มาตรฐาน ISO/IEC 27001:2022

ดร. บรรจง หะรังษี ผู้แปลและเรียบเรียง

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

ข้อ 4 บริบทขององค์กร (Context of the organization)

4.1 การทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context)

องค์กรต้องกำหนดประเด็นที่เป็นปัจจัยภายในและภายนอกที่เกี่ยวข้องกับจุดประสงค์ขององค์กรและที่จะส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อสังเกต การกำหนดประเด็นดังกล่าวหมายถึงการกำหนดบริบทภายในและภายนอกองค์กร ที่มีการพิจารณาในข้อ 5.4.1 ของมาตรฐาน ISO 31000:2018

4.2 การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties)

องค์กรต้องกำหนด:

a) ผู้ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ
b) ความต้องการของผู้ที่เกี่ยวข้องเหล่านั้น
c) ข้อใดของความต้องการเหล่านี้ที่จะมีการดำเนินการผ่านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อสังเกต ความต้องการของผู้ที่เกี่ยวข้องสามารถรวมถึงความต้องการด้านกฎหมายและระเบียบข้อบังคับ และสิ่งที่เป็นข้อผูกพันที่ต้องปฏิบัติตามสัญญาจ้าง

4.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system)

องค์กรต้องกำหนดขอบเขตและการประยุกต์ใช้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อระบุขอบเขตของการดำเนินงาน

ในการระบุขอบเขต องค์กรต้องพิจารณา:

a) ประเด็นที่เป็นปัจจัยภายในและภายนอกขององค์กร โดยอ้างอิงจากข้อ 4.1

b) ความต้องการ โดยอ้างอิงจากข้อ 4.2 และ

c) ความเชื่อมโยงและความสัมพันธ์กันของกิจกรรมในลักษณะที่กิจกรรมหนึ่งขึ้นอยู่กับอีกกิจกรรมหนึ่ง โดยที่กิจกรรมเหล่านั้นอาจดำเนินการโดยองค์กรเอง หรือโดยองค์กรอื่นๆ

ขอบเขตต้องมีพร้อมไว้เป็นลายลักษณ์อักษรให้สามารถใช้งานได้

4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system)

องค์กรต้องกำหนด นำสู่การปฏิบัติ บำรุงรักษา และปรับปรุงอย่างต่อเนื่องสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงกระบวนการที่จำเป็นและความเชื่อมโยงของกระบวนการเหล่านั้น โดยต้องมีความสอดคล้องกับข้อกำหนดในเอกสารมาตรฐานฉบับนี้

ข้อ 5 ภาวะผู้นำ (Leadership)

5.1 ภาวะผู้นำและการให้ความสำคัญ (Leadership and commitment)

ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงภาวะผู้นำและการให้ความสำคัญต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดย

a) ต้องทำให้เกิดความมั่นใจว่ามีการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศขึ้นมา และมีความสอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กรที่กำหนดไว้

b) ต้องทำให้เกิดความมั่นใจว่ามีการบูรณาการความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการขององค์กร

c) ต้องทำให้เกิดความมั่นใจว่าองค์กรมีทรัพยากรที่จำเป็นที่จะนำมาใช้กับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

d) ต้องสื่อสารถึงความสำคัญของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สัมฤทธิ์ผลและการดำเนินการตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

e) ต้องทำให้เกิดความมั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจะบรรลุผลลัพธ์ตามที่ต้องการ

f) ต้องสั่งการและสนับสนุนบุคลากรเพื่อนำสู่ความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

g) ต้องส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง และ

h) ต้องสนับสนุนบทบาทการบริหารที่เกี่ยวข้องอื่นๆ ที่อยู่ภายใต้ความรับผิดชอบของผู้บริหารเหล่านั้น เพื่อแสดงถึงภาวะผู้นำของตนเอง

ข้อสังเกต เมื่อมีการอ้างอิงถึงคำว่า "ธุรกิจ" ในเอกสารฉบับนี้สามารถตีความแบบกว้างๆ ว่าหมายถึงกิจกรรมที่เป็นแกนกลางต่อจุดประสงค์ของการธำรงอยู่ซึ่งกิจการขององค์กรนั้น

5.2 นโยบาย (Policy)

ผู้บริหารระดับสูงต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศซึ่ง:

a) เหมาะสมต่อจุดประสงค์ขององค์กร

b) รวมวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศเข้าไว้ด้วย (ดูข้อ 6.2) หรือกำหนดกรอบการกำหนดวัตถุประสงค์ดังกล่าว

c) รวมการให้ความสำคัญของผู้บริหารเพื่อให้สอดคล้องกับความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และ

d) รวมการให้ความสำคัญของผู้บริหารเพื่อการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

นโยบายความมั่นคงปลอดภัยสารสนเทศ:

e) ต้องมีพร้อมไว้เป็นลายลักษณ์อักษรให้สามารถใช้งานได้

f) ต้องมีการสื่อสารให้เป็นที่ทราบกันภายในองค์กร และ

g) ต้องสามารถเข้าถึงได้โดยผู้ที่เกี่ยวข้องตามความเหมาะสม

5.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ขององค์กร (Organizational roles, responsibilities and authorities)

ผู้บริหารระดับสูงต้องทำให้เกิดความมั่นใจว่าหน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศมีการมอบหมายและสื่อสารให้เป็นที่ทราบกันภายในองค์กร

ผู้บริหารระดับสูงต้องมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่เพื่อ:

a) ทำให้เกิดความมั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีความสอดคล้องกับข้อกำหนดของเอกสารมาตรฐานฉบับนี้ และ

b) ให้มีการรายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

ข้อสังเกต ผู้บริหารระดับสูงสามารถมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่ในการรายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในองค์กรได้

ข้อ 6 การวางแผน (Planning)

6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to address risks and opportunities)

6.1.1 ภาพรวม (General)

เมื่อมีการวางแผนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องพิจารณาประเด็นที่เป็นปัจจัยภายในและภายนอกที่อ้างถึงในข้อ 4.1 และความต้องการที่อ้างถึงในข้อ 4.2 และ

ต้องกำหนดความเสี่ยงและโอกาส (ที่เกี่ยวข้องกับปัจจัยและความต้องการเหล่านั้น) ที่จำเป็นต้องดำเนินการเพื่อ:

a) ทำให้เกิดความมั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจะสามารถบรรลุผลลัพธ์ได้ตามที่ต้องการ

b) ป้องกันหรือลดผลที่ไม่พึงปรารถนาที่อาจจะเกิดขึ้น และ ข้อ ง ล-ง

c) ทำให้มีการปรับปรุงอย่างต่อเนื่อง

องค์กรต้องวางแผน:

d) การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาสเหล่านั้น และ

e) วิธีการที่จะ

1) บูรณาการการดำเนินการดังกล่าวเข้ากับกระบวนการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และนำสู่การปฏิบัติ และ

2) ประเมินความสัมฤทธิ์ผลของการดำเนินการเหล่านั้น

6.1.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

องค์กรต้องกำหนดและประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งต้อง:

a) กำหนดและปรับปรุงเกณฑ์ความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศ ซึ่งต้องรวมถึง

1) เกณฑ์การยอมรับความเสี่ยง และ

2) เกณฑ์สำหรับการประเมินความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศ

b) ทำให้เกิดความมั่นใจว่าการประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศที่ได้ดำเนินการซ้ำได้ผลการประเมินที่สอดคล้องกัน ถูกต้อง และสามารถเปรียบเทียบกันได้

c) ระบุความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ:

1) ประยุกต์กระบวนการประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศเพื่อ

ระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้อง และความพร้อมใช้ของสารสนเทศภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ

2) ระบุผู้เป็นเจ้าของความเสี่ยง

d) วิเคราะห์ความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ:

