบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย 2. ควรกำหนดให้ผู้เข้าเยี่ยมชมติดบัตรผู้เข้าเยี่ยมชมให้เด่นชัดตลอดระยะเวลาที่อยู่ภายในบริเวณที่มีการรักษาความมั่นคงปลอดภัย
(ง) ผู้ให้บริการต้องตรวจสอบดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศของอุปกรณ์สารสนเทศในศูนย์คอมพิวเตอร์ เพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าวสามารถปฏิบัติงานได้อย่างปกติ และมีประสิทธิภาพ	ควรมีระบบควบคุมสภาพแวดล้อมของศูนย์คอมพิวเตอร์ขั้นพื้นฐาน เช่น ระบบน้ำประปา ระบบไฟฟ้าสำรอง ระบบควบคุมอุณหภูมิและความชื้น ระบบตรวจจับควันไฟ ระบบตรวจจับเพลิงไหม้ ซึ่งต้องได้รับการดูแลรักษา และทดสอบเพื่อให้มั่นใจว่าสามารถปฏิบัติงานได้ปกติ
5.8.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	ควรกำหนดนโยบายความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมซึ่งควรประกอบด้วยประเด็นสำคัญดังนี้ – การกำหนดขอบเขตการรักษาความมั่นคงปลอดภัยทางกายภาพ – การกำหนดสิทธิเพื่อเข้าออกบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย – การจัดเก็บอุปกรณ์สารสนเทศภายในบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย – การควบคุมทางกายภาพของทางเข้า – การรักษาความมั่นคงปลอดภัยพื้นที่ปฏิบัติงานและสิ่งอำนวยความสะดวกต่าง ๆ – การดูแลรักษาอุปกรณ์และการป้องกันการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต – การป้องกันภัยคุกคามจากภายนอก – การปฏิบัติเมื่อเข้าถึงบริเวณที่ต้องรักษาความมั่นคงปลอดภัย

ข้อกำหนด	แนวทางปฏิบัติ
	– การควบคุมบริเวณพื้นที่จัดส่งและรับของเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
(ข) ผู้ให้บริการต้องกำหนดขั้นตอนการปฏิบัติงานกรณีเกิดเหตุการณ์ฉุกเฉิน	ควรมีขั้นตอนการปฏิบัติงานกรณีเกิดเหตุการณ์ฉุกเฉิน เช่น อุทกภัย อัคคีภัย แผ่นดินไหว เหตุการณ์ประท้วงจนทำให้ไม่สามารถเข้าพื้นที่ปฏิบัติงานได้ เป็นต้น และมีวิธีปฏิบัติให้บุคลากรที่เกี่ยวข้องสามารถปฏิบัติตามได้เมื่อเกิดเหตุการณ์ฉุกเฉินดังกล่าว
(ค) ผู้ให้บริการต้องทบทวนและอนุมัติรายชื่อบุคลากรที่มีสิทธิเข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยจากผู้ที่มีอำนาจ	1. ควรกำหนดให้มีการทบทวนสิทธิการเข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยของบุคลากรภายในองค์กร 2. ควรทบทวนสิทธิหรือสร้างสิทธิสำหรับบุคลากรเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่ความรับผิดชอบ 3. ควรตรวจสอบกระบวนการกำหนดสิทธิเพื่อให้มั่นใจว่าการกำหนดสิทธิไม่ได้ถูกกำหนดให้แก่ผู้ที่ไม่ได้รับอนุญาต 4. ควรมีการบันทึกข้อมูลการเปลี่ยนแปลงสิทธิของผู้ที่ได้รับสิทธิระดับสูงเพื่อใช้ตรวจสอบในภายหลัง
(ง) ผู้ให้บริการต้องมีข้อกำหนดให้ผู้เข้าเยี่ยมชมรับทราบและปฏิบัติตามนโยบาย และขั้นตอนการปฏิบัติงานขององค์กร	1. ควรสร้างความตระหนักให้ผู้เข้าเยี่ยมชมมีความเข้าใจในหลักเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติตามระหว่างที่อยู่ในบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย 2. ควรแสดงข้อกำหนดหรือข้อห้ามเพื่อให้ผู้เข้าเยี่ยมชมรับทราบและปฏิบัติตามอย่างเคร่งครัดเมื่อเข้าถึงบริเวณที่ต้องรักษาความมั่นคงปลอดภัย
(จ) ผู้ให้บริการต้องดูแลรักษาบันทึกเหตุการณ์ของผู้เข้าเยี่ยมชมที่เข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย	1. ควรจัดทำบันทึกเหตุการณ์ของผู้เข้าเยี่ยมชมทุกคนที่ได้รับอนุญาตให้เข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย 2. ควรมีรายละเอียดในบันทึกเหตุการณ์ของผู้เข้าเยี่ยมชม เช่น – ชื่อ – นามสกุลของผู้เข้าเยี่ยมชม – วัน เวลาเข้า – ออกบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย – เหตุผลในการเข้าเยี่ยมชม – ลายมือชื่อผู้เข้าเยี่ยมชม
(ฉ) ผู้ให้บริการต้องติดตามตรวจสอบทุกครั้งที่มีการเข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย	ควรมีบุคลากรติดตามผู้เข้าเยี่ยมชมตลอดเวลาที่อยู่ในบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยหรือจนกว่าจะเสร็จภารกิจและออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

ข้อกำหนด	แนวทางปฏิบัติ
(ช) ผู้ให้บริการต้องทบทวนนโยบายความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมอย่างสม่ำเสมอ	ควรพิจารณาทบทวนนโยบายความมั่นคงปลอดภัยทางกายภาพ และสภาพแวดล้อมอย่างสม่ำเสมอตามระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ต่อการปฏิบัติงานภายในองค์กร

5.9 วัตถุประสงค์ที่ 9: การรักษาความมั่นคงปลอดภัยของระบบสนับสนุนการดำเนินงาน (security of supporting utilities)

เพื่อกำหนดและบำรุงรักษาอุปกรณ์สนับสนุนการดำเนินงานที่เหมาะสม รวมถึงมีการรักษาความมั่นคงปลอดภัยของอุปกรณ์สนับสนุนการดำเนินงาน เช่น ระบบไฟฟ้า ระบบระบายอากาศ เป็นต้น

ข้อกำหนด	แนวทางปฏิบัติ
5.9.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดกระบวนการป้องกัน ดูแลรักษาระบบสนับสนุนการดำเนินงาน	ควรติดตั้งระบบสนับสนุนการดำเนินงานเพื่อป้องกันการหยุดชะงักของกระแสไฟฟ้า เช่น เครื่องกำเนิดไฟฟ้าสำรอง (generator) และน้ำมันเชื้อเพลิง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้า (UPS) ระบบควบคุมอุณหภูมิความชื้น ระบบระบายอากาศ ระบบสายไฟฟ้า และสายสัญญาณ และระบบอื่น ๆ ที่เกี่ยวข้อง เป็นต้น
5.9.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของระบบสนับสนุนการดำเนินงาน และมีข้อกำหนดในการดูแลรักษาระบบสนับสนุนการดำเนินงาน	1. ควรจัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของระบบสนับสนุนการดำเนินงาน โดยนโยบายดังกล่าวมีรายละเอียดเกี่ยวกับการดูแลรักษาอุปกรณ์สารสนเทศ และมีข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการดำเนินงาน เช่น – ระบบกระแสไฟฟ้า – เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้า – เครื่องกำเนิดไฟฟ้าสำรอง และน้ำมันเชื้อเพลิงสำรอง – ระบบควบคุมอุณหภูมิความชื้น – ระบบระบายอากาศ – การเดินสายไฟ สายสื่อสาร และสายสัญญาณอื่น ๆ – ระบบอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสนับสนุนการดำเนินงาน 2. ควรมีระบบแจ้งเตือนเมื่อระบบสนับสนุนการดำเนินงานปฏิบัติงานไม่ปกติหรือหยุดการปฏิบัติงาน 3. ควรมีการบำรุงรักษาระบบสนับสนุนการดำเนินงานตามระยะเวลาที่เหมาะสมหรือตามคำแนะนำของผู้ผลิต

ข้อกำหนด	แนวทางปฏิบัติ
	4. ควรจัดเก็บบันทึกการบำรุงรักษาระบบสนับสนุนการดำเนินงาน เพื่อใช้ในการตรวจสอบและประเมินผลการดำเนินงานของอุปกรณ์สารสนเทศ 5. ควรทดสอบระบบสนับสนุนการดำเนินงานอย่างสม่ำเสมอเพื่อให้มั่นใจว่า ระบบสนับสนุนการดำเนินงานยังคงสามารถปฏิบัติงานได้อย่างปกติ 6. ควรอนุญาตให้เฉพาะเจ้าหน้าที่ซ่อมบำรุงที่สามารถเข้าบำรุงซ่อมแซมระบบสนับสนุนการดำเนินงานได้ 7. ควรตรวจสอบระบบสนับสนุนการดำเนินงานที่ได้รับการซ่อมแซมเพื่อให้แน่ใจว่าอุปกรณ์ไม่ได้รับการดัดแปลง 8. ควรติดตั้งสายสัญญาณและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันสัญญาณรบกวนซึ่งกันและกัน 9. ควรปิดล็อคห้องที่มีสายสัญญาณต่าง ๆ เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก 10. ควรมีขั้นตอนการควบคุมและการจัดทำบันทึกรายการอุปกรณ์สารสนเทศที่นำไปใช้งานนอกสถานที่ ควรได้รับอนุญาตจากผู้มีอำนาจและปฏิบัติตามคำแนะนำของผู้ผลิต
(ข) ผู้ให้บริการต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของระบบสนับสนุนการปฏิบัติงาน อย่างสม่ำเสมอ	ควรกำหนดให้มีการทบทวนนโยบายสำหรับระบบสนับสนุนการดำเนินงานอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ต่อการดำเนินงานภายในองค์กร

5.10 วัตถุประสงค์ที่ 10: การควบคุมการเข้าถึงระบบเครือข่าย และระบบสารสนเทศ (access control to network and information system)

เพื่อกำหนดนโยบายและข้อกำหนดสำหรับการเข้าถึงแหล่งข้อมูลขององค์กร เช่น ระบบเครือข่าย ระบบบริหารจัดการชื่อผู้ใช้ ระบบการตรวจสอบผู้ใช้งาน ระบบควบคุมการเข้าถึง ระบบไฟร์วอลล์ และความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่าย

ข้อกำหนด	แนวทางปฏิบัติ
5.10.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องระบุข้อมูลผู้ใช้งานที่แตกต่างกัน (unique identifier) และตรวจสอบสิทธิก่อนเข้าใช้งานระบบสารสนเทศหรือบริการ	1. ควรมีขั้นตอนการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ เมื่อมีผู้ขอใช้งานระบบสารสนเทศขององค์กร 2. ควรกำหนดบัญชีผู้ใช้งานที่ไม่ซ้ำกันเพื่อเป็นการระบุตัวตนและเชื่อมโยงไปถึงความรับผิดชอบต่อการกระทำของตนได้

ข้อกำหนด	แนวทางปฏิบัติ
	3. ควรกำหนดให้มีการเพิกถอนบัญชีผู้ใช้งานทันทีเมื่อผู้ใช้งานนั้นพ้นสภาพการเป็นพนักงาน เปลี่ยนตำแหน่งงาน 4. ควรทบทวนบัญชีผู้ใช้งานเป็นประจำ เพื่อลบหรือปิดการใช้งานบัญชีผู้ใช้ที่มีความซ้ำซ้อน
(ข) ผู้ให้บริการต้องกำหนดกลไกควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ เพื่ออนุญาตให้เฉพาะผู้ใช้งานที่ได้รับสิทธิแล้วเท่านั้น	ควรกำหนดวิธีการหรือกลไกสำหรับการควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศซึ่งประกอบด้วยลักษณะดังนี้ – ผู้ใช้งานควรดูแลรักษาอุปกรณ์สารสนเทศที่อยู่ภายใต้ความรับผิดชอบในระหว่างที่ไม่มีการใช้งาน – ไม่มีการแสดงตัวหรือระบุชื่อระบบสารสนเทศจนกว่าจะเข้าสู่ระบบได้สำเร็จ – แสดงคำเตือนให้ทราบว่าคอมพิวเตอร์ควรเข้าถึงได้เฉพาะผู้มีอำนาจเท่านั้น – ไม่ควรแสดงข้อความหรือวิธีการช่วยเหลือใด ๆ ขณะอยู่ในขั้นตอนการเข้าสู่ระบบ – มีการตรวจสอบข้อมูลการเข้าสู่ระบบ และหากเกิดความผิดพลาดขณะเข้าสู่ระบบไม่ควรมีข้อความแสดงว่าความผิดพลาดนั้นเกิดขึ้นจากที่ใด – กำหนดจำนวนครั้งของความผิดพลาดในขั้นตอนการเข้าสู่ระบบ เช่น กรอกรหัสผิดพลาดได้ไม่เกินสามครั้งเป็นต้น – ไม่แสดงรหัสผ่านที่ป้อนระหว่างขั้นตอนการเข้าสู่ระบบ – จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่สำคัญ – ยุติการใช้งานระบบหากไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนดไว้ – จำกัดจำนวนผู้ใช้งานที่สามารถเข้าถึงระบบเครือข่ายได้จากภายนอก – กำหนดคุณสมบัติของรหัสผ่านให้มีความซับซ้อนยากต่อการคาดเดา
5.10.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ	ควรมีการจัดทำนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศซึ่งประกอบด้วยประเด็นสำคัญดังนี้

