มาตรฐาน ISO/IEC 27001 : 2013

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

ข้อกำหนดหลักที่ต้องปฏิบัติตามในการขอการรับรองตามมาตรฐาน ISO/IEC 27001 : 2013

ข้อ 1 บริบทขององค์กร (Context of the organization)

1.1 การทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context)

องค์กรต้องกำหนดประเด็นภายในและภายนอกองค์กรที่เกี่ยวข้องกับจุดประสงค์ขององค์กร และที่ส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อสังเกต การกำหนดประเด็นดังกล่าวหมายถึงการกำหนดบริบทภายในและภายนอกองค์กร ที่มีการพิจารณาในข้อ 2.3 ของมาตรฐาน ISO 31000:2009

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

องค์กรต้องกำหนด:

a) ผู้ที่เกี่ยวข้อง ซึ่งเป็นผู้ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ

b) ความต้องการของผู้ที่เกี่ยวข้องเหล่านั้นซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

ข้อสังเกต ความต้องการของผู้ที่เกี่ยวข้องอาจรวมถึงความต้องการด้านกฎหมายและระเบียบข้อบังคับ และข้อกำหนดในสัญญาจ้าง

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

องค์กรต้องกำหนดกรอบและการประยุกต์ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อระบุขอบเขตการดำเนินการ

ในการระบุขอบเขต องค์กรต้องพิจารณา:

a) ประเด็นภายในและภายนอกองค์กร โดยอ้างอิงจากข้อ 1.1

b) ความต้องการ โดยอ้างอิงจากข้อ 1.2 และ

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

c) การเชื่อมโยงและการสัมพันธ์กันของกิจกรรมในลักษณะที่กิจกรรมขึ้นอยู่กับซึ่งกันและกัน โดยที่กิจกรรมเหล่านั้นอาจดำเนินการโดยองค์กรเองหรือโดยองค์กรอื่นๆ

ขอบเขตต้องสามารถเข้าถึงได้โดยจัดทำเป็นลายลักษณ์อักษร

1.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system)

องค์กรต้องกำหนด ลงมือปฏิบัติ บำรุงรักษา และปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยต้องมีความสอดคล้องกับข้อกำหนดในเอกสารมาตรฐานฉบับนี้

ข้อ 2 ภาวะผู้นำ (Leadership)

2.1 ภาวะผู้นำและการให้ความสำคัญ (Leadership and commitment)

ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงภาวะผู้นำและการให้ความสำคัญต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดย

a) ต้องทำให้นโยบายความมั่นคงปลอดภัยสารสนเทศและวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศมีการกำหนดขึ้นมาและมีความสอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร
b) ต้องทำให้มีการรวมความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการขององค์กร
c) ต้องทำให้มีทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการดำเนินการ
d) ต้องสื่อสารความสำคัญของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สัมฤทธิ์ผลและของการดำเนินการตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้
e) ต้องทำให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลลัพธ์ตามที่ต้องการ
f) ต้องสั่งการและสนับสนุนบุคลากรเพื่อนำสู่ความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
g) ต้องส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง และ
h) ต้องสนับสนุนบทบาทการบริหารอื่นๆ ภายใต้ขอบเขตความรับผิดชอบของเพื่อแสดงภาวะผู้นำของตนเอง

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

2.2 นโยบาย (Policy)

ผู้บริหารระดับสูงต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศซึ่ง:

a) เหมาะสมต่อจุดประสงค์ขององค์กร
b) รวมวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศไว้ด้วย (ดูข้อ 3.2) หรือกำหนดกรอบการปฏิบัติสำหรับการกำหนดวัตถุประสงค์ดังกล่าว
c) รวมการให้ความสำคัญของผู้บริหารเพื่อให้สอดคล้องกับความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และ
d) รวมการให้ความสำคัญของผู้บริหารในการปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

นโยบายความมั่นคงปลอดภัยสารสนเทศ:

e) ต้องสามารถเข้าถึงได้โดยจัดทำเป็นลายลักษณ์อักษร
f) ต้องมีการสื่อสารให้ทราบกันภายในองค์กร และ
g) ต้องสามารถเข้าถึงได้โดยผู้ที่เกี่ยวข้องตามความเหมาะสม

2.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ (Organizational roles, responsibilities and authorities)

ผู้บริหารระดับสูงต้องทำให้หน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศมีการมอบหมายและสื่อสารให้ได้รับทราบกัน

ผู้บริหารระดับสูงต้องมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่เพื่อ:

a) ให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีความสอดคล้องกับข้อกำหนดของเอกสารมาตรฐานฉบับนี้ และ
b) ให้มีการรายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

ข้อสังเกต ผู้บริหารระดับสูงอาจมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่ในการรายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในองค์กรด้วย

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

ข้อ 3 การวางแผน (Planning)

3.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to address risks and opportunities)

3.1.1 ภาพรวม (General)