1) ประเมินผลที่เป็นไปได้ที่จะเกิดขึ้น ถ้าความเสี่ยงที่ระบุไว้ในข้อ 6.1.2 c) 1) เกิดขึ้นจริง

2) ประเมินโอกาสการเกิดขึ้นที่สมจริงของความเสี่ยงที่ระบุไว้ในข้อ 6.1.2 c) 1) และ

3) กำหนดระดับของความเสี่ยง

e) ประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ:

1) เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดไว้ในข้อ 6.1.2 a) และ

2) จัดลำดับความเสี่ยงที่วิเคราะห์นั้นเพื่อการจัดการที่เหมาะสม

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับกระบวนการประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ ไว้อย่างเป็นลายลักษณ์อักษร

6.1.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

องค์กรต้องกำหนดและประยุกต์กระบวนการจัดการความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศซึ่งต้อง:

a) กำหนดทางเลือกที่เหมาะสมในการจัดการกับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ โดยต้องนำผลการประเมินความเสี่ยงมาประกอบการพิจารณาด้วย

b) กำหนดมาตรการทั้งหมดที่จำเป็นเพื่อดำเนินการตามทางเลือกที่กำหนดไว้นั้น

ข้อสังเกต 1 องค์กรสามารถออกแบบมาตรการได้เองตามที่ต้องการ หรือระบุมาตรการโดยอ้างอิงจากแหล่งใดก็ตามที่ต้องการ

c) เปรียบเทียบมาตรการที่กำหนดไว้ในข้อ 6.1.3 b) กับมาตรการใน Annex A และ

ตรวจสอบว่าไม่มีมาตรการข้อใดที่จำเป็นถูกละเลยไป

ข้อสังเกต 2 Annex A ประกอบด้วยรายการของมาตรการความมั่นคงปลอดภัยสารสนเทศที่เป็นไปได้ ให้ผู้ใช้งานมาตรฐานฉบับนี้อ้างอิงไปที่ Annex A เพื่อให้มั่นใจว่าไม่มีมาตรการข้อใดที่จำเป็นแต่ถูกมองข้ามไป

ข้อสังเกต 3 มาตรการความมั่นคงปลอดภัยสารสนเทศที่แสดงไว้ใน Annex A ไม่ได้เป็นมาตรการทั้งหมด มาตรการเพิ่มเติมสามารถเพิ่มเข้ามาได้ตามความจำเป็น

d) จัดทำเอกสารแสดงการใช้มาตรการ SoA (Statement of Applicability) ซึ่งประกอบด้วย

--มาตรการที่จำเป็น (ดูข้อ 6.1.3 b) และ c))

--คำอธิบายเหตุผลของการใช้มาตรการเหล่านั้น

--ไม่ว่ามาตรการเหล่านั้นจะได้รับการดำเนินการไปแล้วหรือไม่ก็ตาม และ

--คำอธิบายเหตุผลของการไม่ใช้มาตรการจาก Annex A

e) จัดทำแผนการจัดการความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ และ

f) ขอการรับรองจากผู้เป็นเจ้าของความเสี่ยงสำหรับแผนการจัดการความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ และการยอมรับสำหรับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศที่ยังหลงเหลืออยู่

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับกระบวนการจัดการกับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ ไว้อย่างเป็นลายลักษณ์อักษร

ข้อสังเกต 4 กระบวนการประเมินและจัดการกับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศในมาตรฐานฉบับนี้สอดคล้องกับหลักการและแนวทางทั่วไปที่เสนอไว้ในมาตรฐาน ISO 31000

6.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information security objectives and plans to achieve them)

องค์กรต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในฟังก์ชันและระดับงานที่เกี่ยวข้อง

วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศต้อง:

a) สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ

b) สามารถวัดผลได้ (ถ้าสามารถทำได้)

c) นำความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ผลการประเมินและการจัดการความเสี่ยงมาพิจารณาประกอบด้วย

d) มีการเฝ้าระวังและติดตาม

e) มีการสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ และ

f) มีการปรับปรุงตามความเหมาะสม

g) มีการจัดทำไว้เป็นลายลักษณ์อักษร

องค์กรต้องจัดเก็บสารสนเทศสำหรับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ไว้อย่างเป็นลายลักษณ์อักษร

เมื่อวางแผนวิธีการที่จะบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องกำหนด:

h) สิ่งที่ต้องดำเนินการ

i) ทรัพยากรที่ต้องใช้

j) ผู้รับผิดชอบในการดำเนินการ

k) ระยะเวลาที่จะดำเนินการให้เสร็จสิ้น และ

l) วิธีประเมินผลการปฏิบัติการ

6.3 การวางแผนการเปลี่ยนแปลง (Planning of changes)

เมื่อองค์กรได้มีการกำหนดความจำเป็นสำหรับการเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศแล้ว การเปลี่ยนแปลงนั้นต้องได้รับการดำเนินการในลักษณะที่เป็นแผนการดำเนินการ

ข้อ 7 การสนับสนุน (Support)

7.1 ทรัพยากร (Resources)

องค์กรต้องกำหนดและให้ทรัพยากรที่จำเป็นสำหรับการกำหนด การนำสู่การปฏิบัติ การบำรุงรักษา และการปรับปรุงอย่างต่อเนื่องสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

7.2 สมรรถนะ (Competence)

องค์กรต้อง:

a) กำหนดสมรรถนะของบุคลากรที่ปฏิบัติงานภายใต้การควบคุมดูแลขององค์กร ซึ่งส่งผลต่อประสิทธิภาพในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรนั้น

b) ทำให้เกิดความมั่นใจว่าบุคลากรเหล่านี้มีความสามารถโดยการให้ความรู้ การฝึกอบรม หรือการฝึกประสบการณ์จากการทำงานที่ได้รับตามความเหมาะสม

c) ดำเนินการตามความเหมาะสมเพื่อให้ได้มาซึ่งสมรรถนะที่จำเป็นเหล่านั้น และประเมินความสัมฤทธิ์ผลของการดำเนินการนั้น และ

d) จัดเก็บสารสนเทศอย่างเป็นลายลักษณ์อักษรตามความเหมาะสมเพื่อใช้เป็นหลักฐานแสดงสมรรถนะ

ข้อสังเกต การดำเนินการตามความเหมาะสมเพื่อให้ได้มาซึ่งสมรรถนะสามารถรวมถึงการฝึกอบรม การเป็นพี่เลี้ยง การมอบหมายหมายงาน หรือการจ้างหรือการทำสัญญากับบุคลากรที่มีความสามารถ เป็นต้น

7.3 การสร้างความตระหนัก (Awareness)

บุคลากรที่ปฏิบัติงานภายใต้การควบคุมดูแลขององค์กรต้องตระหนักถึง:

a) นโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

b) การที่ตนเองมีส่วนในความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย

สารสนเทศ ซึ่งรวมถึงประโยชน์ของการปรับปรุงประสิทธิภาพด้านความมั่นคงปลอดภัยสารสนเทศ และ

c) ผลที่จะเกิดขึ้นของการไม่ปฏิบัติตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

7.4 การสื่อสารให้ทราบ (Communication)

องค์กรต้องกำหนดความจำเป็นสำหรับการสื่อสารให้ทราบทั้งภายในและภายนอกองค์กรที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึง:

a) อะไรบ้างที่ต้องสื่อสารให้ทราบ

b) เมื่อไรที่ต้องสื่อสารให้ทราบ

c) ใครบ้างที่ต้องสื่อสารให้ทราบ

d) วิธีการใดที่ใช้ในการสื่อสาร

7.5 สารสนเทศที่เป็นลายลักษณ์อักษร (Documented information)