ข้อกำหนด	แนวทางปฏิบัติ
	– การกำหนดกฎเกณฑ์ ข้อกำหนดที่เกี่ยวข้องและข้อปฏิบัติที่ผู้ใช้งานต้องปฏิบัติตาม – การกำหนดมาตรการในการควบคุมการเข้าถึง ระบบเครือข่าย และระบบสารสนเทศ และระบบปฏิบัติการ – การควบคุมการเข้าถึงให้เหมาะสมกับชั้นความลับและความสำคัญต่อข้อมูลในระบบ – การแบ่งแยกระบบเครือข่าย – การควบคุมการเข้าถึงทรัพย์สินสารสนเทศที่สำคัญให้มีความมั่นคงปลอดภัย และหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏอยู่ขณะที่ไม่ใช้งาน (clear desk and clear screen) – การอนุมัติการเข้าถึงระบบเครือข่าย และระบบสารสนเทศตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน – การจำกัดการเข้าถึงโปรแกรมอรรถประโยชน์ (utility) – การทบทวนหรือเพิกถอนสิทธิการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ – การกำหนดประเภทของการเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่าย และระบบสารสนเทศ เช่น การเชื่อมต่อจากระยะไกล การเชื่อมต่อผ่านระบบเครือข่ายไร้สาย เป็นต้น – การกำหนดให้บุคคลที่สามตระหนัก เข้าใจ และปฏิบัติตามนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศขององค์กร – การจัดเก็บบันทึกข้อมูลการเข้าถึงของผู้ใช้งาน – การเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน
(ข) ผู้ให้บริการต้องเลือกกลไกสำหรับตรวจสอบและการยืนยันตัวตนของผู้ใช้งานจากผลของการวิเคราะห์ความเสี่ยง	ควรกำหนดกลไกยืนยันตัวตนผู้ใช้งานที่แตกต่างกัน เช่น วิธีการยืนยันตัวตนแบบปัจจัยเดียว (single-sign-on) วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และการยืนยันตัวตนจากระยะไกล (teleworking authentication)
(ค) ผู้ให้บริการต้องติดตามตรวจสอบการเข้าถึงระบบเครือข่าย และระบบสารสนเทศโดยกำหนดกระบวนการอนุมัติและลงทะเบียน เพื่อป้องกัน	1. ควรเก็บบันทึกข้อมูลขณะเข้าสู่ระบบได้สำเร็จ หรือไม่สำเร็จ 2. ควรกำหนดให้ผู้ใช้งานสามารถเข้าถึงได้เฉพาะระบบเครือข่ายที่ได้รับได้รับอนุญาตเท่านั้น

ข้อกำหนด	แนวทางปฏิบัติ
การละเมิดการเข้าถึงและเข้าใช้งานโดยไม่ได้รับอนุญาต	3. ควรจัดทำรายชื่อของผู้ที่มีสิทธิเข้าถึงระบบเครือข่ายและระบบสารสนเทศ 4. ควรบันทึกข้อมูลการใช้งานสิทธิระดับสูง
(ง) ผู้ให้บริการต้องจำกัดจำนวนผู้ใช้งานที่เข้าถึงฟังก์ชันด้านความมั่นคงปลอดภัยให้กับผู้ที่มีความจำเป็นเพื่อให้มีความมั่นคงปลอดภัยของระบบข้อมูล	1. ควรจัดทำรายชื่อของผู้ใช้ที่มีสิทธิเข้าถึงฟังก์ชันด้านความมั่นคงปลอดภัยของระบบเครือข่าย และระบบสารสนเทศ 2. ควรแบ่งเมนูการใช้งานเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบเครือข่าย และระบบสารสนเทศ 3. ควรควบคุมสิทธิของผู้ใช้ เช่น สิทธิในการ อ่าน เขียน และลบข้อมูล
(จ) ผู้ให้บริการต้องมีกระบวนการตรวจสอบการใช้งานสิทธิระดับสูง (privileged account) โดยพิจารณาตั้งแต่กระบวนการสร้างบัญชีผู้ใช้งาน การรับรองสิทธิผู้ใช้งาน และการทบทวนสิทธิผู้ใช้งาน	1. ควรติดตามตรวจสอบการใช้งานสิทธิระดับสูงอย่างสม่ำเสมอ เช่น ดูจากการบันทึกเหตุการณ์การเข้าใช้งานระบบเครือข่าย และระบบสารสนเทศ 2. ควรเพิ่มความถี่สำหรับตรวจสอบสิทธิของบุคลากรที่มีสิทธิระดับสูงให้มากกว่าสิทธิของผู้ใช้งานทั่วไป
(ฉ) ผู้ให้บริการต้องแบ่งแยกระบบเครือข่าย และระบบสารสนเทศตามข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศ	1. ควรแบ่งแยกระบบเครือข่ายเพื่อให้จำกัดผลกระทบจากการโจมตีของโปรแกรมไม่พึงประสงค์ (malware) 2. ควรแบ่งแยกระบบเครือข่ายออกเป็นระบบเครือข่ายภายในและระบบเครือข่ายภายนอก 3. ควรมีข้อกำหนดเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่าย เช่น ติดตั้ง firewall เพื่อป้องกันการบุกรุกหรือเข้าถึงโดยไม่ได้รับอนุญาต 4. ควรมีข้อมูลแสดงความสัมพันธ์ของการแบ่งแยกหน้าที่ (segregation of duties control matrix)

5.11 วัตถุประสงค์ที่ 11: การควบคุมความถูกต้องขององค์ประกอบระบบเครือข่ายและระบบสารสนเทศ (integrity of network components and information system)

เพื่อกำหนดวิธีการควบคุมป้องกันและดูแลรักษาระบบเครือข่ายขององค์กรให้สามารถปฏิบัติงานได้อย่างถูกต้อง โดยกำหนดขั้นตอนเพื่อป้องกันเหตุการณ์ด้านความมั่นคงปลอดภัย ตัวอย่างเช่น ป้องกันการโจมตีจากโปรแกรมไม่พึงประสงค์ เป็นต้น

ข้อกำหนด	แนวทางปฏิบัติ
5.11.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องตรวจสอบเพื่อให้มั่นใจว่าซอฟต์แวร์ที่ติดตั้งบนระบบเครือข่ายและระบบสารสนเทศไม่ได้ถูกดัดแปลงหรือมีการเปลี่ยนแปลง	1. ควรป้องกันซอฟต์แวร์และข้อมูลในระบบเครือข่ายโดยใช้วิธีการควบคุมป้องกัน เช่น ควบคุมการนำเข้าข้อมูล การติดตั้งไฟร์วอลล์ การเข้ารหัสลับ 2. ควรกำหนดสิทธิระดับสูงให้ผู้ที่มีหน้าที่ในการติดตั้งซอฟต์แวร์ในระบบเครือข่าย 3. ควรระบุประเภทของซอฟต์แวร์ที่ได้รับอนุญาตให้สามารถติดตั้งได้ หรือติดตั้งไม่ได้
(ข) ผู้ให้บริการต้องป้องกันข้อมูลที่สำคัญเพื่อป้องกันการถูกเปิดเผยหรือการแก้ไขดัดแปลงข้อมูล	ควรป้องกันความมั่นคงปลอดภัยด้านสารสนเทศของข้อมูลโดยการใช้กลไกป้องกัน เช่น การแยกส่วนจัดเก็บข้อมูล การเข้ารหัสลับ และการแฮชข้อมูล และวิธีการอื่น ๆ เป็นต้น
(ค) ผู้ให้บริการต้องป้องกันการติดตั้งโปรแกรมไม่พึงประสงค์ หรือซอฟต์แวร์ที่ไม่ได้รับอนุญาตภายในระบบเครือข่ายและระบบสารสนเทศ	1. ควรติดตั้งระบบตรวจจับไวรัส โปรแกรมไม่พึงประสงค์ และมีการปรับปรุงฐานข้อมูลไวรัสให้มีความทันสมัยอย่างสม่ำเสมอ 2. ควรจัดเก็บบันทึกการปรับปรุงฐานข้อมูลไวรัสและโปรแกรมไม่พึงประสงค์ 3. ควรจัดเก็บบันทึกการตรวจสอบหรือการสแกนไวรัสและโปรแกรมไม่พึงประสงค์
5.11.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดขั้นตอนการปฏิบัติงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่ายและระบบสารสนเทศ	ควรจัดทำขั้นตอนการปฏิบัติงานการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่ายและระบบสารสนเทศ ซึ่งประกอบด้วยประเด็นสำคัญดังนี้ – การป้องกันการเข้าถึงข้อมูลในระบบเครือข่ายและระบบสารสนเทศโดยไม่ได้รับอนุญาต – การกำหนดบทบาทและหน้าที่ความรับผิดชอบการดูแลระบบเครือข่ายและระบบสารสนเทศ – การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศได้จากระยะไกล – การป้องกันข้อมูลรั่วไหล และความถูกต้องของข้อมูลที่ต้องส่งผ่านระบบเครือข่าย เช่น การส่งข้อมูลผ่านระบบอินเทอร์เน็ต หรือการส่งข้อมูลผ่านจดหมายอิเล็กทรอนิกส์ – การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ดักจับโปรแกรมไม่พึงประสงค์

ข้อกำหนด	แนวทางปฏิบัติ
	– การติดตามตรวจสอบการปฏิบัติงานระบบเครือข่ายและระบบสารสนเทศเพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง – การจัดเก็บบันทึกเหตุการณ์การดำเนินงานของอุปกรณ์สารสนเทศ เพื่อใช้ตรวจสอบในภายหลัง – การแบ่งแยกระบบเครือข่าย
(ข) ผู้ให้บริการต้องมีกลไกหรือระบบป้องกันโปรแกรมไม่พึงประสงค์ที่สามารถควบคุมและบริหารได้จากส่วนกลาง	ควรมีวิธีปฏิบัติหรือระบบตรวจสอบโปรแกรมไม่พึงประสงค์เพื่อตรวจสอบข้อมูลที่มีการแลกเปลี่ยนกันทางระบบเครือข่าย รวมถึงการส่ง – รับข้อมูลหรือไฟล์แนบที่มีการส่งผ่านทางจดหมายอิเล็กทรอนิกส์
(ค) ผู้ให้บริการต้องมีกลไกป้องกันไม่ให้ผู้ใช้งานหลีกเลี่ยงการใช้งานระบบป้องกันโปรแกรมไม่พึงประสงค์	1. ควรมีวิธีปฏิบัติหรือระบบตรวจสอบการปฏิบัติงานและกิจกรรมของผู้ใช้งานอย่างสม่ำเสมอ 2. ควรมีระบบตรวจจับการบุกรุกเพื่อตรวจจับพฤติกรรมการใช้งานที่ผิดปกติของระบบเครือข่ายและระบบสารสนเทศ
(ง) ผู้ให้บริการต้องมีกลไกสำหรับป้องกัน spam ในจุดที่สามารถเข้าถึงระบบเครือข่ายได้ เช่น ที่เครื่องคอมพิวเตอร์แม่ข่าย (server) หรืออุปกรณ์ประมวลผลแบบพกพา (mobile computing) ที่อยู่บนระบบเครือข่าย	1. ควรกำหนดรายชื่อของอุปกรณ์ ซอฟต์แวร์ ที่ได้รับอนุญาตให้สามารถเข้าถึงระบบเครือข่าย เพื่อป้องกันการใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาต 2. ควรตรวจสอบการใช้ทรัพยากรสารสนเทศขององค์กรอย่างสม่ำเสมอ เพื่อป้องกันการใช้งานอย่างผิดวัตถุประสงค์ 3. ควรจำกัดการใช้งานผู้ที่ไม่ได้รับอนุญาตหรือผู้ที่ไม่ได้ลงทะเบียนให้เข้าใช้งานระบบสารสนเทศ

