กรมการขนส่งทางราง
Department of Rail Transport

มขร. - X – 00X – 256X

มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง

CYBER-SECURITY IN RAILWAY

กองมาตรฐานความปลอดภัยและบำรุงทาง

514/1 Lan Luang Road, Dusit, Bangkok, Thailand 10300
http://www.drt.go.th/
Facebook/DRT.OfficialFanpage

มขร – S – 002 – 2564

มาตรฐานความปลอดภัยไซเบอร์ในระบบราง
(Cyber-security in Railway)

1. บทนำ

1.1 วัตถุประสงค์

สหภาพรถไฟระหว่างประเทศ (UIC) ได้จัดทำเอกสารบังคับใช้เล่มนี้ขึ้นเพื่อเป็นแนวทางเฉพาะในด้าน 'ระบบราง' โดยมีจุดประสงค์หลักคือเพื่อการลดความเสี่ยงจากการโจมตีทางไซเบอร์ในอุตสาหกรรมระบบราง และเพื่อรับรองความพร้อมในการใช้งาน ความมั่นคง การรักษาความลับของระบบรถไฟและข้อมูลตลอดอายุการใช้ของเครือข่าย

เอกสารนี้มีเนื้อหาเน้นในเรื่องที่การส่งสัญญาณและการสื่อสารโทรคมนาคมภายในทางระบบราง และแนวทางในการ "ออกแบบระบบ" อธิบายวิธีการประเมินความปลอดภัยผ่าน ISO 27001 และควรนำแนวทางปฏิบัติที่ดีที่สุดที่ใช้ในอุตสาหกรรมอื่น ๆ เช่น การบิน พลังงานนิวเคลียร์ และการทหาร มาปรับใช้

ISO 27001 เป็นมาตรฐานความปลอดภัยของข้อมูล อธิบายการควบคุมที่องค์กรจำเป็นต้องนำมาประยุกต์ใช้ เพื่อรองรับความเสี่ยงที่อาจเกิดขึ้นและการจัดการความปลอดภัยของข้อมูลเชื่อมโยงกับการดำเนินการของระบบการจัดการความปลอดภัยของข้อมูล (ISMS) เสมอ เพื่อเป็นการรักษาความปลอดภัยและรักษาสภาพของข้อมูลทางระบบราง

ในการนำมาตรฐานนี้ไปปฏิบัติใช้ ผู้อ่านควรมีความเชี่ยวชาญในเรื่องระเบียบวิธีทางโครงสร้างความปลอดภัย และมีความคุ้นเคยกับเกณฑ์ที่ใช้อ้างอิงในมาตรฐานนี้ องค์กรต่างๆ ที่นำแนวทางของระบบการจัดการความปลอดภัยของข้อมูลนี้ไปปรับใช้จะได้รับประโยชน์เป็นอย่างยิ่ง จากข้อเท็จจริงที่ว่า ระบบการจัดการความปลอดภัยของข้อมูล (ISMS) ได้รับการรับรองถึงความน่าเชื่อถือจากหลายองค์กรในด้านการจัดการความปลอดภัยข้อมูลขององค์กร จากองค์กรภายนอกซึ่งข้อได้เปรียบหลักคือ ระบบจะช่วยหลีกเลี่ยงระบบสัญญาณที่ไม่สามารถใช้งานได้ รวมไปถึงจะช่วยป้องกันการกระทำที่ขัดต่อความปลอดภัยของฐานข้อมูลอีกด้วย

การพัฒนาอย่างรวดเร็วของเทคโนโลยีเครือข่าย บังคับให้ระบบรางจำเป็นต้องมีการนำเรื่องการส่งสัญญาณในเครือข่ายแบบเปิด รวมถึงในเครือข่ายสาธารณะมาปรับใช้มากขึ้นเรื่อยๆ เนื้อหานี้มีการแนะนำแนวทางใหม่ ๆ รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นและความพร้อมในการใช้งานเครือข่ายโดยเฉพาะอย่างยิ่งหากมีการใช้งานร่วมกับระบบเปิดอื่น ๆ ซึ่งมีความจำเป็นต้องรักษาประสิทธิภาพ ในการใช้งานและความปลอดภัยของระบบ

ดังนั้นจึงมีความจำเป็นอย่างยิ่งที่ต้องจัดให้มีการบริการระบบรางที่มีความปลอดภัย เชื่อถือได้ และที่มีประสิทธิภาพอย่างต่อเนื่องใน ขณะที่เราเผชิญกับการภัยคุกคามทางไซเบอร์ซึ่งมีการพัฒนาอยู่ตลอดเวลา รวมถึงสภานการณ์ปัจจุบันที่ความก้าวหน้าของระบบราง มีการเปลี่ยนไปเป็นระบบดิจิทัลอย่างหลีกเลี่ยงไม่ได้ เราจึงต้องดำเนินการร่วมกันเพื่อปกป้องโลกไซเบอร์แก่ระบบรางของเรา

1.2 ขอบข่าย

ขอบเขตของความปลอดภัยทางไซเบอร์ในระบบรางมีเนื้อหาครอบคลุมในหลายด้าน เช่น ระบบบังคับสัมพันธ์ การควบคุมความเร็ว (ATP), การจัดการการจราจร (ATS), การขับขี่อัตโนมัติ (ATO), SCADA, การระบายอากาศ, การติดตามตรวจสอบแบบระยะไกลและการตรวจตรา, การบริหารของระบบราง, การสื่อสารสำหรับโครงสร้างพื้นฐาน เป็นต้น

การรวมกันอย่างต่อเนื่องของระบบไอทีที่ใช้ในระบบการส่งสัญญาณที่สำคัญ บูรณาการกับการกำหนดเครือข่าย IP ทั่วโลกด้วย ด้วยแนวคิดแบบใหม่ (ในเชิงการสื่อสาร) คือ "การเชื่อมต่อกันทั้วโลก" ซึ่งถือเป็นประโยชน์อย่างยิ่งสำหรับการส่งสัญญาณในระบบราง รวมถึงสามารถควบคุมความเสี่ยงด้านการรักษาความปลอดภัยที่อาจเกิดขึ้นใหม่ด้วย

การใช้งานเครือข่าย IP ในระบบส่งสัญญาณที่สำคัญซึ่ง หมายถึง การใช้เครือข่ายแบบสาธารณะ (open networks) ประกอบด้วยเหตุผลหลักสองประการ:

1) ใช้ในการป้องกันด้วยโปรโตคอลและอุปกรณ์เชิงพาณิชย์ที่มีการใช้จนถึงปัจจุบัน ซึ่งการป้องกันดังกล่าวขึ้นอยู่กับความคลุมเครือของเทคโนโลยี

2) ใช้ในการขยายเครือข่าย - ตามขนาดประเทศ – โดยถูกกระจายไปตามระบบรางและจุดติดตั้งอุปกรณ์หลายจุดซึ่งช่วยให้เข้าถึงเครือข่ายเหล่านี้ได้ง่ายขึ้น

ปัจจัยหลักในการกำหนดความปลอดภัยทางไซเบอร์ของระบบราง ได้แก่ :

- ระบบอัตโนมัติของกระบวนการทางเทคโนโลยีในภาคการขนส่ง
- การสร้างระบบใหม่เพื่อความปลอดภัยในการขนส่ง
- ปริมาณข้อมูลที่เพิ่มขึ้นถูกถ่ายโอนผ่านช่องทางเปิด
- อัตราการเพิ่มขึ้นของอาชญากรรมที่เกี่ยวข้องกับระบบอัตโนมัติ

1.3 ระเบียบปฏิบัติ

จำเป็นต้องมีการร่วมมือกับหน่วยงานเพื่อทำความเข้าใจ ถ่ายทอด และนำมาตรการไปใช้อย่างมีประสิทธิภาพ เนื่องจากการป้องกันภัยคุกคามมีความสำคัญโดยเฉพาะในด้านอาณัติสัญญาณ ซึ่งเป็นความสำคัญลำดับต้นๆ ในเรื่องความวิพากษ์โดยซึ่งปฏิบัติตาม ข้อกำหนดของยุโรป: การใช้ระบบรางร่วมกันในพื้นที่ยุโรป (European requirement: The Single European Railway Area)

1.4 ผู้อ่าน

มาตรฐานนี้ใช้กับ RTOs เป็นหลัก และใช้ได้กับซัพพลายเออร์ ผู้รับเหมา และผู้รับเหมาซ่อมบำรุง ซึ่งจะต้องตระหนักถึงการเปลี่ยนแปลงในอุตสาหกรรมนั้น ๆ ที่ปฏิบัติงานอยู่ด้วย

มาตรฐานนี้เขียนขึ้นเพื่อใช้โดยวิศวกรระบบดิจิทัลหรือสถาปนิกด้านความปลอดภัยที่มีความรู้โดยละเอียดเกี่ยวกับระบบบังคับสัมพันธ์ การออกแบบระบบที่สำคัญ และความปลอดภัยภัยทางไซเบอร์ โดยคาดว่าผู้อ่านคุ้นเคยกับองค์ความรู้ด้านความปลอดภัยของข้อมูลอยู่แล้ว

1.5 แนวคิดพื้นฐาน

เอกสารนี้ถูกดัดแปลงจากมาตรฐานสากล ซีรีส์ IS0 27000 (อ้างอิงตามข้อ 1.6) และมีวัตถุประสงค์ในด้านความปลอดภัยของการส่งสัญญาณและการสื่อสารโทรคมนาคมของระบบราง

การรักษาความปลอดภัยของระบบรางดังกล่าวจะบรรลุได้โดยการปฏิบัติตามข้อกำหนด ดังนี้:

- คำว่า "ต้อง" ที่ใช้ในเอกสารนี้ถูกใช้เพื่อบ่งชี้ข้อกำหนดที่บังคับ
- คำว่า "ควร" ใช้เพื่อบ่งชี้ข้อควรปฏิบัติหรือคำแนะนำในการดำเนินการที่เกี่ยวข้องในการวางแผนด้านเทคนิคและองค์กร

กรณีที่ข้อกำหนดถูกยกเลิกจะมีการตรวจสอบย้อนกลับ การสืบแหล่งที่มาจะได้รับการจัดการเมื่อข้อกำหนดไม่ได้รับการยอมรับ ผู้อ่านควรศึกษาคู่มือโดยการข้อแนะนำสำหรับการอ่านอย่างยิ่งในการอ่านส่วนหนึ่งจากทั้งหมด

1.6 เอกสารอ้างอิง

[1] ISO / IEC 27000-series: ประกอบด้วยข้อมูลและมาตรฐานความปลอดภัยที่เผยแพร่ร่วมกันโดยองค์การระหว่างประเทศเพื่อการมาตรฐาน (ISO) และ International Electro-คณะกรรมการเทคนิค (IEC)

[2] IEC-62443: ความปลอดภัยสำหรับระบบอัตโนมัติทางอุตสาหกรรมและระบบควบคุม

[3] EN 50126: การใช้งานระบบราง – ข้อกำหนดและการสาธิตความน่าเชื่อถือ ความพร้อมใช้งาน การบำรุงรักษา และความปลอดภัย (RAMS)

[4] EN 50128: การใช้งานระบบราง – ระบบสื่อสาร การส่งสัญญาณ และการประมวลผล

[5] EN 50129: การใช้งานระบบราง – ระบบสื่อสาร การส่งสัญญาณ และการประมวลผล -ระบบอิเล็กทรอนิกส์ที่เกี่ยวข้องกับความปลอดภัยในการส่งสัญญาณ

[6] EN 50159: การใช้งานระบบราง ระบบการสื่อสาร การส่งสัญญาณและการประมวลผลการสื่อสารที่เกี่ยวข้องกับความปลอดภัยในระบบส่งกำลัง

[7] วิธีการจำแนกประเภทและมาตรการสำคัญ - ความปลอดภัยทางไซเบอร์ในระบบควบคุมอุตสาหกรรม ANSSI

[8] วัดโดยละเอียด: ความปลอดภัยทางไซเบอร์ของระบบควบคุมอุตสาหกรรม ANSSI

[9] APTA-SS-CCS-RP-002-13 – การกำหนดสถาปัตยกรรมของพื้นที่ปลอดภัยในการขนส่งทางรางและการป้องกันพื้นที่สำคัญ

[10] STO RZD 02.049-2014 – ระบบควบคุมอัตโนมัติของกระบวนการปฏิบัติงานและสิ่งอำนวยความสะดวกด้านเทคนิคระบบราง

1.7 คำศัพท์

ภาคผนวก 4.1

Cyber Attack (การโจมตีทางไซเบอร์): หมายถึง ความพยายามที่จะทำลาย เปิดโปงเปลี่ยนแปลง ปิดใช้งานขโมย การเข้าถึงโดย หรือเข้าใช้ระบบควบคุมหรือระบบเสริมที่ใช้ในการทำงานของระบบราง โดยไม่ได้รับอนุญาต

Cyber Security Risk (ความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์): หมายถึงผลที่อาจจะเกิดขึ้นจากภัยคุกคามโดยใช้ช่องโหว่ของระบบรวมถึงที่ตามมาผลกระทบที่เกิดจากเหตุการณ์ไม่พึงประสงค์นั้นต่อองค์กร

Cyber Threat (ภัยคุกคามทางไซเบอร์): หมายถึง การกระทำที่เป็นภัยต่อพื้นที่เครือข่ายไซเบอร์ ซึ่งเกิดขึ้นได้ทั้งภายในเครือข่ายและภายนอกเครือข่ายหรือเป็นการกระทำที่ต่อต้านระบบและองค์ประกอบพื้นฐานของระบบนั้นๆ โดยที่การกระทำเหล่านี้อาจเกิดขึ้นได้ทันทีหรือมีการพัฒนาล่วงหน้าไว้แล้ว

Vulnerability (ช่องโหว่): หมายถึง จุดอ่อนที่เกิดขึ้นในระบบ การทำงานของระบบ และมาตรการความปลอดภัยหรือการใช้งานที่ภัยคุกคามสามารถใช้ประโยชน์เพื่อก่อกวนระบบความปลอดภัยของระบบไซเบอร์ ช่องโหว่อาจเกิดขึ้นได้จากหลายแหล่งที่มา ได้แก่: การขาดการฝึกอบรมและการตระหนักรู้ในเรื่องของนโยบายและขั้นตอนการปฏิบัติ สถาปัตยกรรมและการออกแบบ การกำหนดค่าและการบำรุงรักษา การบุกรุกทางกายภาพ ซอฟต์แวร์ระบบและการพัฒนาผลิตภัณฑ์การสื่อสารและเครือข่าย

Rail Control System (ระบบควบคุมราง): ระบบใด ๆ (แอปพลิเคชันอุปกรณ์หรือเครือข่าย) ที่ควบคุมการทำงานของรถไฟหรือทางรถไฟ ซึ่งรวมถึงการส่งสัญญาณและการสับเปลี่ยนการทำงานของรถจักรหรือรถไฟทุกรูปแบบ (ทั้งแบบอิสระหรือผ่านผู้ให้บริการ), ระบบสื่อสารระบบราง, การจัดการผู้โดยสาร , การถอนกำลังหรือการข้ามระดับ)

2. ระบบการจัดการ (Governance)

บทนี้มีเนื้อหาอ้างอิงตามมาตรฐาน IS0 27001 ซึ่งเกี่ยวข้องกับการจัดการความปลอดภัยของข้อมูล อย่างไรก็ดี บางข้อปฏิบัติจะต้องพิจารณาคุณลักษณะเฉพาะของระบบการป้องกันภัยทางไซเบอร์ของระบบรางด้วย

เช่นเดียวกับการจัดทำระบบการจัดการความปลอดภัยของข้อมูล (ISMS) อย่างละเอียด ซึ่งจำเป็นต้องมีการพัฒนาระบบการจัดการความปลอดภัยสำหรับระบบป้องกันภัยทางไซเบอร์ของระบบราง

ระบบการจัดการความปลอดภัย SMS นี้เป็นวิธีการที่เป็นระบบ โดยมีเป้าหมายในการกำหนด การใช้งาน การปฏิบัติงาน การติดตามผลการตรวจสอบ การปรับปรุงและการพัฒนาความปลอดภัยทางไซเบอร์ของระบบราง เพื่อให้บรรลุวัตถุประสงค์ขององค์กร โดยขึ้นอยู่กับการจัดการความเสี่ยงและกระบวนการแก้ไขปัญหาในการป้องกันข้อมูลในโลกไซเบอร์

แนวทางเหล่านี้ถูกรวมอยู่ในรูปของการวางแผน ปฏิบัติ ตรวจสอบ และดำเนินการ ดังนี้:

ก) วางแผน – กำหนดนโยบายและวัตถุประสงค์ที่เกี่ยวข้องกับการจัดการความเสี่ยง และการปรับปรุงข้อมูล การรักษาความปลอดภัย และการวางแผน (วิเคราะห์เงื่อนไขขององค์กร กำหนดวัตถุประสงค์โดยรวม และกำหนดเป้าหมายและพัฒนาแผนเพื่อบรรลุเป้าหมาย)

ข) ปฏิบัติ - ดำเนินการตามแผน (ทำในสิ่งที่วางแผนไว้ว่าจะทำ)

ค) ตรวจสอบ - วัดผล (วัด / ติดตามผลลัพธ์ที่สำเร็จตามแผนที่วางไว้)

ง) ดำเนินการ - แก้ไขและปรับปรุงกิจกรรม (เรียนรู้จากข้อผิดพลาดเพื่อปรับปรุงกิจกรรม เพื่อให้บรรลุผลลัพธ์ที่ดียิ่งขึ้น)

2.1 บริบทของการรักษาความปลอดภัยทางไซเบอร์ในระบบราง (Context of the Cybersecurity organization in railway)

เป็นเวลาหลายปีที่อุตสาหกรรมระบบรางได้ดำเนินการหาวิธีการที่ปลอดภัยที่สุดเท่าที่จะเป็นไปได้ในการออกแบบและการทำงานของระบบราง โดยมีกระบวนการ ขั้นตอน และการออกแบบมากมายที่ช่วยให้ระบบปลอดภัยยิ่งขึ้น ตัวอย่างเช่น แนวทางการออกแบบ กระบวนการควบคุมการพัฒนา กระบวนการทดสอบและมาตรการบังคับ ฯลฯ

การเกิดขึ้นของเทคโนโลยีใหม่ ๆ รวมถึงการเติบโตอย่างรวดเร็วของระบบเครือข่ายจะทำให้เกิดทั้งผลดีต่อระบบ – และก่อให้เกิดภัยคุกคามในรูปแบบใหม่ ๆ ที่แตกต่างกัน ในขณะเดียวกัน

ระบบควบคุมรถไฟเป็นระบบป้องกันสองระดับ โดยมีทรัพย์สินที่ควรได้รับการปกป้องในแต่ละระดับดังนี้:

- ระดับโครงสร้างข้อมูล :
  - เครือข่ายข้อมูล
  - ระบบข้อมูล
  - ทรัพยากรสารสนเทศ
  - อุปกรณ์โทรคมนาคมและอุปกรณ์สำหรับเครือข่าย
- ระดับการควบคุมการจราจร :
  - ระบบควบคุมรถไฟอัตโนมัติ (ระบบควบคุมรถไฟจากส่วนกลางและระบบอิเล็กทรอนิกส์)
  - ระบบอัตโนมัติทางรถไฟและอุปกรณ์ telemechanics (การส่งสัญญาณและการเชื่อมต่อกับอุปกรณ์ในส่วนรถไฟและสถานี)

- ระบบอัตโนมัติสำหรับการควบคุมการเคลื่อนที่ของรถไฟ (ระบบปฏิบัติการรถไฟอัตโนมัติ, อุปกรณ์รักษาความปลอดภัยหัวรถจักร)

2.1.1 ความท้าทาย

ในช่วงสองทศวรรษที่ผ่านมาภัยคุกคามรูปแบบใหม่ได้ก่อให้เกิด "กิจกรรมทางไซเบอร์ที่เป็นอันตราย" ซึ่งถือว่าเป็นข้อกังวลในเรื่องของการรักษาความปลอดภัยของระบบไซเบอร์ แต่จากการพัฒนาล่าสุดเห็นได้ชัดว่า การรักษาความมั่งคงมีอิทธิพลโดยตรงต่อความปลอดภัยของระบบไซเบอร์

โดยสามารถศึกษาได้จากศักยภาพของกิจกรรมทางไซเบอร์ที่ส่งผลกระทบต่อโลกทางกายภาพ (ตัวอย่างเช่น ไวรัส Stuxnet) โดยที่ภัยคุกคามประเภทนี้สามารถเกิดขึ้นได้ในกิจการทางราง ในลักษณะเช่น การปิดการใช้งานระบบเบรก หรือเข้าควบคุม OBU และการเรียกค่าไถ่เพื่อให้ระบบสามารถกลับมาใช้งานได้ปกติ

ซึ่งระบบสำคัญเหล่านี้โดยเฉพาะอย่างยิ่งในการส่งสัญญาณและการสื่อสารโทรคมนาคมภายในระบบรางมีการเข้าถึงมากขึ้น ดังนั้นจึงสามารถถูกโจมตีได้ง่ายจากภายนอก

ความท้าทายคือการตระหนักถึงปัจจัยความเป็นไปได้ทั้งหมด เพื่อนำมาออกแบบวิธีการรักษาความปลอดภัยที่มีประสิทธิภาพ

2.1.2 การรักษาความมั่นคงและความปลอดภัย (Security and safety)

ปัญหาด้านความปลอดภัยของไอทีเกิดขึ้น จากการคุกคามต่อความมั่นคงของระบบไอที การคุกคามเหล่านี้เกิดขึ้นจากผู้โจมตี ซึ่งจงใจโจมตีโดยใช้ข้อมูลทั้งหมดเกี่ยวกับระบบที่พวกเขามีขึ้นอยู่กับความสามารถในการโจมหรือการแฮ็ก รวมถึงระดับการโจมตีอาจจะมีความแตกต่างขึ้นอยู่กับผู้โจมตีระบบ

ในสถานการณ์เฉพาะนี้มีการแบ่งสัดส่วนในการทำงานเพื่อเพิ่มประสิทธิภาพของความปลอดภัย โดยการเพิ่มบทบาทซึ่งมีเจตนารมณ์และกลยุทธ์ หากถามว่าบทบาทนี้ได้รวมไว้ในการประเมินผลที่น่าจะเป็นไปได้หรือไม่? คำตอบคือไม่ ดังนั้นแบบจำลองความน่าจะเป็นที่คาดไว้ไม่เพียงพอจะสร้างแบบจำลองพฤติกรรมของระบบข้อมูลที่ถูกโจมตีได้

2.1.3 หลักการรักษาความปลอดภัยทางไซเบอร์ในระบบอาณัติสัญญาณและการสื่อสารระบบราง (Cyber security principle in signaling and communication in railway)

หลักการสำคัญของระบบรักษาความปลอดภัยของไซเบอร์ ในระบบการส่งสัญญาณที่สำคัญของเครือข่าย IP มีดังนี้ :