7.5.1 ภาพรวม (General)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรต้องรวม:

a) สารสนเทศที่เป็นลายลักษณ์อักษรซึ่งกำหนดโดยมาตรฐานฉบับนี้ และ

b) สารสนเทศที่เป็นลายลักษณ์อักษรซึ่งกำหนดโดยองค์กรเองและจำเป็นสำหรับความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อสังเกต ปริมาณของสารสนเทศที่เป็นลายลักษณ์อักษรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสามารถแตกต่างกันได้ในแต่ละองค์กร เนื่องจาก:

a) ขนาดขององค์กรและประเภทของกิจกรรม กระบวนการ ผลิตภัณฑ์ และบริการขององค์กร

b) ความซับซ้อนของกระบวนการและความเชื่อมโยงระหว่างกระบวนการ และ

c) สมรรถนะของของบุคลากร

7.5.2 การสร้างและปรับปรุงสารสนเทศ (Creating and updating)

เมื่อมีการสร้างและปรับปรุงสารสนเทศที่เป็นลายลักษณ์อักษร องค์กรต้องกำหนดประเด็นเหล่านี้ให้มีความเหมาะสม:

a) ชื่อและรายละเอียด (เช่น ชื่อเอกสาร วันที่ ผู้จัดทำ หรือเลขที่อ้างอิงของเอกสาร)

b) รูปแบบ (เช่น ภาษา เวอร์ชั่น กราฟิก) และสื่อบันทึก (เช่น กระดาษ อิเล็กทรอนิกส์) และ

c) การทบทวนและการอนุมัติเพื่อความเหมาะสมและเพียงพอ

7.5.3 การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร (Control of documented information)

สารสนเทศที่เป็นลายลักษณ์อักษรที่จำเป็นต้องมีสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและตามมาตรฐานฉบับนี้ต้องมีการควบคุมเพื่อให้เกิดความมั่นใจว่า:

a) สารสนเทศสามารถเข้าถึงได้และเหมาะสมสำหรับการใช้งาน สถานที่และวันเวลาในการใช้งาน และ

b) สารสนเทศได้รับการป้องกันอย่างเพียงพอ (เช่น จากการสูญเสียความลับ การใช้งานที่ไม่เหมาะสม หรือการสูญเสียความถูกต้อง)

สำหรับการควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร องค์กรต้องระบุกิจกรรมดังต่อไปนี้ตามความเหมาะสม:

c) การแจกจ่าย การเข้าถึง การนำขึ้นมาใช้ และการใช้งาน

d) การจัดเก็บและการรักษาไว้ ซึ่งรวมถึงการรักษาไว้ให้สามารถอ่านใช้งานได้

e) การควบคุมการเปลี่ยนแปลง (เช่น การควบคุมเวอร์ชั่น) และ

f) การจัดเก็บ ระยะเวลาการจัดเก็บ และการทำลาย

สารสนเทศที่มาจากแหล่งภายนอกที่องค์กรกำหนดว่าจำเป็นสำหรับการวางแผนและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องมีการระบุตามความจำเป็น และต้องมีการควบคุม

ข้อสังเกต การเข้าถึงสารสนเทศหมายรวมถึงการตัดสินใจเกี่ยวกับการอนุญาตให้ดูสารสนเทศได้เพียงเท่านั้น หรือการอนุญาตและการให้อำนาจในการดูและเปลี่ยนแปลงสารสนเทศได้ด้วย หรืออื่นๆ

ข้อ 8 การดำเนินการ (Operation)

8.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational planning and control)

องค์กรต้องวางแผน นำสู่การปฏิบัติ และควบคุมกระบวนการที่จำเป็นเพื่อให้สอดคล้องกับความต้องการที่กำหนดไว้ และดำเนินการตามที่ได้กำหนดไว้ในข้อ 6 (ซึ่งได้มีการวางแผนต่างๆ ไว้) โดย

----กำหนดเกณฑ์สำหรับกระบวนการเหล่านั้น

----ดำเนินการควบคุมกระบวนการเหล่านั้นให้เป็นไปตามเกณฑ์ที่กำหนด

สารสนเทศที่เป็นลายลักษณ์อักษรต้องมีจัดเตรียมไว้ในปริมาณที่จำเป็นเพื่อให้เกิดความมั่นใจว่ากระบวนการเหล่านั้นมีการดำเนินการตามแผน

องค์กรต้องควบคุมการเปลี่ยนแปลงที่ได้มีการวางแผนล่วงหน้า และทบทวนผลของการเปลี่ยนแปลงที่เกิดขึ้นอย่างไม่ได้ตั้งใจ (เช่น การเปลี่ยนแปลงที่ไม่ได้วางแผนไว้และเกิดขึ้นแบบฉุกเฉิน) โดยดำเนินการเพื่อลดผลกระทบในทางลบตามความจำเป็น

องค์กรต้องทำให้มั่นใจว่ากระบวนการ ผลิตภัณฑ์ หรือบริการ ที่มีการให้บริการโดยผู้ให้บริการภายนอกและเกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีการควบคุมการดำเนินการ

8.2 การประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

องค์กรต้องดำเนินการประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น หรือเสนอขอดำเนินการ โดยนำเกณฑ์ความเสี่ยงที่กำหนดไว้ในข้อ 6.1.2 a) มาประกอบการพิจารณาด้วย

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรไว้ ซึ่งเป็นผลของการประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ

8.3 การจัดการกับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

องค์กรต้องนำสู่การปฏิบัติตามแผนการจัดการความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรไว้ ซึ่งเป็นผลของการจัดการกับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ

ข้อ 9 การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

9.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมินผล (Monitoring, measurement, analysis and evaluation)

องค์กรต้องกำหนด:

a) สิ่งที่จำเป็นต้องเฝ้าระวังและวัดผล ซึ่งรวมถึงกระบวนการและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ
b) วิธีการในการเฝ้าระวัง วัดผล วิเคราะห์ และประเมินผลตามความเหมาะสม เพื่อให้ได้ผลการประเมินที่ถูกต้อง วิธีการที่กำหนดนั้นควรจะสามารถสร้างผลการประเมินที่เปรียบเทียบกันได้และสามารถทำซ้ำได้เพื่อให้ได้ผลลัพธ์ที่ถูกต้อง
c) เมื่อไรที่การเฝ้าระวังและวัดผลต้องดำเนินการ
d) ใครเป็นผู้เฝ้าระวังและวัดผล
e) เมื่อไรที่ผลจากการเฝ้าระวังและวัดผลต้องได้รับการวิเคราะห์และประเมินผล และ
f) ใครเป็นผู้วิเคราะห์และประเมินผล

สารสนเทศที่เป็นลายลักษณ์อักษรต้องจัดเตรียมให้พร้อมไว้เพื่อใช้เป็นหลักฐานแสดงผลการประเมิน

องค์กรต้องประเมินประสิทธิภาพและประสิทธิผลด้านความมั่นคงปลอดภัยสารสนเทศ และความได้ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

9.2 การตรวจประเมินภายใน (Internal audit)

9.2.1 ทั่วไป (General)

องค์กรต้องดำเนินการตรวจประเมินภายในตามรอบระยะเวลาที่กำหนดไว้เพื่อให้มีสารสนเทศสำหรับการระบุว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ:

a) สอดคล้องกับ

1) ความต้องการขององค์กรเองสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ

2) ข้อกำหนดของมาตรฐานฉบับนี้

b) มีการปฏิบัติและบำรุงรักษาไว้อย่างสัมฤทธิ์ผล

9.2.2 โปรแกรมการตรวจประเมิน (Internal audit programme)

องค์กรต้องวางแผน กำหนด นำสู่การปฏิบัติ และบำรุงรักษาโปรแกรมการตรวจประเมิน ซึ่งรวมถึงความถี่ วิธีการที่ใช้ หน้าที่ความรับผิดชอบ ความต้องการในการตรวจประเมินที่วางแผนไว้ และการรายงานผล