5.12 วัตถุประสงค์ที่ 12: การกำหนดขั้นตอนการปฏิบัติงาน (operating procedures)

เพื่อกำหนดขั้นตอนการปฏิบัติงานกับระบบเครือข่ายและระบบสารสนเทศที่สำคัญต่อการดำเนินงานขององค์กร เช่น เอกสารขั้นตอนการปฏิบัติงาน คู่มือการปฏิบัติงาน ขั้นตอนการปฏิบัติงานสำหรับผู้ดูแลระบบสารสนเทศและระบบเครือข่าย

ข้อกำหนด	แนวทางปฏิบัติ
5.12.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดขั้นตอนการปฏิบัติงาน และมอบหมายหน้าที่ความรับผิดชอบสำหรับการปฏิบัติงานระบบเครือข่ายระบบสารสนเทศที่สำคัญ	ควรจัดทำขั้นตอนการปฏิบัติงานและกำหนดหน้าที่ความรับผิดชอบสำหรับระบบเครือข่ายและระบบสารสนเทศที่สำคัญซึ่งประกอบด้วยประเด็นสำคัญดังนี้ – การติดตั้งและการตั้งค่าเริ่มต้นของระบบสารสนเทศ

ข้อกำหนด	แนวทางปฏิบัติ
	– การประมวลผลและการบริหารจัดการข้อมูลทั้งแบบอัตโนมัติและแบบดำเนินการเอง – การสำรองข้อมูล – วิธีปฏิบัติสำหรับการบริหารจัดการความผิดพลาดซึ่งอาจเกิดขึ้นระหว่างการปฏิบัติงาน รวมถึงข้อจำกัดการใช้งานระบบสนับสนุนการดำเนินงาน – การสนับสนุนการปฏิบัติงาน และรายชื่อผู้ติดต่อของบุคคลที่สามในกรณีที่เกิดเหตุไม่คาดคิดหรือมีปัญหาด้านการปฏิบัติงานและทางเทคนิค – การบริหารจัดการสื่อบันทึกข้อมูล การลบข้อมูลในสื่อบันทึกข้อมูล – ขั้นตอนการเริ่มระบบใหม่ และการกู้คืนระบบสารสนเทศในกรณีที่ระบบเกิดความล้มเหลว – การบริหารจัดการข้อมูลสำหรับการตรวจสอบและระบบบันทึกเหตุการณ์ของระบบสารสนเทศ – ขั้นตอนการปฏิบัติงานการตรวจติดตาม และการเฝ้าระวัง – ขั้นตอนการปฏิบัติงานอื่น ๆ ที่เกี่ยวข้องกับการปฏิบัติงานด้านความมั่นคงปลอดภัย
5.12.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายด้านการปฏิบัติงานสำหรับระบบเครือข่ายและระบบสารสนเทศเพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขั้นตอนการปฏิบัติงานที่ได้กำหนดไว้	ควรจัดทำนโยบายสำหรับการปฏิบัติงานของระบบเครือข่ายและระบบสารสนเทศที่สำคัญรวมถึงระบบระบบอื่น ๆ ที่อยู่ในขอบเขตหรือเกี่ยวข้องกับการปฏิบัติงาน
(ข) ผู้ให้บริการต้องทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานอย่างสม่ำเสมอ	ควรทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร

5.13 วัตถุประสงค์ที่ 13: การบริหารจัดการการเปลี่ยนแปลง (change management)

เพื่อกำหนดวิธีควบคุมการปฏิบัติงานการบริหารจัดการเปลี่ยนแปลงขององค์กร ตัวอย่างเช่น กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลสารสนเทศ และทรัพย์สินสารสนเทศ ที่สำคัญต่อการให้บริการซึ่งมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น รวมถึงเพื่อให้บุคลากรที่เกี่ยวข้องสามารถปฏิบัติงานได้อย่างถูกต้อง และลดความเสี่ยงจากการปฏิบัติงานที่ผิดพลาด

ข้อกำหนด	แนวทางปฏิบัติ
5.13.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศที่สำคัญ	ควรมีขั้นตอนการบริหารจัดการการเปลี่ยนแปลงสำหรับระบบสารสนเทศที่สำคัญซึ่งประกอบด้วยประเด็นสำคัญดังนี้ – การประเมินความเสี่ยงและการวางแผนก่อนการเปลี่ยนแปลงระบบสารสนเทศ – การเปลี่ยนแปลงระบบสารสนเทศโดยผู้ชำนาญ และผ่านการอนุมัติจากผู้มีอำนาจ – การทดสอบระบบสารสนเทศทั้งก่อนและหลังการติดตั้ง เพื่อตรวจสอบว่ามีผลกระทบต่อระบบอื่น ๆ หรือไม่ – ควรจัดเก็บซอฟต์แวร์เวอร์ชันก่อนหน้าพร้อมกับขั้นตอนรายละเอียดการกำหนดค่าพารามิเตอร์และซอฟต์แวร์สนับสนุนไว้ใช้เมื่อเกิดสถานการณ์ด้านความมั่นคงปลอดภัยหรือกรณีที่ไม่สามาถติดตั้งซอฟต์แวร์เวอร์ชันใหม่ได้
(ข) ผู้ให้บริการต้องแจ้งให้ผู้ใช้บริการทราบถึงการเปลี่ยนแปลงของระบบสารสนเทศที่สำคัญซึ่งอาจส่งผลกระทบต่อการให้บริการ	ควรแจ้งข่าวสารเกี่ยวกับการเปลี่ยนแปลงที่สำคัญให้ผู้ใช้บริการรับทราบเมื่อเกิดการเปลี่ยนแปลงกับระบบสารสนเทศ
5.13.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลงเพื่อเป็นแนวทางสำหรับปฏิบัติงานและมั่นใจได้ว่าการปฏิบัติงานเป็นไปตามขั้นตอนการปฏิบัติที่ได้กำหนดไว้	ควรกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลง ซึ่งประกอบด้วยประเด็นสำคัญดังนี้ – ระบุความเร่งด่วนของการเปลี่ยนแปลง เช่น เร่งด่วนมาก เร่งด่วนน้อย หรือปกติ – ระบุวัตถุประสงค์ของการเปลี่ยนแปลง – บันทึกรายละเอียดของการดำเนินงานที่เกี่ยวข้องกับการเปลี่ยนแปลง – การวางแผนการปฏิบัติงานการเปลี่ยนแปลง – การประเมินผลกระทบที่อาจเกิดขึ้น รวมถึงผลกระทบด้านความมั่นคงปลอดภัยของการเปลี่ยนแปลง – การทดสอบการเปลี่ยนแปลงทั้งก่อน และหลังการเปลี่ยนแปลง – การแจ้งผู้ที่เกี่ยวข้องกับการปฏิบัติงานเมื่อเกิดการเปลี่ยนแปลง – การกำหนดแผนสำหรับการถอยกลับสู่สภาพเดิมกรณีที่การเปลี่ยนแปลงไม่สำเร็จ

ข้อกำหนด	แนวทางปฏิบัติ
(ข) ผู้ให้บริการต้องบันทึกการเปลี่ยนแปลงในแต่ละขั้นตอนตามขั้นตอนการปฏิบัติงานที่ได้กำหนดไว้	ควรจัดทำรายงานการเปลี่ยนแปลงที่อธิบายถึงขั้นตอนในแต่ละขั้น และผลลัพธ์ของกระบวนการเปลี่ยนแปลง
(ค) ผู้ให้บริการต้องทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลงอย่างสม่ำเสมอ	ควรทบทวนขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลงอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ต่อการดำเนินงานขององค์กร

5.14 วัตถุประสงค์ที่ 14: การบริหารจัดการสินทรัพย์ (asset management)

เพื่อกำหนดให้มีการบริหารจัดการสินทรัพย์และการควบคุมการกำหนดค่าของระบบเครือข่ายและระบบสารสนเทศที่สำคัญ รวมถึงการระบุทรัพย์สินสารสนเทศและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินสารสนเทศที่เหมาะสม

ข้อกำหนด	แนวทางปฏิบัติ
5.14.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดค่าความมั่นคงปลอดภัยพื้นฐาน (secure baseline configurations) ของระบบสารสนเทศและส่วนประกอบต่าง ๆ ที่มีการพัฒนาขึ้น	1. ควรจัดทำเอกสารกำหนดค่าความมั่นคงปลอดภัยพื้นฐานของระบบเครือข่ายและระบบสารสนเทศ ที่มีคุณสมบัติอย่างน้อยดังนี้ – ขีดความสามารถสำคัญในการดำเนินงาน – ข้อจำกัดการใช้งาน – กำหนดค่าความมั่นคงปลอดภัยเริ่มต้น – พอร์ต โพรโทคอล และ/หรือบริการที่ได้รับการอนุญาต 2. ควรทบทวนการกำหนดค่าความมั่นคงปลอดภัยพื้นฐานของระบบเครือข่ายและระบบสารสนเทศอย่างสม่ำเสมอ
(ข) ผู้ให้บริการต้องมีการบริหารจัดการสินทรัพย์ที่สำคัญ	1. ควรรวบรวมและจัดทำบัญชีทรัพย์สินสารสนเทศที่สำคัญขององค์กร รวมถึงสินทรัพย์ที่สำคัญ เช่นบุคลากร (บุคลากรหลักและบุคลากรที่เกี่ยวข้อง) เป็นต้น 2. ควรทบทวนบัญชีทรัพย์สินสารสนเทศ อย่างสม่ำเสมอ
5.14.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานเกี่ยวกับการบริหารจัดการสินทรัพย์และการควบคุมการกำหนดค่าความมั่นคงปลอดภัย	1. นโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการทรัพย์สินสารสนเทศควรประกอบด้วยหัวข้ออย่างน้อย ดังนี้ – บทบาทหน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ – การกำหนดค่าความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ

ข้อกำหนด	แนวทางปฏิบัติ
	– การใช้งานทรัพย์สินสารสนเทศ ตัวอย่างเช่น การใช้งานจดหมายอิเล็กทรอนิกส์ อินเทอร์เน็ต เครื่องคอมพิวเตอร์ และอุปกรณ์พกพาอื่น ๆ เป็นต้น 2. ควรให้บุคลากรที่เกี่ยวข้องและผู้ใช้งานภายนอกที่มีสิทธิเข้าถึงระบบสารสนเทศขององค์กรได้รับทราบถึงข้อกำหนดการใช้งานทรัพย์สินสารสนเทศที่กำหนดไว้ 3. ควรจัดทำรายการการควบคุมการกำหนดค่าความมั่นคงปลอดภัยของระบบเครือข่ายและระบบสารสนเทศที่สำคัญ 4. ควรระบุผู้รับผิดชอบของทรัพย์สินสารสนเทศแต่ละรายการในบัญชีทรัพย์สินสารสนเทศและความผูกพันระหว่างทรัพย์สินสารสนเทศ 5. ควรทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสินทรัพย์และการควบคุมการกำหนดค่าความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยคำนึงถึงการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร 6. ควรจำแนกประเภททรัพย์สินสารสนเทศตามข้อกำหนดทางกฎหมาย มูลค่า ความสำคัญ และความอ่อนไหวต่อการถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

5.15 วัตถุประสงค์ที่ 15: การตรวจพบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย (security incident detection and response)

เพื่อกำหนดกระบวนการตรวจพบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย รวมถึงการพิจารณาการตรวจพบสถานการณ์ การตอบสนองต่อสถานการณ์ การบรรเทาสถานการณ์ การกู้คืน และการฟื้นฟูจากสถานการณ์ และนำบทเรียนที่ได้รับมาประยุกต์ใช้

ข้อกำหนด	แนวทางปฏิบัติ
5.15.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดกระบวนการหรือระบบสารสนเทศสำหรับตรวจพบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย	1. ควรกำหนดกระบวนการหรือมีระบบสารสนเทศที่สามารถจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ตรวจพบได้ทันเวลาโดยบุคคลที่เหมาะสม 2. ควรมีทะเบียนรายการสถานการณ์ด้านความมั่นคงปลอดภัยที่สำคัญ และในแต่ละสถานการณ์ 3. ควรมีรายละเอียดของ ผลกระทบ สาเหตุ การดำเนินการแก้ไข และบทเรียนที่ได้รับ