เมื่อวางแผนสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องพิจารณาประเด็นภายในและภายนอกที่อ้างถึงในข้อ 1.1 และความต้องการที่อ้างถึงในข้อ 1.2 และต้องกำหนดความเสี่ยงและโอกาสที่จำเป็นต้องจัดการเพื่อ:

a) ให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลลัพธ์ตามที่ต้องการ
b) ป้องกัน หรือลดผลที่ไม่พึงปรารถนา และ
c) ให้บรรลุการปรับปรุงอย่างต่อเนื่อง

องค์กรต้องวางแผน:

d) การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส และ
e) วิธีการที่จะ
    1) รวมการดำเนินการดังกล่าวเข้ากับกระบวนการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและนำสู่การปฏิบัติ และ
    2) ประเมินความสัมฤทธิ์ผลของการดำเนินการดังกล่าว

3.1.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

องค์กรต้องกำหนดและประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งต้อง:

a) กำหนดและปรับปรุงเกณฑ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งต้องรวมถึง
    1) เกณฑ์การยอมรับความเสี่ยง และ
    2) เกณฑ์สำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
b) ทำให้การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้ผลการประเมินที่สอดคล้องกัน ถูกต้อง และเปรียบเทียบกันได้
c) ระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ:
    1) ประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องสมบูรณ์ และสภาพ

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

ความพร้อมใช้ของสารสนเทศภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ

2) ระบุผู้เป็นเจ้าของความเสี่ยง

d) วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ:

1) ประเมินผลที่เป็นไปได้ที่จะเกิดขึ้นถ้าความเสี่ยงที่ระบุไว้ในข้อ 3.1.2 c) เกิดขึ้นจริง

2) ประเมินโอกาสการเกิดขึ้นที่สมจริงของความเสี่ยงที่ระบุไว้ในข้อ 3.1.2 c) และ

3) กำหนดระดับของความเสี่ยง

e) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ:

1) เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดไว้ในข้อ 3.1.2 a) และ

2) จัดลำดับความเสี่ยงที่วิเคราะห์นั้นเพื่อการจัดการที่เหมาะสม

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อย่างเป็นลายลักษณ์อักษร

3.1.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

องค์กรต้องกำหนดและประยุกต์กระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งต้อง:

a) กำหนดทางเลือกที่เหมาะสมในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยต้องนำผลการประเมินความเสี่ยงมาพิจารณาด้วย

b) กำหนดมาตรการทั้งหมดที่จำเป็นเพื่อดำเนินการตามทางเลือกที่กำหนดไว้

ข้อสังเกต องค์กรสามารถออกแบบมาตรการได้เองตามที่ต้องการ หรือระบุมาตรการโดยอ้างอิงจากแหล่งใดก็ตาม

c) เปรียบเทียบมาตรการที่กำหนดไว้ในข้อ 3.1.3 b) กับมาตรการใน Annex A และตรวจสอบว่าไม่มีมาตรการข้อใดที่ละเลยไป

ข้อสังเกต 1 Annex A ประกอบด้วยรายการทั้งหมดของวัตถุประสงค์ของมาตรการและตัวมาตรการของมาตรฐานฉบับนี้ ขอให้ผู้ใช้งานมาตรฐานฉบับนี้อ้างอิงไปยัง Annex A เพื่อให้มั่นใจว่าไม่มีมาตรการข้อใดที่ถูกมองข้ามไป

ข้อสังเกต 2 วัตถุประสงค์ของมาตรการถูกรวมแฝงไว้กับมาตรการที่เลือก

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

วัตถุประสงค์ของมาตรการและมาตรการใน Annex A ยังไม่ได้ครอบคลุมทั้งหมด วัตถุประสงค์และมาตรการเพิ่มเติมอาจจะจำเป็นต้องนำมาใช้ด้วย

d) จัดทำเอกสารแสดงการใช้มาตรการ SoA (Statement of Applicability) ซึ่งประกอบด้วยมาตรการที่จำเป็น (ดูข้อ 3.1.3 b) และ c)) และคำอธิบายเหตุผลของการใช้มาตรการไม่ว่ามาตรการเหล่านั้นจะได้รับการปฏิบัติแล้วหรือไม่ก็ตาม และคำอธิบายเหตุผลของการไม่ใช้มาตรการจาก Annex A

e) จัดทำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และ

f) ขอการรับรองจากผู้เป็นเจ้าของความเสี่ยงสำหรับแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และการยอมรับสำหรับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ยังเหลืออยู่

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับกระบวนการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อย่างเป็นลายลักษณ์อักษร

ข้อสังเกต กระบวนการประเมินและจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในมาตรฐานฉบับนี้สอดคล้องกับหลักการและแนวทางที่เสนอไว้ในมาตรฐาน ISO 31000

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

องค์กรต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในฟังก์ชันงานและระดับที่เกี่ยวข้อง

วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศต้อง:

a) สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ

b) สามารถวัดได้ (ถ้าสามารถปฏิบัติได้)

c) นำความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ผลการประเมินและการจัดการความเสี่ยงมาพิจารณาด้วย

d) มีการสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ และ

e) มีการปรับปรุงตามความเหมาะสม

องค์กรต้องจัดเก็บสารสนเทศสำหรับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ไว้อย่างเป็นลายลักษณ์อักษร