เมื่อกำหนดโปรแกรมการตรวจประเมิน องค์กรต้องพิจารณาความสำคัญของกระบวนการที่เกี่ยวข้องและนำผลของการตรวจประเมินครั้งก่อนมาพิจารณาประกอบด้วย

องค์กรต้อง:

a) กำหนดเกณฑ์การตรวจประเมินและขอบเขตของการตรวจประเมิน (ในแต่ละครั้ง)

b) เลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินให้เป็นไปตามข้อเท็จจริงและหลักฐาน และมีความเป็นกลางของกระบวนการตรวจประเมิน

c) ทำให้เกิดความมั่นใจว่าผลของการตรวจประเมินมีการรายงานไปยังผู้บริหารที่เกี่ยวข้อง

สารสนเทศที่เป็นลายลักษณ์อักษรต้องจัดเตรียมให้พร้อมไว้เพื่อใช้เป็นหลักฐานแสดงโปรแกรมการตรวจประเมินและผลการตรวจประเมิน

9.3 การทบทวนของผู้บริหาร (Management review)

9.3.1 ทั่วไป (General)

ผู้บริหารระดับสูงต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามรอบระยะเวลาที่กำหนดไว้เพื่อทำให้เกิดความมั่นใจในความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผล

9.3.2 ข้อมูลนำเข้าสำหรับการทบทวนของผู้บริหาร (Management review inputs)

การทบทวนของผู้บริหารต้องรวมการพิจารณาในเรื่อง:

a) สถานะของการดำเนินการจากผลการทบทวนครั้งก่อน

b) การเปลี่ยนแปลงในประเด็นที่เป็นปัจจัยภายในและภายนอกขององค์กรที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

c) การเปลี่ยนแปลงความต้องการและความคาดหวังของผู้ที่เกี่ยวข้องในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

d) ผลตอบกลับของประสิทธิภาพและประสิทธิผลด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงแนวโน้มในเรื่อง

1) ความไม่สอดคล้องและการดำเนินการแก้ไข

2) ผลการเฝ้าระวังและวัดผล

3) ผลการตรวจประเมิน และ

4) ความสำเร็จตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

e) ผลตอบกลับจากผู้ที่เกี่ยวข้อง

f) ผลการประเมินความเสี่ยงและสถานะของแผนการจัดการความเสี่ยง และ

g) โอกาสสำหรับการปรับปรุงอย่างต่อเนื่อง

9.3.3 ผลการทบทวนของผู้บริหาร (Management review results)

ผลการทบทวนของผู้บริหารต้องรวมการตัดสินใจเกี่ยวกับโอกาสในการปรับปรุงอย่างต่อเนื่อง (เช่น การปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ) และความจำเป็นสำหรับการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

สารสนเทศที่เป็นลายลักษณ์อักษรต้องจัดเตรียมให้พร้อมไว้เพื่อใช้เป็นหลักฐานแสดงผลการทบทวนของผู้บริหาร

ข้อ 10 การปรับปรุง (Improvement)

10.1 การปรับปรุงอย่างต่อเนื่อง (Continual improvement)

องค์กรต้องปรับปรุงความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

10.2 ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and corrective action)

เมื่อมีความไม่สอดคล้องหนึ่งเกิดขึ้น องค์กรต้อง:

a) ตอบกลับต่อความไม่สอดคล้องนั้นตามความเหมาะสม และ:

1) ดำเนินการเพื่อควบคุมและแก้ไขความไม่สอดคล้อง และ

2) จัดการกับผลที่เกิดขึ้น

b) ประเมินความจำเป็นสำหรับการดำเนินการเพื่อขจัดสาเหตุของความไม่สอดคล้องเพื่อให้ไม่เกิดขึ้นซ้ำอีกหรือไม่เกิดขึ้นในที่อื่นอีกโดย:

1) ทบทวนความไม่สอดคล้องนั้น

2) ระบุสาเหตุของความไม่สอดคล้อง และ

3) ระบุว่าความไม่สอดคล้องที่คล้ายกันมีหรือไม่ หรืออาจเป็นไปได้ที่จะเกิดขึ้นอีกหรือไม่

c) ดำเนินการแก้ไขที่จำเป็น

d) ทบทวนความสัมฤทธิ์ผลของการดำเนินการแก้ไขที่ได้ดำเนินการไป และ

e) ทำการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ถ้าจำเป็น

การดำเนินการแก้ไขต้องมีความเหมาะสมต่อผลของความไม่สอดคล้องที่พบ

สารสนเทศที่เป็นลายลักษณ์อักษรต้องจัดเตรียมให้พร้อมไว้เพื่อใช้เป็นหลักฐานแสดง:

f) สภาพของความไม่สอดคล้องและการดำเนินการแก้ไขใดๆ ที่ได้ดำเนินการไป และ

g) ผลของการดำเนินการแก้ไข

Annex A อ้างอิงมาตรการความมั่นคงปลอดภัยสารสนเทศของมาตรฐาน ISO/IEC 27001:2022

5 มาตรการขององค์กร (Organizational controls)

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตาการควบคุม (Control)
5.1	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)	นโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายเฉพาะแยกตามเรื่องต้องมีการกำหนด อนุมัติโดยผู้บริหาร จัดพิมพ์ สื่อสาร และสร้างการรับรู้ให้แก่บุคลากรและหน่วยงานภายนอกที่เกี่ยวข้อง ตลอดจนทบทวนตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อองค์กร
5.2	บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)	บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและแบ่งความรับผิดชอบตามที่องค์กรต้องการ
5.3	การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)	หน้าที่และส่วนของการปฏิบัติหน้าที่ดังกล่าวที่จะก่อให้เกิดการขัดต่อผลประโยชน์ขององค์กรต้องมีการแยกส่วนของการปฏิบัติหน้าที่ดังกล่าวออกจากกัน
5.4	หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)	ผู้บริหารต้องกำหนดให้บุคลากรทั้งหมดยึดมั่นและรักษาความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้ปฏิบัติตามตามนโยบายความมั่นคงปลอดภัยสารสนเทศ นโยบายเฉพาะแยกตามเรื่อง และขั้นตอนปฏิบัติที่กำหนดไว้
5.5	การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)	องค์กรต้องกำหนดและปรับปรุงข้อมูลสำหรับการติดต่อกับหน่วยงานผู้มีอำนาจ (เพื่อใช้ในการติดต่อประสานงานในเรื่องต่างๆ ที่สำคัญและจำเป็น)
5.6	การติดต่อกับกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน (Contact with special interest groups)	องค์กรต้องกำหนดและปรับปรุงข้อมูลสำหรับการติดต่อกับกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมที่มีความเป็นมืออาชีพ
5.7	ข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย (Threat intelligence)	ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการเก็บรวบรวมและวิเคราะห์ เพื่อจัดทำหรือผลิตข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย
5.8	ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ	ความมั่นคงปลอดภัยสารสนเทศต้องมีการบูรณาการเข้าไปกับการบริหารจัดการโครงการ