ข้อกำหนด	แนวทางปฏิบัติ
(ข) ผู้ให้บริการต้องกำหนดให้บุคลากรมีความพร้อมในการจัดการสถานการณ์ด้านความมั่นคงปลอดภัย	1. ควรสร้างความตระหนักให้แก่บุคลากรหลักถึงกระบวนการและวิธีการจัดการและรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น 2. ควรกำหนดหน้าที่ความรับผิดชอบให้ชัดเจน เพื่อให้มั่นใจได้ว่าการรับมือกับสถานการณ์ที่เกิดขึ้นจะเป็นไปอย่างรวดเร็ว ได้ผล และมีลำดับการดำเนินการที่เหมาะสม
5.15.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดขั้นตอนการปฏิบัติงานสำหรับการตรวจพบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย	1. ควรจัดทำขั้นตอนการปฏิบัติงานสำหรับการตรวจพบและการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ผ่านการอนุมัติจากผู้มีอำนาจ และมีรายละเอียดเกี่ยวกับประเภทของสถานการณ์ที่อาจเกิดขึ้น วัตถุประสงค์ บทบาทหน้าที่และความรับผิดชอบ คำอธิบายโดยละเอียดของสถานการณ์ด้านความมั่นคงปลอดภัย และวิธีการจัดการสถานการณ์ด้านความมั่นคงปลอดภัย เพื่อเป็นข้อมูลสำหรับรายงานให้กับผู้บริหารระดับสูง (CISO) 2. ควรนำเครื่องมือหรือขั้นตอนการปฏิบัติงานต่าง ๆ มาใช้ในการตรวจจับ เช่น ระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (security information and event management: SIEM) ระบบช่วยเหลือการทำงานด้านความมั่นคงปลอดภัย (security helpdesk) สำหรับบุคลากรและผู้ใช้บริการ การรายงานและคำแนะนำต่าง ๆ จากทีม computer security incident response team (CSIRT) ที่ทำหน้าที่ประสานงานและจัดการภัยคุกคามที่เกิดขึ้นกับระบบสารสนเทศหรือขอบเขตเครือข่ายที่กำหนด และเครื่องมือเพื่อตรวจจับความผิดปกติอื่น ๆ เป็นต้น 3. ควรมีการฝึกอบรมบุคลากรที่เกี่ยวข้องถึงการตรวจพบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย และควรบันทึกประวัติการฝึกอบรมเป็นรายบุคคล 4. ควรทบทวนขั้นตอนการปฏิบัติงานสำหรับการตรวจพบและการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยคำนึงถึงสถานการณ์ด้านความมั่นคงปลอดภัยที่ผ่านมา และการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร

ข้อกำหนด	แนวทางปฏิบัติ
(ข) ผู้ให้บริการต้องกำหนดกระบวนการบันทึกและนำส่งสถานการณ์ด้านความมั่นคงปลอดภัยไปยังผู้ที่ได้รับมอบหมายได้ทันเวลา	1. สถานการณ์ด้านความมั่นคงปลอดภัยควรตอบสนองโดยผู้ที่ได้รับมอบหมาย และบุคลากรขององค์กรหรือบุคคลที่สามที่เกี่ยวข้อง ซึ่งการตอบสนองควรจะรวมถึง – การรวบรวมหลักฐานโดยเร็วที่สุดหลังจากเกิดเหตุ – การวิเคราะห์ข้อมูลพยานหลักฐานเพื่อความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนด – การสื่อสารถึงสถานการณ์ด้านความมั่นคงปลอดภัยหรือรายละเอียดที่เกี่ยวข้องใด ๆ ต่อบุคคลที่สามที่จำเป็นต้องรู้ – การจัดการกับจุดอ่อนด้านความมั่นคงปลอดภัยของข้อมูลที่พบว่าก่อให้เกิดหรือมีส่วนร่วมในสถานการณ์ด้านความมั่นคงปลอดภัย – การบันทึกรายละเอียดของการดำเนินการต่าง ๆ เมื่อมีการจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัย ตั้งแต่ต้นจนจบ เพื่อการวิเคราะห์ในภายหลัง – การรายงานให้กับผู้บริหารระดับสูงเมื่อมีความจำเป็น 2. ควรตรวจสอบและวิเคราะห์สถานการณ์ด้านความมั่นคงปลอดภัยที่สำคัญและเตรียมรายงานสถานการณ์ที่ประกอบด้วย การดำเนินการ คำแนะนำเพื่อบรรเทา เพื่อเป็นการลดเวลาในการตอบสนองต่อสถานการณ์ประเภทเดียวกันที่จะเกิดขึ้นในอนาคต

5.16 วัตถุประสงค์ที่ 16: การรายงานสถานการณ์ด้านความมั่นคงปลอดภัย (security incident reporting)

เพื่อกำหนดขั้นตอนการสื่อสารและการรายงานเกี่ยวกับสถานการณ์ด้านความมั่นคงปลอดภัย และวิธีการแก้ไขอย่างเหมาะสม

ข้อกำหนด	แนวทางปฏิบัติ
5.16.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องสื่อสารและรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่กำลังเกิดขึ้นหรือที่ผ่านมาให้กับบุคคลที่สาม ผู้ใช้บริการ หรือหน่วยงานภาครัฐเมื่อมีความจำเป็น	1. ควรจัดทำบัญชีรายชื่อและช่องทางการติดต่อของหน่วยงานกำกับดูแลหรือหน่วยงานที่เกี่ยวข้องสำหรับการรายงานสถานการณ์ด้านความมั่นคงปลอดภัย เช่น ศูนย์เตือนภัยพิบัติและทีมงานภัยพิบัติ บุคคลที่สามและผู้ใช้บริการ เป็นต้น 2. ควรรวบรวมหลักฐานของการสื่อสาร และการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ผ่านมา

ข้อกำหนด	แนวทางปฏิบัติ
5.16.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการสื่อสารและรายงานสถานการณ์ด้านความมั่นคงปลอดภัย	1. ควรกำหนดให้มีผู้รับผิดชอบในการรับแจ้งสถานการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น รวมทั้งข้อมูลสำหรับติดต่อผู้รับแจ้งเหตุ ซึ่งข้อมูลสำหรับการติดต่อควรเป็นที่ทราบกันเป็นอย่างดีภายในองค์กร 2. รายงานสถานการณ์ด้านความมั่นคงปลอดภัย ควรมีรายละเอียดที่อธิบายถึงเหตุผลในการสื่อสารหรือรายงาน (เหตุผลทางธุรกิจ เหตุผลทางกฎหมาย ฯลฯ) ประเภทของสถานการณ์ด้านความมั่นคงปลอดภัยในขอบข่าย เนื้อหาที่จำเป็นในการติดต่อสื่อสาร ช่องทางที่จำเป็นในการแจ้งเตือนหรือรายงาน และบทบาทหน้าที่รับผิดชอบ เพื่อใช้ในการสื่อสารและรายงาน 3. ผู้ที่ทำหน้าที่ในการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยควรมีความรู้และทักษะที่ดีในการรับมือและจัดการกับสถานการณ์ที่เกิดขึ้นได้อย่างเหมาะสม 4. สถานการณ์ที่ควรพิจารณาสำหรับการรายงาน มีดังนี้ – การควบคุมความมั่นคงปลอดภัยที่ไม่ได้ผล – การละเมิดความถูกต้องครบถ้วนของข้อมูลลับหรือความพร้อมใช้งาน – ข้อผิดพลาดของบุคลากร – การไม่ปฏิบัติตามนโยบายหรือหลักเกณฑ์ – การละเมิดข้อตกลงด้านความมั่นคงทางกายภาพ – การเปลี่ยนแปลงระบบสารสนเทศที่ไม่สามารถควบคุมได้ – ความผิดปกติของซอฟต์แวร์หรือฮาร์ดแวร์ – การละเมิดการเข้าถึง 5. ขั้นตอนการปฏิบัติงานสำหรับการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยควรประกอบด้วย – แบบฟอร์มสำหรับการรายงานสถานการณ์ด้านความมั่นคงปลอดภัย – การดำเนินงานเมื่อเกิดสถานการณ์ด้านความมั่นคงปลอดภัย เช่น กำหนดให้มีการสังเกตรายละเอียดที่สำคัญทั้งหมดของเหตุการณ์ที่พบ และรายงานไปยังช่องทางติดต่อรับแจ้งเหตุ เป็นต้น – กระบวนการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยตั้งแต่รับแจ้งเหตุจนจบการแก้ไข

ข้อกำหนด	แนวทางปฏิบัติ
	– กระบวนการทางวินัยสำหรับพนักงานที่กระทำการละเมิดความมั่นคงปลอดภัยขององค์กร 6. ควรทบทวนนโยบายและขั้นตอนการปฏิบัติงานการสื่อสาร และการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร

5.17 วัตถุประสงค์ที่ 17: การดำเนินธุรกิจอย่างต่อเนื่อง (business continuity)

เพื่อกำหนดแผนความต่อเนื่องทางธุรกิจสำหรับรองรับการหยุดชะงักของกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือภัยพิบัติที่เกิดขึ้นเพื่อให้การบริการดำเนินงานได้อย่างต่อเนื่อง

ข้อกำหนด	แนวทางปฏิบัติ
5.17.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องจัดทำแผนความต่อเนื่องทางธุรกิจสำหรับระบบสารสนเทศที่สำคัญ	1. ควรจัดทำแผนความต่อเนื่องทางธุรกิจสำหรับระบบสารสนเทศที่ให้บริการเพื่อรองรับภัยคุกคามต่าง ๆ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว การชุมนุมทางการเมือง การโจมตีทางไซเบอร์ เป็นต้น แผนความต่อเนื่องทางธุรกิจ ควรประกอบด้วยประเด็นสำคัญ ดังนี้ – บทบาทหน้าที่ความรับผิดชอบ – กระบวนการประกาศใช้แผน – รายละเอียดการจัดการจากเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น – ขั้นตอนการกู้คืนกิจกรรมที่มีการจัดลำดับความสำคัญตามระยะเวลาที่กำหนดไว้ – รายละเอียดเกี่ยวกับการตอบสนองต่อเหตุกรณ์ เช่น วิธีการสื่อสาร วิธีการแจ้งผู้ใช้บริการ ผู้แจ้ง เป็นต้น – กระบวนการกลับสู่ภาวะปกติหลังจากเหตุการณ์สิ้นสุด 2. แผนความต่อเนื่องทางธุรกิจควรได้รับการอนุมัติจากผู้บริหารหรือผู้มีอำนาจที่เกี่ยวข้อง 3. ผู้ให้บริการควรตรวจสอบว่า – มีการบริหารจัดการที่เพียงพอ เพื่อเตรียมพร้อมสำหรับการบรรเทาและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย โดยใช้บุคลากรที่มีประสบการณ์ และความสามารถที่เกี่ยวข้อง

ข้อกำหนด	แนวทางปฏิบัติ
	– มีบุคลากรตอบสนองต่อเหตุการณ์ที่มีหน้าที่รับผิดชอบและความสามารถในการจัดการเหตุการณ์ที่เกิดขึ้น
(ข) ผู้ให้บริการต้องทดสอบแผนความต่อเนื่องทางธุรกิจ และปรับปรุงอย่างสม่ำเสมอ	1. ควรตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องทางธุรกิจที่ได้เตรียมไว้ตามระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่าแผนนั้นยังถูกต้องและได้ผลเมื่อมีเหตุฉุกเฉินเกิดขึ้น 2. ควรจัดทำแผนการทดสอบเพื่อทดสอบหรือซักซ้อมความพร้อมในการกู้คืนกระบวนการทางธุรกิจที่สำคัญ แผนการทดสอบควรระบุถึงวัตถุประสงค์และเป้าหมายในการทดสอบ กำหนดการในการทดสอบ สถานการณ์ที่จะใช้ในการทดสอบ เป็นต้น 3. ควรพิจารณาเลือกรูปแบบในการทดสอบหรือซักซ้อมให้สอดคล้องกับสถานการณ์ รวมถึงพิจารณาความเพียงพอของทรัพยากรที่มีอยู่ เช่น การฝึกซ้อมแผนบนโต๊ะ (table top exercise) การทดสอบแบบจำลองสถานการณ์ หรือการทดสอบแบบเต็มรูปแบบซึ่งจะดำเนินการใกล้เคียงกับสถานการณ์จริงกับองค์ประกอบทั้งหมดของแผนความต่อเนื่องทางธุรกิจ เป็นต้น 4. ควรบันทึกผลการทดสอบ เพื่อใช้ในการประเมินและปรับปรุงแผนความต่อเนื่องทางธุรกิจให้ดียิ่งขึ้น
(ค) ผู้ให้บริการต้องติดตามผลเมื่อประกาศใช้แผนและดำเนินการตามแผนความต่อเนื่องทางธุรกิจ รวมถึงการบันทึกระยะเวลาการกู้คืนที่ดำเนินการสำเร็จและไม่สำเร็จ	1. ควรมีกระบวนการตัดสินใจสำหรับการประกาศใช้แผนความต่อเนื่องทางธุรกิจ 2. ควรบันทึกการประกาศใช้แผนและการดำเนินการตามแผนความต่อเนื่องทางธุรกิจ รวมทั้งการดำเนินการตามขั้นตอนการกู้คืนและเวลาสิ้นสุดของการกู้คืนการให้บริการ
5.17.2 ระดับสูง	
(ก) ผู้ให้บริการต้องทบทวนแผนความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ	ควรทบทวนแผนความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ โดยคำนึงถึงข้อคิดเห็น ผลการทดสอบและการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร
(ข) ผู้ให้บริการต้องสร้างความตระหนักให้แก่บุคลากรที่เกี่ยวข้องทราบถึงบทบาทหน้าที่และความรับผิดชอบเกี่ยวกับแผนความต่อเนื่องทางธุรกิจ	ควรสร้างความตระหนักหรือจัดฝึกอบรมเกี่ยวกับบทบาทหน้าที่และความรับผิดชอบตามแผนความต่อเนื่องทางธุรกิจให้กับบุคลากรที่เกี่ยวข้อง