- มีแนวทางการป้องกันหลายระดับ: ควรมีด่านในการป้องกันหลายทางจากทุกภัยคุกคามอย่างยิ่ง ซึ่งแนวทางนี้สามารถเอาชนะภัยคุกคามได้ดีผู้โจมตีจำเป็นต้องที่มีทักษะความสามารถที่เชี่ยวชาญในหลากหลายด้าน
- ควรใช้วิธีแก้ปัญหาที่ได้รับการพิสูจน์แล้วเท่านั้น ซึ่งความเสี่ยงและมาตรการรับมือเหล่านั้นต้องได้ผ่านการทดสอบทางทฤษฎีและทางปฏิบัติอย่างครอบคลุมแล้ว
- การสร้างระบบด้วยส่วนประกอบที่มีความน่าเชื่อถือสูง
- การป้องกันที่ไม่หยุดชะงักทั้งในเรื่องของระยะเวลาหรือพื้นที่ และไม่มีความเป็นไปได้ในการข้ามผ่านระบบป้องกันนี้: ระบบควรได้รับป้องกันตลอดเวลาการทำงาน ควรมีมาตรการเพื่อป้องกันไม่ให้ระบบป้องกันการหยุดทำงาน
- การลดสิทธิพิเศษ: นโยบายความปลอดภัยควรตั้งอยู่บนแนวคิด: "ทุกสิ่งที่ห้ามมีให้ได้รับอนุญาต" พนักงานควรมีการจำกัดสิทธิเฉพาะในเรื่องการปฏิบัติหน้าที่เท่านั้นซึ่งหลักการนี้มีความสำคัญมากในเรื่องบริบท เพราะเกี่ยวข้องกับการเข้าถึงและการเชื่อมต่อของระบบรถไฟ
- การปรับปรุงอย่างต่อเนื่องและไม่หยุดพัฒนา การปรับปรุงอย่างต่อเนื่องของมาตรการและวิธีการป้องกันของทรัพยากรทางไอทีและโครงสร้างพื้นฐาน และขึ้นอยู่กับความต่อเนื่องขององค์กร วิธีการแก้ปัญหาทางเทคนิค บุคลากร และการวิเคราะห์วิธีการทำงานของระบบป้องกัน การตระหนักถึงการพัฒนาหลักการและขั้นตอนในการประมวลผลข้อมูล ข้อกำหนดในการป้องกันข้อมูลและความเชี่ยวชาญในด้านนี้ (V-model)
    - จนถึงตอนนี้ การรักษาความปลอดภัยได้ถูกสร้างขึ้น ด้วยการกำหนดที่ไม่ชัดเจนของระบบเดิม
    - อุปกรณ์ใหม่เป็นฮาร์ดแวร์ที่มีจำหน่ายทั่วไป (COTS) และกรรมสิทธิ์ซอฟต์แวร์เป็นของผู้จำหน่าย
    - สำหรับหุ้นส่วนส่วนใหญ่แล้ว การรักษาความปลอดภัยขึ้นอยู่กับผู้จำหน่าย
    - สำหรับส่วนน้อยมีการตั้งข้อกำจัดสำหรับอุปกรณ์ที่นำเข้า หรือบังคับให้ผู้จำหน่ายระบุคุณลักษณะของระบบ

2.1.4 หลักประกันของระบบราง (คุณลักษณะที่เชื่อถือได้และความปลอดภัย) (Railway Stakes)

ระบบรางทำงานตลอด 24 ชม. และตลอดทั้งปี ดังนั้นความไม่พร้อมในการส่งสัญญาณของระบบที่สำคัญอาจนำไปสู่สถานการณ์ที่ไม่ปลอดภัยได้ เครือข่ายที่สำคัญเป็นเครือข่ายแบบเรียลไทม์ จึงไม่สามารถใช้วิธีแก้ปัญหาบางอย่างแบบเดิมได้ นี่จึงเป็นปัญหาอีกส่วนที่สำคัญสำหรับความปลอดภัยในการส่งสัญญาณ

คุณสมบัติด้านล่างนี้เป็นคุณสมบัติหลักของระบบในด้านวิศวกรรมที่เชื่อถือได้:

- **ความน่าเชื่อถือ** เป็นคุณลักษณะที่สะท้อนถึงความเป็นไปได้ที่ระบบจะให้บริการภายใต้เงื่อนไขที่ระบุไว้ตามระยะเวลาที่กำหนด
- **ความพร้อมใช้งาน** คือ ความสามารถของระบบในการให้บริการจริง กล่าวอีกนัยหนึ่งคือความพร้อมของระบบในการให้บริการที่ถูกต้อง หรือกล่าวอย่างเป็นทางการคือความเป็นไปได้ที่ระบบจะมีความพร้อมใช้งาน โดยที่พร้อมใช้งานในทันทีหรือสามารถระบุเวลาได้

  สิ่งสำคัญสำหรับทั้งสองคุณสมบัติคือ ค่าคาดหมายฟังก์ชันและความหนาแน่นของการซ่อมแซม การประเมินพื้นฐานพื้นฐานของความน่าเชื่อถือคือ MTTF (mean time to failure หรือเวลาเฉลี่ยที่ขัดข้อง) ซึ่งเป็นค่าที่คาดหมายไว้ของฟังก์ชันความหนาแน่นของความล้มเหลว และ MTTR ซึ่งเป็นค่าที่คาดหมายไว้ของฟังก์ชันความหนาแน่นของการซ่อมแซม โดยที่เวลาเฉลี่ยระหว่างความล้มเหลวคือผลรวมของสองสิ่งนี้:

  $$MTBF = MTTF + MTTR$$

  ความพร้อมในการใช้งานหมายถึง ความเป็นไปได้ที่ระบบหรือบริการจะพร้อมใช้งานเมื่อจำเป็น ซึ่งสามารถและคำนวณได้ดังนี้:

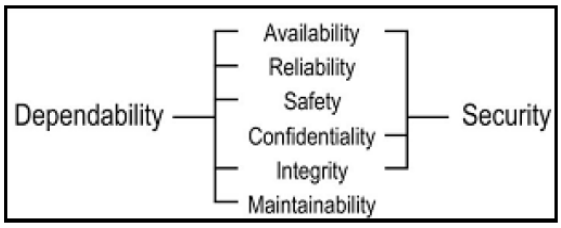
  $$A = \frac{MTTF}{MTBF}$$

  ความน่าเชื่อถือ หมายถึง ความต่อเนื่องของการบริการซึ่งเป็นความน่าจะเป็นที่ระบบหรือบริการยังคงอยู่ใช้งานได้ตามระยะเวลาที่กำหนด:

  $$(t)=Pr[\text{no failure in } [0,t]=1Q(t)$$

  โดยที่ () คือฟังก์ชันการแจกแจงสะสมความล้มเหลว
- **ความมั่นคง** คือ การไม่มีการเปลี่ยนแปลงของระบบอย่างไม่เหมาะสม
- **ความสามารถในการซ่อมบำรุง** หมายถึง คุณสมบัติที่แสดงถึงความสามารถของระบบในการปรับเปลี่ยนและซ่อมแซม
- **ความสามารถในการซ่อมแซม** คือ ความสามารถของอุปกรณ์เครื่องจักรหรือระบบที่เสียหายหรือขัดข้องกลับคืนสู่สภาพการใช้งานที่ยอมรับได้ภายในระยะเวลาที่กำหนด (เวลาซ่อม)
- **ความสามารถในการใช้งาน** คือ ความสามารถในการเก็บรักษาอุปกรณ์ระบบหรือการติดตั้ง ให้อยู่ในสภาพการทำงานที่ปลอดภัยและเชื่อถือได้ตามข้อกำหนดการปฏิบัติงานที่ระบุไว้ล่วงหน้า
- **ประสิทธิภาพในการปฏิบัติงาน** เป็นคุณสมบัติที่จำเป็นของระบบที่มีประสิทธิภาพตามข้อกำหนดการบริการ อ้างอิงตามมาตรการ QoS (คุณภาพของบริการ) อาทิเช่น

ความล่าช้า การประเมินข้อมูลเฉพาะที่มีประโยชน์ และปริมาณข้อมูลที่ส่งจากต้นทาง ประสิทธิภาพในการปฏิบัติงานช่วยอธิบายทฤษฎีของความเชื่อถือได้ดังรูปด้านล่าง



คำศัพท์ในโลกของความปลอดภัยนั้นมีประวัติมากมาย ความปลอดภัยของคอมพิวเตอร์ ความปลอดภัยในการสื่อสาร, ความปลอดภัยของข้อมูล และการประกันข้อมูล ซึ่งเป็นศัพท์ที่มีการพัฒนามายาวนานและใช้ในกลุ่มนักวิจัยและผู้ปฏิบัติงานด้านความปลอดภัย

โดยส่วนใหญ่ไม่มีข้ออ้างอิงโดยตรงถึงความน่าเชื่อถือ อย่างไรก็ตามคำศัพท์เหล่านี้สามารถแบ่งออกในลักษณะของความปลอดภัย 3 ประการ ได้แก่ การรักษาความลับ ความมั่นคง และความพร้อมใช้งาน

คุณสมบัติหลักของความปลอดภัยถูกกำหนดไว้ดังนี้:

- **ความพร้อมใช้งาน** คือ ความพร้อมในการใช้งาน ซึ่งคือความเป็นไปได้ที่ระบบหรือการบริการจะทำงานได้เมื่อจำเป็นต้องใช้งาน
- **ความมั่นคง** คือ ความสามารถของระบบไอทีในการป้องกันไม่ให้เข้าถึงข้อมูล การแก้ไขหรือการลบ โดยไม่ได้รับอนุญาต
- **การรักษาความลับ** คือความสามารถของระบบไอทีในการป้องกันการเปิดเผยข้อมูลไปยังบุคคลที่ไม่ได้รับอนุญาต

2.1.5 ความปลอดภัยในการใช้ประโยชน์และดำเนินงานของระบบขนส่งทางราง

การใช้ประโยชน์และดำเนินงานของระบบขนส่งทางรางประกอบด้วย (ความปลอดภัยของเครือข่าย ความปลอดภัยในการใช้งาน ความปลอดภัยของสัญญาณ) จะต้องได้รับการพิจารณาในขอบข่ายทั้งหมดของตลอดช่วงที่มีการพัฒนา (การออกแบบและสถาปัตยกรรมคอมพิวเตอร์ ...)

ความปลอดภัยในการขนส่งทางรางประกอบด้วยปัจจัยต่างๆ ดังนี้ :

- **<u>ความมั่นคงปลอดภัยของเครือข่าย:</u>** คือ ความปลอดภัยของเครือข่ายในทุกด้านที่เกี่ยวข้องกับการป้องกันเครือข่ายโทรคมนาคมซึ่งทำหน้าที่เป็นผู้ให้บริการข้อมูลของการส่งสัญญาณ ซึ่งเป็นการป้องกันโครงสร้างพื้นฐานของระบบเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานในทางที่ผิด การทำงานที่ผิดปกติ การดัดแปลงแก้ไข การทำลายหรือการเปิดเผยที่ไม่เหมาะ อ้างอิงมาตรฐาน IEC 62443 ซึ่งมีการระบุไว้ว่า การรักษาความปลอดภัยเครือข่ายประกอบด้วย 3 หลักสำคัญ ซึ่งช่วยในการสร้างความปลอดภัย ได้แก่ เทคโนโลยี กระบวนการ และกลุ่มบุคคล โดยมีการกำหนดเทคโนโลยีเป็นชุดทรัพยากรที่ใช้เพื่อรักษาความพร้อมใช้งาน ความมั่นคง และการรักษาความลับหลักต่อไปคือกระบวนการซึ่งกระบวนการนี้เกี่ยวข้องกับการกำหนดแนวทางและมาตรฐานที่นำมาใช้ เพื่อกำหนดขั้นตอนที่ชัดเจนโดยต้องปฏิบัติตามเพื่อให้เกิด

ความมั่นใจในความปลอดภัย และหลักสุดท้ายนั้นคือ กลุ่มคน เรามีการจัดกลุ่มบุคคลตามข้อกำหนดเกี่ยวกับพนักงาน การฝึกอบรมของพนักงาน และการกำหนดบทบาทความรับผิดชอบและการเข้าถึงตามหน้าที่ที่บุคลากรจะนำไปปรับใช้ ซึ่งมีการครอบคลุมถึงระบบการจัดการคนที่ทำงานโดยตรงหรือโดยอ้อมกับอุปกรณ์และเครือข่ายสัญญาณ เช่น สิทธิพิเศษสำหรับบุคคลในการเข้าถึงอุปกรณ์หรือสถานที่ส่งสัญญาณในทางกายภาพหรือทางตรรกศาสตร์ ตลอดจนข้อกำหนดในการจ้างบุคลากรเหล่านี้

- **<u>ความปลอดภัยของสัญญาณ:</u>** ปัจจัยนี้มีความเกี่ยวเนื่องกับเทคนิคและเทคโนโลยีทั้งหมดที่เกี่ยวข้องกับระบบการส่งสัญญาณและกลไกที่ใช้ สำหรับการเผชิญกับการโจมตีหรือความผิดปกติที่อาจเกิดขึ้นได้ (สำหรับข้อมูลเพิ่มเติมสามารถอ่านได้จากหัวข้อ 5.3) ประเด็นเหล่านี้มีความเชื่อมโยงอย่างยิ่งกับปัญหาด้านความปลอดภัย โดยแบ่งออกเป็น 2 กลุ่มกลุ่มที่ 1 จะเกี่ยวข้องกับการวิเคราะห์การทำงานซึ่งเป็นการจัดการภายในเพื่อตรวจสอบ “ความน่าเชื่อถือ” ของข้อความที่ส่งหรือข้อความที่ได้รับ การทดสอบความน่าเชื่อถือสามารถทำได้สองส่วนคือ: การบังคับสัมพันธ์และศูนย์ควบคุม ตัวอย่างเช่น ในกรณีที่คำสั่งที่ส่งออกไปตรงกับลักษณะของสัญญาณในเส้นทางที่กำหนดไว้ล่วงหน้า นอกจากนี้ยังเกี่ยวข้องกับโครงสร้างและสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในระบบอาณัติสัญญาณ (โปรโตคอลเพื่อความปลอดภัย ความมั่นคงปลอดภัย ฯลฯ) กลุ่มที่ 2 คือ ความต่อเนื่องของระบบซึ่งมีความเกี่ยวข้องกับเทคนิคและวิธีการทั้งหมดที่ใช้ เพื่อรับประกันความต่อเนื่องของการบริการในสภาวะที่ไม่เอื้ออำนวย เช่น การทดสอบการบุกรุก ความร่วมมือกับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ ฯลฯ

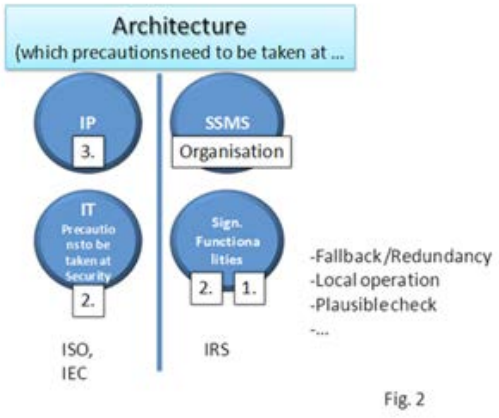


Fig. 2

- **<u>ความปลอดภัยในการปรับใช้:</u>** ปัจจัยเกี่ยวข้องกับขั้นตอนการปฏิบัติงานที่องค์กรนำไปปรับใช้เพื่อจัดการเครือข่ายของสัญญาณและอุปกรณ์ และครอบคลุมในอีกแง่หนึ่งซึ่งรวมถึงวิธีการที่นำไปใช้ในการเพิ่มอุปกรณ์ใหม่หรือแทนที่อุปกรณ์ตัวเก่าโดยที่ยังคงรักษาเสถียรภาพของความมั่งคงและปลอดภัย องค์ประกอบของปัจจัยนี้ยังรวมไปถึงข้อตกลงในการใช้งานซึ่งกำหนดขึ้นระหว่างผู้ผลิต (supplier) และผู้จัดการโครงสร้างพื้นฐานทางราง (railway infrastructure manager) ในแง่ของการกำหนดด้านความปลอดภัย

ของผลิตภัณฑ์ และการบริการหลังการขายผลิตภัณฑ์ตลอดอายุการใช้งาน ซึ่งประเด็นเหล่านี้จะต้องได้รับการพิจารณาในมาตรฐานการพัฒนาตามวงรอบเช่นกัน

2.2 ภาวะผู้นำ (Leadership)

2.2.1 นโยบาย (Policy)

ผู้บริหารระดับสูงจำเป็นต้องกำหนดนโยบายการรักษาความปลอดภัยของข้อมูลดังนี้:

- มีความเหมาะสมกับวัตถุประสงค์ขององค์กร
- มีวัตถุประสงค์ด้านความปลอดภัยของข้อมูลหรือมีกรอบแนวคิดในการกำหนดวัตถุประสงค์ด้านความปลอดภัยของข้อมูล
- มีความมุ่งมั่นที่จะปฏิบัติตามข้อกำหนดที่เกี่ยวกับความปลอดภัยของข้อมูล
- มีความมุ่งมั่นในการปรับปรุงระบบการจัดการความปลอดภัยของข้อมูลอย่างต่อเนื่อง
- นโยบายความปลอดภัยของข้อมูลจะต้อง:
  - มีข้อมูลที่ระบุได้
  - มีการสื่อสารภายในองค์กร และ
  - เปิดให้บริการแก่ผู้ที่สนใจตามความเหมาะสม

2.2.2. การมีส่วนร่วมของผู้บริหาร (Management involvement)

ด้วยสภาวะความเป็นผู้นำและการตัดสินใจ (หรือการดำเนินการ) ฝ่ายบริหารควรสร้างสภาพแวดล้อมที่ผู้ปฏิบัติทุกคน (พนักงาน ลูกค้า บุคคลที่เกี่ยวข้อง ผู้ให้บริการ ...) สามารถมีส่วนร่วมอย่างเต็มที่ เพื่อให้บรรลุวัตถุประสงค์ขององค์กร ภายใต้การดำเนินการดังนี้:

- ปรับปรุงการรับผิดชอบ (accountability) ในมาตรฐานความปลอดภัยของข้อมูล
- การจัดหาทรัพยากรที่เหมาะสมที่สุดสำหรับการรักษาความปลอดภัยของข้อมูล
- การระบุตัวตน (identification) และการป้องกันอย่างเพียงพอสำหรับทรัพย์สินที่สำคัญขององค์กร
- กระบวนการควบคุม (จัดการ) และมาตรการรักษาความปลอดภัย

ฝ่ายบริหารต้องแสดงข้อพิสูจน์ถึงพันธกิจในการจัดตั้ง การนำไปปฏิบัติ การดำเนินการ การตรวจสอบ การเฝ้าสังเกตุ การทบทวน การบำรุงรักษาและการปรับปรุงตามหลัก ระบบการจัดการความปลอดภัยของข้อมูล(ISMS) โดย:

- อนุมัติและเผยแพร่เอกสารนโยบายความปลอดภัยของข้อมูลและสื่อสารกับพนักงานและบุคคลภายนอกที่เกี่ยวข้องทั้งหมด
- ตรวจสอบให้แน่ใจว่ามีการกำหนดวัตถุประสงค์และแผนงาน
- การกำหนดบทบาทและความรับผิดชอบในการรักษาความปลอดภัยข้อมูล
- จัดหาทรัพยากรที่เพียงพอในการจัดตั้ง การนำไปปฏิบัติ การดำเนินการ การตรวจสอบ การเฝ้าสังเกตุ การทบทวน การบำรุงรักษาและการปรับปรุง ISMS
- จัดตั้งเกณฑ์ในการยอมรับความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้

- ตรวจสอบให้แน่ใจว่ามีการตรวจสอบ ISMS ภายใน
- ดำเนินการทบทวนการจัดการของหลัก ISMS

2.2.3 บทบาทและหน้าที่ขององค์กร (Organizational roles and responsibilities)

ฝ่ายบริหารต้องตรวจสอบให้แน่ใจว่าพนักงาน ผู้รับเหมาและผู้ใช้ที่เป็นบุคคลภายนอกทุกคน มีความเข้าใจเกี่ยวกับภัยคุกคามและข้อกังวลด้านการรักษาความปลอดภัยของข้อมูล โดยหน้าที่และความรับผิดชอบของพวกเราคือการพร้อมที่จะสนับสนุนนโยบายการรักษาความปลอดภัยขององค์กรในระหว่างการทำงานและลดปัจจัยความเสี่ยงที่เกิดจากมนุษย์

นอกจากนี้ผู้ใช้ทุกคนควรได้รับการฝึกอบรม รับรอง และควบคุมโดยผ่านระบบโปรแกรมการตระหนักถึงความมั่นคงปลอดภัยเครือข่ายไซเบอร์ทั่วโลก ดังต่อไปนี้:

- จำเป็นต้องมีการฝึกอบรมผู้ใช้ก่อนที่จะมีการแทรกแซงใด ๆ ในระบบควบคุมอุตสาหกรรมในระบบราง (Industrial Control Systems)
- การฝึกอบรมการรักษาความมั่งคงปลอดภัยทางไซเบอร์ควรดำเนินการโดยผู้ให้บริการที่ได้รับการรับรอง
- การฝึกอบรมและการเพิ่มความตระหนักของความมั่งคงปลอดภัยทางไซเบอร์ของระบบควบคุมอุตสาหกรรมในระบบราง ควรจัดขึ้นพร้อมกันเฉกเช่นเดียวกับการอบรมด้านความปลอดภัยและการรักษาความปลอดภัย

ห่วงโซ่ความรับผิดชอบในการรักษาความมั่งคงปลอดภัยทางไซเบอร์ควรมีการดำเนินการที่ครอบคลุมระบบควบคุมอุตสาหกรรมในระบบรางทั้งหมด

- ข้อมูลประจำตัวและรายละเอียดการติดต่อของบุคคลที่รับผิดชอบจากองค์กรที่มีหน้าที่รักษาความมั่งคงปลอดภัยทางไซเบอร์ ต้องถูกส่งไปยังหน่วยงานป้องกันทางไซเบอร์
- ขอบเขตของความรับผิดชอบควรมีการตรวจสอบอย่างน้อยปีละครั้ง

2.3 การวางแผน (Planning)

องค์กรต้องพิจารณาปัญหาและข้อกำหนดตามมาตรฐาน และวางแผนการดำเนินการดังต่อไปนี้ เพื่อรับมือกับความเสี่ยงและโอกาสที่จะเกิดปัญหาเหล่านี้ขึ้น:

- ตรวจสอบให้แน่ใจว่าระบบจัดการความปลอดภัยของข้อมูลสามารถปฏิบัติได้ตามแผนที่วางไว้
  - ระบุความเสี่ยงและโอกาสที่ต้องจัดการปัญหา
  - วางแผนการปฏิบัติการ (ความเสี่ยงและโอกาสในการนำไปใช้และประเมินประสิทธิผล)
- ป้องกันหรือลดผลกระทบที่ไม่พึงประสงค์
  - กำหนดและปรับปรุงหลักเกณฑ์ของความเสี่ยงและระดับของความเสี่ยงที่ยอมรับได้ให้เป็นปัจจุบันอยู่เสมอ
  - ระบุ วิเคราะห์และประเมินความเสี่ยงต่างๆ
- การประเมินความเสี่ยง
  - ระบุและเลือกตัวเลือกสำหรับการจัดการความเสี่ยง
  - กำหนดมาตรการในการดำเนินการของตัวเลือก

- เปรียบเทียบมาตรการกับ "ภาคผนวก ก" ของมาตรฐาน IS0 27001 ในการจัดการความเสี่ยง
  - หมายเหตุ: ภาคผนวก ก ประกอบด้วย รายการที่มีเนื้อหาครอบคลุมเกี่ยวกับวัตถุประสงค์และการควบคุมที่เกี่ยวข้องกับองค์กร ผู้ใช้มาตรฐานนี้ควรอ้างอิง "ภาคผนวก ก" ซึ่งเป็นจุดตั้งต้นของตัวเลือกในการควบคุม เพื่อให้แน่ใจว่าตัวเลือกในการควบคุมที่สำคัญไม่ได้ถูกข้ามไป
  - การควบคุม (มาตรการ) ที่ระบุไว้ใน "ภาคผนวก ก" อาจจะไม่ละเอียดและอาจมีการเลือกวัตถุประสงค์และการดำเนินการควบคุมเพิ่มเติม
- เตรียมคำชี้แจงสำหรับการใช้งาน
  - หมายเหตุ: คำชี้แจงในการใช้งานเป็นการสรุปข้อมูลการตัดสินใจเกี่ยวกับการปฏิบัติต่อความเสี่ยง การยกเว้นข้อแสดงถึงเหตุผลเป็นการตรวจสอบเทียบเคียงว่าไม่มีการควบคุมใดถูกละเว้นโดยไม่ได้ตั้งใจ
  - มีการเตรียมคำชี้แจงการใช้งานซึ่งรวมถึงสิ่งต่อไปนี้:

    ก) วัตถุประสงค์ของการควบคุมและควบคุมต่างๆ รวมถึงเหตุผลในการเลือก

    ข) วัตถุประสงค์การควบคุมและการควบคุมที่ดำเนินการในปัจจุบัน

    ค) การยกเว้นวัตถุประสงค์การควบคุมและการควบคุมใด ๆ ใน "ภาคผนวก ก" และในสำหรับการยกเว้น
- กำหนดแผนการจัดการความเสี่ยง
- ได้รับการอนุมัติจากผู้บริหารเกี่ยวกับความเสี่ยงคงเหลือที่เสนอ