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตาการควบคุม (Control)
	(Information security in project management)	
5.9	บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ (Inventory of information and other associated assets)	บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ รวมถึงเจ้าของทรัพย์สินต้องมีการจัดทำและปรับปรุง (เพื่อให้ข้อมูลมีความเป็นปัจจุบันและถูกต้อง)
5.10	การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)	กฎเกณฑ์การใช้อย่างเหมาะสมและขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ ต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร และนำไปปฏิบัติ
5.11	การคืนทรัพย์สิน (Return of assets)	บุคลากรและผู้ที่เกี่ยวข้องจากหน่วยงานภายนอกต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดหรือเปลี่ยนการจ้างงาน สัญญาจ้าง หรือข้อตกลงการจ้าง
5.12	ชั้นความลับของข้อมูล (Classification of information)	ข้อมูลต้องมีการแยกหมวดหมู่ให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยพิจารณาจากความลับ ความถูกต้อง ความพร้อมใช้ และความต้องการจากหน่วยงานต่างๆ ที่เกี่ยวข้อง
5.13	การบ่งชี้ข้อมูล (Labeling of information)	ชุดขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลตามความเหมาะสม ต้องมีการกำหนดขึ้นมาและมีการนำไปปฏิบัติให้มีความสอดคล้องกับวิธีการจัดชั้นความลับของข้อมูลที่องค์กรได้กำหนดไว้
5.14	การถ่ายโอนข้อมูล (Information transfer)	กฎเกณฑ์ ขั้นตอนปฏิบัติ หรือข้อตกลงสำหรับการถ่ายโอนข้อมูล ต้องมีการกำหนดขึ้นมาสำหรับเครื่องมือหรืออุปกรณ์ในการถ่ายโอนข้อมูลทุกประเภท ทั้งการถ่ายโอนภายในองค์กร ระหว่างองค์กร ตลอดจนหน่วยงานภายนอกอื่นๆ
5.15	การควบคุมการเข้าถึง (Access control)	กฎเกณฑ์สำหรับการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ ทั้งทางกายภาพและที่ไม่ได้เป็นการเข้าถึงทางกายภาพ (ที่เรียกว่าการเข้าถึงทางตรรกะ เช่น การเข้าถึงระบบจากระยะไกล) ต้องมีการกำหนดและนำสู่การปฏิบัติ โดยขึ้นอยู่กับความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ
5.16	การบริหารจัดการอัตลักษณ์ (ที่ใช้ในการพิสูจน์ตัวตนเข้าระบบ) (Identity management)	วัฏจักรทั้งวงจรชีวิตของข้อมูลอัตลักษณ์ (ที่เป็นส่วนหนึ่งของการพิสูจน์ตัวตนในการเข้าถึงระบบ) ต้องได้รับการบริหารจัดการตลอดวงจรชีวิตของข้อมูลดังกล่าว

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตาการควบคุม (Control)
5.17	ข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน (Authentication information)	การจัดสรรและการบริหารจัดการข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตนต้องได้รับการควบคุมผ่านกระบวนการบริหารจัดการ ซึ่งรวมถึงการให้คำแนะนำแก่บุคลากรเกี่ยวกับการจัดการอย่างเหมาะสมสำหรับข้อมูลการพิสูจน์ตัวตนดังกล่าว
5.18	สิทธิการเข้าถึง (Access rights)	สิทธิการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ ต้องมีการดำเนินการทบทวน ปรับปรุง และถอดถอนให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องและกฎเกณฑ์สำหรับควบคุมการเข้าถึงขององค์กร
5.19	ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)	กระบวนการและขั้นตอนปฏิบัติต้องมีการกำหนดและนำสู่การปฏิบัติเพื่อบริหารจัดการความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอก
5.20	การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงการให้บริการของผู้บริการภายนอก (Addressing information security within supplier agreements)	ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกแต่ละราย โดยขึ้นอยู่กับประเภทและความสัมพันธ์กับผู้ให้บริการภายนอกนั้น
5.21	การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่การให้บริการและผลิตภัณฑ์ด้าน ICT	กระบวนการและขั้นตอนปฏิบัติต้องมีการกำหนดและนำสู่การปฏิบัติเพื่อบริหารจัดการความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับห่วงโซ่การให้บริการและผลิตภัณฑ์ด้าน ICT (โดยห่วงโซ่การให้บริการนี้เกิดขึ้นจากผู้ให้บริการภายนอกขององค์กรมีการจ้างต่อหรือที่เรียกว่า "จ้างช่วง" ไปยังผู้ให้บริการภายนอกในลำดับถัดไป จึงทำให้เกิดลักษณะของห่วงโซ่ที่เชื่อมโยงจากองค์กรไปสู่ผู้ให้บริการภายนอกและผู้ให้บริการในลำดับถัดไป)
5.22	การติดตาม การทบทวน และการบริหารจัดการการเปลี่ยนแปลงของบริการจากผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)	องค์กรต้องมีการติดตาม ทบทวน ประเมิน และบริหารจัดการการเปลี่ยนแปลงอย่างสม่ำเสมอในวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและการส่งมอบบริการของผู้ให้บริการภายนอก

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตาการควบคุม (Control)
5.23	ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการ Cloud (Information security for use of cloud services)	กระบวนการสำหรับการจัดหา การใช้บริการ การบริหารจัดการ และการสิ้นสุดการใช้บริการ Cloud ต้องมีการกำหนดโดยให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร
5.24	การวางแผนและการเตรียมการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)	องค์กรต้องมีการวางแผนและเตรียมการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ โดยต้องกำหนดและสื่อสารกระบวนการ บทบาท และหน้าที่ความรับผิดชอบสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
5.25	การประเมินและตัดสินใจสำหรับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)	องค์กรต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (ที่ได้รับแจ้งเข้ามานั้น) และตัดสินใจว่าเหตุดังกล่าวนั้นจัดอยู่ในประเภทของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศหรือไม่ (เพื่อรับมือกับเหตุการณ์ที่เกิดขึ้นนั้นต่อไป)
5.26	การรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)	เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการรับมือให้เป็นไปตามขั้นตอนปฏิบัติที่กำหนดไว้อย่างเป็นลายลักษณ์อักษร
5.27	การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)	ความรู้ที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศต้องนำมาใช้เพื่อเสริมสร้างความแข็งแกร่งและปรับปรุงมาตรการความมั่นคงปลอดภัยสารสนเทศ
5.28	การเก็บรวบรวมหลักฐาน (Collection of evidence)	องค์กรต้องมีการกำหนดและนำไปปฏิบัติสำหรับขั้นตอนปฏิบัติเพื่อระบุ รวบรวม ค้นหาเพื่อให้ได้มา และเก็บรักษาหลักฐานของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ
5.29	ความมั่นคงปลอดภัยสารสนเทศในช่วงที่เกิดการหยุดชะงัก (Information security during disruption)	องค์กรต้องวางแผนเพื่อรักษาความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่เหมาะสมในช่วงที่เกิดการหยุดชะงัก (เช่น ของระบบสารสนเทศขององค์กร ความมั่นคงปลอดภัยสารสนเทศจะหมายรวมถึงความพร้อม