5.18 วัตถุประสงค์ที่ 18: การกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery capabilities)

เพื่อกำหนดความสามารถในการกู้คืนระบบสารสนเทศเมื่อเกิดภัยพิบัติสำหรับการให้บริการ ในกรณีเกิดเหตุการณ์ความเสียหายขึ้น

ข้อกำหนด	แนวทางปฏิบัติ
5.18.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการกู้คืนระบบสารสนเทศเมื่อเกิดภัยพิบัติ	1. นโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการกู้คืนระบบสารสนเทศเมื่อเกิดภัยพิบัติ ควรประกอบด้วยรายละเอียดของภัยพิบัติที่สำคัญที่อาจส่งผลกระทบต่อการให้บริการ กระบวนการทางธุรกิจที่สำคัญ รายชื่อผู้ที่เกี่ยวข้องในการกู้คืน (ทั้งที่มีอยู่ภายในหรือใช้บริการจากผู้ให้บริการภายนอก) บทบาทหน้าที่ความรับผิดชอบ และระยะเวลาเป้าหมายในการกู้คืน 2. ควรมีกระบวนการในการจัดการกับภัยพิบัติ ตัวอย่างเช่น มีสถานที่ตั้งสำหรับระบบสารสนเทศสำรองซึ่งทำหน้าที่แทนในกรณีที่ระบบสารสนเทศหลักหยุดทำงาน มีการสำรองข้อมูลสำคัญไปยังสถานที่อื่นที่มีความมั่นคงปลอดภัย หรือมีศูนย์สำรองข้อมูลและกู้คืนสำหรับบริการระบบคลาวด์ เป็นต้น 3. ระบบสารสนเทศและโครงสร้างพื้นฐานของศูนย์ข้อมูลที่ให้บริการ ควรออกแบบมาเพื่อความพร้อมใช้งาน โดยสามารถทำงานทดแทนซึ่งกันและกันได้อย่างมีประสิทธิภาพ ตัวอย่างเช่น อุปกรณ์ใดอุปกรณ์หนึ่งไม่สามารถใช้งานได้ เป็นต้น โดยข้อมูลควรถูกถ่ายโอนไปจัดเก็บแบบทันที หรือระบบสารสนเทศสำรองอื่น ๆ ที่ดีกว่า
(ข) ผู้ให้บริการต้องจัดทำและทดสอบแผนการกู้คืนระบบสารสนเทศตามนโยบายหรือขั้นตอนการปฏิบัติงานอย่างสม่ำเสมอ	1. ควรจัดทำแผนการกู้คืนระบบสารสนเทศและกำหนดระยะเวลาการตรวจสอบ ทบทวน และประเมินแผนการกู้คืนระบบสารสนเทศที่ได้เตรียมไว้ เพื่อให้มั่นใจว่าแผนนั้นยังถูกต้องและได้ผลเมื่อมีเหตุฉุกเฉินเกิดขึ้น 2. ควรจัดทำแผนการทดสอบเพื่อทดสอบหรือซักซ้อมความพร้อมในการกู้คืนระบบสารสนเทศ แผนการทดสอบควรระบุถึงวัตถุประสงค์และเป้าหมายในการทดสอบ กำหนดการในการทดสอบ สถานการณ์ที่จะใช้ในการทดสอบ เป็นต้น 3. ควรพิจารณาเลือกรูปแบบในการทดสอบ ตามข้อ 5.17.1 (ข)

ข้อกำหนด	แนวทางปฏิบัติ
	4. ควรกำหนดให้มีการบันทึกผลการทดสอบ เพื่อเอาไว้ใช้ในการประเมินและปรับปรุงแผนให้ดียิ่งขึ้น
5.18.2 ระดับสูง	
(ก) ผู้ให้บริการต้องทบทวนแผนการกู้คืนระบบสารสนเทศอย่างสม่ำเสมอ	ควรทบทวนแผนการกู้คืนระบบสารสนเทศอย่างสม่ำเสมอ โดยคำนึงถึงข้อคิดเห็น ผลการทดสอบ และการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร
(ข) ผู้ให้บริการต้องสร้างความตระหนักให้แก่บุคลากรที่เกี่ยวข้องทราบถึงบทบาทหน้าที่และความรับผิดชอบเกี่ยวกับแผนการกู้คืนระบบสารสนเทศ	ควรสร้างความตระหนักหรือจัดฝึกอบรมเกี่ยวกับบทบาทหน้าที่และความรับผิดชอบตามแผนการกู้คืนระบบสารสนเทศให้กับบุคลากรที่เกี่ยวข้อง

5.19 วัตถุประสงค์ที่ 19: การเฝ้าติดตามและการบันทึกเหตุการณ์ (monitoring and logging)

เพื่อกำหนดขั้นตอนการเฝ้าติดตามและการบันทึกเหตุการณ์ของการให้บริการ สำหรับตรวจสอบปัญหาหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น

ข้อกำหนด	แนวทางปฏิบัติ
5.19.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องเฝ้าติดตามและบันทึกเหตุการณ์ของระบบเครือข่ายและระบบสารสนเทศที่สำคัญ	1. ควรบันทึกเหตุการณ์แสดงการเข้าถึงหรือที่เกี่ยวข้องกับระบบเครือข่ายและระบบสารสนเทศที่ให้บริการ ดังนี้ – ชื่อบัญชีผู้ใช้งาน – กิจกรรมการใช้งานระบบสารสนเทศ – วันที่และเวลาและรายละเอียดของเหตุการณ์ (เช่น การ log-on, log-off ผิดพลาด) – ข้อมูลประจำตัวของอุปกรณ์หรือตำแหน่ง – การเข้าถึงระบบสารสนเทศที่สำเร็จและไม่สำเร็จ – ข้อมูลความพยายามในการเข้าถึงทรัพยากรของระบบสารสนเทศทั้งที่สำเร็จและไม่สำเร็จ เช่น การเข้าถึงไฟล์ต่าง ๆ ในระบบ – การเปลี่ยนแปลงการกำหนดค่าของระบบสารสนเทศ – การใช้สิทธิพิเศษ – การเข้าถึงระบบสารสนเทศที่สำเร็จและไม่สำเร็จ – การเข้าถึงไฟล์และชนิดของการเข้าถึง – การแจ้งเตือนของระบบสารสนเทศ – ที่อยู่เครือข่ายและโพรโทคอล เป็นต้น

ข้อกำหนด	แนวทางปฏิบัติ
	2. ควรกำหนดให้ผู้ดูแลระบบไม่สามารถลบหรือยกเลิกข้อมูลบันทึกเหตุการณ์ที่แสดงถึงกิจกรรมที่เกี่ยวข้องกับตนเอง 3. ควรกำหนดให้มีการติดตามตรวจสอบการแจ้งเตือนหรือการล้มเหลวในการทำงานของระบบสารสนเทศ ซึ่งสามารถตรวจสอบได้จากข้อมูลบันทึกเหตุการณ์ เช่น – การแจ้งเตือนจากคอนโซล (console) ของผู้ดูแลระบบ – การแจ้งเตือนเมื่อระบบทำงานผิดปกติ เช่น ฮาร์ดดิสก์เต็ม เป็นต้น – การแจ้งเตือนจากโปรแกรมบริหารจัดการเครือข่าย – การแจ้งเตือนจากระบบควบคุมการเข้าถึง – การแจ้งเตือนจากระบบป้องกันการบุกรุก – การแจ้งเตือนการทำงานของระบบเกิดการล้มเหลวหรือหยุดชะงัก
(ข) ผู้ให้บริการต้องเฝ้าติดตามและบันทึกเหตุการณ์การใช้งานของผู้ใช้บริการอย่างสม่ำเสมอ	1. ควรบันทึกเหตุการณ์ที่เกี่ยวข้องกับข้อมูลผู้ใช้บริการ ตัวอย่างเช่น รหัสผู้ใช้งาน กิจกรรมของผู้ใช้ วันที่และเวลาของเหตุการณ์ การเข้าถึงระบบสารสนเทศที่สำเร็จและไม่สำเร็จ การเข้าถึงไฟล์และชนิดของการเข้าถึง การเปลี่ยนแปลงการกำหนดค่าของระบบสารสนเทศ การบุกรุก ที่อยู่เครือข่ายและโพรโทคอล เป็นต้น 2. ควรรายงานการบันทึกเหตุการณ์และรายงานการเฝ้าติดตามข้อมูลที่เกี่ยวข้องให้กับผู้ใช้บริการเมื่อมีเหตุจำเป็นหรือเหตุสงสัย 3. ควรป้องกันการเปลี่ยนแปลงข้อมูลบันทึกเหตุการณ์ทั้งหมดและบันทึกการดำเนินงานที่ไม่ได้รับอนุญาต ตัวอย่างเช่น การปรับเปลี่ยนประเภทของข้อความที่บันทึกไว้ ข้อมูลการบันทึกเหตุการณ์ถูกแก้ไข หรือลบ เป็นต้น
(ค) ผู้ให้บริการต้องตั้งค่าเวลาให้ตรงและถูกต้องเทียบกับแหล่งอ้างอิงที่น่าเชื่อถือ	ระบบเวลาของระบบสารสนเทศต่างๆ ที่เกี่ยวข้องกับอุปกรณ์ประมวลผลข้อมูลภายในองค์กร ควรได้รับการตั้งค่าเวลาจากแหล่งเวลาที่น่าเชื่อถือ
5.19.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานเกี่ยวกับ	1. นโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการเฝ้าติดตามและการบันทึกเหตุการณ์ควรรวมถึงความต้องการ

ข้อกำหนด	แนวทางปฏิบัติ
การเฝ้าติดตาม และการบันทึกเหตุการณ์ของระบบเครือข่ายและระบบสารสนเทศที่สำคัญ	ขั้นต่ำในการเฝ้าติดตามและการบันทึกเหตุการณ์ ระยะเวลาเก็บรักษา และวัตถุประสงค์โดยรวมของการจัดเก็บข้อมูลการเฝ้าติดตามและการบันทึก 2. ควรบันทึกเหตุการณ์ที่เกิดขึ้นเพื่อรองรับการตรวจสอบที่ประกอบด้วยประเด็นสำคัญ ดังนี้ – วันที่และเวลาของเหตุการณ์ – ระบบสารสนเทศที่เกิดเหตุการณ์ขึ้น – ประเภทของเหตุการณ์ – ข้อมูลผู้ใช้งาน – ผลลัพธ์ของเหตุการณ์ 3. ควรทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานเกี่ยวกับการเฝ้าติดตามและการบันทึกเหตุการณ์อย่างสม่ำเสมอ โดยคำนึงถึงข้อคิดเห็น การเปลี่ยนแปลง และสถานการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น
(ข) ผู้ให้บริการต้องนำเครื่องมือสำหรับใช้ในการเฝ้าติดตาม (monitoring systems) และรวบรวมข้อมูลการบันทึกเหตุการณ์ (collecting logs) ของระบบสารสนเทศและข้อมูลผู้ใช้บริการที่ให้บริการ	1. ควรนำเครื่องมือสำหรับระบบการเฝ้าติดตามและรวบรวมข้อมูลการบันทึกเหตุการณ์มาช่วยสนับสนุนการปฏิบัติงานขององค์กร 2. ควรแสดงรายการข้อมูลการเฝ้าติดตาม และข้อมูลการบันทึกเหตุการณ์ได้ตามนโยบายที่กำหนดไว้ 3. ควรทบทวนข้อมูลบันทึกเหตุการณ์ประเภทต่าง ๆ ที่กล่าวถึงในหัวข้อนี้ โดยกำหนดระยะเวลาการทบทวนตามระดับความเสี่ยงหรือระดับความสำคัญของระบบสารสนเทศที่มีต่อองค์กร

5.20 วัตถุประสงค์ที่ 20: การทดสอบระบบ (system test)