➢ ทำการปรับปรุงอย่างต่อเนื่องได้สำเร็จ

2.3.1 แผนการจัดการโครงการ

ประกอบด้วยเอกสารที่สรุปรายละเอียดไว้ กำหนดเป็นแผนงาน เมื่อเสนอแผนจะได้รับการอนุมัติจากผู้บริหารอย่างเป็นทางการ เนื่องจากเป็นการส่งเสริมองค์กรในแง่ของทรัพยากรข้อมูลและบุคคล รวมทั้งทางการเงินด้วย

โดยทั่วไปรวมถึงสิ่งต่อไปนี้:

- ➢ คำอธิบายแนวทางหรือกลยุทธ์การบริหารโครงการ
- ➢ นิยามความหมายของวัตถุประสงค์ของโครงการและปัจจัยแห่งความสำเร็จ
- ➢ การระบุความเสี่ยง
- ➢ การประเมินทรัพยากรภายในที่จำเป็น
- ➢ ความหมายของขั้นตอนการวางแผนและการดำเนินการ
- ➢ การทบทวนบทบาทของแต่ละบุคคลที่เกี่ยวข้อง
- ➢ การทบทวนเอกสารโครงการ
- ➢ การจัดรูปแบบเนื้อหาตามวัตถุประสงค์ของโครงการและสิ่งที่ส่งมอบ

- ปัญหาและการตัดสินใจที่รอดำเนินการ
- ความหมายของความถี่และเนื้อหาของการประชุมโครงการ

2.4 การสนับสนุน (Support)

2.4.1 ทรัพยากร (Resources)

องค์กรต้องกำหนดและจัดหาทรัพยากรที่จำเป็นสำหรับการจัดตั้ง การดำเนินการ การบำรุงรักษา และการพัฒนาในระบบการจัดการรักษาความปลอดภัยของข้อมูลอย่างต่อเนื่อง

2.4.2 ทักษะ (Skill)

องค์กรจะต้อง

- กำหนดทักษะที่จำเป็นสำหรับผู้ใช้ในการทำงานที่มีผลต่อประสิทธิภาพของการรักษาความมั่งคงปลอดภัยของข้อมูล
- ตรวจสอบให้แน่ใจว่าผู้ใช้มีความสามารถและมีประสบการณ์ที่เหมาะสมในด้านความปลอดภัยของข้อมูลหรือได้ปฏิบัติตามการฝึกอบรมเฉพาะ
- หากมิใช่ ควรดำเนินการเพื่อฝึกฝนผู้ใช้ เพื่อเรียนรู้ตามความสามารถที่เหมาะสม และประเมินผลของงานที่ทำ และเก็บข้อมูลที่ถูกต้องไว้เป็นหลักฐานของความสามารถเหล่านี้

2.4.3 การสร้างความตระหนัก (Awareness)

ผู้ใช้ที่ปฏิบัติงานภายใต้การควบคุมขององค์กรต้อง:

- ตระหนักถึงนโยบายความปลอดภัยของข้อมูล
- ตระหนักถึงการมีส่วนร่วม และการเกี่ยวข้องของผู้ใช้ที่ปฏิบัติงานในระบบการจัดการความปลอดภัยของข้อมูล รวมถึงผลลัพธ์ในเชิงบวกของการเพิ่มประสิทธิภาพในการรักษาความปลอดภัยข้อมูล
- ตระหนักถึงผลกระทบในการไม่ปฏิบัติตามข้อกำหนดของระบบการจัดการความปลอดภัยของข้อมูล

2.4.4 การสื่อสารให้ทราบ (Communication)

องค์กรต้องกำหนดความจำเป็นในการสื่อสารภายในและภายนอกอย่างละเอียดเกี่ยวกับ:

- สื่อสารกับอะไร? (เรื่องไหน)
- สื่อสารเมื่อไหร่? (ในขณะนั้น)
- กับใครที่ต้องติดต่อสื่อสาร?
- กระบวนการระหว่างการสื่อสารจะต้องเสร็จสมบูรณ์

2.4.5 การจัดทำเอกสาร (Documentation)

ISMS ควรรวมถึง:

- ข้อมูลที่เป็นเอกสารควรรวมถึงเอกสารทั้งหมดที่จำเป็นตามมาตรฐาน IS027001
    - บันทึกการตัดสินใจของฝ่ายบริหารทำให้มั่นใจได้ว่าการดำเนินการนั้นสามารถตรวจสอบย้อนกลับไปยังการตัดสินใจและนโยบายของฝ่ายบริหารได้ และเพื่อให้แน่ใจว่าผลที่บันทึกนั้นสามารถคัดลอกได้

- สิ่งสำคัญคือต้องสามารถพิสูจน์ถึงความสัมพันธ์จากการควบคุมที่เลือกกลับไปสู่ผลของการประเมินความเสี่ยงและกระบวนการบริหารความเสี่ยง จากนั้นจึงกลับไปที่นโยบายของ ISMS และวัตถุประสงค์

➢ ข้อมูลเอกสารทั้งหมดที่องค์กรพิจารณาว่าจำเป็นต่อประสิทธิภาพของ ISMS

2.4.6 การสร้างและปรับปรุงเอกสาร (Creation and update documentation)

➢ การสร้างและการปรับปรุงเอกสารควรมีองค์ประกอบดังต่อไปนี้

- การระบุและคำอธิบาย (ชื่อเรื่อง วันที่ ผู้แต่ง การไอดีอ้างอิง...
- รูปแบบ (ภาษา เวอร์ชันซอฟต์แวร์) และอุปกรณ์ช่วยเหลือ (เอกสารอิเล็กทรอนิกส์)
- การตรวจสอบและสอบทวนความถูกต้อง

2.4.7 การควบคุมเอกสาร (Control of documents)

➢ เอกสารที่ ISMS กำหนดจะต้องได้รับการคุ้มครองและควบคุม ขั้นตอนที่เป็นเอกสารควรมีการกำหนดขึ้นเพื่อการดำเนินการจัดการที่จำเป็นในการ:

- อนุมัติเอกสารเพื่อความเพียงพอก่อนออก
- ตรวจสอบและปรับปรุงเอกสารตามความจำเป็นและอนุมัติเอกสารอีกครั้ง
- ตรวจสอบให้แน่ใจว่ามีการเปลี่ยนแปลงและรูปแบบปัจจุบันของเอกสารมีการระบุไว้เรียบร้อย
- ตรวจสอบให้แน่ใจว่าเอกสารที่เกี่ยวข้องมีอยู่ ณ จุดใช้งาน
- ตรวจสอบให้แน่ใจว่าเอกสารยังคงชัดเจนและสามารถระบุข้อมูลได้อย่างง่ายดาย
- ตรวจสอบให้แน่ใจว่ามีเอกสารสำหรับผู้ที่ต้องการและถูกถ่ายโอน จัดเก็บและกำจัดเป็นขั้นตอนสุดท้ายตามขั้นตอนที่เกี่ยวข้องกับการจำแนกประเภท
- ตรวจสอบให้แน่ใจว่าเอกสารที่ภายนอกมีการระบุไว้เรียบร้อยแล้ว
- ตรวจสอบให้แน่ใจว่ามีการควบคุมการแจกจ่ายเอกสาร
- ป้องกันการนำเอกสารที่ล้าสมัยไปใช้ โดยไม่ได้ตั้งใจ
- ใช้การระบุข้อมูลที่เหมาะสมกับเอกสารหากถูกเก็บไว้เพื่อวัตถุประสงค์ใด ๆ

2.5 การบริหารความเสี่ยง (Risk management)

2.5.1 บทนำ

ในการวิเคราะห์ช่องโหว่ทางไซเบอร์ของระบบรางควรทำการวิเคราะห์ความเสี่ยงโดยอ้างอิงตามภัยคุกคามความมั่งคงปลอดภัยทางไซเบอร์ ปัจจุบันมีวิธีการประเมินความเสี่ยงที่หลากหลายและในประเทศต่าง ๆ มีการเสนอทางเลือกต่างๆสำหรับระบบอุตสาหกรรมและระบบราง

ในส่วนนี้เราจะวิเคราะห์ข้อบกพร่องของการใช้การวิเคราะห์ความเสี่ยงแบบดั้งเดิมโดยตรงกับความมั่งคงปลอดภัยในโลกไซเบอร์ในลักษณะเดียวกับที่ทำเพื่อความปลอดภัย เพื่อที่จะเอาชนะข้อจำกัดเหล่านี้ เราขอเสนอรูปแบบการประเมินความเสี่ยงที่สอดคล้องกับมาตรฐานความปลอดภัยทางไซเบอร์แบบใหม่ทั่วโลก

และในส่วนนี้ยังมีการเสนอคำจำกัดความสำหรับภัยคุกคามทั่วไปต่อระบบรถไฟเพื่อประเมินในการวิเคราะห์ความเสี่ยงด้านความปลอดภัย

นอกจากนี้เรายังกำหนดระดับความปลอดภัยตามความเชื่อมั่นที่มีให้เพื่อลบช่องโหว่ของความมั่งคงปลอดภัยทางไซเบอร์หรือผลกระทบ ระดับความเสี่ยงด้านความปลอดภัยแต่ละระดับสามารถนำมาเชื่อมโยงกับชุดมาตรการและเทคโนโลยีที่สามารถนำไปใช้เพื่อให้ได้รับความมั่งใจยิ่งขึ้นของระดับความเสี่ยงในระดับนั้นๆ

โครงสร้างทั้งหมดของการบริหารความเสี่ยงจะเป็นไปตามประเด็นดังต่อไปนี้:

1) ปัญหาของการวิเคราะห์ความเสี่ยงในปัจจุบัน

2) การเลือกเกณฑ์การยอมรับความเสี่ยง

3) การระบุระดับความเสี่ยงด้านความปลอดภัยสำหรับโซนและท่อร้อยสาย

4) ภัยคุกคามในระบบและการวิเคราะห์ข้อกำหนดต่างๆ

2.5.2 การควบคุมการปฏิบัติงาน (Control in operations)

ควรดำเนินการควบคุม 3 ด้าน ผ่านมาตรฐาน ISO27001

- การควบคุมเชิงป้องกัน: กีดกันและป้องกันปัญหา
- การควบคุมการตรวจจับ: ปัญหาในการค้นหา ตรวจจับ และระบุ
- การควบคุมการแก้ไข: แก้ไขปัญหาที่ตรวจพบและหยุดการเกิดซ้ำ

2.5.3 การประเมินและการแก้ไขความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment and treatment)

วิธีการประเมินความเสี่ยงที่เลือกจะต้องทำให้แน่ใจว่าสามารถให้ผลลัพธ์ที่เทียบเคียงและทำซ้ำได้ วิธีการวิเคราะห์ความเสี่ยงเฉพาะสำหรับระบบรางประกอบด้วยขั้นตอนต่อไปนี้:

- การสร้างขอบเขตของความปลอดภัย (พื้นที่ผลกระทบ เกณฑ์ความน่าจะเป็นและเมทริกซ์ความเสี่ยงที่ยอมรับได้)
- การระบุทรัพย์สินหลัก
- การประเมินผลกระทบที่อาจเกิดขึ้นจากการโจมตีที่ประสบความสำเร็จในสินทรัพย์หลักโดยมีสถานการณ์มาสนับสนุนให้เกิดขึ้น
- การระบุทรัพย์สินสนับสนุนที่ได้รับจากทรัพย์สินหลัก
- การระบุภัยคุกคามที่มุ่งเป้าไปที่ทรัพย์สินสนับสนุน
- การเลือกการโจมตีของเหตุการณ์การภัยคุกคาม
- การประเมินระดับความเสี่ยงในแต่ละสถานการณ์ภัยคุกคามที่มีเป้าหมายคือสินทรัพย์สนับสนุน โดยพิจารณาจากความเป็นไปได้และผลกระทบของสถานการณ์ภัยคุกคามเหล่านั้น
- การเลือกตัวเลือกของการจัดการรักษาความเสี่ยง (ยอมรับ ลด ย้าย หลีกเลี่ยง) ในแต่ละสถานการณ์ภัยคุกคามที่มีการเสนอให้ดำเนินการจัดการความเสี่ยง (ระดับความเสี่ยงระดับปานกลางและสูง)
- การเลือกรายการการควบคุมเพิ่มเติมเพื่อลดความเสี่ยงด้านความปลอดภัย

2.6 การประเมินประสิทธิภาพ (Performance evaluation)

2.6.1 การเฝ้าระวัง และการวัดผล (Monitoring and measurement)

องค์กรควรวัดประสิทธิภาพของการรักษาความปลอดภัยข้อมูลและประสิทธิผลของหลักISMS ดังกำหนดดังนี้:

- สิ่งจำเป็นในการตรวจสอบและวัดผลรวมถึงกระบวนการและมาตรการรักษาความปลอดภัยคืออะไร
- ดำเนินการติดตาม วัดผล วิเคราะห์ และประเมินผลเพื่อให้แน่ใจว่าผลลัพธ์มีความถูกต้อง
- ควรตรวจสอบเมื่อไหร่
- ใครเป็นผู้รับผิดชอบ
- เมื่อไหร่และใครเป็นผู้วิเคราะห์ผลลัพธ์

2.6.2 การตรวจประเมิน (Audit)

องค์กรต้องดำเนินการตรวจสอบหลัก ISMS ภายในช่วงเวลาที่วางแผนไว้เพื่อพิจารณาว่าวัตถุประสงค์การควบคุม การควบคุม กระบวนการและขั้นตอนของ ISMS:

- เป็นไปตามข้อกำหนดของมาตรฐานสากลฉบับนี้และกฎหมายหรือระเบียบที่เกี่ยวข้อง;
- เป็นไปตามข้อกำหนดด้านความปลอดภัยของข้อมูลที่ระบุไว้
- มีการนำไปใช้และบำรุงรักษาอย่างมีประสิทธิภาพ
- ดำเนินการตามที่คาดไว้

รวมถึงควรมีการวางแผนโปรแกรมการตรวจสอบ โดยคำนึงถึงสถานะและความสำคัญของกระบวนการและพื้นที่ที่ต้องตรวจสอบตลอดจนผลการตรวจสอบก่อนหน้านี้ การตรวจสอบจะต้องมีกำหนดและจะต้องมีอย่างน้อย:

- คำอธิบายของเกณฑ์ ขอบเขต ความถี่ และวิธีการ
- คำอธิบายของบทบาทและความรับผิดชอบ
- เอกสารประกอบที่รับรองความเที่ยงธรรมและความเป็นกลางของกระบวนการตรวจสอบ
- การวางแผนการตรวจสอบ
- ขั้นตอนในการเก็บรักษาและบันทึกกิจกรรมที่เก็บไว้และบันทึก (logs)

ผู้ตรวจสอบไม่ควรตรวจสอบงานของตนเอง

2.7 การปรับปรุง (Improvement)

2.7.1 ความไม่สอดคล้อง (Nonconformity)

องค์กรต้องกำหนดกระบวนการที่จะปฏิบัติตาม เมื่อตรวจพบการความไม่สอดคล้องตามข้อกำหนด ให้ดำเนินการดังนี้:

- ตอบสนองเพื่อควบคุมและแก้ไข
  - ระบุการความไม่สอดคล้อง และระบุหน่วงงานที่สามารถแก้ไขได้

- ประเมินว่าจำเป็นหรือไม่ที่จะการดำเนินการเพื่อกำจัดสาเหตุ
  - อธิบายความไม่สอดคล้อง (ใคร อะไร ที่ไหน เมื่อไร ทำไม อย่างไร กี่คน)
- ดำเนินการทุกส่วนที่จำเป็นเพื่อนำไปปรับปรุงกระบวนการดำเนินงาน
- ทบทวนประสิทธิภาพของการดำเนินการแก้ไข
- อัปเดตหลัก ISMS หากจำเป็น
- บันทึกผลทั้งหมดและล็อกผลด้วย

2.7.2 การดำเนินการแก้ไข (Corrective action)

องค์กรต้องดำเนินการเพื่อขจัดสาเหตุของความไม่สอดล้องข้อกับข้อกำหนดของ ISMS เพื่อป้องกันการเกิดซ้ำ ขั้นตอนที่เป็นเอกสารในการดำเนินการแก้ไขควรมีการระบุข้อกำหนดสำหรับ:

- การระบุความไม่สอดคล้อง
- การระบุสาเหตุของการไม่ปฏิบัติตามข้อกำหนด
- การประเมินความจำเป็นในการดำเนินการเพื่อให้แน่ใจว่าการไม่ปฏิบัติตามข้อกำหนดจะไม่เกิดขึ้นอีก
- การดำเนินการแก้ไขที่จำเป็น
- การจัดเก็บผลของการดำเนินการแก้ไข
- การทบทวนการดำเนินการแก้ไขที่ได้ดำเนินการไป

2.7.3 การปรับปรุงอย่างต่อเนื่อง (Continual improvement)

องค์กรควรปรับปรุงประสิทธิภาพของ ISMS อย่างต่อเนื่อง โดยใช้นโยบายการรักษาความปลอดภัยของข้อมูล วัตถุประสงค์ในการรักษาความปลอดภัยข้อมูล ผลการตรวจสอบ การวิเคราะห์ตรวจสอบเหตุการณ์ การดำเนินการแก้ไขและการป้องกัน และการทบทวนการจัดการ

องค์กรควรปฏิบัติดังต่อไปนี้อย่างสม่ำเสมอ

- ดำเนินการปรับปรุงที่ระบุไว้ใน ISMS
- ดำเนินการแก้ไขและป้องกันที่เหมาะสม
- ใช้บทเรียนที่ได้รับจากประสบการณ์ด้านความปลอดภัยขององค์กรอื่นและขององค์กรเอง
- สื่อสารถึงการดำเนินการและการปรับปรุง ไปยังผู้สนใจทั้งหมดพร้อมกับรายละเอียดที่เหมาะสมกับสถานการณ์และการดำเนินการอย่างไรตามที่ตกลงกันไว้
- ตรวจสอบให้แน่ใจว่าการปรับปรุงบรรลุวัตถุประสงค์ที่ตั้งไว้

การบริหารจัดการเหตุการณ์ไม่ปกติ: การรายงานเหตุการณ์และจุดอ่อนด้านความปลอดภัยของข้อมูล

- วัตถุประสงค์: เพื่อให้แน่ใจว่าเหตุการณ์ด้านความมั่งคงปลอดภัยของข้อมูลและจุดอ่อนที่เกี่ยวข้องกับระบบสารสนเทศได้รับการสื่อสารในลักษณะที่ช่วยให้สามารถดำเนินการแก้ไขได้อย่างทันท่วงที

ข้อกำหนดในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

- ฝ่ายบริหารของบริษัทระบบรางควรได้รับการแจ้งทันทีเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลและควรมีคำแนะนำถึงขั้นตอนต่อไปนี้สำหรับการตั้งค่าและการใช้งานส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง
  - การแจ้งเตือนและการตอบสนองต่อเหตุการณ์
  - คำติชมเกี่ยวกับผลการตอบสนองต่อเหตุการณ์
  - การวิเคราะห์ข้อผิดพลาด เพื่อให้แน่ใจว่าข้อผิดพลาดจะถูกกำจัดและใช้มาตรการแก้ไข โดยที่มาตรการเหล่านั้นไม่ถูกบุกรุกและการดำเนินการทั้งหมดต้องได้รับอนุญาตอย่างถูกต้อง

การบริหารจัดการเหตุการณ์ไม่ปกติควรรวมถึงการตรวจจับ การวิเคราะห์ การป้องกัน การแก้ไขปัญหา และการกู้คืนส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบรางหลังเหตุการณ์เหล่านี้ได้เกิดขึ้น เหตุการณ์ด้านความมั่งคงปลอดภัยของข้อมูลทั้งหมดควรได้รับการตรวจสอบและจัดทำเป็นเอกสารอย่างต่อเนื่อง และควรจัดทำรายงานเหตุการณ์เพื่อกำหนดผู้รับตามรูปแบบความถี่และรายการที่กำหนด

การจัดการเหตุการณ์ทางนิติเวชและการตอบสนองจะต้องเป็นไปตามมาตรฐานสากล ข้อกำหนดและข้อมูลของเจ้าหน้าที่ที่รับมือกับสถานการณ์ฉุกเฉิน (CERT)

2.7.4 กิจกรรมต่อเนื่อง (Continuity activity)

การรักษาความมั่นคงปลอดภัยสารสนเทศของการจัดการความต่อเนื่องทางธุรกิจ

- วัตถุประสงค์: เพื่อลดการหยุดชะงักของกิจกรรมทางธุรกิจและปกป้องกระบวนการทางธุรกิจที่สำคัญจากผลกระทบของความล้มเหลวครั้งใหญ่ของระบบสารสนเทศหรือภัยพิบัติและเพื่อให้แน่ใจว่าจะเริ่มต้นใหม่ได้อย่างทันท่วงที

3. วิธีการแก้ปัญหา (Solution)

3.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

นโยบายความปลอดภัยของข้อมูลมีความจำเป็นในอุตสาหกรรมระบบราง เพื่อความเป็นระเบียบสำหรับแนวทางขององค์กรในการจัดการความปลอดภัยของข้อมูลได้ตรงวัตถุประสงค์ ซึ่งจะต้องสอดคล้องกับความต้องการทางธุรกิจและเกี่ยวข้องกับมาตรฐาน

นโยบายความปลอดภัยของข้อมูลควรสอดคล้องกับ

- ยุทธศาสตร์ทางธุรกิจ
- ข้อบังคับ กฎหมาย และสัญญา
- สถานการณ์ปัจจุบัน และ แผนที่วางไว้สำหรับความปลอดภัยของข้อมูลต่อภัยคุกคามของสิ่งแวดล้อม

หมายเหตุ: ในงานระบบรางนั้น ไม่ได้มีข้อบังคับและกฎหมายกำหนด และมีบางมาตรฐานเท่านั้นที่นำมาเป็นแนวทาง เพื่อใช้ในการพิจารณา

เพื่อให้เกิดความสอดคล้องระหว่าง มาตรฐานสากลและแนวทางเฉพาะของความมั่งคงทางไซเบอร์ (เช่น ANSI...) โดยนโยบายด้านความปลอดภัยของข้อมูลควรบรรจุข้อความต่อไปนี้ลงไปด้วย :

- คำจำกัดความของ ความปลอดภัยของข้อมูล วัตถุประสงค์และหลักการ เพื่อเป็นแนวทางในการปฏิบัติในส่วนที่เกี่ยวข้อง
- ความปลอดภัยของข้อมูล;
- การมอบหมาย ความรับผิดชอบทั่วไปและเฉพาะ สำหรับการจัดการความปลอดภัยของข้อมูลเพื่อกำหนดบทบาทหน้าที่;
- ขั้นตอนในการปฏิบัติ สำหรับการเบี่ยงเบนและข้อยกเว้น

หัวข้อนโยบายในงานระบบรางที่ควรระบุมีดังนี้:

- ระบบควบคุมการเข้าออก;
- การจำแนกประเภทของข้อมูล (การจัดการ);
- ความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม;
- หัวข้อที่มุ่งเน้นเกี่ยวกับผู้ใช้งาน เช่น:
  - การใช้ทรัพย์สินอย่างเหมาะสม
  - โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์
  - การถ่ายโอนข้อมูล
  - อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานระยะไกล
  - การจำกัดการเข้าถึงในการติดตั้งโปรแกรมและการใช้งาน
  - การสำรองข้อมูล
  - การป้องกันจากโปรแกรมที่ไม่พึงประสงค์
  - การบริหารจัดการช่องโหว่ทางเทคนิค
  - มาตรการเข้ารหัสข้อมูล
  - ความมั่นคงทางการสื่อสาร
  - ความเป็นส่วนตัวและความปลอดภัยของข้อมูลส่วนบุคคล
  - ความสัมพันธ์กับผู้ผลิต

นโยบายทางความมั่นคงปลอดภัยของสารสนเทศต้องมีการกำหนดขึ้น อนุมัติจากฝ่ายบริหาร ตีพิมพ์และ สื่อสารไปยังบุคลากรและผู้ที่เกี่ยวข้องภายนอก(รวมไปถึง ผู้ให้บริการและผู้ผลิตในระบบราง)

นโยบายควรมีการสื่อสารในรูปแบบที่เหมาะสม ผู้อ่านสามารถเข้าถึงได้และเข้าใจได้ง่าย

3.2 โครงสร้างด้านความปลอดภัยสารสนเทศขององค์กร (Organization of information security)