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

เมื่อวางแผนวิธีการที่จะบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องกำหนด:

f) สิ่งที่ต้องดำเนินการ

g) ทรัพยากรที่ต้องใช้

h) ผู้รับผิดชอบในการดำเนินการ

i) ระยะเวลาที่จะดำเนินการให้เสร็จ และ

j) วิธีประเมินผลการปฏิบัติการ

ข้อ 4 การสนับสนุน (Support)

4.1 ทรัพยากร (Resources)

องค์กรต้องกำหนดและให้ทรัพยากรที่จำเป็นสำหรับการกำหนด การลงมือปฏิบัติ การบำรุงรักษา และการปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4.2 สมรรถนะ (Competence)

องค์กรต้อง:

a) กำหนดสมรรถนะของบุคลากรที่ทำงานภายใต้การควบคุมดูแลขององค์กร ซึ่งส่งผลต่อประสิทธิภาพในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ

b) ทำให้บุคลากรเหล่านี้มีความสามารถโดยการให้ความรู้ การฝึกอบรม หรือจากประสบการณ์การทำงานที่ได้รับ

c) ดำเนินการตามความเหมาะสมเพื่อให้ได้มาซึ่งสมรรถนะที่จำเป็น และประเมินความสัมฤทธิ์ผลของการดำเนินการนั้น และ

d) จัดเก็บสารสนเทศที่เหมาะสมอย่างเป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดงสมรรถนะ

ข้อสังเกต การดำเนินการตามความเหมาะสมอาจรวมถึงการฝึกอบรม การเป็นพี่เลี้ยง การมอบหมายหมายงานให้ผู้อื่น หรือการจ้างหรือทำสัญญากับบุคลากรที่มีความสามารถ เป็นต้น

4.3 การสร้างความตระหนัก (Awareness)

บุคลากรที่ทำงานภายใต้การควบคุมดูแลขององค์กรต้องตระหนักถึง:

a) นโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

b) การที่ตนเองมีส่วนในความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

สารสนเทศ ซึ่งรวมถึงข้อดีของการปรับปรุงประสิทธิภาพในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง และ

c) สิ่งที่เกี่ยวข้องของการไม่ปฏิบัติตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4.4 การสื่อสารให้ทราบ (Communication)

องค์กรต้องกำหนดความจำเป็นสำหรับการสื่อสารให้ทราบทั้งภายในและภายนอกที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึง:

a) อะไรบ้างที่ต้องสื่อสารให้ทราบ

b) เมื่อไรที่ต้องสื่อสารให้ทราบ

c) ใครบ้างที่ต้องสื่อสารให้ทราบ

d) ใครเป็นผู้สื่อสารออกไป และ

e) กระบวนการที่เกี่ยวข้องกับการสื่อสาร

4.5 สารสนเทศที่เป็นลายลักษณ์อักษร (Documented information)

4.5.1 ภาพรวม (General)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรต้องรวม:

a) สารสนเทศที่เป็นลายลักษณ์อักษรซึ่งกำหนดโดยมาตรฐานฉบับนี้ และ

b) สารสนเทศที่เป็นลายลักษณ์อักษรซึ่งกำหนดโดยองค์กรเองและจำเป็นสำหรับความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อสังเกต ปริมาณของสารสนเทศที่เป็นลายลักษณ์อักษรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสามารถแตกต่างกันในแต่ละองค์กร เนื่องจาก:

a) ขนาดขององค์กรและประเภทของกิจกรรม กระบวนการ ผลิตภัณฑ์ และบริการขององค์กร

b) ความซับซ้อนของกระบวนการและการเชื่อมโยงระหว่างกระบวนการ และ

c) ความสามารถของบุคลากร

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

4.5.2 การสร้างและปรับปรุง (Creating and updating)

เมื่อมีการสร้างและปรับปรุงสารสนเทศที่เป็นลายลักษณ์อักษร องค์กรต้องกำหนดประเด็นเหล่านี้ให้มีความเหมาะสม:

a) ชื่อและรายละเอียด (เช่น ชื่อเอกสาร วันที่ ผู้แต่ง หรือเลขที่อ้างอิง)

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

c) การทบทวนและการอนุมัติเพื่อความเหมาะสมและเพียงพอ

4.5.3 การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร (Control of documented information)

สารสนเทศที่เป็นลายลักษณ์อักษรที่จำเป็นต้องมีสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและตามมาตรฐานฉบับนี้ต้องมีการควบคุมเพื่อให้:

a) สารสนเทศสามารถเข้าถึงได้และเหมาะสมสำหรับการใช้งาน สถานที่และวันเวลาในการใช้งาน และ

b) สารสนเทศได้รับการป้องกันอย่างเพียงพอ (เช่น จากการสูญเสียความลับ การใช้งานที่ไม่เหมาะสม หรือการสูญเสียความถูกต้องสมบูรณ์)

สำหรับการควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร องค์กรต้องระบุกิจกรรมดังต่อไปนี้ตามความเหมาะสม:

c) การแจกจ่าย การเข้าถึง การนำขึ้นมาใช้ และการใช้งาน

d) การจัดเก็บและการรักษาไว้ รวมถึงการรักษาไว้ให้สามารถอ่านใช้งานได้

e) การควบคุมการเปลี่ยนแปลง (เช่น การควบคุมเวอร์ชั่น) และ

f) การจัดเก็บ ระยะเวลาการจัดเก็บ และการทำลาย

สารสนเทศที่มาจากแหล่งภายนอกที่องค์กรกำหนดว่าจำเป็นสำหรับการวางแผนและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องมีการระบุตามความจำเป็น และต้องมีการควบคุม

ข้อสังเกต การเข้าถึงสารสนเทศหมายรวมถึงการตัดสินใจเกี่ยวกับการอนุญาตให้ดูสารสนเทศได้เท่านั้น หรือการอนุญาตและการให้อำนาจในการดูและเปลี่ยนแปลงสารสนเทศได้ด้วย หรืออื่นๆ

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

ข้อ 5 การดำเนินการ (Operation)

5.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational planning and control)

องค์กรต้องวางแผน ลงมือปฏิบัติ และควบคุมกระบวนการที่จำเป็นเพื่อให้สอดคล้องกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และลงมือปฏิบัติตามที่กำหนดไว้ในข้อ 3.1 องค์กรยังต้องลงมือปฏิบัติตามแผนเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ในข้อ 3.2

องค์กรต้องเก็บรักษาสารสนเทศที่เป็นลายลักษณ์อักษรในระดับที่จำเป็นเพื่อให้มีความมั่นใจว่ากระบวนการเหล่านั้นมีการดำเนินการตามแผน

องค์กรต้องควบคุมการเปลี่ยนแปลงที่มีการวางแผนล่วงหน้า และทบทวนผลของการเปลี่ยนแปลงที่เกิดขึ้นอย่างไม่ได้ตั้งใจ (เช่น การเปลี่ยนแปลงที่ไม่ได้วางแผนไว้และเกิดขึ้นแบบฉุกเฉิน) ดำเนินการเพื่อลดผลในทางลบตามความจำเป็น

องค์กรต้องทำให้มั่นใจว่ากระบวนการที่มีการจ้างหน่วยงานภายนอกดำเนินการมีการระบุและควบคุมการดำเนินการ

5.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

องค์กรต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มากเสนอขอดำเนินการ หรือเมื่อมีการเปลี่ยนแปลงที่มากเกิดขึ้น โดยนำเกณฑ์ความเสี่ยงที่กำหนดไว้ในข้อ 3.1.2 a) มาพิจารณาด้วย

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร ซึ่งเป็นผลของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

5.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

องค์กรต้องลงมือปฏิบัติตามแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร ซึ่งเป็นผลของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

ข้อ 6 การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

6.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน (Monitoring, measurement, analysis and evaluation)

องค์กรต้องประเมินประสิทธิภาพและประสิทธิผลและความได้ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องกำหนด:

a) อะไรที่จำเป็นต้องเฝ้าระวังและวัดผล ซึ่งรวมถึงกระบวนการและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

b) วิธีการในการเฝ้าระวัง วัดผล วิเคราะห์ และประเมินตามที่เหมาะสม เพื่อให้ได้ผลการประเมินที่ถูกต้อง

ข้อสังเกต วิธีการที่เลือกใช้ควรให้ผลการประเมินที่สามารถเปรียบเทียบกันได้และที่สามารถทำซ้ำได้เพื่อให้ได้ผลที่ถูกต้อง

c) เมื่อไรที่การเฝ้าระวังและวัดผลต้องดำเนินการ

d) ใครเป็นผู้เฝ้าระวังและวัดผล

e) เมื่อไรที่ผลจากการเฝ้าระวังและวัดผลต้องได้รับการวิเคราะห์และประเมิน และ

f) ใครเป็นผู้วิเคราะห์และประเมินผล

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรที่เหมาะสม เพื่อใช้เป็นหลักฐานแสดงการเฝ้าระวังและวัดผล

6.2 การตรวจประเมินภายใน (Internal audit)

องค์กรต้องดำเนินการตรวจประเมินภายในตามรอบระยะเวลาที่กำหนดไว้เพื่อให้มีสารสนเทศสำหรับการระบุว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ:

a) สอดคล้องกับ

1) ความต้องการขององค์กรเองสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ

2) ข้อกำหนดของมาตรฐานฉบับนี้

b) มีการปฏิบัติและบำรุงรักษาไว้อย่างสัมฤทธิ์ผล

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

องค์กรต้อง:

c) วางแผน กำหนด ลงมือปฏิบัติ และบำรุงรักษาโปรแกรมการตรวจประเมิน ซึ่งรวมถึงความถี่ วิธีการที่ใช้ หน้าที่ความรับผิดชอบ ความต้องการในการตรวจประเมินที่วางแผนไว้ และการรายงานผล โปรแกรมการตรวจประเมินต้องนำความสำคัญของกระบวนการที่เกี่ยวข้องและผลการตรวจประเมินครั้งก่อนมาพิจารณาร่วมด้วย

d) กำหนดเกณฑ์การตรวจประเมินและขอบเขตของการตรวจประเมินแต่ละครั้ง

e) เลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินซึ่งเป็นไปตามข้อเท็จจริงและหลักฐาน และมีความเป็นกลางของกระบวนการตรวจประเมิน

f) ทำให้ผลของการตรวจประเมินมีการรายงานไปยังผู้บริหารที่เกี่ยวข้อง และ

g) จัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดงโปรแกรมการตรวจประเมินและผลการตรวจประเมิน