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตาการควบคุม (Control)
		ใช้ของระบบด้วย ดังนั้นการหยุดชะงักของระบบจึงมีความเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรด้วย จึงมีความจำเป็นต้องวางแผนเพื่อรักษาความมั่นคงปลอดภัยสารสนเทศนี้ไว้ให้อยู่ในระดับที่เหมาะสมและเพียงพอต่อความต้องการขององค์กรด้วย)
5.30	ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)	ความพร้อมด้าน ICT ต้องมีการวางแผน นำไปปฏิบัติ บำรุงรักษา และมีการทดสอบ (เพื่อให้เกิดความมั่นใจและมีความพร้อมอยู่เสมอ) โดยให้เป็นไปตามวัตถุประสงค์และความต้องการด้านความต่อเนื่องทางธุรกิจและของระบบ ICT ที่เกี่ยวข้อง
5.31	ความต้องการที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง (Legal, statutory, regulatory and contractual requirements)	ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ อันสืบเนื่องมาจากกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างที่องค์กรต้องปฏิบัติตามและวิธีการขององค์กรที่จะต้องปฏิบัติเพื่อให้สอดคล้องกับความต้องการเหล่านั้น ต้องมีการกำหนด บันทึกไว้เป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบัน
5.32	สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)	องค์กรต้องมีและนำสู่การปฏิบัติสำหรับขั้นตอนปฏิบัติที่เหมาะสมเพื่อป้องกันสิทธิในทรัพย์สินทางปัญญา (เพื่อป้องกันการละเมิดทรัพย์สินทางปัญญาทั้งขององค์กรและของผู้อื่น)
5.33	การป้องกันข้อมูล (Protection of records)	ข้อมูลขององค์กรต้องได้รับการป้องกันจากการสูญหาย การทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่ออกไปโดยไม่ได้รับอนุญาต (ข้อมูลในลักษณะ record โดยทั่วไปหมายถึงข้อมูลที่มีลักษณะเป็นชุด เช่น ข้อมูลประวัติของพนักงาน ข้อมูลการฝึกอบรมของพนักงาน ข้อมูลค่าใช้จ่ายของพนักงาน ข้อมูลเหล่านี้มีลักษณะเป็นชุดของข้อมูล)
5.34	ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)	องค์กรต้องระบุและดำเนินการให้สอดคล้องกับความต้องการที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลตามที่กฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างได้กำหนดให้ต้องปฏิบัติตาม
5.35	การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent review of information security)	วิธีการขององค์กรในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการนำสู่การปฏิบัติ ซึ่งรวมถึงบุคลากร กระบวนการ และเทคโนโลยีที่ใช้เพื่อดำเนินการ ต้องมีการทบทวนอย่างเป็นอิสระตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น (ผู้ที่ต้องปฏิบัติตามกระบวนการด้านความมั่นคงปลอดภัย

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตาการควบคุม (Control)
		สารสนเทศขององค์กร ไม่ควรดำเนินการทบทวนด้านความมั่นคงปลอดภัยสารสนเทศด้วยตนเอง ควรมีหน่วยงานแยกที่เป็นหน่วยงานอิสระเข้ามาดำเนินการทบทวนและควรเป็นหน่วยงานที่ไม่เกี่ยวข้องกับการปฏิบัติตามกระบวนการดังกล่าว จึงจะถือว่ามีความโปร่งใสในการดำเนินการทบทวน)
5.36	การปฏิบัติตามนโยบาย กฎเกณฑ์ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)	การปฏิบัติตามนโยบาย นโยบายเฉพาะแยกตามเรื่อง กฎเกณฑ์ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรต้องมีการทบทวนอย่างสม่ำเสมอ
5.37	ขั้นตอนปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	ขั้นตอนปฏิบัติที่เกี่ยวข้องกับงานประมวลผลข้อมูล (ซึ่งอาจเป็นระบบหรืออุปกรณ์ประมวลผลข้อมูลก็ตาม) ต้องมีการจัดทำอย่างเป็นลายลักษณ์อักษร และต้องมีพร้อมไว้สำหรับบุคลากรที่มีความจำเป็นต้องใช้งาน

6 มาตรการด้านบุคลากร (People controls)

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตรการควบคุม (Control)
6.1	การคัดเลือก (Screening)	การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการก่อนที่ผู้สมัครนั้นจะเริ่มเข้ามาปฏิบัติงานกับองค์กร โดยพิจารณาควบคู่ไปกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง
6.2	ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)	ข้อตกลงในสัญญาจ้างงานต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรและขององค์กร
6.3	การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)	บุคลากรขององค์กรและผู้ที่เกี่ยวข้องจากหน่วยงานภายนอกต้องได้รับการสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม ตลอดจนการให้ความรู้เป็นประจำเกี่ยวกับนโยบายความมั่นคงปลอดภัยสารสนเทศ นโยบายเฉพาะแยกตามเรื่อง และขั้นตอนปฏิบัติที่มีความเกี่ยวข้องกับงานที่ต้องปฏิบัติของบุคลากรเหล่านั้น
6.4	กระบวนการทางวินัย (Disciplinary process)	กระบวนการทางวินัยต้องมีการกำหนดอย่างเป็นทางการและสื่อสารให้ได้รับทราบ ตลอดจนการดำเนินการต่อบุคลากรและผู้ที่เกี่ยวข้องจากหน่วยงานภายนอกสำหรับการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร
6.5	ความรับผิดชอบภายหลังการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)	ความรับผิดชอบและหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศที่ต้องคงไว้หลังสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ต้องมีการกำหนด บังคับให้เป็นไปตามที่กำหนดนั้น และสื่อสารไปยังบุคลากรและหน่วยงานที่เกี่ยวข้องต่างๆ
6.6	ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)	ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ ที่สะท้อนถึงความต้องการขององค์กรในการป้องกันข้อมูล ต้องมีการระบุ จัดทำเป็นลายลักษณ์อักษร ทบทวนอย่างสม่ำเสมอ และมีการลงนามโดยบุคลากรและผู้ที่เกี่ยวข้องจากหน่วยงานต่างๆ

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตรการควบคุม (Control)
6.7	การปฏิบัติงานจากระยะไกล (Remote working)	มาตรการความมั่นคงปลอดภัยต้องมีการปฏิบัติเมื่อบุคลากรกำลังจะปฏิบัติงานจากระยะไกล เพื่อป้องกันข้อมูลที่มีการเข้าถึง ประมวลผล หรือจัดเก็บไว้ภายนอกองค์กร
6.8	การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)	องค์กรต้องมีกลไกสำหรับบุคลากรในการรายงานเหตุการณ์ที่ตนสังเกตพบหรือที่เกิดความสงสัยเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ โดยผ่านช่องทางการรายงานที่เหมาะสมและอย่างทันกาล

7 มาตรการทางกายภาพ (Physical controls)

ลำดับ (No.)	ชื่อมาตาการ (Control Name)	มาตรการควบคุม (Control)
7.1	ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)	ขอบเขตหรือบริเวณโดยรอบที่ต้องการการรักษาความมั่นคงปลอดภัยทางกายภาพ ต้องมีการกำหนดขึ้นมาเพื่อใช้ในการป้องกันพื้นที่ที่มีข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ (ที่ตั้งอยู่ภายในขอบเขตหรือบริเวณดังกล่าว)
7.2	การควบคุมการเข้าออกทางกายภาพ (Physical entry)	พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการป้องกันโดยควบคุมการเข้าออกพื้นที่และควบคุมจุดที่มีการเข้าถึงอย่างเหมาะสม
7.3	การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)	ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอุปกรณ์ต่างๆ ต้องมีการออกแบบและนำสู่การปฏิบัติ (เพื่อให้เกิดการป้องกันอย่างเป็นรูปธรรม)
7.4	การเฝ้าระวังด้านความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)	บริเวณ อาคาร หรือสถานที่ขององค์กรต้องมีการเฝ้าระวังและติดตามอย่างต่อเนื่องเพื่อป้องกันการเข้าถึงการกายภาพโดยไม่ได้รับอนุญาต
7.5	การป้องกันต่อภัยคุกคามทางกายภาพ และด้านสภาพแวดล้อม (Protecting against physical and environmental threats)	การป้องกันต่อภัยคุกคามทางกายภาพและด้านสภาพแวดล้อม เช่น ภัยพิบัติทางธรรมชาติ ภัยคุกคามทางกายภาพทั้งที่เจตนาหรือไม่เจตนาก็ตาม ต้องมีการออกแบบและนำสู่การปฏิบัติ
7.6	การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)	มาตรการความมั่นคงปลอดภัยสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการออกแบบและนำสู่การปฏิบัติ
7.7	โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen)	กฎเกณฑ์ 'โต๊ะทำงานปลอดเอกสารสำคัญ' เพื่อป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และกฎเกณฑ์ 'การป้องกันหน้าจอคอมพิวเตอร์' เพื่อป้องกันข้อมูลในอุปกรณ์ประมวลผลข้อมูล ต้องมีการกำหนดและบังคับใช้งาน (เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร)