การบริหารจัดการและขั้นตอนการดำเนินการภายในองค์กรควรจะมีการพิจารณาการประเมินปลอดภัยอย่างครอบคลุม

ขั้นตอนการดำเนินการภายในองค์กรมีส่วนเกี่ยวข้องกับแนวทางและมาตรฐานที่จะนำมาปรับใช้ต้องระบุขั้นตอนการปฏิบัติ

ติให้ชัดเจนเกี่ยวกับซึ่งจะต้องมั่นใจได้ว่ามีความมั่นคงปลอดภัย

3.2.1 โครงสร้างภายในองค์กร (Internal organization)

ควรกำหนดกรอบการบริหารจัดการเพื่อเริ่มต้นและควบคุมการปฏิบัติงาน และดำเนินการด้านความมั่นคงสารสนเทศภายในองค์กร

3.2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

ควรนำห่วงโซ่ความรับผิดชอบสำหรับความมั่งคงทางไซเบอร์มาประยุกต์ใช้ โดยข้อมูลส่วนบุคคลและข้อมูลติดต่อของผู้ปฏิบัติงานในสายบังคับบัญชาจะต้องมีการแจ้งต่อหน่วยงานป้องกันความมั่งคงทางไซเบอร์

หน้าที่ความรับผิดควรมีการปรับปรุงเป็นระยะ อย่างน้อยปีละหนึ่งครั้ง

3.2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

จำเป็นต้องมีการแยกบุคคลที่อาจจะก่อให้เกิดความเสียหายกับการปฏิบัติหน้าที่ปกติออกจากกัน

บุคคลที่เกี่ยวข้องกับการปฏิบัติงานในส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบรางสามารถแบ่งเป็น 4 กลุ่มหลัก คือ

- พนักงานให้บริการ - พนักงานในองค์กรซึ่งปฏิบัติงานในส่วนจัดการ บำรุงรักษาและซ่อมบำรุง ส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง
- ผู้ใช้งาน - บุคคลซึ่งหมอบหมายงานให้กับพนักงานให้บริการและมีความเกี่ยวข้องโดยตรงกับการประมวลผลสารสนเทศ
- พนักงานส่วนสนับสนุน - พนักงานในองค์กรซึ่งทำหน้าที่ประสานงานในส่วนที่ไม่มีความเกี่ยวข้องกันส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง
- ผู้ดูแล - บุคคลซึ่งมีหน้าที่รับผิดชอบในการติดตั้งและดำเนินการในบำรุงรักษาโปรแกรม ในส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง ซึ่งบุคคลเหล่านี้เป็นพนักงานขององค์กรภายนอก ผู้พัฒนา ผู้ผลิต (ผู้ขาย) ผู้เชี่ยวชาญพิเศษ(ศูนย์ให้บริการ) ซึ่งดำเนินการภายใต้สัญญาที่ระบุไว้กับบริษัทระบบราง

ซึ่งแต่ละบุคคลจะต้องยอมรับข้อกำหนดเบื้องต้นด้านความมั่นคงสารสนเทศของบุคคลแต่ประเภท ดังนี้

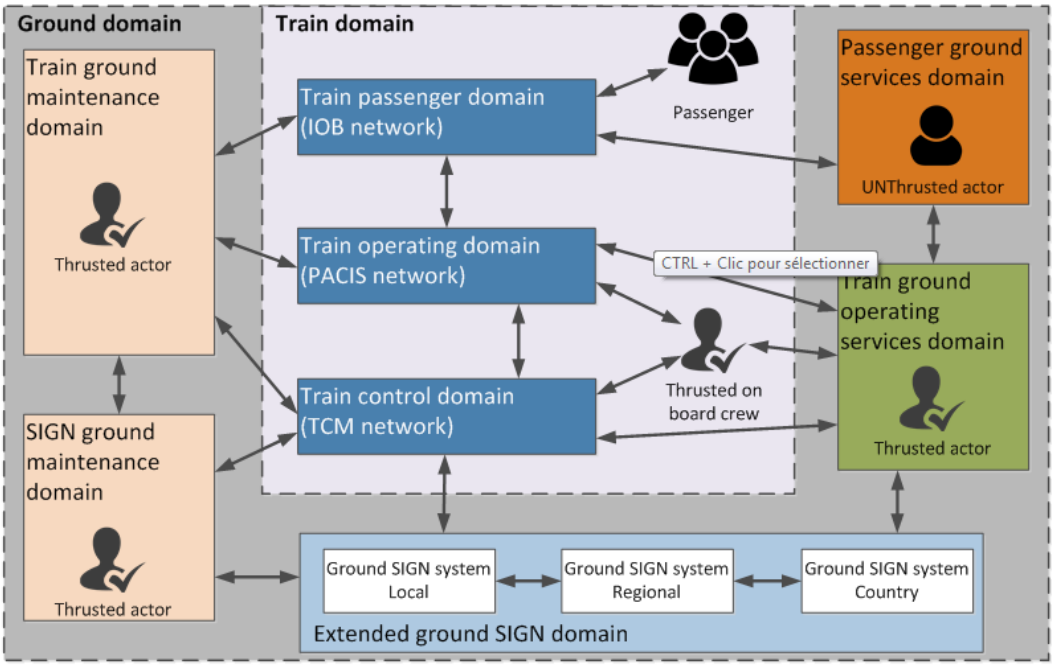
- บุคคลซึ่งมีหน้าที่เป็น **พนักงานให้บริการ** ควรปฏิบัติเฉพาะงานที่อยู่ในขอบเขตหน้าที่เท่านั้น โดยที่ภาระงานต่างๆ ต้องไม่ละเมิดสิทธิ์ที่กำหนดไว้ในการเข้าถึงและไม่ละเมิดความปลอดภัยของข้อมูลรวมถึงความพยายามที่จะ
  - กระทำการอันใดโดยไม่ได้รับกับองค์ประกอบด้านกายภาพของส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง
  - ใช้อุปกรณ์เก็บข้อมูลที่ไม่ได้มาตรฐาน
  - ใช้โปรแกรมที่ไม่เกี่ยวข้องกับฟังก์ชันการทำงานของส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง
  - หลีกเลี่ยงการสร้างเงื่อนไขในการเข้าใช้งาน

- เข้าใช้งานผ่านเครือข่ายสาธารณะ
- กระทำการอันใดซึ่งอาจจะส่งผลกระทบต่อความมั่นคงสารสนเทศ

➢ **ผู้ใช้งาน** ของส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง
- ผู้ใช้ควรรายงานการประนีประนอมต่อความปลอดภัยของข้อมูลและหรือความผิดพลาดที่เกิดขึ้นเองในทันทีเมื่อมีการประมวลผลข้อมูล พวกเขาไม่ควรค้นหาสาเหตุของการละเมิดหรือข้อผิดพลาดด้วยตนเอง
- ผู้ใช้งานไม่ควรพยายามที่จะลบโปรแกรมที่น่าสงสัยด้วยตนเอง

➢ **พนักงานส่วนสนับสนุน** และรวมถึงพนักงานที่ปฏิบัติหน้าที่อื่นๆ ที่เกี่ยวข้องในองค์กร จะต้องปฏิบัติตามข้อกำหนดเบื้องต้นเกี่ยวกับความมั่งคงสารสนเทศดังนี้
- พนักงานควรทำความเข้าใจกับระดับของอำนาจหน้าที่ ซึ่งขอบเขตจะต้องระบุไว้ในคำบรรยายลักษณะงาน
- ในกรณีที่มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของพนักงานหรือมีการย้ายไปปฏิบัติงานอื่นที่ได้รับหมอบหมาย จำเป็นต้องมีการปรับปรุงแอตทริบิวต์และเครื่องมือที่พนักงานสามารถใช้เข้าถึงระบบได้ โดยบัญชีเก่าของพนักงานควรมีการยกเลิกการเข้าใช้งาน และ สร้างบัญชีใหม่ทดแทน
- พนักงานที่ออกจากองค์กรไปแล้ว จะต้องถูกยกเลิกสิทธิในเข้าถึงระบบในส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง พนักงานจะต้องส่งคืนแอตทริบิวต์และเครื่องมือที่เกี่ยวข้องกับส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง สิทธิในเข้าถึงข้อมูลที่ถูกสร้างโดยพนักงานที่พ้นจากหน้าที่ไปแล้ว จะต้องมีการโอนไปยังพนักงานคนอื่นที่ยังปฏิบัติหน้าที่อยู่โดยทันที
- ในกรณีที่พนักงานที่มีบทบาทในการรายงานการฝ่าฝืนความมั่นคงสารสนเทศและพลาดในการรายงานการฝ่าฝืนต่อฝ่ายบริหารในทันท่วงทีควรมีการพิจารณาโทษทางวินัยในแบบที่เหมาะสม โดยที่พนักงานควรต้องได้รับการแจ้งถึงการพิจารณาโทษล่วงหน้า

➢ การกระทำอันใดของ **ผู้ดูแล** ที่เกี่ยวข้องกับส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบรางควรกระทำภายใต้การดูแลอย่างเคร่งครัดจากหัวหน้างานผู้มีอำนาจ และจัดทำเป็นเอกสารบันทึกด้วย



3.2.1.3 การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

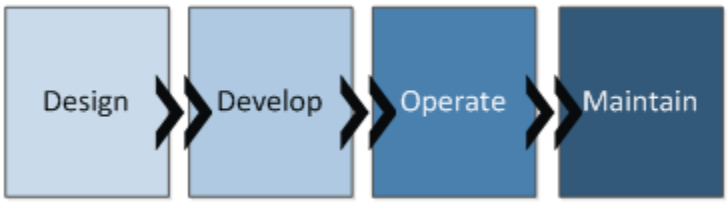
ประกาศโดยกรมการขนส่งทางราง

3.2.1.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

ประกาศโดยกรมการขนส่งทางราง

3.2.1.5 ความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการ (Information security in project management)

เน้นย้ำการบริหารโครงการในส่วนของระบบราง (ระยะเวลา,วิไซเคิล)



3.2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

จำเป็นต้องมีการรับรองความมั่นคงปลอดภัยของสารสนเทศทุกครั้งเมื่อมีการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาและสิ่งอำนวยความสะดวกในการปฏิบัติงานระยะไกล เพื่อปฏิบัติงานบนเครือข่ายระบบราง การป้องกันที่จำเป็นต้องสอดคล้องกับความเสี่ยงที่เฉพาะเจาะจงเหล่านี้ ซึ่งเกิดจากการปฏิบัติงาน

ในกรณีที่มีการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา ควรมีการป้องกันความเสี่ยงจากการใช้งานที่เกิดขึ้นในสภาพแวดล้อมที่ไม่ปลอดภัยด้วย

3.2.2.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

เครือข่ายไร้สายของอุปกรณ์คอมพิวเตอร์แบบพกพามีความคล้ายกับการเชื่อมต่อกับเครือข่ายประเภทอื่นๆ แต่มีข้อแตกต่างที่สำคัญซึ่งควรพิจารณาคือ การควบคุมการยืนยันตัวตน

โดยความแตกต่างของแต่ละประเภทแตกต่างกันคือ

ก) มีเครือข่ายไร้สายบางชนิด ที่กฎเกณฑ์วิธียังไม่สมบูรณ์และมีข้อด้อย

ข) ข้อมูลที่เก็บไว้บนคอมพิวเตอร์พกพาอาจจะไม่ได้รับการสำรองข้อมูล เพราะข้อกำจัดด้านความเร็วในการเชื่อมต่อกับเครือข่าย และ/หรือ เพราะอุปกรณ์นั้นไม่ได้เชื่อมต่อตามเวลาที่กำหนดสำหรับมีการสำรองข้อมูล

ควรมีการกำหนดนโยบายอย่างเป็นทางการและนำการประเมินความมั่งคงปลอดภัยที่เหมาะสมมาใช้ในการป้องกันความเสี่ยงจากการใช้อุปกรณ์คอมพิวเตอร์แบบพกพาและการเชื่อมต่อสิ่งอำนวยความสะดวกในระบบอาณัติสัญญาณและการสื่อสารโทรคมนาคม ซึ่งนโยบายควรประกอบด้วย

- กฎและคำแนะนำของการเชื่อมต่อสิ่งอำนวยความสะดวกกับเครือข่ายส่วนตัวของระบบราง และคำแนะนำเมื่อมีการใช้งานสิ่งอำนวยความสะดวกนี้ในที่สาธารณะ
- ข้อกำหนดเบื้องต้นสำหรับการป้องกันทางกายภาพ การควบคุมการเขาถึง เทคนิคการเข้ารหัสข้อมูล การสำรองข้อมูล การป้องกันไวรัส

นโยบายสำหรับเครื่องคอมพิวเตอร์แบบพกพา ควรคำนึงถึงความเสี่ยงในการทำงานบนอุปกรณ์ภายใต้สิ่งแวดล้อมที่ไม่ปลอดภัย เมื่อมีการใช้งานเครื่องคอมพิวเตอร์แบบพกพาและการเชื่อมต่อสิ่งอำนวยความสะดวก เช่น โน้ตบุ๊กคอมพิวเตอร์ แล็ปท็อปคอมพิวเตอร์ ปาล์มท็อป สมาร์ตการ์ด และโทรศัพท์มือถือ ควรใช้ความระมัดระวังเป็นพิเศษเพื่อให้แน่ใจว่าข้อมูลทางธุรกิจจะไม่ถูกบุกรุก

3.2.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)

การปฏิบัติงานจากระยะไกลใช้เทคโนโลยีในการสื่อสารเพื่อให้บุคลากรสามารถทำงานจากสถานที่ห่างไกลภายนอกองค์กรได้

ควรมีการพัฒนานโยบายของแผนการปฏิบัติงานและระเบียบขั้นตอนการปฏิบัติงานและนำไปปรับใช้ในการปฏิบัติงานจากระยะไกล ซึ่งในการปฏิบัติงานจากระยะไกลนั้นองค์กรจะต้องให้การป้องกันกับสถานที่ปฏิบัติงานนั้น และจะต้องมั่นใจว่ามีการจัดการที่เหมาะสมกับลักษณะการปฏิบัติงานนั้นด้วย

การฝึกอบรมจะต้องถูกจัดเตรียมให้กับบุคลากรที่ใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา เพื่อสร้างความตระหนักรู้ถึงความเสี่ยงที่เพิ่มขึ้นจากการปฏิบัติงานนั้นและการควบคุมที่ต้องนำไปปฏิบัติ

แนวทางและการจัดการที่จะต้องพิจารณาควรประกอบด้วย

ก) การจัดเตรียมอุปกรณ์และเฟอร์นิเจอร์ที่เหมาะสมสำหรับการปฏิบัติงานจากระยะไกลที่ไม่อนุญาตให้ใช้งานอุปกรณ์ส่วนตัวที่ไม่ได้รับการควบคุมจากองค์กร

ข) ให้คำนิยามเกี่ยวกับการอนุญาตทำงาน ชั่วโมงในการทำงาน การจำแนกประเภทของข้อมูลซึ่งจะถูกจัดเก็บภายในระบบและให้บริการแก่ผู้ปฏิบัติงานที่ได้รับอนุญาตในการใช้งาน

ค) การจัดเตรียมอุปกรณ์สำหรับใช้ในการติดต่อสื่อสารอย่างเหมาะสม ซึ่งรวมถึงวิธีรักษาความปลอดภัยจากการเข้าใช้งานระยะไกล

ง) ความมั่งคงทางกายภาพ

จ) กฎระเบียบและแนวทางสำหรับบุคคลภายในและบุคคลภายนอก ในการใช้งานอุปกรณ์และเข้าถึงข้อมูล

ฉ) การจัดเตรียมการสนับสนุนและซ่อมบำรุงของอุปกรณ์และโปรแกรม

ช) การจัดเตรียมในเรื่องการประกันภัย

ซ) ระเบียบขั้นตอนสำหรับการสำรองข้อมูลและความต่อเนื่องทางธุรกิจ

ฌ) การตรวจสอบและความปลอดภัย

ญ) เพิกถอนอำนาจและสิทธิในการเข้าถึงและส่งคืนอุปกรณ์ เมื่อการเข้าใช้งานระยะไกลนั้นสิ้นสุดลง

การประเมินความมั่นคงปลอดภัยควรจะนำมาใช้กับการบริหารความเสี่ยงที่มาจากการเดินทางและทำงานนอกบริษัทระบบราง โดยควรมีการออกแบบการประเมินเพื่อลดความเสี่ยงเหล่านั้นลง

- ไม่อนุญาตให้มีตรวจสอบการจำแนกประเภทของข้อมูลบริษัทในสถานที่สาธารณะหรือในสถานที่นอกเหนือการควบคุม
- ความเสียหาย การงัดแงะ การถูกขโมย การสูญหายของเอกสาร สื่อหรืออุปกรณ์ (เช่น คอมพิวเตอร์ส่วนบุคคล โทรศัพท์มือถือ สมาร์ทการ์ด กระดาษ สื่อจัดเก็บข้อมูลแบบถอดได้) เมื่อมีการใช้งานหรือจัดเก็บ
- ควรมีการตรวจสอบคู่มือของบริษัทผู้ผลิตสำหรับอุปกรณ์ป้องกันตลอดเวลา

3.3 ความมั่นคงปลอดภัยของทรัพยากรบุคคล (Human resource security)

คุณสมบัติหลักของความน่าเชื่อถือของบุคลากรในระบบรางที่ควรพิจารณาคือความรู้เฉพาะทางและทางเทคนิคที่พนักงานควรมี รวมไปถึงข้อจำกัดด้านเวลาความสำคัญของผู้รับเหมาและการหมุนเวียน

3.3.1 การจ้างงาน (Prior to employment)

ควรนำขั้นตอนการจ้างงานโดยทั่วไปควรกำหนดเป็นนโยบาย รวมถึงนโยบายการตรวจสอบภูมิหลังซึ่งกำหนดเป็นแนวหลักและเป็นกลางในการพิจารณาประสบการณ์ของผู้สมัครซึ่งเป็นส่วนหนึ่งของการตัดสินใจจ้างงาน

คุณสมบัติเฉพาะในอุตสาหกรรมระบบราง คือ ความรู้เฉพาะด้านของพนักงาน ข้อจำกัดด้านเวลา ผู้รับเหมา การหมุนเวียน และความมุ่งมั่นของทีม

3.3.1.1 การคัดเลือก (Screening)

การคัดเลือกก่อนจ้างงานซึ่งเป็นส่วนหนึ่งของกระบวนการสรรหาพนักงานกระทำโดยตรวจสอบภูมิหลังของพนักงานก่อนการจ้างงาน ซึ่งควรรวมไปถึง

- ตรวจสอบประวัติอาชญากรรมและประวัติการทำงานในปีที่ผ่านมา
- ส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลที่สาม (เพื่อย้ำเตือนถึงการปฏิบัติตามข้อผูกมัดภายใต้การปฏิบัติตามการป้องกันข้อมูล)

การตรวจสอบภูมิหลังต้องปฏิบัติตามระเบียบข้อกำหนดในการตรวจสอบประวัติอาชญากรรมและประวัติการทำงาน ซึ่งจะรับประกันความน่าเชื่อถือของพนักงาน

ทุกตำแหน่งงานควรปฏิบัติให้เป็นไปตามเงื่อนไขให้เรียบร้อยก่อนกระบวนการสรรหาพนักงานจะดำเนินการแล้วเสร็จ

3.3.1.2 ข้อตกลงและเงื่อนไขในการจ้างงาน (Terms and conditions of employment)

ควรมีการตรวจสอบให้มั่นใจว่าพนักงาน ผู้รับเหมาและบุคคลที่สามได้ตระหนักถึงภัยคุกคามทางความมั่นคงสารสนเทศ และหน้าที่ความรับผิดชอบของตนเองด้วย ซึ่งพร้อมที่จะสนับสนุนนโยบายความมั่นคงขององค์กรระหว่างการปฏิบัติงาน และลดความเสี่ยงที่เกิดจากความผิดพลาดของผู้ปฏิบัติงานเอง

รวมทั้งต้องตรวจสอบให้มั่นใจว่าพนักงานและผู้รับเหมาเหมาะสมกับหน้าที่ ที่พวกเขาได้รับการพิจารณา

3.3.2 ช่วงระหว่างการจ้างงาน (During employment)

ควรกำหนดความรับผิดชอบในการบริหารเพื่อที่จะมั่นใจได้ว่ามีการใช้การรักษาความมั่นคงปลอดภัยตลอดการจ้างงานของแต่ละบุคลากรภายในองค์กร

มีการให้ความรู้ความเข้าใจและฝึกอบรมในเรื่องการดำเนินการทางความมั่นคงปลอดภัยในระดับที่เพียงพอ และวิธีการใช้งานอุปกรณ์ในการประมวลผลข้อมูลอย่างถูกวิธีแก่พนักงานทุกคน ผู้รับเหมาและบุคคลที่สามเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้น รวมถึงควรกำหนดกระบวนการทางวินัยสำหรับการละเมิดความมั่นคงปลอดภัยด้วย

3.3.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ผู้บริหารควรจัดหาทรัพยากรที่จำเป็นและดำเนินการควบคุมความมั่นคงภายในองค์กรด้วยองค์กรที่ชัดเจน แสดงให้เห็นถึงความมุ่งมั่น การมอบหมายงานที่ชัดเจนและการรับทราบถึงความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้บริหารควรกำหนดให้ผู้ที่ทำสัญญาจ้างและบุคคลภายนอกปฏิบัติตามนโยบายความมั่นคงและขั้นตอนปฏิบัติขององค์กรที่กำหนดไว้

ถ้าพนักงาน ผู้ที่ทำสัญญาจ้าง และบุคคลที่สามที่ไม่ได้ตระหนักถึงความรับผิดชอบต่อความมั่นคง อาจจะก่อให้เกิดความเสียหายอย่างมากต่อองค์กร ซึ่งบุคคลที่มีการผลักดัน

แนวโน้มที่มีความน่าเชื่อถือยิ่งขึ้นและลดความเสี่ยงด้านความความมั่นคงปลอดภัยสารสนเทศ

3.3.2.2 การสร้างความตระหนัก การให้ความรู้และการฝึกอบรมความมั่งคงปลอดภัยสารสนเทศ (Information security awareness, education and training)

บุคลากรควรตระหนักถึงนโยบายและกระบวนการที่มีการระบุไว้กำหนดซึ่งบังคับใช้กับความความมั่นคงปลอดภัยทางสารสนเทศ โดยที่จำเป็นต้องมีการกำหนดนโยบายและการบังคับใช้ที่ชัดเจนสำหรับบุคลากร (ทั้งภายในหรือภายนอก) ที่ทำงานในส่วนปฏิบัติการหรือส่วนซ่อมบำรุง ตลอดอายุการทำงานของอุปกรณ์นั้น และต้องมีการบูรณาการความมั่นคงปลอดภัยทางเครือข่ายให้ครอบคลุมการใช้ประโยชน์ในแง่ต่างๆ ซึ่งเป็นสิ่งสำคัญที่บุคลากรทุกคนต้องมีความเข้าใจ การตระหนักและได้รับการฝึกอบรมเพื่อนำไปปรับใช้เตรียมกับความมั่นคงปลอดภัยทางเครือข่าย

ผู้ใช้ทุกคนที่มีความเกี่ยวข้องความมั่นคงปลอดภัยทางสารสนเทศจะต้องได้รับการรับรองและควบคุม ซึ่งการฝึกอบรมความมั่นคงปลอดภัยทางไซเบอร์เพื่อการออกใบรับรองควรดำเนินการโดยผู้ให้บริการที่ได้รับการรับรองและมีข้อจำกัดดังนี้

- จำเป็นต้องมีการฝึกอบรมผู้ใช้ก่อนที่จะมีการแทรกแซงใด ๆ บนระบบจัดการองค์กรสำหรับการบัญชาการ ICS (Incident Command System)
- การฝึกอบรมความมั่นคงปลอดภัยทางไซเบอร์ควรดำเนินการโดยผู้ให้บริการที่ได้รับการรับรอง

การฝึกอบรมความมั่นคงปลอดภัยทางไซเบอร์ของระบบจัดการองค์กรสำหรับการบัญชาการและการสร้างความตระหนักรู้ควรจัดขึ้นพร้อมกันกับการอบรมเรื่องความปลอดภัยและความมั่นคง