เพื่อกำหนดขั้นตอนการทดสอบระบบเครือข่ายและระบบสารสนเทศที่สนับสนุนการให้บริการอย่างเหมาะสม

ข้อกำหนด	แนวทางปฏิบัติ
5.20.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องทดสอบระบบเครือข่ายและระบบสารสนเทศก่อนนำไปใช้งานหรือเชื่อมต่อกับระบบสารสนเทศที่มีการใช้งานอยู่	1. ควรทดสอบระบบเครือข่ายและระบบสารสนเทศ เมื่อมีการเปลี่ยนแปลงที่สำคัญหรือมีระบบสารสนเทศใหม่ 2. ควรจัดทำรายงานผลการทดสอบของระบบเครือข่ายและระบบสารสนเทศ เพื่อเป็นหลักฐานในการตรวจสอบและความถูกต้องของระบบสารสนเทศ

ข้อกำหนด	แนวทางปฏิบัติ
	3. ระบบสารสนเทศใหม่และระบบสารสนเทศที่มีการปรับปรุงใหม่ควรได้รับการทดสอบและการตรวจสอบอย่างละเอียดในระหว่างกระบวนการพัฒนา
(ข) ผู้ให้บริการต้องมีกระบวนการ ติดตั้งหรือการถอนการติดตั้งโปรแกรมสำหรับแก้ไขข้อบกพร่อง (patch)	1. ควรตรวจสอบและปรับปรุง patch ให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ 2. ควรได้รับการทดสอบและประเมิน patch ก่อนติดตั้งเพื่อให้มั่นใจว่ามีประสิทธิภาพและยอมรับได้ 3. ควรได้รับความเห็นชอบหรือการอนุมัติจากผู้มีอำนาจก่อนดำเนินการติดตั้งหรือถอนการติดตั้ง patch ทุกครั้ง
5.20.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการทดสอบระบบเครือข่ายและระบบสารสนเทศ	1. ควรจัดทำนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการทดสอบระบบเครือข่ายและระบบสารสนเทศ และเมื่อมีการทดสอบควรจัดทำแผนการทดสอบ กรณีทดสอบ (test cases) และรายงานผลการทดสอบ 2. เอกสารกิจกรรมการทดสอบ ควรประกอบด้วยหัวข้ออย่างน้อย ดังนี้ – วัตถุประสงค์ บทบาทและความรับผิดชอบ – ขอบข่ายของแผนการทดสอบ – รายละเอียดของผลการทดสอบที่เป็นไปตามแผน – ความถี่ในการทดสอบ 3. ควรทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานเกี่ยวกับการทดสอบระบบเครือข่ายและระบบสารสนเทศอย่างสม่ำเสมอ โดยคำนึงถึงสถานการณ์ด้านความมั่นคงปลอดภัย และการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร 4. อาจนำเครื่องมือในการทดสอบอัตโนมัติมาใช้ในการทดสอบเพื่อช่วยลดความผิดพลาด ตัวอย่างเช่น เครื่องมือทดสอบฟังก์ชันการทำงานของระบบและทดสอบสมรรถนะการทำงานของระบบ เป็นต้น

5.21 วัตถุประสงค์ที่ 21: การประเมินการรักษาความมั่นคงปลอดภัย (security assessments)

เพื่อกำหนดให้มีการประเมินด้านความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศที่สำคัญอย่างเหมาะสม

ข้อกำหนด	แนวทางปฏิบัติ
5.21.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องได้รับการตรวจสอบความมั่นคงปลอดภัย (security scan) และทดสอบความมั่นคงปลอดภัย (security testing) ระบบสารสนเทศที่มีความสำคัญอย่างสม่ำเสมอ โดยเฉพาะอย่างยิ่งเมื่อมีระบบสารสนเทศใหม่ หรือมีการเปลี่ยนแปลงเกิดขึ้น	1. ควรกำหนดกระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศขององค์กร รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบในการดำเนินการ 2. ควรรายงานผลการตรวจสอบความมั่นคงปลอดภัยและทดสอบความมั่นคงปลอดภัยรวมถึงผลลัพธ์การแก้ไขเพื่อปิดช่องโหว่ที่พบ 3. ควรจัดทำรายงานการตรวจสอบความมั่นคงปลอดภัย
(ข) ผู้ให้บริการต้องมีการติดตาม ตรวจสอบและประเมินผลช่องโหว่ที่ตรวจพบ	1. ควรระบุระยะเวลาที่จะดำเนินการแก้ไขช่องโหว่เมื่อได้รับแจ้งหรือทราบช่องโหว่นั้น 2. ข้อมูลเกี่ยวกับช่องโหว่ของระบบสารสนเทศ ควรได้รับการติดตาม การตรวจสอบ การประเมินผลและระบุวิธีการควบคุมเพื่อจัดการความเสี่ยงที่เกี่ยวข้อง 3. ควรมีวิธีการแก้ไขโดยเร็วสำหรับช่องโหว่ที่มีระดับความสำคัญสูงหรือหาแนวทางที่เหมาะสมเพื่อลดความเสี่ยงที่พบนั้น สำหรับกรณีที่ยังไม่มีโปรแกรมแก้ไขช่องโหว่ ควรมีการควบคุมอื่น ๆ เช่น – ทำการปิดบริการหรือปิดฟังก์ชันที่มีช่องโหว่นั้นไว้ชั่วคราว – ดำเนินการปรับหรือเพิ่มการควบคุมการเข้าถึงระบบสารสนเทศที่มีช่องโหว่นั้น – เพิ่มการตรวจสอบเพื่อตรวจหาการโจมตีที่เกิดขึ้น – เพิ่มความตระหนักถึงภัยคุกคามจากช่องโหว่นั้น 4. ควรเฝ้าติดตามและประเมินระบบสารสนเทศหลังจากที่ได้ดำเนินการแก้ไขช่องโหว่ เพื่อดูว่าระบบทำงานสมบูรณ์ตามปกติหรือไม่
5.21.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการประเมินและการทดสอบด้านความมั่นคงปลอดภัย	1. นโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการประเมินและการทดสอบด้านความมั่นคงปลอดภัย ควรมีรายละเอียดของทรัพย์สินสารสนเทศที่สำคัญ ประเภทของการประเมินและทดสอบด้านความมั่นคงปลอดภัย บทบาทหน้าที่และความรับผิดชอบที่เกี่ยวกับการจัดการช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ ความถี่ในการประเมินและทดสอบ หน่วยงานในการอนุมัติ (ภายในหรือภายนอก) ระดับการรักษาความลับสำหรับ

ข้อกำหนด	แนวทางปฏิบัติ
	การประเมินและผลการทดสอบ และวัตถุประสงค์การประเมินและการทดสอบด้านความมั่นคงปลอดภัย 2. ควรทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการประเมินและการทดสอบด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยคำนึงถึงการข้อคิดเห็นและการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร
(ข) ผู้ให้บริการต้องกำหนดผู้ประสานงานและช่องทางการติดต่อสื่อสารสำหรับปัญหาด้านความมั่นคงปลอดภัยของผู้ที่เกี่ยวข้อง	ควรจัดทำบัญชีรายชื่อและช่องทางในการติดต่อบุคคลที่สามหรือผู้เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร เช่น ผู้ผลิต (manufacturers) หรือผู้จำหน่าย (vendors) เป็นต้น

5.22 วัตถุประสงค์ที่ 22: การปฏิบัติตามข้อกำหนด (compliance)

เพื่อกำหนดให้มีการติดตามและตรวจสอบการปฏิบัติงานที่สอดคล้องกับนโยบายหรือแนวปฏิบัติภายในรวมถึงข้อกำหนดทางกฎหมายและมาตรฐานสากล เพื่อเป็นการหลีกเลี่ยงการละเมิดกฎหมาย ระเบียบข้อบังคับ หรือข้อผูกพันตามสัญญาที่เกี่ยวกับความมั่นคงปลอดภัย

ข้อกำหนด	แนวทางปฏิบัติ
5.22.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องปฏิบัติตามมาตรฐาน ระเบียบข้อบังคับ ข้อกำหนดทางกฎหมายที่เกี่ยวข้อง	1. ควรระบุกฎหมาย ระเบียบ ข้อบังคับ ข้อกำหนดตามข้อตกลง และข้อกำหนดอื่น ๆ ที่ต้องปฏิบัติตาม 2. ควรติดตามและทบทวนข้อมูลที่เกี่ยวข้องกับกฎหมาย ระเบียบ ข้อบังคับ ข้อกำหนดตามข้อตกลง และข้อกำหนดอื่น ๆ ที่ควรปฏิบัติตามอย่างสม่ำเสมอ 3. ควรจัดทำรายงานที่อธิบายถึงผลการตรวจติดตามการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง 4. ควรมีกระบวนการที่สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามข้อตกลงที่เกี่ยวกับสิทธิในทรัพย์สินทางปัญญาและการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ 5. การคุ้มครองข้อมูลส่วนบุคคลควรสอดคล้องกับกฎหมายและข้อกำหนดตามข้อตกลงต่าง ๆ ของหน่วยงาน
5.22.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการติดตามและตรวจสอบการปฏิบัติตามข้อกำหนด	1. ควรจัดทำนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการติดตามและตรวจสอบการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับการดำเนินงานด้านทรัพย์สินสารสนเทศ กระบวนการและโครงสร้างพื้นฐาน ซึ่งประกอบด้วยการกำหนดระยะเวลาในการตรวจสอบ แนวทางการตรวจสอบ

ข้อกำหนด	แนวทางปฏิบัติ
	(ภายในหรือภายนอก) นโยบายความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ภายใต้การตรวจสอบตามวัตถุประสงค์ วิธีการตรวจสอบตามข้อกำหนด และรูปแบบรายงานการตรวจสอบ เป็นต้น 2. ควรจัดทำแผนการตรวจสอบอย่างละเอียด รวมถึงวัตถุประสงค์และการวางแผนในระยะยาว
(ข) ผู้ให้บริการต้องทำการตรวจสอบการปฏิบัติตามข้อกำหนดให้เป็นไปตามนโยบายหรือขั้นตอนการปฏิบัติงานและแผนการตรวจสอบที่กำหนดไว้	1. ควรเลือกผู้ตรวจสอบและดำเนินการตรวจสอบซึ่งเป็นไปตามข้อเท็จจริง และมีความเป็นกลางของกระบวนการตรวจสอบ 2. ควรวิเคราะห์สาเหตุเมื่อมีความไม่สอดคล้องเกิดขึ้น และวางแผนการดำเนินการแก้ไข รวมถึงทบทวนประสิทธิผลของการดำเนินการแก้ไขให้เป็นไปตามนโยบายหรือขั้นตอนการปฏิบัติงาน และข้อกำหนดที่เกี่ยวข้อง 3. ควรจัดทำรายงานและนำเสนอผลการตรวจสอบให้กับผู้บริหารหรือผู้ที่เกี่ยวข้องรับทราบ

5.23 วัตถุประสงค์ที่ 23: การรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บ (security of data at rest)

เพื่อกำหนดวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลที่ถูกจัดเก็บอย่างมีประสิทธิผลและเหมาะสม เพื่อป้องกันความลับ การพิสูจน์ตัวตนและความถูกต้องครบถ้วนของข้อมูล เช่น ข้อมูลองค์กร ฐานข้อมูล และข้อมูลที่จัดเก็บอยู่ในสื่อบันทึกข้อมูลประเภทต่าง ๆ เป็นต้น

ข้อกำหนด	แนวทางปฏิบัติ
5.23.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องระบุข้อมูลที่สำคัญที่อยู่ในความรับผิดชอบขององค์กร โดยต้องคำนึงถึงความต้องการทางธุรกิจที่เกี่ยวข้องและภาระผูกพันทางกฎหมาย	ควรมีวิธีการควบคุมการเข้าถึงข้อมูล การใช้งานร่วมกัน การคัดลอก การส่งและการแจกจ่าย สำหรับข้อมูลที่สำคัญและข้อมูลลับ
(ข) ผู้ให้บริการต้องเก็บรักษาข้อมูลที่สำคัญไว้ตามระยะเวลาที่กำหนด โดยขึ้นอยู่กับชนิดของข้อมูลและความสำคัญของข้อมูล	1. ควรเก็บรักษาข้อมูลที่สำคัญไว้ช่วงระยะเวลาหนึ่งให้สอดคล้องกับกฎหมายหรือข้อตกลงที่กำหนด เพื่อเป็นหลักฐานทางกฎหมายและการดำเนินการให้บริการ 2. ควรมีวิธีการเก็บรักษาข้อมูลที่มีความมั่นคงปลอดภัย เพื่อให้มั่นใจว่าสามารถเข้าถึงข้อมูลได้ตลอดระยะเวลาเก็บรักษา
(ค) ผู้ให้บริการต้องมีกลไกการเข้ารหัสลับ (cryptographic) เพื่อปกป้องข้อมูลลับ	1. ควรบันทึกเหตุการณ์และตรวจสอบกิจกรรมที่เกี่ยวกับการรับหรือส่งข้อมูลทั้งภายในและภายนอกองค์กร