6.3 การทบทวนของผู้บริหาร (Management review)

ผู้บริหารระดับสูงต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามรอบระยะเวลาที่กำหนดไว้เพื่อให้มีความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผล

การทบทวนของผู้บริหารต้องรวมการพิจารณาในเรื่อง:

a) สถานะของการดำเนินการจากผลการทบทวนครั้งก่อน

b) การเปลี่ยนแปลงในประเด็นภายในและภายนอกองค์กรที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

c) ผลตอบกลับของประสิทธิภาพและประสิทธิผลด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงแนวโน้มในเรื่อง

1) ความไม่สอดคล้องและการดำเนินการแก้ไข

2) ผลการเฝ้าระวังและวัดผล

3) ผลการตรวจประเมิน และ

4) ความสำเร็จตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

d) ผลตอบกลับจากผู้ที่เกี่ยวข้อง

e) ผลการประเมินความเสี่ยงและสถานะของแผนการจัดการความเสี่ยง และ

f) โอกาสสำหรับการปรับปรุงอย่างต่อเนื่อง

ผลการทบทวนของผู้บริหารต้องรวมการตัดสินใจเกี่ยวกับโอกาสในการปรับปรุงอย่างต่อเนื่องและความจำเป็นสำหรับการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดงผลการทบทวนของผู้บริหาร

ข้อ 7 การปรับปรุง (Improvement)

7.1 ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and corrective action)

เมื่อความไม่สอดคล้องหนึ่งเกิดขึ้น องค์กรต้อง:

a) ตอบกลับต่อความไม่สอดคล้องนั้นตามความเหมาะสม และ:

1) ดำเนินการเพื่อควบคุมและแก้ไขความไม่สอดคล้อง และ

2) จัดการกับผลที่เกิดขึ้น

b) ประเมินความจำเป็นสำหรับการดำเนินการเพื่อขจัดสาเหตุของความไม่สอดคล้องเพื่อให้ไม่เกิดขึ้นซ้ำหรือไม่เกิดขึ้นในที่อื่นโดย:

1) การทบทวนความไม่สอดคล้อง

2) การระบุสาเหตุของความไม่สอดคล้อง และ

3) การระบุว่าความไม่สอดคล้องที่คล้ายกันมีหรือไม่ หรืออาจเป็นไปได้ที่จะเกิดขึ้น

c) ดำเนินการแก้ไขที่จำเป็น

d) ทบทวนความสัมฤทธิ์ผลของการดำเนินการแก้ไขที่ได้ดำเนินการไป และ

e) ทำการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ถ้าจำเป็น

การดำเนินการแก้ไขต้องเหมาะสมต่อผลของความไม่สอดคล้องที่พบ

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดง:

f) สภาพของความไม่สอดคล้องและการดำเนินการใดๆ ที่ได้ดำเนินการไป และ

g) ผลของการดำเนินการแก้ไข

7.2 การปรับปรุงอย่างต่อเนื่อง (Continual improvement)

องค์กรต้องปรับปรุงความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

วัตถุประสงค์ เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

1.1.1 นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)

นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศต้องมีการจัดทำ อนุมัติโดยผู้บริหาร เผยแพร่และสื่อสารให้พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ

1.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security)

นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร เพื่อให้นโยบายมีความเหมาะสม เพียงพอ และได้ผล

2. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)

2.1 โครงสร้างภายในองค์กร (Internal organization)

วัตถุประสงค์ เพื่อให้มีการกำหนดกรอบการบริหารจัดการโดยต้องมีการเริ่มต้นและควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและมอบหมายความรับผิดชอบ

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

หน้าที่และส่วนงานที่รับผิดชอบที่จะทำให้เกิดการขัดต่อการปฏิบัติงานโดยจะทำให้มีการเปลี่ยนแปลงทรัพย์สินขององค์กรหรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกัน เพื่อลดโอกาสการเกิดขึ้นนั้น

2.1.3 การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

การติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้องต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

2.1.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมอาชีพ ต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.1.5 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตามต้องมีการระบุความมั่นคงปลอดภัยสารสนเทศของโครงการนั้น

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

2.2.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาต้องมีการนำมาใช้งานเพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว

2.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)

นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกลต้องมีการนำมาใช้งานเพื่อป้องกันข้อมูลที่มีการเข้าถึง การประมวลผล หรือการจัดเก็บ จากสถานที่ดังกล่าว

3. ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

3.1 ก่อนการจ้างงาน (Prior to employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา

3.1.1 การคัดเลือก (Screening)

การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมายระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

3.1.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

ข้อตกลงและเงื่อนไขในสัญญาจ้างกับพนักงานและผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน ของผู้ที่ทำสัญญาจ้าง และขององค์กร

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

3.2 ระหว่างการจ้างงาน (During employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

3.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ผู้บริหารต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมดรักษาความมั่นคงปลอดภัยสารสนเทศโดยปฏิบัติให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กรที่กำหนดไว้

3.2.2 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)

พนักงานขององค์กรทั้งหมดและผู้ที่ทำสัญญาจ้างที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก ให้ความรู้ และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการเรียนรู้และทบทวนเพิ่มเติมในนโยบายและขั้นตอนปฏิบัติขององค์กรที่เกี่ยวข้องกับงานที่ตนเองปฏิบัติ

3.2.3 กระบวนการทางวินัย (Disciplinary process)

กระบวนการทางวินัยต้องมีการกำหนดอย่างเป็นทางการและมีการสื่อสารให้พนักงานได้รับทราบ เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์ เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

3.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)

หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่ยังต้องคงไว้หลังการสิ้นสุดหรือเปลี่ยนการจ้างงาน ต้องมีการกำหนดและสื่อสารให้ได้รับทราบต่อพนักงานหรือผู้ที่ทำสัญญาจ้าง รวมทั้งควบคุมให้ปฏิบัติตามอย่างสอดคล้อง

4. การบริหารจัดการทรัพย์สิน (Asset Management)

4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

วัตถุประสงค์ เพื่อให้มีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

4.1.1 บัญชีทรัพย์สิน (Inventory of assets)

ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องมีการระบุ จัดทำเป็นทะเบียนทรัพย์สิน และปรับปรุงให้ทันสมัย

4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of assets)

ทรัพย์สินในทะเบียนทรัพย์สินต้องมีผู้ถือครองทรัพย์สิน

4.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

กฎเกณฑ์การใช้อย่างเหมาะสมสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการระบุ จัดทำเป็นลายลักษณ์อักษร และบังคับใช้ให้เป็นไปอย่างสอดคล้อง

4.1.4 การคืนทรัพย์สิน (Return of assets)

พนักงานและลูกจ้างของหน่วยงานภายนอกทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง

4.2 การจัดชั้นความลับของสารสนเทศ (Information classification)

วัตถุประสงค์ เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

4.2.1 ชั้นความลับของสารสนเทศ (Classification of information)

สารสนเทศต้องมีการจัดชั้นความลับโดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

4.2.2 การบ่งชี้สารสนเทศ (Labeling of information)

ขั้นตอนปฏิบัติสำหรับการบ่งชี้สารสนเทศต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

4.2.3 การจัดการทรัพย์สิน (Handling of assets)

ขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สินต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

วัตถุประสงค์ เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการกับสื่อบันทึกข้อมูลที่ถอดแยกได้ต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media)

สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ

4.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)

สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

5. การควบคุมการเข้าถึง (Access Control)

5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

วัตถุประสงค์ เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

5.1.1 นโยบายควบคุมการเข้าถึง (Access control policy)

นโยบายควบคุมการเข้าถึงต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร และทบทวนตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

5.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

วัตถุประสงค์ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

5.2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

กระบวนการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการให้สิทธิการเข้าถึง

5.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)

กระบวนการจัดการสิทธิการเข้าถึงของผู้ใช้งานต้องมีการปฏิบัติตาม ทั้งให้และถอดถอนสิทธิการเข้าถึงสำหรับผู้ใช้งานทุกประเภทและทุกระบบและบริการทั้งหมดขององค์กร

5.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

การให้และใช้สิทธิการเข้าถึงตามระดับสิทธิต้องมีการจำกัดและควบคุม

5.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)

การมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ ต้องมีการควบคุมโดยผ่านกระบวนการบริหารจัดการที่เป็นทางการ

5.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้

5.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

5.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information)

ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ

5.4 การควบคุมการเข้าถึงระบบ (System and application access control)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

5.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

5.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

กรณีมีการกำหนดโดยนโยบายควบคุมการเข้าถึง การเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)

ระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ

5.4.4 การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

5.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

การเข้าถึงซอร์สโค้ดของโปรแกรมต้องมีการจำกัดและควบคุม

6. การเข้ารหัสข้อมูล (Cryptography)

6.1 มาตรการเข้ารหัสข้อมูล (Cryptographic controls)

วัตถุประสงค์ เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

6.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

นโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศต้องมีการจัดทำและปฏิบัติตาม

6.1.2 การบริหารจัดการกุญแจ (Key management)

นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ

7. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)

7.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

7.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

ขอบเขตหรือบริเวณโดยรอบพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการกำหนดขึ้นมาเพื่อใช้ในการป้องกันพื้นที่สำคัญดังกล่าวอันประกอบไปด้วยสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศที่มีความสำคัญ

7.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการป้องกันโดยมีการควบคุมการเข้าออกอย่างเหมาะสม โดยกำหนดให้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถเข้าถึงพื้นที่สำคัญได้