3.3.2.3 กระบวนการทางวินัย (Disciplinary process)

ในกรณีที่พนักงานที่มีหน้าที่รับผิดชอบต่อการละเมิดความปลอดภัยของข้อมูลและไม่รายงานการละเมิดนี้ต่อฝ่ายบริหารหรือไม่สามารถรายงานได้ในทันที พนักงานควรถูกแยกออกมาและดำเนินการทางวินัยที่เหมาะสม โดยที่พนักงานควรได้รับแจ้งให้ทราบล่วงหน้าถึงการลงโทษทางวินัย

3.3.3 การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

พนักงานที่ออกจากองค์กรไปแล้ว จะต้องถูกการยกเลิกสิทธิในเข้าถึงระบบในส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง พนักงานจะต้องส่งคืนคุณลักษณะและเครื่องมือที่เกี่ยวข้องกับส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบราง สิทธิในเข้าถึงข้อมูลที่ถูกสร้างโดยพนักงานที่พ้นจากหน้าที่ไปแล้ว จะต้องถูกส่งต่อไปยังพนักงานคนอื่นที่ยังปฏิบัติหน้าที่อยู่โดยทันที

3.4 การบริหารจัดการทรัพย์สิน (Asset management)

อ้างอิงจากมาตรฐาน UIC ก่อนหน้านี้ : คำแนะนำสำหรับ“การดำเนินการจัดการสินทรัพย์ในทางปฏิบัติผ่านมาตรฐาน ISO 550013”

3.4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)

วัตถุประสงค์ของหัวข้อนี้คือเพื่อให้บรรลุและรักษาไว้ซึ่งการปกป้องทรัพย์สินขององค์กรอย่างเหมาะสม

ทรัพย์สินทั้งหมดควรได้รับการบันทึกไว้และมีผู้แทนของบริษัทในการพิจารณาซึ่งควรกำหนดเจ้าของ ของทรัพย์สินทั้งหมดและมอบหมายความรับผิดชอบในการบำรุงรักษาที่เหมาะสม

การดำเนินการตามการควบคุมเฉพาะอาจจะขึ้นอยู่กับดุลยพินิจของเจ้าของตามความเหมาะสม โดยที่เจ้าของยังคงต้องรับผิดชอบต่อการปกป้องทรัพย์สินอย่างเหมาะสม

3.4.1.1 บัญชีทรัพย์สิน (Inventory of assets)

ควรมีการระบุทรัพย์สินทั้งหมดไว้อย่างชัดเจน และต้องมีการรวบรวมรายการและบำรุงรักษาบัญชีทรัพย์สินที่สำคัญทั้งหมดไว้ด้วย

องค์กรควรจำแนกทรัพย์สินและเอกสารที่สำคัญของทรัพย์สินเหล่านี้ทั้งหมดซึ่งองค์กรควรเน้นที่ระบบมากกว่าอุปกรณ์ซึ่งประกอบด้วย PLC, DCS, SCADA และระบบเครื่องมือวัดขั้นพื้นฐานที่ใช้เป็นอุปกรณ์เฝ้าสังเกตการณ์ เช่น HMI

ในบัญชีทรัพย์สินควรมีข้อมูลทั้งหมดที่จำเป็นในการกู้คืนจากภัยอันตรายด้วย รวมถึงประเภทของทรัพย์สิน รูปแบบ ตำแหน่ง ข้อมูลสำรอง ใบอนุญาตและมูลค่าทางธุรกิจ ใบบัญชีทรัพยท์สินไม่ควรมีการทำสำเนารายการที่ไม่จำเป็น แต่ต้องมั่นใจว่าเนื้อหานั้นสอดคล้องกัน

ทีมงานควรตรวจสอบและอัปเดตรายการทรัพย์สินเป็นประจำทุกปีและหลังจากการเพิ่มหรือลบเนื้อหาแต่ละครั้ง นอกจากนี้ควรมีการตกลงและจัดทำเป็นเอกสารแสดงความเป็นเจ้าของและข้อมูลสำหรับแต่ละประเภทของสินทรัพย์

มูลค่าทางธุรกิจและการจัดประเภทความปลอดภัย ระดับของการป้องกันที่สอดคล้องกับระดับความสำคัญของสินทรัพย์ ควรได้รับการระบุอย่างชัดเจนโดยยึดตามความสำคัญของสินทรัพย์

ทรัพย์สินมีหลายประเภท ประกอบด้วย

- ทรัพย์สินอุตสาหกรรม: PLC, DCS, SCADA
- สารสนเทศ: ฐานข้อมูลและไฟล์ข้อมูล สัญญาและข้อตกลง คู่มือระบบ ข้อมูลการวิจัย คู่มือใช้งาน อุปกรณ์ในการฝึกอบรม ขั้นตอนการปฏิบัติงานหรือการสนับสนุน แผนความต่อเนื่องทางธุรกิจ การจัดการทางเลือก ขั้นตอนในการตรวจสอบ และข้อมูลที่เก็บถาวร
- ทรัพย์สินทางซอฟต์แวร์: ซอฟต์แวร์แอปพลิเคชัน ซอฟต์แวร์ระบบ เครื่องมือพัฒนา และสิ่งอำนวยความสะดวก
- ทรัพย์สินทางกายภาพ: อุปกรณ์คอมพิวเตอร์ อุปกรณ์ในการสื่อสาร อุปกรณ์แบบถอดได้และอุปกรณ์อื่น ๆ

- บริการ: การบริการคอมพิวเตอร์และการสื่อสาร สิ่งอำนวยความสะดวกทั่วไป เช่น ระบบทำความร้อน แสงสว่าง ไฟฟ้า และเครื่องปรับอากาศ
- บุคคลและคุณสมบัติ ทักษะ และประสบการณ์
- สิ่งที่จับต้องไม่ได้ เช่น ชื่อเสียงและภาพลักษณ์ขององค์กร

3.4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of assets)

ข้อมูลและทรัพย์สินทั้งหมดที่เกี่ยวข้องกับสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลควรถูกกำหนดโดยเจ้าของ[1] ซึ่งเป็นส่วนหนึ่งของการจัดการองค์กร ซึ่งอาจมีการมอบหมายงานประจำ เช่น ผู้ดูแลทรัพย์สินมีหน้าที่ดูแลทรัพย์สินเป็นประจำทุกวัน แต่ความรับผิดชอบนั้นยังคงอยู่กับผู้ถือครองทรัพย์สิน

หน้าที่รับผิดชอบของผู้ถือครองทรัพย์สินมีดังนี้

ก) ตรวจสอบให้แน่ใจว่าข้อมูลและทรัพย์สินที่เกี่ยวข้องกับสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลนั้นถูกกำหนดอย่างเหมาะสมแล้ว

ข) กำหนดและตรวจสอบข้อจำกัดในการเข้าถึงข้อมูลเป็นระยะและการจำแนกประเภทเป็นระยะ โดยคำนึงถึงนโยบายการควบคุมการเข้าถึงที่เกี่ยวข้อง

ความเป็นเจ้าของอาจถูกจัดสรรให้กับ:

- กระบวนการทางธุรกิจ
- ชุดกิจกรรมที่กำหนด
- ใบสมัคร; หรือ
- ชุดข้อมูลที่กำหนด

1 คำว่า "เจ้าของ" ระบุบุคคลหรือนิติบุคคลที่ได้อนุมัติความรับผิดชอบในการจัดการควบคุมการผลิต การพัฒนา การบำรุงรักษา การใช้และการรักษาความปลอดภัยของทรัพย์สิน คำว่า 'เจ้าของ' ไม่ได้หมายความว่าบุคคลนั้นมีสิทธิ์ในทรัพย์สินใด ๆ ในทรัพย์สินนั้นจริงๆ

3.4.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

ควรมีการระบุกฎเกณฑ์สำหรับการใช้ข้อมูลและทรัพย์สินที่เกี่ยวข้องกับสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล จัดทำเป็นลายลักษณ์อักษรและนำไปปฏิบัติ

ควรมีการจัดเตรียมกฎระเบียบหรือคำแนะนำเฉพาะโดยฝ่ายบริหารที่เกี่ยวข้อง พนักงาน ผู้รับเหมา ผู้ใช้งาน บุคคลภายนอกที่ใช้หรือมีสิทธิ์เข้าถึงทรัพย์สินขององค์กร ควรรับผิดชอบต่อการใช้ทรัพยากรการประมวลผลข้อมูลและการใช้งานดังกล่าวจะดำเนินการภายใต้ความรับผิดชอบของตน

3.4.1.4 การคืนทรัพย์สิน (Return of assets)

พนักงาน ผู้รับเหมาและผู้ใช้งานที่เป็นบุคคลภายนอกควรส่งคืนทรัพย์สินที่มีส่วนเกี่ยวข้องกับส่วนควบคุมอัตโนมัติและส่วนกลไกระยะไกลของระบบรางขององค์กรที่อยู่ในความครอบครองของตนทั้งหมดเมื่อหมดสัญญาจ้างหรือข้อตกลง

ในกรณีที่พนักงาน ผู้รับเหมาหรือผู้ใช้บุคคลภายนอกมีความรู้ที่สำคัญต่อการดำเนินงานอย่างต่อเนื่อง ข้อมูล ความรู้ นั้นควรได้รับการจัดทำเป็นเอกสารและถ่ายโอนไปยังองค์กร

ขั้นตอนสุดท้ายของการส่งคืนทรัพย์สินควรทำให้เป็นระเบียบแบบแผน ซึ่งประกอบด้วยการส่งคืนซอฟต์แวร์ เอกสารขององค์กร และอุปกรณ์ก่อนหน้านี้ทั้งหมด รวมไปถึงคืนทรัพย์สินอื่นๆ ขององค์กร เช่น อุปกรณ์คอมพิวเตอร์พกพา บัตรเครดิต บัตรเข้าใช้งาน ซอฟต์แวร์ คู่มือและข้อมูลที่เก็บไว้ในสื่ออิเล็กทรอนิกส์

3.4.2 การจัดชั้นความลับของสารสนเทศ (Information classification)

วัตถุประสงค์ของบทนี้คือเพื่อให้สารสนเทศได้รับการป้องกันในระดับที่เหมาะสม และเพื่อบ่งชี้ลำดับความสำคัญและระดับการป้องกันที่คาดหวังเมื่อจัดการข้อมูล ซึ่งข้อมูลมีระดับความอ่อนไหวและความสำคัญต่างกันไป เช่น ใช้ภายใน ลับ และ ลับมาก บางข้อมูลอาจต้องมีระดับการป้องกันเพิ่มเติมหรือการจัดการรูปแบบพิเศษ ควรใช้รูปแบบการจำแนกประเภทของข้อมูลเพื่อกำหนดชุดระดับการป้องกันที่เหมาะสมและสื่อสารถึงความต้องการมาตรการจัดการพิเศษ

3.4.2.1 ชั้นความลับของสารสนเทศ (Classification of information)

ข้อมูลควรได้รับการจัดประเภทตามคุณลักษณะ ข้อกำหนดทางกฎหมาย ความอ่อนไหวและความสำคัญต่อองค์กร รวมถึงพนักงานที่จัดการความปลอดภัยขององค์กรจะต้องกำหนดรายชื่อบุคคลหรือบทบาทต่อหน้าที่ในการจำแนกข้อมูลที่ได้รับการจัดการ (เช่น: สมาชิกคณะกรรมการบริหาร)

การจำแนกประเภทและการควบคุมการป้องกันที่เกี่ยวข้องสำหรับข้อมูลควรคำนึงถึงความต้องการทางธุรกิจในการแบ่งปันหรือการจำกัดข้อมูลและผลกระทบทางธุรกิจที่เกี่ยวข้องกับความต้องการดังกล่าว ระดับการป้องกันสามารถประเมินได้โดยการวิเคราะห์ชั้นความลับ ความสมบูรณ์ ความพร้อมใช้งาน และข้อกำหนดอื่นๆ ของข้อมูลที่ใช้พิจารณา

แนวทางในการจำแนกประเภทควรรวมถึงข้อตกลงสำหรับการจำแนกประเภทขั้นพื้นฐานและการจัดประเภทใหม่ตามกาลเวลา ซึ่งอ้างอิงตามนโยบายการควบคุมการเข้าถึงที่มีการกำหนดไว้ล่วงหน้า รวมถึงควรแจ้งกฎที่เกี่ยวข้องกับการป้องกันข้อมูลเหล่านี้แก่พนักงานและเจ้าหน้าที่บุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงข้อมูลขององค์กร

เจ้าของสินทรัพย์ควรเป็นผู้รับผิดชอบในการจำแนกประเภทของสินทรัพย์ ตรวจสอบทรัพย์สินเป็นระยะเพื่อให้แน่ใจว่าได้รับการปรับปรุงให้เป็นปัจจุบันและอยู่ในระดับที่เหมาะสม โดยควรคำนึงถึงผลของการรวบรวมที่กล่าวไว้ในส่วนที่ 3.4.3.2

ซึ่งโดยทั่วไปแล้ว การจำแนกประเภทให้กับข้อมูลเป็นวิธีการเขียนข้อความอย่างย่อด้วยสัญลักษณ์ในการพิจารณาว่าจะจัดการและป้องกันข้อมูลนี้อย่างไร

3.4.2.2 การบ่งชี้สารสนเทศ (Labeling of information)

ควรมีการพัฒนาชุดขั้นตอนที่เหมาะสมสำหรับการบ่งชี้สารสนเทศและดำเนินการตามรูปแบบการจำแนกประเภทที่การรถไฟนำมาใช้

ขั้นตอนในการบ่งชี้สารสนเทศจำเป็นต้องครอบคลุมทรัพย์สินข้อมูลในรูปแบบทางกายภาพและอิเล็กทรอนิกส์

ซึ่งการบ่งชี้ควรแสดงถึงการจำแนกประเภทตามกฎที่กำหนดไว้ในส่วนที่ 3.4.2.1

ควรใช้ระบบการบ่งชี้ที่ผ่านการตกลงแล้ว สำหรับข้อมูลที่ละเอียดอ่อนหรือสำคัญ เพื่อให้มั่นใจว่ามีการเข้าใจความหมายของการบ่งชี้สารสนเทศทันทีและข้อมูลนั้นได้รับการปกป้องอย่างเหมาะสม

3.4.2.3 การจัดการทรัพย์สิน (Handling of assets)

ควรมีการพัฒนาขั้นตอนปฏิบัติที่เหมาะสมสำหรับการจัดการข้อมูลและดำเนินการตามรูปแบบการจำแนกประเภทที่การรถไฟนำมาใช้

ควรกำหนดขั้นตอนการจัดการรวมถึงการประมวลผลที่ปลอดภัย การจัดเก็บ การส่งผ่าน การแยกประเภท และการทำลายล้างในแต่ละระดับการจำแนกประเภท

นอกจากนี้ยังควรรวมถึงขั้นตอนสำหรับการดูแลต่อเนื่องและการบันทึกเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัย การจัดการชั้นความลับของข้อมูลอย่างปลอดภัยเป็นข้อกำหนดหลักสำหรับการเตรียมการแบ่งปันข้อมูล ฉลากทางกายภาพเป็นรูปแบบทั่วไปของการติดฉลาก

3.4.3 การจัดการสื่อบันทึกข้อมูล (Media handling)

ควรมีการกำหนดขั้นตอนการปฏิบัติงานที่เหมาะสมเพื่อปกป้องเอกสาร สื่อคอมพิวเตอร์ เช่น เทป ดิสก์ ข้อมูลเข้า/ข้อมูลออก และเอกสารระบบจากการเปิดเผยโดยไม่ได้รับอนุญาต การแก้ไข การลบหรือการทำลายทรัพย์สิน และการแทรกแซงของกิจกรรมทางธุรกิจ

สื่อควรได้รับการควบคุมและป้องกันทางกายภาพด้วยเช่นกัน

3.4.3.1. การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)

สื่อที่ถอดแยกได้ รวมถึง เทป ดิสก์ แฟลชดิสก์ ฮาร์ดไดรฟ์แบบถอดได้ ซีดี ดีวีดี และสื่อสิ่งพิมพ์ ควรมีขั้นตอนปฏิบัติสำหรับการจัดการสื่อแบบถอดได้เหล่านี้โดยพิจารณาจาก

ก) หากไม่ต้องการเก็บสื่อไว้อีกต่อไป ควรทำให้เนื้อหาของสื่อที่ใช้ซ้ำได้ ซึ่งจะถูกลบออกจากองค์กรไม่สามารถกู้คืนได้

ข) ในกรณีที่จำเป็นควรมีการอนุญาตเพื่อกำจัดสื่อออกจากองค์กรและควรเก็บบันทึกการลบดังกล่าวไว้เพื่อการตรวจสอบภายหลัง

ค) สื่อทั้งหมดควรถูกจัดเก็บในสภาพแวดล้อมที่ปลอดภัยตามข้อกำหนดของผู้ผลิต

ง) ข้อมูลที่ถูกจัดเก็บบนสื่อที่จำเป็นต้องนำมาใช้งานนานกว่าอายุการใช้งานของสื่อ (ตามข้อกำหนดของผู้ผลิต) ควรนำไปจัดเก็บไว้ที่อื่นเพื่อหลีกเลี่ยงข้อมูลสูญหายเนื่องจากการเสื่อมสภาพของสื่อ

จ) ควรมีการลงทะเบียนสื่อแบบถอดได้เพื่อป้องกันโอกาสที่ข้อมูลจะสูญหาย

ช) ไดร์ฟสื่อแบบถอดได้ควรเปิดใช้งานก็ต่อเมื่อมีเหตุผลทางธุรกิจในการทำเช่นนั้น

3.4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media)

สื่อบันทึกข้อมูลต้องมีการกำจัดอย่างมั่นคงและปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนการปฏิบัติที่มีการกำหนดอย่างเป็นทางการ จะช่วยลดความเสี่ยงของการรั่วไหลของข้อมูลที่ละเอียดอ่อนไปยังบุคคลที่ไม่ได้รับอนุญาต

ขั้นตอนการปฏิบัติสำหรับการกำจัดสื่อที่มีข้อมูลที่มีความอ่อนไหวอย่างปลอดภัย ควรปฏิบัติให้สอดคล้องกับความอ่อนไหวของข้อมูลนั้น ดังนี้

- จัดเก็บและกำจัดอย่างมั่นคงและปลอดภัย เช่น กำจัดโดยการเผา หั่นย่อย หรือลบข้อมูลโดยใช้โดยแอปพลิเคชันอื่นภายในองค์กร
- ควรมีขั้นตอนปฏิบัติสำหรับการจำแนกสิ่งของที่จำเป็นต้องมีการกำจัดอย่างปลอดภัย
- ควรบันทึกการกำจัดสื่อที่มีความอ่อนไหว เพื่อเป็นหลักฐานสำหรับการตรวจสอบ
- หลายองค์กรเสนอว่าการรวบรวมและกำจัดเอกสารอุปกรณ์และสื่อต่างๆ ควรใช้ความระมัดระวังในการเลือกผู้ทำสัญญาจ้างที่เหมาะสมพร้อมกับการควบคุมและประสบการณ์ที่เพียงพอ

3.4.3.3. การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)

สื่อบันทึกข้อมูลที่มีข้อมูลบรรจุอยู่ต้องมีการปกป้องจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ในทางที่ผิดวัตถุประสงค์ หรือความเสียหายระหว่างการขนส่งที่อยู่นอกขอบเขตทางกายภาพขององค์กร เช่น เมื่อส่งสื่อผ่านบริการไปรษณีย์หรือผ่านคนส่งเอกสาร

สิ่งที่ควรพิจารณาคือ

- ควรใช้การขนส่งหรือบริการจัดส่งที่เชื่อถือได้
- รายชื่อผู้ให้บริการจัดส่งที่ได้รับอนุญาตควรได้รับความเห็นชอบจากฝ่ายบริหาร
- ควรมีการพัฒนาขั้นตอนปฏิบัติในการตรวจสอบยืนยันตัวตนของผู้ให้บริการจัดส่ง
- บรรจุภัณฑ์ที่ใช้ในการขนส่งสื่อต้องมีการปกป้องที่เพียงพอจากความเสียหายทางกายภาพที่อาจเกิดขึ้นระหว่างการขนส่งและยึดตามข้อกำหนดของผู้ผลิต (เช่น ข้อกำหนดสำหรับซอฟต์แวร์) ตัวอย่างการป้องกันปัจจัยแวดล้อมใด ๆ ที่อาจลดประสิทธิภาพในการฟื้นฟูของสื่อเช่นการสัมผัสกับความร้อน ความชื้นหรือสนามแม่เหล็กไฟฟ้า
- ควรนำหลักการควบคุมมาใช้ในกรณีที่จำเป็นเพื่อปกป้องข้อมูลที่มีความอ่อนไหวจากการถูกเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต ตัวอย่าง เช่น
  1) การใช้บรรจุภัณฑ์ที่ล็อคได้
  2) ขนย้ายด้วยความระมัดระวัง
  3) ป้องกันการปลอมแปลงบรรจุภัณฑ์ (ซึ่งเผยให้เห็นถึงความพยายามในการเข้าถึงข้อมูล)
  4) ในกรณีพิเศษ การจัดส่งสินค้าอาจจะแบ่งออกเป็นมากกว่าหนึ่งการจัดส่งและจัดส่งตามเส้นทางที่แตกต่างกัน

3.5 การควบคุมการเข้าถึง (Access control)

วัตถุประสงค์คือเพื่อควบคุมการเข้าถึง และ จำกัดการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล

- เฉพาะบุคคลที่ได้รับอนุญาตในการเข้าใช้งานเท่านั้นที่จะสามารถเข้าถึงเครือข่าย หรือองค์ประกอบของการส่งสัญญาณได้

ซึ่งต้องมีการกำหนดแนวทางการแก้ไขและขั้นตอนปฏิบัติเพื่อตอบสนองต่อวัตถุประสงค์

3.5.1. ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

ควรมีการควบคุมการเข้าถึงข้อมูล อุปกรณ์ในการประมวลผลข้อมูล และขั้นตอนปฏิบัติทางธุรกิจ (การซ่อมบำรุง, การดำเนินการทางเทคนิค) ตามข้อกำหนดพื้นฐานของระบบรางและการรักษาความปลอดภัย

กฎในการควบคุมการเข้าถึงควรพิจารณาตามนโยบายการเผยแพร่และการอนุญาตในการเข้าถึงข้อมูล

3.5.1.1. นโยบายการควบคุมการเข้าถึง (Access control policy)

ควรมีการกำหนดนโยบายในการควบคุมการเข้าถึง จัดทำเป็นลายลักษณ์อักษร และทบทวนตามความต้องการในการเข้าถึงของหน่วยงานระบบราง และความมั่นคงปลอดภัย รวมไปถึงควรพิจารณาการควบคุมการเข้าถึงทั้งในเชิงตรรกะ และเชิงกายภาพ

ควรมีการระบุถึงกฎและสิทธิในการควบคุมการเข้าถึงและหน้าที่ความรับผิดชอบของแต่ละผู้ใช้หรือกลุ่มผู้ใช้อย่างชัดเจนในนโยบายการควบคุมการเข้าถึง ผู้ใช้และผู้ให้บริการควรได้รับคำชี้แจงอย่างชัดเจนถึงข้อกำหนดทางธุรกิจที่ซึ่งต้องตอบสนองต่อหลักการควบคุมการเข้าถึง โดยนโยบายควรตระหนักถึงสิ่งต่อไปนี้

- ข้อกำหนดด้านความปลอดภัยของระบบอัตโนมัติของรางรถไฟแต่ละตัว ระบบควบคุมทางกลระยะไกล และ ซอฟต์แวร์ทางเทคโนโลยี
- การจำแนกสารสนเทศที่เกี่ยวข้องกับระบบอัตโนมัติของรางรถไฟ ระบบควบคุมทางกลระยะไกล ซอฟต์แวร์ทางเทคโนโลยี และความเสี่ยงที่สารสนเทศกำลังเผชิญอยู่
- นโยบายสำหรับการเผยแพร่และการอนุญาตในการเข้าถึงสารสนเทศ เช่น จำเป็นต้องทราบถึงหลักปฏิบัติการ และระดับการรักษาความปลอดภัยและการจำแนกประเภทของสารสนเทศ
- ความสอดคล้องระหว่างนโยบายการควบคุมการเข้าถึง และการจำแนกประเภทสารสนเทศบนระบบและเครือข่ายที่แตกต่างกัน
- กฎหมายที่เกี่ยวข้อง และภาระผูกพันของสัญญาใดๆ ที่เกี่ยวกับการคุ้มครองการเข้าถึงสารสนเทศหรือบริการ
- ประวัติการเข้าถึงของผู้ใช้มาตรฐานสำหรับงานทั่วไปในองค์กร
- การบริหารจัดการสิทธิ์ในการเข้าถึงของระบบการประมวลผลแบบกระจายและแบบเครือข่าย ซึ่งจดจำการเชื่อมต่อทุกประเภทที่พร้อมใช้งาน