ลำดับ (No.)	ชื่อมาตาการ (Control Name)	มาตรการควบคุม (Control)
7.8	การจัดวางและป้องกันอุปกรณ์ (Equipment sitting and protection)	อุปกรณ์ต้องมีการจัดวางและป้องกันให้มีความปลอดภัย
7.9	ความมั่นคงปลอดภัยของทรัพย์สินที่มีการใช้งานนอกองค์กร (Security of assets off-premises)	ทรัพย์สินที่มีการใช้งานนอกองค์กรต้องมีการป้องกัน
7.10	สื่อบันทึกข้อมูล (Storage media)	สื่อบันทึกข้อมูลต้องได้รับการบริหารจัดการตลอดวัฏจักรชีวิต นับตั้งแต่การจัดหา การใช้งาน การขนย้าย/การขนส่ง และการจำหน่ายออก โดยให้เป็นไปตามวิธีการจัดชั้นความลับและการจัดการข้อมูลและทรัพย์สินที่เกี่ยวข้องขององค์กรที่ได้กำหนดไว้
7.11	ระบบสาธารณูปโภคสนับสนุน (Supporting utilities)	ระบบหรืออุปกรณ์ประมวลผลข้อมูลต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่นๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบสาธารณูปโภคสนับสนุน (ระบบสาธารณูปโภคดังกล่าวครอบคลุมถึง ไฟฟ้า ประปา เป็นต้น)
7.12	ความมั่นคงปลอดภัยของสายสัญญาณ (Cabling security)	สายสัญญาณที่นำพาไฟฟ้า ข้อมูล หรือบริการสนับสนุนด้านข้อมูลอื่นๆ ต้องได้รับการป้องกันจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย
7.13	การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มีความพร้อมใช้งาน สามารถรักษาความถูกต้อง และความลับของข้อมูล
7.14	ความมั่นคงปลอดภัยสำหรับการจำหน่ายออกหรือการทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)	อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องมีการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการจำหน่ายออกอุปกรณ์หรือก่อนการนำอุปกรณ์นั้นไปใช้งานอย่างอื่น

8 มาตรการทางเทคโนโลยี (Technological controls)

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตรการควบคุม (Control)
8.1	อุปกรณ์ปลายทางของผู้ใช้งาน (User end point devices)	ข้อมูลที่มีการจัดเก็บไว้ มีการประมวลผล หรือมีการเข้าถึงโดยอุปกรณ์ปลายทางของผู้ใช้งาน ต้องได้รับการป้องกัน (อุปกรณ์ปลายทางนี้โดยทั่วไปหมายรวมถึง เครื่องคอมพิวเตอร์โน๊ตบุ๊ค โทรศัพท์มือถือ ปาล์ม และอุปกรณ์ที่สามารถประมวลผลข้อมูลอื่นๆ ที่มีการใช้งานโดยผู้ใช้งาน โดยทั่วไปอุปกรณ์เหล่านี้สามารถ ติดต่อสื่อสารข้อมูลผ่านทางเครือข่ายได้)
8.2	สิทธิการเข้าถึงในระดับพิเศษ (Privileged access rights)	การจัดสรรและให้สิทธิการเข้าถึงในระดับพิเศษ (เช่น ระดับของผู้ดูแลระบบ ระดับของผู้จัดการ) ต้องมีการจำกัดและบริหารจัดการ
8.3	การจำกัดการเข้าถึงข้อมูล (Information access restriction)	การควบคุมการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ ต้องมีการจำกัดให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับการควบคุมการเข้าถึงที่ได้กำหนดไว้
8.4	การจำกัดการเข้าถึงซอร์สโค้ด (Access to source code)	การเข้าถึงซอร์สโค้ด เครื่องมือที่ใช้ในการพัฒนาระบบ และซอฟต์แวร์ไลบรารี่ ที่สามารถอ่านและเขียนทับข้อมูลเหล่านั้นได้ ต้องมีการบริหารจัดการอย่างเหมาะสม
8.5	การพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย (Secure authentication)	เทคโนโลยีและขั้นตอนปฏิบัติสำหรับใช้ในการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย ต้องมีการนำสู่การปฏิบัติโดยขึ้นอยู่กับการจำกัดการเข้าถึงข้อมูลและนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับการควบคุมการเข้าถึง
8.6	การบริหารจัดการขีดความสามารถของระบบ (Capacity management)	การใช้ทรัพยากรของระบบต้องมีการเฝ้าระวัง ติดตาม และปรับปรุงให้เป็นไปตามความต้องการทรัพยากรในปัจจุบันและที่คาดการณ์ว่าจะเกิดขึ้น
8.7	การป้องกันจากโปรแกรมไม่ประสงค์ดี (Protection against malware)	การป้องกันจากโปรแกรมไม่ประสงค์ดีต้องมีการนำสู่การปฏิบัติ และได้รับการสนับสนุนโดยการสร้างความตระหนักให้แก่ผู้ใช้งานอย่างเหมาะสม
8.8	การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)	ข้อมูลที่เกี่ยวข้องกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่มีการใช้งาน ต้องมีการติดตามเพื่อให้ได้มาซึ่งข้อมูลดังกล่าว ความเสี่ยงต่อช่องโหว่ดังกล่าวขององค์กรต้องได้รับการ

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตรการควบคุม (Control)
		ประเมิน และมีการกำหนดมาตรการที่เหมาะสมเพื่อดำเนินการ
8.9	การบริหารจัดการการตั้งค่าระบบ (Configuration Management)	การตั้งค่าระบบ ซึ่งรวมถึงการตั้งค่าด้านความมั่นคงปลอดภัยของฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่าย ต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร นำสู่การปฏิบัติ ติดตาม และทบทวน (เพื่อให้เป็นไปตามการตั้งค่าที่กำหนดไว้นั้น)
8.10	การลบข้อมูล (Information deletion)	ข้อมูลที่มีการจัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือบนสื่อบันทึกข้อมูลอื่นๆ ต้องมีการลบทำลายเมื่อไม่มีความจำเป็นในการใช้งานอีกต่อไป
8.11	การปิดบังข้อมูล (Data masking)	การปิดบังข้อมูล (เพื่อไม่ให้ข้อมูลที่จัดเก็บไว้ในระบบถูกมองเห็น หรือถูกนำไปใช้ประโยชน์ได้) ต้องมีการนำมาใช้งานโดยให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับการควบคุมการเข้าถึง นโยบายเฉพาะแยกตามเรื่องอื่นๆ ที่เกี่ยวข้อง และความต้องการทางธุรกิจขององค์กร โดยต้องพิจารณากฎหมายที่เกี่ยวข้องประกอบด้วย
8.12	การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)	มาตรการการป้องกันการรั่วไหลของข้อมูล ต้องมีการนำมาประยุกต์ใช้กับระบบ เครือข่าย และอุปกรณ์ต่างๆ ที่มีการประมวลผล จัดเก็บ หรือรับส่งข้อมูลสำคัญ
8.13	การสำรองข้อมูล (Information backup)	สำเนาของข้อมูล ซอฟต์แวร์ และระบบต้องมีการจัดเก็บรักษาไว้ และทดสอบอย่างสม่ำเสมอ โดยให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับการสำรองข้อมูล
8.14	การสำรองอุปกรณ์ประมวลผลข้อมูล (Redundancy of information processing facilities)	อุปกรณ์ประมวลผลข้อมูลต้องมีการเตรียมการสำรองไว้ให้เพียงพอเพื่อให้เป็นไปตามความต้องการด้านสภาพความพร้อมใช้ของอุปกรณ์เหล่านั้น
8.15	การบันทึกข้อมูลล็อก (Logging)	ข้อมูลล็อกที่มีการบันทึกกิจกรรมต่างๆ ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์ที่เกี่ยวข้องอื่นๆ ของระบบ ต้องมีการจัดเตรียมระบบไว้ สำหรับข้อมูลล็อกดังกล่าว เพื่อให้สามารถผลิต จัดเก็บ ป้องกัน และนำมาวิเคราะห์ข้อมูลได้
8.16	กิจกรรมการเฝ้าระวังการทำงานของระบบและอุปกรณ์ (Monitoring Activities)	เครือข่าย ระบบ และแอพพลิเคชั่นต้องมีการเฝ้าระวังการทำงานเพื่อตรวจหาพฤติกรรมที่ผิดปกติ และดำเนินการเพื่อ