ข้อกำหนด	แนวทางปฏิบัติ
และความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บอยู่ในสื่อบันทึกข้อมูลระหว่างการส่งออกนอกพื้นที่ที่มีการควบคุม และในการรับหรือส่งข้อมูลภายในและระหว่างองค์กร	2. ควรกำหนดให้มีการใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามข้อตกลงต่าง ๆ ขององค์กร เพื่อป้องกันข้อมูลที่สำคัญและข้อมูลลับ 3. ควรมีแนวทางการบริหารจัดการกุญแจเข้ารหัสลับ (cryptographic key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับขององค์กร ตัวอย่างเช่น กำหนดบทบาทและหน้าที่ การจัดเก็บ การเปลี่ยนเปลง การยกเลิกการใช้งาน การบันทึกและตรวจสอบกิจกรรมการจัดการที่สำคัญ เป็นต้น
(ง) ผู้ให้บริการต้องมีกลไกการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่ถูกจัดเก็บ โดยไม่ได้รับอนุญาต	ควรป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่จัดเก็บ ตัวอย่างเช่น การลงลายมือชื่ออิเล็กทรอนิกส์ และการใช้ฟังก์ชันแฮช (hash function) เป็นต้น เพื่อใช้ตรวจสอบความถูกต้องครบถ้วนของข้อมูล
(จ) ผู้ให้บริการต้องมีกลไกการทำลายข้อมูลด้วยวิธีการที่มีความมั่นคงปลอดภัยไปปฏิบัติหลังจากใช้ข้อมูลถูกต้องตามกฎหมาย	1. ควรมีหลักฐานการตรวจสอบอุปกรณ์หรือสื่อบันทึกข้อมูลเพื่อตรวจสอบว่าข้อมูลถูกนำออกหรือถูกแทนที่อย่างปลอดภัยก่อนทำลายข้อมูล 2. ควรมีวิธีการทำลายข้อมูลที่ไม่ได้ใช้งานด้วยวิธีการที่มีความมั่นคงปลอดภัย เช่น การลบด้วยโปรแกรมประยุกต์ และมีผู้รับผิดชอบในการทำหน้าที่ควบคุมการทำลายสื่อบันทึกข้อมูล เป็นต้น
5.23.2 ระดับสูง	
(ก) ผู้ให้บริการต้องจำแนกประเภทข้อมูลสารสนเทศให้สอดคล้องกับหลักเกณฑ์การจำแนกประเภทที่คำนึงถึงมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับ และความสำคัญต่อองค์กร	ควรมีกระบวนการสำหรับการจำแนกประเภทข้อมูลสารสนเทศ เพื่อใช้จัดการกับข้อมูลสารสนเทศขององค์กรให้มีการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน (ตัวอย่างการจำแนกประเภทข้อมูลสารสนเทศตามระดับชั้นความลับ ได้แก่ ข้อมูลเผยแพร่ ข้อมูลใช้ภายใน ข้อมูลลับ ข้อมูลลับมาก)
(ข) ผู้ให้บริการต้องไม่ใช้สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (removable media) ยกเว้นกรณีที่จำเป็น ต้องได้รับอนุญาตจากผู้บริหารก่อนใช้งาน	1. ควรกำหนดขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ที่ควรประกอบด้วยรายละเอียดของการลบหรือทำลายข้อมูล การจัดเก็บ การนำสื่อบันทึกข้อมูลสำคัญออกนอกองค์กร การส่งสื่อบันทึกข้อมูลไปยังอีกสถานที่หนึ่ง การป้องกันการเสื่อมอายุ การขออนุญาตใช้งาน เป็นต้น 2. ควรมีหลักฐานในการอนุญาตให้ใช้สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้จากผู้มีอำนาจ หรืออาจกำหนดแบบฟอร์มในการขอใช้สื่อบันทึกข้อมูล

ข้อกำหนด	แนวทางปฏิบัติ
(ค) ผู้ให้บริการต้องรักษาความลับและความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บ และให้เป็นไปตามการจำแนกประเภทข้อมูลสารสนเทศที่กำหนดไว้	1. ควรกำหนดมาตรฐานการเข้ารหัสลับที่ใช้งาน เพื่อควบคุมและป้องกันการรับส่งข้อมูลทางอิเล็กทรอนิกส์ ซึ่งการเข้ารหัสลับจะถูกบังคับใช้กับสื่ออิเล็กทรอนิกส์ที่มีข้อมูลลับ 2. ควรมีกลไกที่สนับสนุนการรักษาความลับและความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บ ตัวอย่างเช่น กลไกการเข้ารหัสลับ การจัดเก็บข้อมูลแบบออฟไลน์ที่ปลอดภัย และการลบข้อมูลสำคัญจากสื่อบันทึกข้อมูลและอื่น ๆ ที่เป็นไปตามหลักเกณฑ์การจำแนกข้อมูลสารสนเทศ 3. ควรมีกลไกการสร้างและการบริหารจัดการกุญแจเข้ารหัสลับ (เฉพาะกรณีที่ใช้งานการเข้ารหัสลับ)
(ง) ผู้ให้บริการต้องกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานที่ครอบคลุมถึงการรักษาความลับและความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บ การเข้ารหัสลับข้อมูลที่จัดเก็บ และการเก็บรักษาข้อมูลที่จัดเก็บ รวมถึงให้บุคลากรที่เกี่ยวข้องมีความตระหนักถึงนโยบายหรือขั้นตอนการปฏิบัติงานดังกล่าว	1. นโยบายการรักษาความลับและความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บ ควรครอบคลุมถึงการป้องกันข้อมูลสำคัญหรือข้อมูลลับ โดยจัดทำข้อตกลงการรักษาความลับระหว่างผู้ให้บริการกับผู้ใช้บริการหรือบุคคลที่สามที่จำเป็นต้องเข้าถึงข้อมูลของผู้ใช้บริการ ซึ่งควรประกอบด้วยประเด็นสำคัญ ดังนี้ – ช่วงระยะเวลาของข้อตกลงการรักษาความลับ (เช่น ช่วงระยะเวลาที่ข้อตกลงนี้เป็นผล) – สิ่งที่ต้องปฏิบัติเมื่อข้อตกลงสิ้นสุดหรือจบลง – หน้าที่ความรับผิดชอบที่ต้องปฏิบัติกับข้อมูลสำคัญหรือข้อมูลลับ – ผู้เป็นเจ้าของข้อมูลสำคัญหรือข้อมูลลับ – เงื่อนไขการใช้ข้อมูลสำคัญหรือข้อมูลลับ – การสงวนสิทธิในการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับข้อมูลสำคัญหรือข้อมูลลับ – การดำเนินการทางกฎหมายหากมีการละเมิดข้อตกลง 2. นโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการเข้ารหัสลับข้อมูลที่จัดเก็บ ควรประกอบด้วยประเด็นสำคัญ ดังนี้ – หลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสลับ – มาตรฐานการเข้ารหัสลับที่ใช้ในองค์กร – การเข้ารหัสลับข้อมูลที่ส่งผ่านสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้หรือผ่านสายสื่อสาร – วิธีการบริหารจัดการกุญแจเข้ารหัสลับ

ข้อกำหนด	แนวทางปฏิบัติ
	– บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสลับ – การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการเข้ารหัสลับที่องค์กรต้องปฏิบัติตาม 3. ควรกำหนดระยะเวลาการเก็บรักษาข้อมูลแต่ละประเภทตามระยะเวลาที่กฎหมายหรือระเบียบข้อบังคับที่กำหนดไว้ 4. ควรสร้างความตระหนักเกี่ยวกับนโยบายหรือขั้นตอนเกี่ยวกับการรักษาความลับและความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บให้บุคลากรที่เกี่ยวข้องเพื่อให้เข้าใจถึงหน้าที่ของตนเอง
(จ) ผู้ให้บริการต้องกำหนดขั้นตอนในการปฏิบัติงานสำหรับการทำลายสินทรัพย์ทางกายภาพ (physical asset) ที่มีความมั่นคงปลอดภัย	1. ควรมีวิธีการทำลายสื่อบันทึกข้อมูลที่มีข้อมูลความลับและไม่ได้ใช้งานได้รับการทำลายด้วยวิธีการที่มีความมั่นคงปลอดภัย 2. ควรมีหลักฐานในการอนุญาตให้มีการทำลายสินทรัพย์จากผู้มีอำนาจ หรืออาจกำหนดแบบฟอร์มในการทำลายสินทรัพย์
(ฉ) ผู้ให้บริการต้องกำหนดขั้นตอนการปฏิบัติงานสำหรับการทำป้ายบ่งชี้สารสนเทศให้สอดคล้องกับหลักเกณฑ์การจำแนกข้อมูลสารสนเทศ	ควรมีขั้นตอนการปฏิบัติงานสำหรับการทำป้ายบ่งชี้ที่ครอบคลุมถึงทรัพย์สินสารสนเทศที่เกี่ยวข้องทั้งแบบกายภาพและอิเล็กทรอนิกส์ให้สอดคล้องกับหลักเกณฑ์การจำแนกประเภทข้อมูลสารสนเทศ

5.24 วัตถุประสงค์ที่ 24: การรักษาความมั่นคงปลอดภัยของส่วนเชื่อมต่อบริการ (interface security)

เพื่อกำหนดนโยบายการความมั่นคงปลอดภัยด้านสารสนเทศสำหรับส่วนเชื่อมต่อบริการระหว่างองค์กรที่ใช้ข้อมูลอิเล็กทรอนิกส์

ข้อกำหนด	แนวทางปฏิบัติ
5.24.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศที่ครอบคลุมถึงส่วนเชื่อมต่อบริการระหว่างองค์กร	นโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับส่วนเชื่อมต่อบริการระหว่างองค์กร ควรประกอบด้วย ขอบข่ายของบริการ วัตถุประสงค์ด้านความมั่นคงปลอดภัย ทรัพย์สินสารสนเทศสำคัญที่สนับสนุนการบริการ และการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ เพื่อควบคุมการใช้ข้อมูลร่วมกัน และการรักษาความมั่นคงปลอดภัยในส่วนเชื่อมต่อระบบสารสนเทศหรือระบบเครือข่ายของผู้ใช้บริการ

ข้อกำหนด	แนวทางปฏิบัติ
(ข) ผู้ให้บริการต้องมีกระบวนการรับและส่งข้อมูลที่มีความมั่นคงปลอดภัย	1. ควรมีวิธีการปกป้องข้อมูลด้วยการส่งข้อมูลผ่านช่องทางที่เข้ารหัสลับ เช่น การใช้ TLS 1.2 หรือเวอร์ชันที่สูงกว่า 2. ควรมีวิธีการควบคุมทางเครือข่ายเพื่อรักษาความลับและความถูกต้องครบถ้วนของข้อมูลสำคัญที่มีการรับส่งผ่านทางเครือข่ายสาธารณะหรือผ่านเครือข่ายไร้สายหรือระบบสารสนเทศที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ
(ค) ผู้ให้บริการต้องระบุข้อมูลที่แตกต่างกัน (unique identifier) สำหรับผู้ใช้บริการแต่ละราย เพื่อใช้ในการระบุตัวตนผู้ใช้งาน	ควรระบุตัวตนสำหรับผู้ใช้บริการ ตัวอย่างเช่น กำหนดเลขที่หรือรหัสประจำตัวหรือชื่อผู้ใช้บริการ (ภาษาอังกฤษ) หรือชื่ออื่น ๆ ที่ระบบรองรับได้ และสามารถสื่อความหมายถึงข้อมูลผู้ใช้บริการได้อย่างชัดเจน
5.24.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับข้อมูล (data security) รวมถึงวิธีการป้องกันข้อมูลผู้ใช้บริการที่มีการเชื่อมต่อไปยังระบบสารสนเทศหรือระบบเครือข่าย	1. นโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับข้อมูลควรประกอบด้วยเงื่อนไขการใช้ทรัพย์สินสารสนเทศที่เกี่ยวข้อง ตัวอย่างเช่น การจัดการรหัสผ่าน การใช้งานอินเทอร์เน็ต การใช้งานอีเมล การจัดการอุปกรณ์พกพาขององค์กรและของพนักงาน การใช้งานซอฟต์แวร์ลิขสิทธิ์ รวมถึงการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น 2. ควรกำหนดวิธีการป้องกันข้อมูลผู้ใช้บริการที่เชื่อมต่อระหว่างองค์กรหรือบริการ ตัวอย่างเช่น วิธีการเข้ารหัสลับ หรือ วิธีการยืนยันตัวตนแบบหลายปัจจัย เป็นต้น 3. ควรสร้างความตระหนักเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับข้อมูล และวิธีการป้องกันข้อมูลผู้ใช้บริการ ให้กับบุคลากรที่เกี่ยวข้องเพื่อเข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตนเองที่เกี่ยวกับการบริการและการใช้ข้อมูลของผู้ใช้บริการ
(ข) ผู้ให้บริการต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับข้อมูลและการเชื่อมต่อบริการ รวมถึงวิธีการป้องกันข้อมูลผู้ใช้บริการที่มีการเชื่อมต่อไปยังระบบสารสนเทศหรือระบบเครือข่าย	ควรทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับข้อมูลและการเชื่อมต่อบริการ รวมถึงวิธีการป้องกันข้อมูลผู้ใช้บริการอย่างสม่ำเสมอ โดยคำนึงถึงข้อคิดเห็นการเปลี่ยนแปลงที่เกิดขึ้น สถานการณ์ด้านความมั่นคงปลอดภัย ข้อยกเว้น ผลการทดสอบ และเหตุการณ์ด้านความมั่นคงปลอดภัยที่ส่งผลต่อองค์กรหรือผู้ใช้บริการ