- การแบ่งบทบาทการควบคุมการเข้าถึง เช่น การร้องขอเข้าถึง สิทธิ์ในการเข้าถึง การดูแลระบบการเข้าถึง
- ข้อกำหนดสำหรับรูปแบบของการร้องขอสิทธิ์ในการเข้าถึง
- ข้อกำหนดสำหรับการตรวจสอบการควบคุมการเข้าถึงเป็นระยะ
- การยกเลิกสิทธิ์การเข้าถึง (ดูในบทที่ 3.5.2.6)

ควรใช้ความระมัดระวังในการกำหนดกฎของการควบคุมการเข้าถึงเพื่อนำไปพิจารณา

- การแยกความแตกต่างระหว่างกฎที่มีการบังคับใช้อยู่ตลอดเวลา และแนวปฏิบัติว่าเป็น แบบทางเลือกหรือแบบมีเงื่อนไข
- การจัดทำกฎโดยอ้างอิงตามหลักที่ว่า “ทุกสิ่งเป็นสิ่งต้องห้ามเว้นแต่จะได้รับอนุญาตอย่างชัดแจ้ง” มากกว่าหลักที่ว่า “ทุกสิ่งได้รับการอนุญาตเว้นแต่จะมีการห้ามอย่างชัดแจ้ง”
- การเปลี่ยนแปลงที่เกิดขึ้นในการบ่งชี้สารสนเทศที่เกิดขึ้นโดยอัตโนมัติจากอุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศและดุลยพินิจของผู้ใช้
- การเปลี่ยนแปลงที่เกิดขึ้นในการอนุญาตผู้ใช้ที่เกิดขึ้นโดยอัตโนมัติบนระบบสารสนเทศและจากผู้ดูแลระบบ
- กฎที่ต้องได้รับการอนุมัติเป็นการเฉพาะก่อนประกาศใช้และกฎที่ไม่ต้องได้รับการอนุมัติก่อนการประกาศใช้

3.5.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

ควรมีการจัดตั้งนโยบายโดยคำนึงถึงการเข้าใช้งานเครือข่ายและการบริการเครือข่าย ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการตามที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

รวมถึงผู้ใช้งานควรตระหนักถึงการรักษาความมั่นคงปลอดภัยของการบริการเครือข่ายโดยตรวจสอบให้แน่ใจว่า

- การเชื่อมต่อที่เหมาะสมอยู่ในพื้นที่ระหว่าง ระบบเครือข่าย เครือข่ายที่ให้บริการโดยองค์กรอื่น และเครือข่ายสาธารณะ
- มีการใช้กลไกการตรวจสอบที่เหมาะสมสำหรับผู้ใช้และอุปกรณ์
- ควบคุมของผู้ใช้เข้าถึงข้อมูลการบริการต้องถูกบังคับ

การเชื่อมต่อกับการส่งสัญญาณเครือข่ายที่ไม่ผ่านการรับรองและไม่ปลอดภัยอาจส่งผลกระทบต่อองค์กรในทุกๆ ด้าน การควบคุมนี้มีความสำคัญอย่างยิ่งสำหรับการเชื่อมต่อเครือข่ายที่มีความอ่อนไหวหรือมีความสำคัญต่อการส่งสัญญาณและการสื่อสารโทรคมนาคมหรือต่อผู้ใช้งานในสถานที่ที่มีความเสี่ยงสูง เช่น พื้นที่สาธารณะหรือพื้นที่ภายนอกที่อยู่นอกเหนือการจัดการและการควบคุมความปลอดภัยขององค์กร

3.5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

วัตถุประสงค์คือเพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงเครือข่ายจากการส่งสัญญาณโดยไม่ได้รับอนุญาต

ควรมีการกำหนดกระบวนการปฏิบัติอย่างเป็นทางการเพื่อควบคุมการจัดสรรสิทธิ์การเข้าถึงเครือข่ายสัญญาณและอุปกรณ์

กระบวนการควรครอบคลุมทุกขั้นตอนของวงจรการเข้าถึงของผู้ใช้งานตั้งแต่การลงทะเบียนครั้งแรกของผู้ใช้ใหม่ จนถึงการยกเลิกการลงทะเบียนซึ่งเป็นขั้นสุดท้ายของผู้ใช้ที่ไม่ต้องการเข้าถึงข้อมูลระบบและบริการอีกต่อไป ควรให้ความสนใจเป็นพิเศษตามความเหมาะสมกับความจำเป็นในการควบคุมการจัดสรรสิทธิ์พิเศษในการเข้าถึงซึ่งอนุญาตให้ผู้ใช้งานเข้าถึงการควบคุมระบบได้ทุกส่วน

3.5.2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

ควรมีขั้นตอนการลงทะเบียนและการยกเลิกผู้ใช้อย่างเป็นทางการในการอนุญาตและการเพิกถอนการเข้าถึงระบบและบริการของระบบรางทั้งหมด

ขั้นตอนควบคุมการเข้าถึงสำหรับการลงทะเบียนและยกเลิกการลงทะเบียนผู้ใช้ควรรวมถึง

- การใช้ ไอดี ผู้ใช้ที่ไม่ซ้ำกันเพื่อให้ผู้ใช้สามารถเชื่อมโยงและรับผิดชอบต่อการกระทำของตนบนระบบไซเบอร์ ควรอนุญาตให้ใช้ ไอดี กลุ่มเฉพาะในกรณีที่จำเป็นสำหรับเหตุผลทางธุรกิจหรือเหตุผลในการปฏิบัติงานซึ่งควรผ่านการอนุมัติและจัดทำเป็นลานลักษณ์อักษร
- ตรวจสอบการอนุมัติสิทธิ์การเข้าถึงจากเจ้าของระบบสำหรับการใช้งานของระบบและบริการของระบบราง อาจมีการอนุมัติสิทธิ์การเข้าถึงแยกต่างหากจากฝ่ายบริหาร
- ตรวจสอบให้แน่ใจว่าระดับการเข้าถึงของผู้ใช้ที่ได้รับนั้นเหมาะสมกับวัตถุประสงค์ทางธุรกิจและสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร เช่น ไม่ส่งผลกระทบต่อการแบ่งแยกบทบาทเฉพาะหน้าที่
- ให้คำชี้แจงสิทธิ์การเข้าถึงแก่ผู้ใช้เป็นลายลักษณ์อักษร
- ต้องมีการให้ผู้ใช้ลงนามเพื่อระบุว่าเข้าใจเงื่อนไขในการเข้าถึงการใช้งาน
- ตรวจสอบให้แน่ใจว่าผู้ให้บริการไม่จัดให้มีการเข้าถึงได้ จนกว่าขั้นตอนการขออนุญาตสิทธ์ในการเข้าถึงจะแล้วเสร็จสมบูรณ์
- เก็บรักษาบันทึกข้อมูลที่ลงทะเบียนเพื่อใช้บริการของผู้ใช้งานทุกคน
- ยกเลิกหรือปิดกั้นการเข้าถึงของผู้ใช้ที่เปลี่ยนบทบาท หน้าที่ หรือ ออกจากองค์กรไปแล้วโดยทันที
- ตรวจสอบ ยกเลิก หรือ ปิดกั้น ไอดีผู้ใช้และบัญชีที่ซ้ำซ้อน เป็นระยะ
- ตรวจสอบให้แน่ใจว่าไม่มีการออก ไอดี ผู้ใช้ที่ซ้ำซ้อนให้กับผู้ใช้รายอื่น

3.5.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)

ควรมีการควบคุมการจัดสรรของรหัสผ่านเข้าใช้งานผ่านกระบวนการการจัดการอย่างเป็นทางการ

กระบวนการการจัดการควรมีข้อกำหนดต่อไปนี้

- ผู้ใช้ต้องเก็บรักษารหัสผ่านของตนเอง โดยควรได้รับรหัสผ่านชั่วคราวที่ปลอดภัยในเบื้องต้นสำหรับการเข้าใช้งานครั้งแรก และต้องทำการเปลี่ยนรหัสผ่านโดยทันที
- ให้ผู้ใช้มีการลงนามเป็นลายลักษณ์อักษรว่าจะเก็บรักษารหัสเข้าใช้งานของตัวเองเป็นความลับและหลีกเลี่ยงการแบ่งปันรหัสให้คนอื่น ซึ่งการลงนามอย่างเป็นลายลักษณ์อักษรอาจจะรวมอยู่ในข้อกำหนดหรือเงื่อนไขในการจ้างงานด้วย
- จัดทำขั้นตอนเพื่อตรวจสอบการระบุตัวตนของผู้ใช้ก่อนสร้างหรือเปลี่ยนรหัสใหม่หรือให้รหัสชั่วคราว และการปรับปรุงรหัสในช่วงเวลาปกติ
- ผู้ใช้ควรได้รับรหัสผ่านชั่วคราวด้วยวิธีการที่มีความปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลที่สาม หรือ ข้อความอีเมลอิเล็กทรอนิกส์ที่ไม่ได้รับการป้องกัน
- รหัสผ่านชั่วคราวควรมีเอกลักษณ์เฉพาะแต่ละบุคคลและควรคาดเดาได้ยาก
- ผู้ใช้ควรมีการตอบกลับถึงการได้รับรหัสผ่าน
- รหัสผ่านไม่ควรถูกเก็บบนระบบคอมพิวเตอร์ในรูปแบบไร้การป้องกัน
- ควรเปลี่ยนรหัสผ่านเริ่มต้นของผู้ให้บริการ หลังการติดตั้งของระบบหรือซอฟต์แวร์

รหัสผ่านเป็นวิธีการทั่วไปของการตรวจสอบการระบุตัวตนของผู้ใช้ก่อนได้รับการเข้าถึงข้อมูลของระบบ หรือบริการ ตามสิทธิ์ของผู้ใช้และยังมีเทคโนโลยีอื่นที่ใช้สำหรับการระบุและยืนยันตัวตนของผู้ใช้ โดยการตรวจสอบเชิงชีวภาพ ตัวอย่างเช่น การตรวจสอบลายนิ้วมือ การตรวจสอบลายเซ็น และการตรวจสอบโดยใช้อุปกรณ์โทเค็น ตัวอย่างเช่น สมาร์ทการ์ด ซึ่งสามารถนำมาใช้ได้ และควรได้รับการพิจารณาตามความเหมาะสม

3.5.2.3 การจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

ระบบปฏิบัติการที่รองรับผู้ใช้งานได้มากกว่า 2 คนที่จำเป็นต้องมีการป้องกันเพื่อต่อต้านการเข้าถึงแบบไม่ได้รับอนุญาต ควรมีการจำกัดและถูกควบคุมการใช้สิทธิ์พิเศษในการเข้าถึง

ควรมีการระบุรายการของเข้าถึงวัตถุต่างๆ เช่นเดียวกับรายการของการผู้ใช้แต่ละประเภทที่ได้รับอนุญาตและมีสิทธิในการเข้าถึง การเปลี่ยนแปลงสิทธิ์การเข้าถึงสามารถทำได้โดยผู้ดูแลระบบรถไฟอัตโนมัติและระบบควบคุมทางกลระยะไกลเท่านั้น

ซอฟต์แวร์ระบบรถไฟอัตโนมัติและระบบควบคุมทางกลระยะไกลควรมีระบบการทำงานที่อนุญาตการเข้าถึงวัตถุที่ไม่ผ่านการรับรองและประเภทการเข้าถึงต่างๆ ที่ถูกปฏิเสธ

3.5.2.4 การจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)

ผู้ใช้งานทุกคนควรมีการระบุตัวตนที่เป็นอัตลักษณ์ (user ID) สำหรับการใช้งานส่วนบุคคลเท่านั้น และควรเลือกเทคนิคการตรวจสอบที่เหมาะสมเพื่อให้สามารถนำมาอ้างสิทธิในการยืนยันตัวตนผู้ใช้ได้ รวมถึงควรนำการระบุตัวตน (user ID) มาใช้ในการติดตามกิจกรรมต่างๆ เพื่อหาบุคคลที่รับผิดชอบกิจกรรมเหล่านั้นด้วย และกิจกรรมทั่วไปของผู้ใช้งานไม่ควรดำเนินการจากบัญชีที่ได้รับสิทธิพิเศษ

ในกรณีพิเศษ ที่มีการชี้แจงผลประโยชน์ทางธุรกิจอย่างชัดเจน สามารถใช้งาน user ID ร่วมกันได้ในกลุ่มผู้ใช้งาน 2 คนขึ้นไป หรือในงานเฉพาะเจาะจง โดยควรมีการอนุมัติจากฝ่ายบริหารและต้องจัดทำเป็นลายลักษณ์อักษร อาจต้องมีการควบคุมเพิ่มเติมเพื่อคงไว้ซึ่งความรับผิดชอบ

ไอดีทั่วไปสำหรับใช้งานส่วนบุคคลควรได้รับอนุญาตเฉพาะระบบทำงานที่เข้าถึงได้หรือการใช้งานที่ไม่จำเป็นต้องถูกติดตาม เช่น การเข้าถึงแบบอ่านอย่างเดียว (read only access) หรือ มีการควบคุมอื่นๆ เช่น รหัสผ่านของไอดีทั่วไปที่มีการออกให้แก่พนักงานครั้งละหนึ่งคนและบันทึกการดำเนินการดังกล่าวไว้

ในกรณีที่ต้องการให้มีการตรวจสอบและยืนยันตัวตนที่เข้มงวดขึ้น ควรใช้วิธีการตรวจสอบที่เป็นทางเลือกแทนการใช้รหัสผ่าน เช่น การเข้ารหัสลับ สมาร์ทการ์ด โทเค็น หรือวิธีการทางชีวภาพ (biometric means)

3.5.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

ฝ่ายบริหารควรตรวจสอบสิทธิในการเข้าถึงของผู้ใช้งานเป็นระยะ โดยใช้กระบวนที่เป็นทางการในการตรวจสอบ โดยจำเป็นอย่างยิ่งที่จะต้องตรวจสอบสิทธิในการเข้าถึงอยู่เป็นประจำเพื่อคงไว้ซึ่งประสิทธิภาพในการควบคุมการเข้าถึงสารสนเทศและบริการสารสนเทศของระบบรถไฟอัตโนมัติ ระบบทางกลระยะไกล และซอฟต์แวร์เทคโนโลยี

การตรวจสอบสิทธิ์การเข้าถึงควรพิจารณาดังแนวทางต่อไปนี้

- ควรตรวจสอบสิทธิการเข้าถึงของผู้ใช้งานเป็นระยะ เช่น มีการตรวจสอบทุก 6 เดือน และหลังจากการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง การลดตำแหน่ง หรือการเลิกจ้าง
- ควรตรวจสอบสิทธิในการเข้าถึงของผู้ใช้งานและจัดสรรใหม่เมื่อมีการย้ายจากหน่วยงานหนึ่งไปยังอีกหน่วยงานหนึ่งภายในองค์กรเดียวกัน
- ควรตรวจสอบการอนุมัติสิทธิพิเศษในการเข้าถึงเป็นระยะๆ เช่น มีการตรวจสอบทุกๆ 3 เดือน
- ควรตรวจสอบการจัดสรรสิทธิพิเศษเป็นระยะเพื่อให้แน่ใจว่าไม่มีการจัดสรรสิทธิที่ไม่ผ่านการอนุมัติ
- มีการบันทึกการเปลี่ยนแปลงของบัญชีผู้ใช้ที่ได้รับสิทธิพิเศษเป็นระยะ

3.5.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้า (Removal or adjustment of access rights)

สิทธิในการเข้าถึงของพนักงาน ลูกจ้างของหน่วยงาน และบุคคลภายนอกต่อสารสนเทศและอุปกรณ์ในการประมวลผลสารสนเทศควรได้รับการถอดถอนเมื่อมีการสิ้นสุดสัญญาว่าจ้าง หมดสัญญาหรือข้อตกลง หรือปรับปรุงเมื่อมีการเปลี่ยนการจ้างงานใดๆ รวมถึง

- ไม่ว่าจะเป็นการสิ้นสุดสัญญาหรือการเปลี่ยนแปลงสัญญาจ้างที่เกิดจากพนักงาน ลูกจ้างของหน่วยงาน บุคคลภายนอก หรือโดยฝ่ายบริหาร และสาเหตุในการสิ้นสุดการว่าจ้าง
- หน้าที่รับผิดชอบปัจจุบันของพนักงาน ลูกจ้างของหน่วยงาน หรือผู้ใช้ประเภทอื่นๆ
- มูลค่าของทรัพย์สินที่เข้าถึงได้ในปัจจุบัน

เมื่อมีการสิ้นสุดสัญญาจ้างงาน ควรมีการทบทวนสิทธิในการเข้าถึงทรัพย์สินที่เกี่ยวข้องกับการบริการและระบบของรถไฟอัตโนมัติและระบบควบคุมทางกลระยะไกลของแต่ละบุคคลใหม่ ซึ่งจะเป็นตัวกำหนดว่าจำเป็นต้องถอดถอนสิทธิในการเข้าถึงหรือไม่

ควรมีการถอดถอนหรือแก้ไขสิทธิในการเข้าถึงรวมทั้งการเข้าถึงเชิงกายภาพและเชิงตรรกะ เช่น รหัสผ่าน บัตรระบุตัวตน อุปกรณ์ในการประมวลผลสารสนเทศ ข้อมูลในการสมัครสมาชิกต่างๆ และการเพิกถอนข้อมูลออกจากเอกสารใดๆ ที่มีการระบุว่าเป็นสมาชิกปัจจุบันขององค์กร

- ควรมีการตรวจสอบสถานภาพและวิธีดำเนินการในการเข้าถึงของพนักงานเมื่อมีการเปลี่ยนแปลงหน้าที่รับผิดชอบของงานหรือมีการสับเปลี่ยนตำแหน่ง
- หากพนักงานลาออกจากองค์กร ควรระงับการเข้าถึงอุปกรณ์ของพนักงานดังกล่าวและควรส่งคืนสถานภาพและวิธีดำเนินการเข้าถึงทั้งหมดแก่องค์กรหรือหน่วยงาน รวมถึงข้อมูลสารสนเทศที่สร้างขึ้นโดยพนักงานที่ลาออก ควรถูกตรวจสอบโดยบุคลากรหรือพนักงานที่ได้รับอนุญาตในเวลาที่เหมาะสม
- หากพนักงาน ลูกจ้างของหน่วยงาน หรือบุคคลภายนอกที่ลาออกไปแล้วทราบรหัสผ่านของบัญชีที่ยังมีการใช้งานอยู่ ควรเปลี่ยนรหัสผ่านเหล่านั้นทันทีเมื่อมีการสิ้นสุดหรือเปลี่ยนแปลงการว่าจ้าง สัญญา หรือข้อตกลง

3.5.3. หน้าที่รับผิดชอบของผู้ใช้งาน (User responsibilities)

ผู้ใช้งานมีหน้าที่ในการป้องกันผู้ใช้ที่เข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหล หรือการโจรกรรมสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ความร่วมมือของบรรดาผู้ใช้ที่ได้รับอนุญาตแล้วมีความสำคัญอย่างยิ่งในแง่ของการักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพ

ผู้ใช้ควรตระหนักถึงความรับผิดชอบของตนเองเพื่อคงไว้ซึ่งการควบคุมการเข้าถึงที่มีประสิทธิภาพ โดยเฉพาะการใช้รหัสผ่านและความปลอดภัยของอุปกรณ์ผู้ใช้ พนักงานแต่ละคนควรปฏิบัติงานที่อยู่ในขอบเขตหน้าที่ความรับผิดชอบของตนเองเท่านั้น โดยไม่ละเมิดสิทธิในการเข้าถึงที่ถูกจัดสรรไว้ และไม่ละเมิดความมั่นคงปลอดภัยใดๆ รวมถึง

- ทำการเปลี่ยนแปลงสถาปัตยกรรมฮาร์ดแวร์หรือซอฟต์แวร์โดยไม่ได้รับอนุญาต
- ใช้ผู้ให้บริการข้อมูลที่ไม่ผ่านการรับรองหรือตรวจสอบ
- เริ่มต้นใช้ซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการทำงานของอุปกรณ์

- ข้ามขั้นตอนปฏิบัติในการเข้าถึงที่กำหนดไว้
- การเข้าถึงระบบเครือข่ายสาธารณะ
- การดำเนินการอื่นๆ ที่อาจก่อให้เกิดภัยคุกคาม

ควรนำนโยบายการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์มาปรับใช้เพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือความเสียหายต่อเอกสาร สื่อ และอุปกรณ์ประมวลผลสารสนเทศ รวมถึงการใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ

3.5.4 การควบคุมการเข้าถึงระบบ (System and application access control)

วัตถุประสงค์ คือ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

ควรมีการนำอุปกรณ์อำนวยความสะดวกด้านความปลอดภัยมาใช้เพื่อจำกัดการเข้าถึงระบบปฏิบัติการกับผู้ใช้งานที่ได้รับสิทธิในการเข้าถึง รวมไปถึงควรมีการตั้งค่าเพื่อป้องกันการทำงานของโปรแกรมที่ไม่ต้องการให้ทำงาน และป้องกันการเชื่อมต่อกับอุปกรณ์เก็บข้อมูลที่ยังไม่ผ่านการรับรองบนระบบควบคุมรางรถไฟอัตโนมัติและควบคุมระยะไกล และซอฟต์แวร์เทคโนโลยี

อุปกรณ์อำนวยความสะดวกที่นำมาใช้ควรมีศักยภาพดังนี้

- สามารถพิสูจน์ตัวตนของผู้ใช้งานที่มีสิทธิในการเข้าถึง ตามนโยบายการควบคุมการเข้าถึงที่มีการกำหนดไว้
- สามารถบันทึกความสำเร็จและความล้มเหลวของระบบยืนยันตัวตน
- สามารถบันทึกการใช้งานของระบบสิทธิพิเศษ
- สามารถแจ้งเตือนเมื่อมีการละเมิดนโยบายความมั่นคงปลอดภัยของระบบ
- สามารถจัดให้มีวิธีการยืนยันตัวตนที่เหมาะสม
- สามารถจำกัดเวลาในการเชื่อมต่อของผู้ใช้ได้อย่างเหมาะสม

3.5.4.1 ขั้นตอนการปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

ควรมีการควบคุมการเข้าถึงระบบปฏิบัติการผ่านทางขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบหรือล็อกอินที่มีความปลอดภัย ตัวอย่างเช่น หากรหัสผ่านถูกส่งผ่านผ่านเครือข่ายในลักษณะข้อความที่ชัดเจนระหว่างที่มีการเข้าระบบอยู่ รหัสผ่านอาจถูกดักจับโดยโปรแกรมดักจับข้อมูล (สนิฟเฟอร์) บนเครือข่าย

ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าสู่ระบบปฏิบัติการควรได้รับการออกแบบเพื่อลดโอกาสของการเข้าถึงโดยไม่ได้รับอนุญาต ดังนั้น ควรมีการเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงการให้ความช่วยเหลือใดๆที่ไม่จำเป็นแก่ผู้ใช้ที่ไม่ได้รับอนุญาตให้เข้าถึงระบบ

ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าสู่ระบบที่ดี ควรจะ:

- ไม่แสดงระบบหรือแอปพลิเคชันจนกว่ากระบวนการเข้าสู่ระบบจะเสร็จสมบูรณ์
- มีการแจ้งเตือนว่าคอมพิวเตอร์ควรเข้าถึงได้โดยผู้ใช้ที่ได้รับอนุญาตหรือมีสิทธิ
- ในการเข้าถึงเท่านั้น