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตรการควบคุม (Control)
		ประเมินความเป็นไปได้ของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น
8.17	การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)	นาฬิกาของระบบสารสนเทศที่มีการใช้งานภายในองค์กร ต้องได้รับการตั้งค่าเวลาให้เที่ยงตรงโดยเทียบกับแหล่งเทียบเวลาที่ได้รับการรับรอง
8.18	การใช้โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิในระดับพิเศษ (Use of privileged utility programs)	การใช้โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิในระดับพิเศษ ซึ่งทำให้สามารถละเมิดมาตรการควบคุมของแอพพลิเคชั่นและระบบ ต้องมีการจำกัดและควบคุมการใช้งานอย่างเคร่งครัด
8.19	การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)	ขั้นตอนปฏิบัติและมาตรการที่จำเป็นต้องมีการนำสู่การปฏิบัติเพื่อบริหารจัดการการติดตั้งซอฟต์แวร์บนระบบให้บริการให้มีความมั่นคงปลอดภัย (ระบบให้บริการเป็นระบบที่ไม่ได้เป็นระบบสำหรับการทดสอบ และไม่ได้เป็นระบบที่ใช้ในการพัฒนา ระบบเมื่อผ่านขั้นตอนการพัฒนาและได้รับการทดสอบเป็นที่เรียบร้อยแล้ว จะมีการนำไปติดตั้งบนระบบให้บริการเพื่อให้บริการแก่ผู้ใช้งาน ดังนั้นการปฏิบัติงานภายในองค์กรของผู้ใช้งานจะกระทำบนระบบให้บริการ)
8.20	ความมั่นคงปลอดภัยของเครือข่าย (Networks security)	เครือข่ายและอุปกรณ์เครือข่าย ต้องมีการรักษาความมั่นคงปลอดภัย ได้รับการบริหารจัดการ และมีการควบคุมเพื่อป้องกันข้อมูลทั้งในระบบและแอพพลิเคชั่น (ที่มีการทำงานผ่านเครือข่ายและอุปกรณ์เครือข่ายขององค์กร)
8.21	ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)	กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการด้านบริการที่มีต่อบริการเครือข่ายหนึ่ง (ที่อาจมาจากผู้บริหารหรือผู้มีส่วนได้ส่วนเสียของบริการดังกล่าว) ต้องมีการกำหนด นำสู่การปฏิบัติ ติดตาม และเฝ้าระวัง (เพื่อให้เป็นไปตามกลไก ระดับการให้บริการ และความต้องการที่ได้กำหนดไว้นั้น)
8.22	การแบ่งแยกเครือข่าย (Segregation in networks)	กลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบสารสนเทศต้องมีการแบ่งแยกออกจากกันในเครือข่ายขององค์กร (ตามความต้องการขององค์กร)
8.23	การคัดกรองเว็บ (Web filtering)	การเข้าถึงเว็บไซต์ภายนอกต้องได้รับการบริหารจัดการเพื่อลดโอกาสการเข้าถึงเนื้อหาที่เป็นอันตราย (เช่น โปรแกรมไม่

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตรการควบคุม (Control)
		ประสงค์ดี ซอฟต์แวร์ที่เป็นอันตรายต่างๆ เป็นต้น ที่อาจสร้างความเสียหายให้แก่ข้อมูลและเครื่องคอมพิวเตอร์ขององค์กรได้ในลักษณะใดลักษณะหนึ่ง)
8.24	การใช้การเข้ารหัสข้อมูล (Use of cryptography)	กฎเกณฑ์สำหรับการใช้การเข้ารหัสข้อมูลที่ได้ผล ซึ่งรวมถึงการบริหารจัดการกุญแจสำหรับการเข้ารหัส ต้องมีการกำหนดและนำสู่การปฏิบัติ
8.25	วัฏจักรการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development life cycle)	กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบให้มีความมั่นคงปลอดภัย ต้องมีการกำหนดและนำสู่การปฏิบัติ
8.26	ความต้องการด้านความมั่นคงปลอดภัยของแอพพลิเคชั่น (Application security requirements)	ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของแอพพลิเคชั่นต้องมีการกำหนดและอนุมัติเมื่อมีการพัฒนาหรือจัดหาแอพพลิเคชั่น
8.27	สถาปัตยกรรมของระบบที่มีความมั่นคงปลอดภัยและหลักการวิศวกรรมระบบ (Secure system architecture and engineering principles)	หลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัย (หลักการการออกแบบและพัฒนาระบบให้มีความมั่นคงปลอดภัย) ต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร ปรับปรุง และนำมาปฏิบัติต่อกิจกรรมการพัฒนาระบบสารสนเทศ (เพื่อให้ระบบที่ออกแบบและพัฒนามีความมั่นคงปลอดภัย)
8.28	การเขียนโปรแกรมให้มีความมั่นคงปลอดภัย (Secure Coding)	หลักการการเขียนโปรแกรมให้มีความมั่นคงปลอดภัยต้องมีการนำมาปฏิบัติกับการพัฒนาซอฟต์แวร์
8.29	การทดสอบด้านความมั่นคงปลอดภัยในการพัฒนาและรับรองระบบ (Security testing in development and acceptance)	กระบวนการสำหรับการทดสอบด้านความมั่นคงปลอดภัยต้องมีการกำหนดและนำสู่การปฏิบัติในวัฏจักรของการพัฒนาระบบ
8.30	การพัฒนาระบบโดยหน่วยงานภายนอก (Outsourced development)	องค์กรต้องกำกับดูแล เฝ้าระวัง ติดตาม และทบทวนกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ
8.31	การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation	สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการแยกออกจากกันและต้องมีการรักษาความมั่นคงปลอดภัย

ลำดับ (No.)	ชื่อมาตรการ (Control Name)	มาตรการควบคุม (Control)
	of development, testing and operational environments)	
8.32	การบริหารจัดการการเปลี่ยนแปลง (Change management)	การเปลี่ยนแปลงต่ออุปกรณ์ประมวลผลข้อมูลและระบบสารสนเทศ ต้องมีการควบคุมผ่านขั้นตอนปฏิบัติสำหรับการบริหารจัดการการเปลี่ยนแปลง
8.33	ข้อมูลสำหรับการทดสอบ (Test information)	ข้อมูลสำหรับการทดสอบระบบต้องมีการคัดเลือก มีการป้องกัน และมีการบริหารจัดการอย่างเหมาะสม
8.34	การป้องกันระบบสารสนเทศในช่วงที่มีการทดสอบระบบโดยผู้ตรวจประเมิน (Protection of information systems during audit testing)	การทดสอบระบบโดยผู้ตรวจประเมินและกิจกรรมการตรวจประเมินอื่นๆ ที่เกี่ยวข้องกับการประเมินระบบให้บริการต้องมีการวางแผนและตกลงกันระหว่างผู้ดำเนินการทดสอบและผู้บริหารที่เกี่ยวข้อง (เพื่อป้องกันปัญหาต่างๆ ที่อาจจะเกิดขึ้นกับระบบให้บริการ เช่น ระบบเกิดการหยุดชะงักในระหว่างที่ทำการทดสอบ ข้อมูลสำคัญในระบบถูกเข้าถึงโดยไม่ได้รับอนุญาต เป็นต้น)