7.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)

ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอุปกรณ์ต่างๆ ต้องมีการออกแบบและดำเนินการ

7.1.4 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external end environmental threats)

การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ

7.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

ขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการจัดทำและปฏิบัติตาม

7.1.6 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

จุดหรือบริเวณที่สามารถเข้าถึงองค์กร เช่น พื้นที่สำหรับรับส่งสิ่งของ บริเวณอื่นๆ ที่ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่ขององค์กรได้ ต้องมีการควบคุม และหากเป็นไปได้ จุดหรือบริเวณ

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

ดังกล่าวควรแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

7.2 อุปกรณ์ (Equipment)

วัตถุประสงค์ เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สินและป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

7.2.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

อุปกรณ์ต้องมีการจัดตั้งและป้องกันเพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายด้านสภาพแวดล้อม และจากโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

7.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

อุปกรณ์ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่นๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ

7.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

การเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งส่งข้อมูลหรือสนับสนุนบริการสารสนเทศต้องมีการป้องกันจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย

7.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้องเพื่อให้มีสภาพความพร้อมใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง

7.2.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of assets)

อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ ต้องไม่มีการนำออกนอกสำนักงาน โดยปราศจากการขออนุญาตก่อน

7.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off- premises)

ทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยโดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกสำนักงาน

7.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องมีการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์ หรือก่อนการนำอุปกรณ์ไปใช้งานอย่างอื่น

7.2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)

ผู้ใช้งานต้องมีการป้องกันอุปกรณ์อย่างเหมาะสม ซึ่งเป็นอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล

7.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

นโยบาย 'โต๊ะทำงานปลอดเอกสารสำคัญ' เพื่อป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และนโยบาย 'การป้องกันหน้าจอคอมพิวเตอร์' เพื่อป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการนำมาใช้งาน (เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร

8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

วัตถุประสงค์ เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

8.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

ขั้นตอนการปฏิบัติงานต้องมีการจัดทำเป็นลายลักษณ์อักษรและต้องสามารถเข้าถึงได้โดยผู้ที่จำเป็นต้องใช้งาน

8.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)

การเปลี่ยนแปลงต่อองค์กร กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลสารสนเทศ และระบบที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศ ต้องมีการควบคุมการดำเนินการ

8.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

การใช้ทรัพยากรของระบบต้องมีการติดตาม ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ

8.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกันเพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

8.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์ เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

8.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

8.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์ เพื่อป้องกันการสูญหายของข้อมูล

8.3.1 การสำรองข้อมูล (Information backup)

ข้อมูลสำรองสำหรับสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการดำเนินการสำรองไว้และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้

8.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์ เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

8.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)

ข้อมูลล็อกแสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บ และทบทวนอย่างสม่ำเสมอ

8.4.2 การป้องกันข้อมูลล็อก (Protection of log information)

อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต

8.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อก ข้อมูลดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ

8.4.4 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

นาฬิกาของระบบที่เกี่ยวข้องทั้งหมดภายในองค์กรหรือในขอบเขตหนึ่ง ต้องมีการตั้งให้ตรงและถูกต้องเทียบกับแหล่งอ้างอิงเวลาแห่งหนึ่ง

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

วัตถุประสงค์ เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

8.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

ขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมีการปฏิบัติตามให้สอดคล้อง

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์ เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้งานต้องมีการติดตามอย่างทันกาล จุดอ่อนต่อช่องโหว่ดังกล่าวขององค์กรต้องมีการประเมิน และมาตรการที่เหมาะสมต้องถูกนำมาใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง

8.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

กฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม

8.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

วัตถุประสงค์ เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ

8.7.1 มาตรการการตรวจประเมินระบบ (Information systems audit controls)

ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการต้องมีการวางแผนและตกลงร่วมกันอย่างระมัดระวังเพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ

9. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

9.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

วัตถุประสงค์ เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ

9.1.1 มาตรการเครือข่าย (Network controls)

เครือข่ายต้องมีการบริหารจัดการและควบคุมเพื่อป้องกันสารสนเทศในระบบต่างๆ

9.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าบริการเหล่านี้จะมีการให้บริการโดยองค์กรเองหรือจ้างการให้บริการก็ตาม

9.1.3 การแบ่งแยกเครือข่าย (Segregation in networks)

กลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบ ต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด

9.2 การถ่ายโอนสารสนเทศ (Information transfer)

วัตถุประสงค์ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

9.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

นโยบาย ขั้นตอนปฏิบัติ และมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการต้องมีการปฏิบัติเพื่อป้องกันสารสนเทศที่มีการถ่ายโอน โดยผ่านทางการใช้อุปกรณ์การสื่อสารทุกประเภท

9.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

ข้อตกลงสำหรับการถ่ายโอนสารสนเทศทางธุรกิจให้มีความมั่นคงปลอดภัยต้องมีการระบุระหว่างองค์กรกับหน่วยงานภายนอก

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

9.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)

สารสนเทศที่เกี่ยวข้องกับการส่งข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม

9.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

ความต้องการในการรักษาความลับหรือการไม่เปิดเผยความลับซึ่งสะท้อนถึงความจำเป็นขององค์กรในการป้องกันสารสนเทศ ต้องมีการระบุ ทบทวนอย่างสม่ำเสมอ และบันทึกไว้อย่างเป็นลายลักษณ์อักษร

10. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

10.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

10.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification)

ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องมีการรวมเข้ากับความต้องการสำหรับระบบใหม่หรือการปรับปรุงระบบที่มีอยู่แล้ว

10.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันจากการฉ้อโกง การโต้เถียง และการเปิดเผยและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต

10.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

10.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

10.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการพัฒนาระบบขององค์กร

10.2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change control procedures)

การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบต้องมีการควบคุมโดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ

10.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบสำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร

10.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

การเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปต้องไม่อนุญาตการดำเนินการ จำกัดการเปลี่ยนแปลงเท่าที่จำเป็น และต้องมีการควบคุมอย่างรัดกุม

10.2.5 หลักการวิศวะกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

หลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัยต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร ปรับปรุงอย่างต่อเนื่อง และประยุกต์กับงานการพัฒนาระบบ

10.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

องค์กรต้องจัดทำและป้องกันอย่างเหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

10.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

องค์กรต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ

10.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่ระบบอยู่ในช่วงการพัฒนา

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

10.2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

แผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการจัดทำสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชั่นใหม่

10.3 ข้อมูลสำหรับการทดทดสอบ (Test data)

วัตถุประสงค์ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

10.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

ข้อมูลสำหรับการทดสอบระบบต้องมีการคัดเลือกอย่างระมัดระวัง มีการป้องกัน และควบคุมการนำมาใช้งาน

11. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

11.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)

วัตถุประสงค์ เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

11.1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินขององค์กรโดยผู้ให้บริการภายนอก ต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอก และจัดทำเป็นลายลักษณ์อักษร

11.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการโครงสร้างพื้นฐานของระบบสำหรับ สารสนเทศขององค์กรโดยผู้ให้บริการภายนอก

11.1.3 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

ข้อตกลงกับผู้ให้บริการภายนอกต้องรวมความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

11.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์ เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

11.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services)

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

องค์กรต้องมีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

11.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)

การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอก รวมทั้งการปรับปรุงนโยบาย ขั้นตอนปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบัน ต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ ระบบ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องทบทวนการประเมินความเสี่ยงใหม่

12. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

12.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการต้องมีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

12.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

12.1.3 การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)

พนักงานและผู้ที่ทำสัญญาจ้างซึ่งใช้ระบบและบริการสารสนเทศขององค์กรต้องสังเกตและรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศในระบบหรือบริการที่สังเกตพบหรือที่สงสัย

12.1.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

12.1.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

12.1.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องถูกนำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

12.1.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)

องค์กรต้องกำหนดและประยุกต์ใช้ขั้นตอนปฏิบัติสำหรับการระบุ การรวบรวม การจัดหาและการจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐาน

13. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

13.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศและด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติหนึ่ง

13.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)

องค์กรต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุง กระบวนการ ขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

13.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมการไว้ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้องและได้ผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

13.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์ เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

13.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

14. ความสอดคล้อง (Compliance)

14.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

วัตถุประสงค์ เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และที่เป็นความต้องการด้านความมั่นคงปลอดภัย

14.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)

ความต้องการทั้งหมดที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง รวมทั้งวิธีการขององค์กรเพื่อให้สอดคล้องกับความต้องการดังกล่าว ต้องมีการระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัย สำหรับแต่ละระบบและสำหรับองค์กร

14.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

ขั้นตอนปฏิบัติที่เหมาะสมต้องได้รับการปฏิบัติอย่างสอดคล้อง เพื่อให้มั่นใจว่ามีความสอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง ที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์

14.1.3 การป้องกันข้อมูล (Protection of records)

ข้อมูลขององค์กรต้องได้รับการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่โดยไม่ได้รับอนุญาต โดยต้องสอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง และความต้องการทางธุรกิจ

14.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)

ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลต้องมีการดำเนินการให้สอดคล้องกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา

14.1.5 ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic controls)

มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับทั้งหมดที่เกี่ยวข้อง

14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

วัตถุประสงค์ เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

14.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติขององค์กร (กล่าวคือ วัตถุประสงค์ มาตรการ นโยบาย กระบวนการ และขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัยสารสนเทศ) ต้องมีการทบทวนอย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงองค์กรที่มากเกิดขึ้น

14.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

ผู้จัดการต้องดำเนินการทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลสารสนเทศและขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบาย มาตรฐาน และความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

14.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

ระบบต้องได้รับการทบทวนอย่างสม่ำเสมอเพื่อพิจารณาความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

บริษัท ที-เน็ต จำกัด จัดทำเอกสารเผยแพร่ฉบับนี้มีจุดประสงค์เพื่อใช้ในการศึกษา ค้นคว้า และวิจัยพัฒนา