- ไม่มีการแสดงข้อความใดๆในระหว่างขั้นตอนการเข้าสู่ระบบเพื่อให้ความช่วยเหลือผู้ใช้ที่ไม่ได้รับอนุญาตในการเข้าถึงระบบ
- ตรวจสอบความถูกต้องของข้อมูลในการเข้าสู่ระบบเฉพาะข้อมูลที่มีการป้อนเข้าสำเร็จแล้วเท่านั้น
- จำกัดจำนวนครั้งในการอนุญาตให้พยายามเข้าสู่ระบบ เช่น จำกัดจำนวนสามครั้ง รวมไปถึง:

  1) การบันทึกการพยามยามเข้าสู่ระบบที่สำเร็จและไม่สำเร็จ

  2) การบังคับให้มีการหน่วงเวลาก่อนที่จะอนุญาตให้พยายามเข้าสู่ระบบครั้งต่อไปหรือการปฏิเสธความพยายามเข้าสู่ระบบที่ไม่ได้รับอนุญาตเป็นการเฉพาะ

  3) การตัดการเชื่อมต่อข้อมูล

  4) การส่งข้อความแจ้งเตือนไปยังคอนโซลระบบหากการพยายามเข้าสู่ระบบถึงจำนวนครั้งสูงสุด

  5) การตั้งค่าการจำกัดจำนวนครั้งในการลองรหัสผ่านใหม่ร่วมกับความยาวขั้นต่ำของรหัสผ่าน และค่าของระบบที่ได้รับการคุ้มครอง
- จำกัดจำนวนครั้งสูงสุดและต่ำสุดสำหรับขั้นตอนการเข้าสู่ระบบ หากเกินจำนวนครั้งที่ตั้งไว้ ระบบควรยกเลิกการเข้าสู่ระบบ
- แสดงข้อมูลต่อไปเมื่อมีการเข้าสู่ระบบสำเร็จ:

  1) วันและเวลาของการเข้าสู่ระบบสำเร็จของครั้งล่าสุด

  2) รายละเอียดของการพยายามเข้าสู่ระบบใดๆที่ไม่สำเร็จนับตั้งแต่การเข้าสู่ระบบสำเร็จครั้งล่าสุด
- ไม่แสดงรหัสผ่านที่กำลังใส่ หรืออาจซ่อนรหัสผ่านโดยใช้สัญลักษณ์แสดงแทน
- ไม่ส่งรหัสผ่านที่ชัดเจนบนโครงข่าย

3.5.4.2 การจำกัดการเข้าถึงข้อมูล (Information access restriction)

การเข้าถึงข้อมูลและฟังก์ชันระบบแอพลิเคชั่นโดยผู้ใช้และบุคลากรสนับสนุนควรถูกจำกัดตามนโยบายการควบคุมที่กำหนดไว้ พนักงานควรตระหนักถึงข้อจำกัดสิทธิ์ของพวกเขาที่ควรกำหนดในคำอธิบายรายละเอียดงานของพวกเขา

ควรพิจารณาแนวทางต่อไปนี้เพื่อรองรับข้อกำหนดของการจำกัดการเข้าถึง:

- มีเมนูเพื่อควบคุมการเข้าถึงฟังก์ชันระบบแอปพลิเคชัน
- การควบคุมสิทธิการเข้าถึงของผู้ใช้งาน เช่น สิทธิในการอ่าน สิทธิในการลบข้อมูล และสิทธิในการดำเนินการ
- ควบคุมสิทธิ์การเข้าถึงของแอพลิเคชั่นอื่นๆ
- ตรวจสอบให้แน่ใจว่าเอาต์พุตระบบแอปพลิเคชันที่ใช้ในการจัดการข้อมูลอ่อนไหวมีเฉพาะข้อมูลที่เกี่ยวข้องกับการใช้เอาต์พุตและถูกส่งไปยังปลายทางและสถานที่ที่ผ่านการรับรองแล้ว

3.5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)

ข้อกำหนดของการจัดการการเข้าถึง คือ การยืนยันและตรวจสอบตัวตนผู้ใช้โดยอ้างอิงจากรหัสผ่าน ควรเกิดขึ้นระหว่างมีการเข้าสู่ระบบ

ระบบการจัดการรหัสผ่านควรเป็นแบบระบบโต้ตอบและควรตรวจสอบให้แน่ใจว่าเป็นรหัสผ่านที่มีคุณภาพ ดังนั้นการใช้รหัสผ่านเริ่มต้นอาจทำให้ผู้ประสงค์ร้ายสามารถเข้าถึงบัญชีเริ่มต้นของการติดตั้งได้โดยตรง ซึ่งมักมีการยกระดับสิทธิพิเศษ

ผู้ใช้งานทุกคนบนระบบควบคุมรางรถไฟอัตโนมัติและการควบคุมทางกลระยะไกลจะต้อง:

- ตั้งรหัสผ่านแบบใช้งานได้หลากหลายประกอบด้วยตัวอักษรและตัวเลขอย่างน้อย 12 ตัว และไม่มีข้อมูลส่วนบุคคลหรือข้อมูลอื่นใดที่สามารถระบุตัวผู้ใช้งานได้

หากรหัสผ่านถูกเปลี่ยน ผู้ประสงค์ร้ายสามารถที่จะโจมตีด้วยวิธีการสุ่มเดารหัสด้วยคำศัพท์พจนานุกรม (dictionary attack) เพื่อให้ได้รหัสผ่านที่ถูกต้องและเข้าถึงบัญชีดังกล่าวได้

ระบบบริหารจัดการรหัสผ่าน ควรจะ:

- บังคับใช้ไอดีและรหัสผ่านส่วนบุคคลเพื่อคงไว้ซึ่งความรับผิดชอบ
- อนุญาตให้ผู้ใช้เลือกและเปลี่ยนรหัสผ่านของตนเอง และขั้นตอนการยืนยันในกรณีเกิดข้อผิดพลาดในการป้อนข้อมูล
- บังคับให้เลือกรหัสผ่านที่มีคุณภาพ
- บังคับให้มีการเปลี่ยนรหัสผ่าน
- บังคับให้มีการเปลี่ยนรหัสผ่านชั่วคราวในครั้งแรกของการเข้าสู่ระบบ
- เก็บรักษาบันทึกรหัสผ่านเดิมของผู้ใช้งานและป้องกันการนำกลับมาใช้ใหม่
- งดแสดงรหัสผ่านบนหน้าจอขณะที่มีป้อนรหัสผ่านอยู่
- จัดเก็บไฟล์รหัสผ่านแยกจากข้อมูลระบบแอปพลิเคชัน
- จัดเก็บและส่งต่อรหัสผ่านในรูปแบบที่มีการป้องกัน เช่น รูปแบบกการเข้ารหัสหรือแฮช

แอปพลิเคชันบางตัวจำเป็นต้องให้หน่วยงานอิสระกำหนดรหัสผ่านของผู้ใช้งาน หากเกิดกรณีดังกล่าว ข้อ b) d) และ e) ของคำแนะนำข้างต้นจะไม่มีผลบังคับใช้ เนื่องจากส่วนใหญ่ผู้ใช้จะเป็นผู้เลือกและเก็บบันทึกรหัสผ่านโดยตนเอง

3.5.4.4 การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

ควรมีการจำกัดและควบคุมการใช้โปรแกรมอรรถประโยชน์ที่อาจสามารถแทนที่การควบคุมระบบและแอปพลิเคชันอย่างเข้มงวด

ควรพิจารณาแนวทางต่อไปนี้สำหรับการใช้ยูทิลิตีระบบ:

- การใช้การยืนยันตัวตน การรับรองความถูกต้อง และขั้นตอนการอนุมัติยูทิลิตีระบบ
- การแยกยูทิลิตีระบบออกจากซอฟต์แวร์แอปพลิเคชัน

- ข้อจำกัดของการใช้ยูทิลิตีระบบต่อจำนวนขั้นต่ำของผู้ใช้ที่เชื่อถือได้และได้รับอนุญาต
- การอนุญาตให้ใช้ระบบยูทิลิตีเฉพาะกิจ
- ข้อจำกัดของความพร้อมใช้งานของยูทิลิตีระบบ เช่น ในช่วงระยะเวลาของการเปลี่ยนแปลงที่ได้รับอนุญาต
- การบันทึกการใช้ยูทิลิตีระบบ
- การกำหนดและการบันทึกระดับการอนุญาตสำหรับยูทิลิตีระบบ
- การลบหรือการปิดใช้งานโปรแกรมอรรถประโยชน์และซอฟต์แวร์ระบบที่ใช้ซอฟต์แวร์ที่ไม่จำเป็น
- ไม่อนุญาตให้ยูทิลิตีระบบพร้อมใช้งานสำหรับผู้ใช้ที่เข้าถึงแอปพลิเคชันบนระบบต่างๆในกรณีที่ต้องมีการแบ่งแยกหน้าที่เกิดขึ้น

3.5.4.5. ควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

ควรมีการจำกัดหรือควบคุมการเข้าถึงซอร์สโค้ดโปรแกรมและอื่นๆที่เกี่ยวข้อง เช่น การออกแบบ ข้อกำหนด แผนการตรวจสอบ และแผนการตรวจสอบความถูกต้องอย่างเข้มงวด เพื่อป้องกันการเปิดฟังก์ชั่นที่ไม่ได้รับอนุญาตและเพื่อหลีกเลี่ยงการเปลี่ยนแปลงที่ไม่เจตนา ซึ่งสามารถทำได้โดยการควบคุมพื้นที่จัดเก็บส่วนกลางของโค้ดดังกล่าว โดยเฉพาะอย่างยิ่งในซอร์สไลบรารีของโปรแกรม

ควรพิจารณาแนวทางต่อไปนี้เพื่อควบคุมซอร์สไลบรารีของโปรแกรมดังกล่าวเพื่อลดโอกาสในการเกิดความเสียหายบนโปรแกรมคอมพิวเตอร์:

- ไม่ควรเก็บซอร์สไลบรารีของโปรแกรมไว้ในระบบปฏิบัติการหากเป็นไปได้
- ควรมีการจัดการซอร์สโค้ดของโปรแกรมและซอร์สไลบรารีของโปรแกรมตามขั้นตอนที่มีการกำหนดไว้
- บุคลากรฝ่ายสนับสนุนไม่ควรเข้าถึงซอร์สไลบรารีของโปรแกรมได้อย่างไม่จำกัด
- การปรับปรุงโปรแกรม ซอร์สไลบรารี และอื่นๆที่เกี่ยวข้อง รวมถึงการเผยแพร่แหล่งที่มาของโปรแกรมให้กับโปรแกรมเมอร์ ควรทำหลังจากมีการอนุญาตที่เหมาะสมแล้วเท่านั้น
- ควรจัดเก็บรายการโปรแกรมต่างๆในสภาพแวดล้อมที่ปลอดภัย
- ควรมีการดูแลรักษาบันทึกการตรวจสอบการเข้าถึงซอร์สไลบรารีของโปรแกรมทั้งหมด
- การบำรุงรักษาและการสำเนาซอร์สไลบรารีของโปรแกรมควรอยู่ภายใต้ขั้นตอนการควบคุมการเปลี่ยนแปลงที่เข้มงวด

3.6. วงจรชีวิตของผลิตภัณฑ์ (Life cycle product)

วัตถุประสงค์ คือ เพื่อกำหนดความปลอดภัยในด้านต่างๆและนำมาพิจารณาร่วมกับวงจรชีวิตของอุปกรณ์หรือผลิตภัณฑ์ที่ทำหน้าที่ส่งสัญญาณทั้งหมด

ผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ด้านความปลอดภัย มีดังนี้:

- ความเสียหายของการใช้งานของระบบ
- การด้อยค่าของประสิทธิภาพของระบบ
- มีการยักย้ายหรือเกิดความเสียหายของข้อมูล
- ความเสียหายของการควบคุมการผลิต
- ภัยพิบัติสิ่งแวดล้อม
- ความเสี่ยงต่อการเสียชีวิตและการบาดเจ็บสาหัส
- สร้างความเสียหายต่อภาพลักษณ์ขององค์กร
- หายนะทางการเงิน

3.6.1. การออกแบบและแนวคิด (Design and conception)

ในระหว่างขั้นตอนการออกแบบ ทีมบริหารโครงการหรือผู้จัดการความปลอดภัยข้อมูลควรมีการระบุ ตรวจสอบ และดำเนินการตามแนวคิดและวิธีการรักษาความปลอดภัยพื้นฐานภายในโครงการส่งสัญญาณ

นอกจากนี้ยังควรรวมการประเมินความเสี่ยงด้านความปลอดภัยในกระบวนการจัดการโครงการ รวมถึงการเคารพข้อกำหนดด้านความปลอดภัยของข้อมูล

การประเมินความเสี่ยงควรประกอบด้วยรายการต่อไปนี้:

- เอกสารนโยบายและขั้นตอนของระบบ และรายละเอียดของการดำเนินการ
- รายการคู่ภัยคุกคามหรือช่องโหว่ พร้อมความรุนแรงของผลกระทบและโอกาสที่จะเกิดขึ้น
- รายการมาตรการป้องกันเพื่อการควบคุมภัยคุกคามและช่องโหว่เหล่านี้
- รายการการเปลี่ยนแปลงที่แนะนำ โดยมีการประมาณระดับความพยายามของแต่ละรายการ
- การลดความเสี่ยงที่ตามมาของการเปลี่ยนแปลงที่แนะนำในแต่ละครั้ง
- ระดับความเสี่ยงที่อาจยังคงหลงเหลืออยู่หลังจากการเปลี่ยนแปลงที่แนะนำได้รับการดำเนินการแล้วเสร็จ

ขั้นตอนในการจัดทำคู่มือระบบเป็นขั้นตอนที่มีการระบุคำอธิบายของระบบและข้อมูลที่จัดการดูแลไว้ว่า เป็นทรัพย์สินสารสนเทศที่ใช้เพื่อบรรลุภารกิจทางธุรกิจขององค์กร ซึ่งขั้นตอนนี้จะช่วยกำหนดกรอบของขั้นตอนการประเมินความเสี่ยงที่จะตามมา

ควรมีการจัดทำคลังคู่มือระบบ รายการส่วนประกอบทั้งหมดของระบบ และขอบเขตวัตถุประสงค์ของโครงการ ซึ่งควรประกอบด้วยด้วยคำอธิบายของส่วนประกอบต่างๆ ในระบบข้อมูลหรือสารสนเทศ และค่าคาดหวังของผลิตภัณฑ์ และสิทธิใดๆที่กำหนดไว้แก่ผลิตภัณฑ์นั้นๆ

ควรมีการกำหนดและดำเนินการวัดและการควบคุมสำหรับการบำรุงรักษาและตรวจสอบอย่างเหมาะสม ตัวอย่างเช่น ตัวชี้วัดและเป้าหมายที่เป็นไปได้อาจคือการเพิ่มมูลค่าของผลิตภัณฑ์ถึง 20% หรือลดต้นทุนเนื่องจากมีการเรียกคืนผลิตภัณฑ์ เกิดข้อผิดพลาดของผลิตภัณฑ์ และภาระหนี้สินลงได้ถึง 75 %

3.6.2. การผลิต (Production)

ตรวจสอบให้แน่ใจว่าได้ตระหนักถึงหลักเกณฑ์ด้านความปลอดภัยระหว่างขั้นตอนการผลิต โดยมีการนำแนวทางปฏิบัติและมาตรการด้านความปลอดภัยที่ดีที่สุดที่ถูกกำหนดไว้ในการประเมินความเสี่ยงด้านความปลอดภัยมาปรับใช้และดำเนินการในขั้นตอนนี้ของโครงการ เพื่อหลีกเลี่ยงการขาดการรักษาความปลอดภัยและทำให้ต้องหยุดการดำเนินการโครงการ

3.6.3. การดำเนินการ (Operation)

3.6.3.1. ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedures and responsibilities)

ควรมีการกำหนดความรับผิดชอบและขั้นตอนในการบริหารจัดการและการดำเนินงานของอุปกรณ์ประมวลผลสารสนเทศทั้งหมดเพื่อให้แน่ใจว่าอุปกรณ์เหล่านั้นมีการดำเนินการอย่างถูกต้องแม่นยำและมั่นคงปลอดภัย ซึ่งรวมถึงการพัฒนาขั้นตอนการดำเนินงานที่เหมาะสมด้วย

ควรมีการแบ่งแยกหน้าที่รับผิดชอบตามความเหมาะสม เพื่อลดความเสี่ยงของการใช้ระบบโดยประมาทหรือจงใจในทางที่ผิด

3.6.3.2. เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

ขั้นตอนการปฏิบัติงานควรมีการบันทึกเป็นลายลักษณ์อักษร และให้บริการแก่ผู้ใช้งานทุกคนที่ต้องการเข้าถึง ควรมีการจัดเตรียมขั้นตอนในการจัดทำเอกสารสำหรับกิจกรรมบนระบบที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศและการสื่อสาร เช่น ขั้นตอนการเปิดและปิดคอมพิวเตอร์ การสำรองข้อมูล การบำรุงรักษาอุปกรณ์ การจัดการสื่อ การจัดการห้องคอมพิวเตอร์และการจัดการจดหมาย และความปลอดภัย

ขั้นตอนการปฏิบัติงานควรมีการชี้แจงคำแนะนำในการดำเนินงานโดยละเอียดของแต่ละงาน รวมถึง:

- การประมวลผลและการจัดการข้อมูล
- การสำรองข้อมูล (ดูที่ข้อ 3.6.3)
- ข้อกำหนดเกี่ยวกับการจัดตารางเวลา รวมถึงการพึ่งพากันกับระบบอื่น ๆ การเริ่มงานเร็วที่สุดและเวลาเสร็จสิ้นงานล่าสุด
- คำแนะนำในการจัดการข้อผิดพลาดหรือเงื่อนไขพิเศษอื่น ๆ ที่อาจเกิดขึ้นระหว่างดำเนินงาน รวมถึงข้อจำกัดในการใช้ยูทิลิตี้ระบบ (ดูที่ข้อ 3.5.4.4)
- การติดต่อฝ่ายสนับสนุนในกรณีเกิดปัญหาทางเทคนิคหรือระหว่างปฏิบัติงานโดยไม่คาดคิด
- คำสั่งของเอาต์พุตพิเศษและการจัดการสื่อ เช่น การใช้สเตชันเนอรีพิเศษ การจัดการเอาต์พุตที่เป็นความลับ รวมถึงขั้นตอนสำหรับการกำจัดเอาต์พุตจากงานที่ล้มเหลวอย่างปลอดภัย (ดู 3.4.2.3 และ 3.4.3.2)
- การเริ่มต้นระบบใหม่และขั้นตอนการกู้คืนค่าในกรณีที่ระบบล้มเหลว
- การจัดการข้อมูลเส้นทางการตรวจสอบและบันทึกระบบ

ขั้นตอนการดำเนินงานและเอกสารขั้นตอนการดำเนินงานของระบบรางอัตโนมัติและการควบคุมทางกลระยะไกล รวมถึงกิจกรรมซอฟต์แวร์ทางเทคโนโลยี ควรถือเป็นเอกสารและการเปลี่ยนแปลงที่ได้รับอนุญาตจากฝ่ายบริหาร และควรมีการจัดการระบบสารสนเทศควรอย่างสม่ำเสมอ โดยใช้ขั้นตอนการดำเนินงานและยูทิลิตี้ระบบเดียวกับข้างต้นหากมีความเป็นไปได้ในทางเทคนิค

3.6.3.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

การใช้ทรัพยากรควรได้รับการตรวจสอบ ปรับแต่ง และคาดการณ์ตามความต้องการความจุหรือพื้นที่จัดเก็บบนระบบในอนาคต เพื่อนำไปตรวจสอบประสิทธิภาพที่จำเป็นของระบบ

ควรมีการระบุความต้องการความจุหรือพื้นที่จัดเก็บบนระบบสำหรับแต่ละกิจกรรมที่เกิดขึ้นใหม่และที่กำลังดำเนินการอยู่ รวมถึงควรใช้หลักการปรับและการตรวจสอบระบบเพื่อให้แน่ใจว่าจะสามารถพัฒนาความพร้อมใช้งานและประสิทธิภาพของระบบต่างๆได้ในกรณีจำเป็น

มาตรการควบคุมการตรวจสอบควรนำมาปรับใช้เพื่อบ่งชี้ปัญหาภายในเวลาที่กำหนด และการคาดการณ์ความต้องการความจุหรือพื้นที่จัดเก็บบนระบบในอนาคตควรตระหนักถึงความต้องการทางธุรกิจและระบบใหม่ๆ รวมถึงแนวโน้มของความจุในการประมวลผลข้อมูลในปัจจุบันและอนาคตขององค์กรนั้นๆ

จำเป็นต้องให้ความสำคัญแก่ทรัพยากรใดๆที่ใช้ระยะเวลาในการจัดหาที่ยาวนานหรือมีต้นทุนสูง ดังนั้นผู้จัดการจึงควรติดตามตรวจสอบการใช้ทรัพยากรหลักของระบบและควรระบุแนวโน้มการใช้งาน โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับแอปพลิเคชันทางธุรกิจหรือเครื่องมือจัดการระบบข้อมูล

ผู้จัดการควรใช้ข้อมูลนี้เพื่อแยกแยะและหลีกเลี่ยงอุปสรรคที่อาจเกิดขึ้นและการพึ่งพาบุคลากรสำคัญที่อาจก่อให้เกิดภัยคุกคามต่อความปลอดภัยหรือบริการของระบบ และควรวางแผนการดำเนินการที่เหมาะสม

การจัดสรรความจุของระบบที่เพียงพอสามารถทำได้โดยเพิ่มความจุของระบบหรือลดความต้องการเหล่านั้น ตัวอย่างการจัดการความต้องของความจุ ได้แก่

- การลบข้อมูลที่ล้าสมัยในดิสก์จัดเก็บข้อมูล
- การถอนการติดตั้งแอปพลิเคชัน ระบบ ฐานข้อมูล หรือรายการใดๆ
- เพิ่มประสิทธิภาพกระบวนการและการจัดตารางแบบกลุ่ม
- การเพิ่มประสิทธิภาพตรรกะของแอปพลิเคชันหรือการสืบค้นฐานข้อมูล
- การปฏิเสธหรือจำกัดแบนด์วิดท์สำหรับบริการที่ใช้ทรัพยากร หากไม่มีความสำคัญในเชิงธุรกิจ เช่น การสตรีมวิดีโอ

ควรนำแผนการจัดการความจุที่มีการจัดทำเป็นลายลักษณ์อักษรมาพิจารณาใช้ในระบบวิกฤติที่สำคัญ การควบคุมนี้ยังกล่าวถึงอัตราความจุของทรัพยากรบุคคล ตลอดจนสำนักงานและสิ่งอำนวยความสะดวกใดๆ

3.6.4 การพิสูจน์ การทดสอบและการตรวจรับงาน (Verification, test and commissioning)

ตรวจสอบให้แน่ใจว่าระบบหรือผลิตภัณฑ์สามารถรักษาระดับความปลอดภัยตลอดอายุการใช้งาน และมีความสามารถในการติดตามหรือแจ้งเตือนอย่างต่อเนื่องเมื่อจำเป็น

ควรมีการดำเนินการทดสอบอย่างเหมาะสมและตระหนักเมื่อมีการกำหนดการตรวจสอบอุปกรณ์ โดยคำนึงถึงว่าการบำรุงรักษานี้ดำเนินการโดยบุคลากรภายในหรือภายนอกองค์กร

ผู้จัดการฝ่ายรักษาความปลอดภัยควรตรวจสอบและยืนยันความปลอดภัยของผลิตภัณฑ์ก่อนเริ่มใช้งาน และแน่ใจว่าได้นำหลักเกณฑ์ความปลอดภัยทั้งหมดไปใช้และทดสอบในสถานการณ์จริงกับผลิตภัณฑ์ ซึ่งเป็นไปตามข้อกำหนดและการปฏิบัติตามข้อกำหนด รวมถึงมีการจัดส่งเอกสารและนโยบายไปพร้อมกับผลิตภัณฑ์แล้ว

3.6.5. การบำรุงรักษา (Maintenance)

วัตถุประสงค์ คือ เพื่อป้องกันการสูญเสีย ความเสียหาย การโจรกรรมหรือเป็นภัยต่อทรัพย์สินและขัดต่อการดำเนินงานขององค์กร