5.25 วัตถุประสงค์ที่ 25: การรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ (software security)

เพื่อกำหนดแนวทางที่ทำให้มั่นใจว่าซอฟต์แวร์ที่ให้บริการมีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

ข้อกำหนด	แนวทางปฏิบัติ
5.25.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดแนวทางสำหรับการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์	1. แนวทางการรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์ที่จัดหาหรือพัฒนาขึ้นมาใช้งาน ควรพิจารณาประเด็นต่อไปนี้ – การรักษาความมั่นคงปลอดภัยของสภาพแวดล้อมการพัฒนา – คำแนะนำเกี่ยวกับความมั่นคงปลอดภัยในวงจรการพัฒนาซอฟต์แวร์ เช่น การรักษาความมั่นคงปลอดภัยในวิธีการพัฒนาซอฟต์แวร์ และแนวทางการเขียนโปรแกรมอย่างปลอดภัย – ข้อกำหนดด้านความมั่นคงปลอดภัยในขั้นตอนการออกแบบ – การเก็บรักษาที่มีความมั่นคงปลอดภัย – การควบคุมเวอร์ชัน – ความมั่นคงปลอดภัยของซอฟต์แวร์ที่ต้องการ – ความสามารถของบุคลากรในการตรวจพบและแก้ปัญหาช่องโหว่ด้านความมั่นคงปลอดภัย 2. ควรสร้างความตระหนักเกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ให้กับบุคลากรหลัก
5.25.2 ระดับสูง	
(ก) ผู้ให้บริการต้องมีกระบวนการรักษาความมั่นคงปลอดภัยเกี่ยวกับสภาพแวดล้อมสำหรับการพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย (secure development environment) และการป้องกันชุดข้อมูลสำหรับใช้ในการทดสอบ (test data) รวมถึงวิธีหรือเทคนิคการทดสอบซอฟต์แวร์	1. ควรจัดทำขั้นตอนการปฏิบัติงานหรือแนวทางรักษาความมั่นคงปลอดภัยเกี่ยวกับสภาพแวดล้อมสำหรับการพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย และการป้องกันชุดข้อมูลสำหรับใช้ในการทดสอบ 2. ควรมีผลการทดสอบการใช้งานซอฟต์แวร์บนสภาพแวดล้อมสำหรับการพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัยและมาตรการควบคุมสำหรับการป้องกันชุดข้อมูลทดสอบ 3. ควรแสดงถึงวิธีการทดสอบซอฟต์แวร์ที่เลือกไว้สำหรับสถานการณ์การทดสอบ และคำอธิบายเกี่ยวกับสถานการณ์นั้น เช่น white box testing เป็นต้น 4. ข้อมูลที่นำมาใช้ในการทดสอบ ตัวอย่างเช่น ข้อมูลลับ ข้อมูลส่วนบุคคล ควรเลือกขึ้นมาใช้งานอย่างระมัดระวัง และได้รับการป้องกันและควบคุมอย่างเหมาะสม เพื่อป้องกันข้อมูลสำคัญรั่วไหลหรือเข้าถึงโดยไม่ได้รับอนุญาต เช่น ไม่อนุญาตให้ใช้ข้อมูลสำคัญใช้ในการ

ข้อกำหนด	แนวทางปฏิบัติ
	ทดสอบกับระบบสารสนเทศ กำหนดให้มีการอนุมัติก่อนทุกครั้งก่อนที่จะนำข้อมูลไปใช้ในการทดสอบ 5. ควรจำกัดการเข้าถึง source code ของระบบสารสนเทศและข้อมูลอื่น ๆ ที่เกี่ยวข้อง
(ข) ผู้ให้บริการต้องแบ่งแยกสภาพแวดล้อมของระบบสารสนเทศสำหรับการพัฒนา (development) การทดสอบ (testing) และการให้บริการ (production) ออกจากกัน	1. ควรแยกสภาพแวดล้อมของระบบสารสนเทศสำคัญสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน เพื่อป้องกันผลกระทบจากการทำงานของระบบสารสนเทศหนึ่งที่มีต่ออีกระบบสารสนเทศหนึ่ง และป้องกันการเข้าถึงข้อมูลบนสภาพแวดล้อมของระบบสารสนเทศสำคัญให้บริการโดยไม่ได้รับอนุญาต 2. ควรควบคุมการถ่ายโอนระบบสารสนเทศจากสภาพแวดล้อมที่ใช้สำหรับการพัฒนาไปสู่เครื่องที่ใช้สำหรับการให้บริการ 3. ควรมีสภาพแวดล้อมสำหรับการทดสอบเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ 4. ควรแยกบัญชีผู้ใช้งานออกจากกันสำหรบระบบสารสนเทศที่ใช้ในการพัฒนา การทดสอบ และการให้บริการ เช่น บัญชีผู้ใช้งานของผู้พัฒนาระบบ ผู้ดูแลระบบ เป็นต้น เพื่อลดความเสี่ยงในการเกิดข้อผิดพลาด

5.26 วัตถุประสงค์ที่ 26: การทำงานร่วมกันและการโอนย้ายบริการ (interoperability and portability)

เพื่อกำหนดกระบวนการหรือขั้นตอนการทำงานร่วมกันระหว่างผู้ให้บริการกับผู้ใช้บริการและมั่นใจได้ว่าผู้ให้บริการได้ออกแบบระบบที่สามารถทำงานร่วมกันกับผู้ใช้บริการได้ และ รองรับการย้ายไปยังผู้ให้บริการรายอื่น ๆ ที่มีการบริการที่คล้ายกันได้

ข้อกำหนด	แนวทางปฏิบัติ
5.26.1 ระดับพื้นฐาน	
(ก) ผู้ให้บริการต้องกำหนดกระบวนการและขั้นตอนการปฏิบัติงานสำหรับการทำงานร่วมกันและการโอนย้ายบริการไปยังผู้ให้บริการรายอื่นที่มีบริการในลักษณะที่คล้ายกัน	ควรจัดทำกระบวนการและขั้นตอนการปฏิบัติงานสำหรับการทำงานร่วมกันและการย้ายการใช้บริการ เพื่อให้ผู้ใช้บริการสามารถย้ายการใช้บริการไปยังผู้ให้บริการรายอื่น ๆ ได้
(ข) ผู้ให้บริการต้องนำมาตรฐานอุตสาหกรรมหรือมาตรฐานที่เป็นที่ยอมรับมาช่วยส่งเสริมการทำงานร่วมกันและการโอนย้ายบริการ	ควรนำมาตรฐานอุตสาหกรรมมาใช้ในการทำงานร่วมกัน ตัวอย่างเช่น – ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ข้อกำหนด	แนวทางปฏิบัติ
	ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน ที่เป็นแนวทางการจัดทำเอกสารและข้อความให้อยู่ในรูปของ XML File การสร้างและการตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ และใช้เป็นแนวทางการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ – ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์ สำหรับการซื้อขายสินค้าและบริการ เป็นมาตรฐานที่กำหนดรูปแบบโครงสร้างข้อมูล XML สำหรับการซื้อขายสินค้าและบริการ เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ – การใช้งาน openID ที่เป็นโพรโทคอลที่ใช้ยืนยันตัวตนและการตรวจสอบผู้ใช้งานระหว่างผู้ใช้งานและผู้ให้บริการ เป็นต้น
(ค) ผู้ให้บริการต้องกำหนดข้อตกลงร่วมกันกับผู้ใช้บริการสำหรับการทำงานร่วมกันและการโอนย้ายบริการ	1. ควรจัดทำข้อตกลงร่วมกันระหว่างผู้ให้บริการกับผู้ใช้บริการสำหรับการทำงานร่วมกันและการโอนย้ายบริการให้ชัดเจน เช่น การพัฒนาระบบ การแลกเปลี่ยนข้อมูล การใช้งานระบบสารสนเทศ ความถูกต้องครบถ้วนของข้อมูล การโอนย้ายการใช้บริการไปยังผู้ให้บริการรายอื่น และสิทธิในทรัพย์สินทางปัญญาหรือสิทธิอื่นใดที่ได้สร้างสรรค์ขึ้นมาจากการให้บริการภายใต้ข้อตกลง เป็นต้น 2. ควรรองรับการจัดทำข้อมูลทั้งหมดในรูปแบบที่มีโครงสร้างและไม่มีโครงสร้างให้แก่ผู้ใช้บริการหากมีการโอนย้ายบริการหรือมีการร้องขอ เช่น ไฟล์ชนิด .doc, .xls, .pdf, log และ flat file เป็นต้น
5.26.2 ระดับสูง	
(ก) ผู้ให้บริการต้องกำหนดขั้นตอนการปฏิบัติงานสำหรับการถอยกลับสู่สภาพเดิม (fallback procedure) สำหรับการทำงานร่วมกันและการโอนย้ายบริการ	ควรมีขั้นตอนการปฏิบัติงานสำหรับการถอยกลับสู่สภาพเดิมที่อธิบายไว้อย่างชัดเจนในกรณีย้ายบริการไปยังผู้ให้บริการรายอื่นไม่สำเร็จ หรือทำการเปลี่ยนแปลงไม่สำเร็จ

6. ภาคผนวก

ตารางที่ 4 เปรียบเทียบวัตถุประสงค์ด้านความมั่นคงปลอดภัยกับมาตรฐานสากล

วัตถุประสงค์ด้านความมั่นคงปลอดภัย	ENISA	ISO27001
1. การกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (information security policy)	●	●
2. การบริหารจัดการความเสี่ยง (risk management)	●	●
3. การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (security roles)	●	●
4. การบริหารจัดการบุคคลที่สาม (third party management)	●	●
5. การตรวจสอบประวัติบุคลากร (background checks)	●	●
6. การสร้างความตระหนักด้านความมั่นคงปลอดภัย (security awareness)	●	●
7. การเปลี่ยนแปลงบุคลากร (personnel changes)	●	●
8. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)	●	●
9. การรักษาความมั่นคงปลอดภัยของระบบสนับสนุนการดำเนินงาน (security of supporting utilities)	●	●
10. การควบคุมการเข้าถึงระบบเครือข่าย และระบบสารสนเทศ (access control to network and information system)	●	●
11. การควบคุมความถูกต้องขององค์ประกอบระบบเครือข่าย และระบบสารสนเทศ (integrity of network components and information system)	●	●
12. การกำหนดขั้นตอนการปฏิบัติงาน (operating procedures)	●	●
13. การบริหารจัดการการเปลี่ยนแปลง (change management)	●	●
14. การบริหารจัดการสินทรัพย์ (asset management)	●	●
15. การตรวจพบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย (security incident detection and response)	●	●
16. การรายงานสถานการณ์ด้านความมั่นคงปลอดภัย (security incident reporting)	●	●
17. การดำเนินธุรกิจอย่างต่อเนื่อง (business continuity)	●	●
18. การกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery capabilities)	●	●
19. การเฝ้าติดตามและการบันทึกเหตุการณ์ (monitoring and logging)	●	●
20. การทดสอบระบบ (system test)	●	●
21. การประเมินการรักษาความมั่นคงปลอดภัย (security assessments)	●	●
22. การปฏิบัติตามข้อกำหนด (compliance)	●	●
23. การรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บ (security of data at rest)	●	●
24. การรักษาความมั่นคงปลอดภัยของส่วนเชื่อมต่อบริการ (interface security)	●	-
25. การรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ (software security)	●	-
26. การทำงานร่วมกันและการโอนย้ายบริการ (interoperability and portability)	●	-