ควรพิจารณาแนวทางต่อไปนี้สำหรับการบำรุงรักษาอุปกรณ์:

- ควรบำรุงรักษาอุปกรณ์ตามช่วงเวลาและข้อกำหนดในการให้บริการตามคำแนะนำของผู้ให้บริการ
- การซ่อมแซมและบริการอุปกรณ์ควรดำเนินการโดยเจ้าหน้าที่ฝ่ายบำรุงรักษาที่มีการรับรองแล้วเท่านั้น
- ควรเก็บบันทึกข้อผิดพลาดที่น่าสงสัยหรือเกิดขึ้นจริง รวมถึงบันทึกการบำรุงรักษาเชิงป้องกันและแก้ไขทั้งหมด
- ควรปฏิบัติตามข้อกำหนดในการบำรุงรักษาที่มีการกำหนดโดยกรมธรรม์ประกันภัย
- ก่อนที่จะนำอุปกรณ์กลับมาใช้งานหลังการบำรุงรักษา ควรตรวจสอบเพื่อให้แน่ใจว่าอุปกรณ์ไม่ได้ผ่านการดัดแปลงและสามารถทำงานได้ปกติ

หากจำเป็น ควรมีการล้างข้อมูลที่เป็นความลับออกจากอุปกรณ์นั้นๆ หรือควรลดอัตราเจ้าหน้าที่บำรุงรักษาให้เพียงพอ

3.7 การพัฒนาซอฟต์แวร์ (Software development)

3.7.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

ระบบและซอฟต์แวร์ทางเทคนิคของรถไฟอัตโนมัติและระบบควบคุมทางกลระยะไกลไม่ควรประกอบไปด้วย

- การพัฒนาซอฟต์แวร์และเครื่องมือการดีบัก
- เครื่องมือที่อนุญาตให้ปรับเปลี่ยนโค้ดที่คอมไพล์ในระหว่างการประมวลผลข้อมูล
- ควรมีการปรับปรุงและตรวจสอบประสิทธิภาพเครื่องมือในการกู้คืนโปรแกรมที่อนุญาตให้สำรองสำเนาของระบบและส่วนประกอบซอฟต์แวร์เทคโนโลยีได้สองชุดอยู่เป็นประจำ

ควรมีการระบุข้อกำหนดในการรับประกันการทำงานทางอินเทอร์เน็ตที่ปลอดภัยเมื่อมีการมอบหมายให้แก่บริษัทรถไฟหรือส่วนย่อยที่เกี่ยวข้องให้กับรถไฟอัตโนมัติและระบบควบคุมทางกลระยะไกลซึ่งสามารถเข้าถึงได้จากระยะไกลตามเงื่อนไขการดำเนินงาน

3.7.2 ความมั่นคงปลอดภัยของกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

3.7.2.1 สภาพแวดล้อมของการพัฒนาระบบทีมีความมั่นคงปลอดภัย (Secure development environment)

วัตถุประสงค์ คือ เพื่อให้แน่ใจว่าความปลอดภัยข้อมูลเป็นส่วนหนึ่งของระบบสารสนเทศตลอดอายุการใช้งาน ซึ่งรวมถึงข้อกำหนดสำหรับระบบสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะด้วย

สภาพแวดล้อมการพัฒนาที่ปลอดภัยนั้นประกอบด้วย ผู้คนกระบวนการและเทคโนโลยีที่เกี่ยวข้องกับการพัฒนาและบูรณาการระบบ

องค์กรควรประเมินความเสี่ยงที่เกี่ยวข้องกับความพยายามในการพัฒนาระบบในแต่ละครั้ง และควรกำหนดสภาพแวดล้อมการพัฒนาที่ปลอดภัยสำหรับความพยายามในการพัฒนาระบบโดยเฉพาะ โดยพิจารณาจาก:

- ความอ่อนไหวของข้อมูลที่มีการประมวลผล จัดเก็บ และส่งต่อโดยระบบ
- ข้อกำหนดภายนอกและภายในองค์กรที่เกี่ยวข้อง เช่น จากกฎระเบียบหรือนโยบาย
- การควบคุมความปลอดภัยที่ดำเนินการแล้วโดยองค์กรที่สนับสนุนการพัฒนาระบบ
- ความน่าเชื่อถือของบุคลากรที่ทำงานในสภาพแวดล้อมนั้นๆ
- ระดับของการว่าจ้างบุคคลภายนอกที่เกี่ยวข้องกับการพัฒนาระบบ
- ความจำเป็นในการแบ่งแยกของสภาพแวดล้อมในการพัฒนาที่แตกต่างกัน
- การควบคุมการเข้าถึงสภาพแวดล้อมในการพัฒนา
- การติดตามการเปลี่ยนแปลงของสภาพแวดล้อมและรหัสที่เก็บไว้ในนั้น
- มีการเก็บและสำรองข้อมูลไว้ในสถานที่ภายนอกองค์กรที่มีความปลอดภัย
- ควบคุมการเคลื่อนที่ของข้อมูลทั้งจากและสู่สภาพแวดล้อมนั้นๆ

เมื่อมีการกำหนดระดับการป้องกันสำหรับสภาพแวดล้อมของการพัฒนาที่เฉพาะเจาะจงแล้ว องค์กรควรจัดทำกระบวนการที่เกี่ยวข้องในขั้นตอนการพัฒนาที่ปลอดภัยในรูปแบบเอกสารและจัดเตรียมให้กับบุคลากรทุกคนที่ต้องการ

กระบวนการเหล่านี้เป็นแนวทางการแก้ไขที่มุ่งเน้นด้านความปลอดภัย ซึ่งอาจนำมาใช้สำหรับการตรวจสอบความปลอดภัยได้เช่นเดียวกัน เพื่อเพิ่มความทนทานในระบบที่สำคัญให้มีมากยิ่งขึ้น

3.7.2.2 การจำกัดการปรับแต่งซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

ควรใช้แพ็คเกจซอฟต์แวร์ที่จัดหาให้โดยผู้จำหน่ายมากที่สุดเท่าที่เป็นไปได้โดยไม่ต้องมีการแก้ไขปรับแต่ง

ควรพิจารณาประเด็นต่อไปนี้ในกรณีที่จำเป็นต้องมีการแก้ไขหรือปรับแต่งแพ็คเกจซอฟต์แวร์นั้นๆ:

- ความเสี่ยงที่การควบคุมแบบบูรณาการและกระบวนการคงความถูกต้องของข้อมูลจะถูกบุกรุก
- ควรได้รับความยินยอมจากผู้จำหน่ายก่อนมีการดัดแปลงหรือไม่
- ความเป็นไปได้ที่จะได้รับการเปลี่ยนแปลงที่จำเป็นจากผู้จำหน่ายในรูปแบบการปรับปรุงพัฒนาโปรแกรมแบบมาตรฐาน
- ผลกระทบที่ตามมาหากองค์กรต้องเป็นผู้รับผิดชอบในการบำรุงรักษาซอฟต์แวร์ในอนาคตอันเป็นผลมาจากการดัดแปลงซอฟต์แวร์
- ความเข้ากันได้กับซอฟต์แวร์อื่นที่มีการใช้งานอยู่

หากจำเป็นต้องมีการดัดแปลงใดๆ ควรเก็บซอฟต์แวร์ต้นฉบับไว้ และนำการดัดแปลงไปใช้กับสำเนาที่กำหนด

ควรใช้กระบวนการจัดการการอัปเดตซอฟต์แวร์เพื่อให้แน่ใจว่าแพทช์และการอัปเดตแอปพลิเคชันที่ได้รับการอนุมัติล่าสุดถูกติดตั้งบนซอฟต์แวร์ที่ผ่านการรับรองแล้ว การดัดแปลงแก้ไขทั้งหมดควรผ่านการทดสอบและจัดทำเป็นลายลักษณ์อักษรอย่างสมบูรณ์เพื่อให้สามารถนำไปใช้กับการอัพเกรดซอฟต์แวร์ในอนาคตได้หากจำเป็น รวมถึงควรให้หน่วยงานประเมินอิสระทดสอบและรับรองการปรับแต่งของซอฟต์แวร์นั้นๆด้วย

3.7.2.3 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอกควรได้รับการดูแลและตรวจสอบจากองค์กร

ควรพิจารณาประเด็นดังต่อไปนี้ ในกรณีที่มีการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก:

- การจัดการสิทธิการใช้งาน ความเป็นเจ้าของรหัส และสิทธิในทรัพย์สินทางปัญญา
- การรับรองคุณภาพและความถูกต้องของงานที่ดำเนินการ
- การจัดเตรียมสัญญาค้ำประกันหรือเอสโครว์ในกรณีที่บุคคลภายนอกทำงานผิดพลาด
- สิทธิในการเข้าถึงเพื่อตรวจสอบคุณภาพและความถูกต้องของงานที่ทำ
- ข้อกำหนดตามสัญญาสำหรับการทำงานด้านคุณภาพและความปลอดภัยของโค้ด
- การทดสอบก่อนการติดตั้งเพื่อตรวจจับรหัสที่เป็นอันตรายและโทรจัน

3.7.2.4 การทบทวนทางเทคนิคของแอปพลิเคชันหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

วัตถุประสงค์ คือ เพื่อลดความเสี่ยงที่เกิดจากการใช้ประโยชน์จากช่องโหว่ทางเทคนิคที่มีการเผยแพร่แล้ว

กระบวนการจัดการช่องโหว่ทางเทคนิคควรมีการดำเนินการอย่างมีประสิทธิภาพเป็นระบบ และสามารถทำซ้ำได้โดยใช้วิธีการวัดผลเพื่อยืนยันประสิทธิภาพของกระบวนการดังกล่าว

กระบวนการนี้ควรครอบคลุม:

- การทบทวนขั้นตอนการควบคุมและความสมบูรณ์ของแอปพลิเคชันเพื่อให้แน่ใจว่าไม่ได้รับความเสียหายจากการเปลี่ยนแปลงของแพลตฟอร์มปฏิบัติการ
- การตรวจสอบให้แน่ใจว่ามีการแจ้งเตือนการเปลี่ยนแปลงแพลตฟอร์มปฏิบัติการในทันที เพื่อให้สามารถทดสอบและทบทวนได้อย่างเหมาะสมก่อนมีการดำเนินการ
- ตรวจสอบให้แน่ใจว่ามีการเปลี่ยนแปลงแผนความต่อเนื่องทางธุรกิจอย่างเหมาะสม

ข้อควรพิจารณาเหล่านี้ควรรวมถึงระบบปฏิบัติการและแอปพลิเคชันอื่นๆที่มีการใช้งานอยู่

3.7.3. การแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการปฏิบัติงานออกจากกัน (Separation of development, testing and operational environments)

ควรแยกอุปกรณ์ที่ใช้ในการพัฒนา การทดสอบ และการปฏิบัติงาน เพื่อลดความเสี่ยงของการเข้าถึงโดยไม่ได้รับอนุญาต หรือ การเปลี่ยนแปลงของระบบการส่งสัญญาณ

ควรจำแนกระดับของการแยกระหว่างสภาพแวดล้อมการปฏิบัติงาน การทดสอบ และการพัฒนา ซึ่งจำเป็นต่อการป้องกันปัญหาในการปฏิบัติงาน

ควรมีการพิจารณาประเด็นต่อไปนี้:

- ควรมีการกำหนดกฎสำหรับการถ่ายโอนซอฟต์แวร์จากสถานะพัฒนาไปสู่สถานะดำเนินงาน และจัดทำเป็นลายลักษณ์อักษร
- ซอฟต์แวร์สำหรับการพัฒนาและปฏิบัติการควรทำงานบนระบบหรือหน่วยประมวลผลคอมพิวเตอร์ที่แตกต่างกัน รวมถึงในโดเมนหรือไดเร็กทอรีที่แตกต่างกัน
- การเปลี่ยนแปลงระบบบนปฏิบัติการและแอปพลิเคชันควรได้รับการทดสอบในสภาพแวดล้อมที่จัดขึ้นเพื่อทดสอบหรือจัดเตรียมก่อนที่จะนำไปปรับใช้กับระบบปฏิบัติการ
- นอกเหนือจากกรณีพิเศษแล้ว การทดสอบไม่ควรทำบนระบบปฏิบัติการใดๆ
- ไม่ควรจัดให้มีการเข้าถึงคอมไพเลอร์ เครื่องมือที่ใช้ในการแก้ไข และเครื่องมือพัฒนาหรือยูทิลิตี้ระบบจากระบบปฏิบัติการได้หากไม่จำเป็น
- ผู้ใช้ควรใช้โปรไฟล์ที่แตกต่างกันบนระบบปฏิบัติการและทดสอบ และเมนูควรแสดงข้อความระบุตัวตนที่เหมาะสมเพื่อลดความเสี่ยงของข้อผิดพลาด

- ข้อมูลที่มีความอ่อนไหวไม่ควรถูกสำเนาและนำเข้าสู่สภาพแวดล้อมของระบบทดสอบ เว้นแต่จะมีการควบคุมที่เท่าเทียมกันสำหรับระบบการทดสอบ

กิจกรรมต่างๆของการพัฒนาและทดสอบระบบอาจก่อให้เกิดปัญหาที่ร้ายแรงได้ เช่น การดัดแปลงแก้ไขที่ไม่พึงประสงค์ของไฟล์หรือสภาพแวดล้อมของระบบ รวมถึงการล้มเหลวของระบบดังนั้น จึงมีความจำเป็นอย่างยิ่งที่จะต้องรักษาสภาพแวดล้อมที่คุ้นเคยและมีเสถียรภาพเพื่อทำการทดสอบที่สำคัญและเพื่อป้องกันการเข้าถึงสภาพแวดล้อมของการปฏิบัติงานโดยนักพัฒนาที่ขาดคุณสมบัติในการเข้าถึง

ในกรณีที่บุคลากรด้านการพัฒนาและทดสอบสามารถเข้าถึงระบบปฏิบัติการและข้อมูลของระบบปฏิบัติการได้ พวกเขาอาจสามารถนำรหัสที่ไม่ผ่านการรับรองและการทดสอบเข้ามาในระบบ หรือเปลี่ยนแปลงข้อมูลการปฏิบัติงานได้

ในบางระบบ ความสามารถนี้อาจถูกนำไปใช้ในทางที่ผิดเพื่อกระทำการฉ้อโกงหรือนำโค้ดที่ไม่ผ่านการทดสอบหรือเป็นอันตรายเข้าสู่ระบบ ซึ่งอาจก่อให้เกิดปัญหาด้านการดำเนินงานที่ร้ายแรงได้

บุคลากรด้านการพัฒนาและทดสอบยังถือเป็นภัยคุกคามต่อการรักษาความลับของข้อมูลการปฏิบัติงาน กิจกรรมการพัฒนาและทดสอบอาจทำให้เกิดการเปลี่ยนแปลงโดยไม่ได้ตั้งใจต่อซอฟต์แวร์หรือข้อมูลหากบุคลากรเหล่านั้นมีสภาพแวดล้อมในการประมวลผลเดียวกัน

ดังนั้น การแยกสภาพแวดล้อมด้านการพัฒนา การทดสอบ และการปฏิบัติงานจึงเป็นสิ่งที่พึงกระทำเพื่อลดความเสี่ยงของการเปลี่ยนแปลงโดยไม่ได้ตั้งใจหรือการเข้าถึงซอฟต์แวร์ปฏิบัติการและข้อมูลทางธุรกิจโดยไม่ได้รับอนุญาต

3.7.4 การควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (Control of operational software)

ควรมีการจัดทำขั้นตอนในการควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ

ควรพิจารณาแนวทางต่อไปนี้เพื่อลดความเสี่ยงของการเกิดความเสียหายและควบคุมการเปลี่ยนแปลงบนระบบปฏิบัติการ:

- การอัปเดตซอฟต์แวร์ปฏิบัติการ แอปพลิเคชัน และไลบรารีโปรแกรมควรดำเนินการโดยผู้ดูแลระบบที่ผ่านการฝึกอบรมและได้รับอนุญาตจากฝ่ายบริหารอย่างเหมาะสมแล้ว
- ระบบปฏิบัติการควรเก็บรักษาเฉพาะรหัสประมวลผลที่ได้รับการอนุมัติเท่านั้น ซึ่งไม่รวมรหัสพัฒนาหรือคอมไพเลอร์
- ควรใช้แอปพลิเคชันและซอฟต์แวร์ระบบปฏิบัติการหลังจากมีการทดสอบอย่างละเอียดและเสร็จสิ้นแล้วเท่านั้น
- การทดสอบควรรวมถึงการทดสอบการใช้งาน ความปลอดภัย ผลกระทบต่อระบบอื่นๆ ความเป็นมิตรต่อผู้ใช้ และควรดำเนินการในระบบที่แยกต่างหาก รวมถึงควรตรวจสอบให้แน่ใจว่าไลบรารีซอร์สของโปรแกรมที่เกี่ยวข้องทั้งหมดได้รับการอัปเดตแล้ว
- ควรใช้ระบบควบคุมการปรับแต่งเพื่อควบคุมซอฟต์แวร์ที่นำมาใช้ทั้งหมดตลอดจนคู่มือระบบ

- ควรนำกลยุทธ์การย้อนกลับมาใช้ก่อนที่จะทำการเปลี่ยนแปลง
- บันทึกการตรวจสอบควรคงไว้ซึ่งการอัปเดตทั้งหมดของไลบรารีโปรแกรมปฏิบัติการ
- ซอฟต์แวร์แอปพลิเคชันรุ่นก่อนหน้าควรเก็บไว้เป็นมาตรการฉุกเฉิน
- ซอฟต์แวร์รุ่นเก่าควรถูกจัดเก็บอย่างถาวร พร้อมด้วยข้อมูลและพารามิเตอร์ ขั้นตอนต่างๆ รายละเอียดการปรับแต่ง และซอฟต์แวร์สนับสนุนที่จำเป็นทั้งหมดตราบเท่าที่ข้อมูลอยู่ในแฟ้มจัดเก็บถาวร

การตัดสินใจอัปเกรดเป็นรุ่นใหม่ ควรคำนึงถึงความต้องการทางธุรกิจในด้านการเปลี่ยนแปลงและความมั่นคงปลอดภัยของรุ่นนั้นๆ เช่น การแนะนำฟังก์ชั่นการรักษาความปลอดภัยใหม่หรือจำนวนและความรุนแรงของปัญหาด้านความปลอดภัยที่ส่งผลกระทบต่อรุ่นนี้

ควรนำแพทช์ซอฟต์แวร์มาปรับใช้หากสามารถช่วยกำจัดหรือลดความอ่อนแอด้านความปลอดภัยได้เท่านั้น

3.7.4.1 การบริหารจัดการกุญแจ (Key management)

มาตรฐาน EN 50159 ระบุว่าหากใช้ "เครือข่ายแบบเปิด" ในการส่งสัญญาณทางระบบราง ต้องใช้กลไกการเข้ารหัสเพื่อป้องกันเครือข่ายจากผู้บุกรุก

การใช้เครือข่ายแบบเปิดอาจดูเหมือนเป็นวิธีที่ประหยัดค่าใช้จ่ายในการส่งสัญญาณทางระบบราง ดังนั้นการใช้วิธีการเข้ารหัสอาจเป็นความคิดที่ดี อย่างไรก็ตาม การใช้วิธีการดังกล่าวยังคงมีข้อเสียต่อการส่งสัญญาณบนระบบรางอยู่เช่นกัน

เนื่องจากเวลาที่จำเป็นสำหรับการประมวลผลด้วยการเข้ารหัส (โดยทั่วไปคือ 50 มิลลิวินาทีสำหรับการดำเนินการแต่ละครั้ง ทั้งช่วง เข้ารหัสและถอดรหัส) การใช้วิธีการเข้ารหัสอาจถือว่ามีข้อเสียในเรื่องของความล่าช้าที่ยอมรับไม่ได้โดยเฉพาะอย่างยิ่ง สำหรับเครือข่าย L0 ที่เวลาตอบสนองต้องน้อยกว่า 50 มิลลิวินาที

นอกจากนี้แล้ว เมื่อมีการใช้อัลกอริธึมเข้ารหัสเพื่อรักษาความปลอดภัยในการสื่อสารด้วยสัญญาณจะต้องตระหนักถึงวงจรชีวิตขององค์ประกอบการส่งสัญญาณ รวมไปถึงความเสถียรภาพของอัลกอริธึมเข้ารหัสนั้นๆด้วย

แม้ว่าจะมีคำแนะนำระดับสากลพร้อมวันที่โดยประมาณสำหรับความถูกต้องของแต่ละอัลกอริธึม แต่โดเมนความปลอดภัยด้านเทคโนโลยีสารสนเทศจะมีการเปลี่ยนแปลงทุกวันและไม่สามารถการันตีช่องโหว่ใหม่ที่อาจเกิดขึ้นของอัลกอริธึมเข้ารหัสได้

3.7.4.2 การควบคุมการเข้ารหัส (Cryptographic controls)

วัตถุประสงค์ คือ เพื่อปกป้องความลับ ความถูกต้อง หรือความสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัส ควรมีการพัฒนานโยบายมาตรการเข้ารหัสข้อมูล และนำหลักการบริหารจัดการกุญแจมาปรับใช้เพื่อรองรับเทคนิคการเข้ารหัส

3.7.4.3. นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

ควรมีการพัฒนาและดำเนินนโยบายมาตรการเข้ารหัสข้อมูลเพื่อป้องกันข้อมูล และพิจารณาประเด็นต่อไปนี้ในการพัฒนานโยบายการเข้ารหัสข้อมูล:

- จากการประเมินความเสี่ยง ควรมีการจำแนกระดับการป้องกันที่ต้องการโดยคำนึงถึงประเภท ความเสถียรภาพ และคุณภาพของอัลกอริธึมเข้ารหัสที่ต้องการ
- การใช้วิธีการเข้ารหัสเพื่อป้องกันข้อมูลที่ส่งผ่านโดยอุปกรณ์สื่อเคลื่อนที่หรืออุปกรณ์สื่อที่สามารถถอดประกอบได้ รวมถึงผ่านสายการสื่อสารต่างๆ
- แนวทางการบริหารจัดการกุญแจ รวมถึงวิธีการจัดการกับการป้องกันกุญแจเข้ารหัสและการกู้คืนข้อมูลที่เข้ารหัสในกรณีกุญแจเกิดการสูญหาย ถูกโจรกรรมหรือมีความเสียหาย
- แนวทางในการจัดการที่สำคัญ รวมถึงวิธีการจัดการกับการป้องกันคีย์การเข้ารหัสและการกู้คืนข้อมูลที่เข้ารหัสในกรณีที่คีย์สูญหาย ถูกบุกรุกหรือเสียหาย
- บทบาทและความรับผิดชอบ เช่น ใครเป็นผู้รับผิดชอบ:
  1) การดำเนินการตามนโยบาย
  2) การบริหารจัดการกุญแจรวมถึงการสร้างกุญแจ
- มาตรฐานต่างๆ ที่จะนำมาใช้สำหรับการดำเนินการอย่างมีประสิทธิภาพทั่วทั้งองค์กร (โซลูชันใดที่ใช้สำหรับกระบวนการทางธุรกิจ)
- ผลกระทบจากการใช้ข้อมูลที่เข้ารหัสต่อการควบคุมที่อาศัยการตรวจสอบเนื้อหา (เช่น การตรวจจับมัลแวร์)

เมื่อนำนโยบายการเข้ารหัสลับขององค์กรไปปรับใช้ ควรพิจารณาระเบียบข้อบังคับและข้อจำกัดสากลที่อาจนำไปใช้กับการใช้เทคนิคการเข้ารหัสลับในส่วนต่างๆ ของโลกและประเด็นเรื่องการไหลของข้อมูลที่เข้ารหัสข้ามพรมแดน

มาตรการเข้ารหัสข้อมูลสามารถใช้เพื่อให้บรรลุวัตถุประสงค์ด้านความปลอดภัยของข้อมูลที่แตกต่างกัน เช่น:

- เพื่อรักษาความลับ โดยการใช้การเข้ารหัสข้อมูลเพื่อปกป้องข้อมูลที่มีความอ่อนไหวหรือสำคัญ ทั้งที่จัดเก็บหรือนำส่ง
- เพื่อความสมบูรณ์หรือความถูกต้อง โดยการใช้ลายเซ็นดิจิทัลหรือรหัสตรวจสอบข้อความเพื่อยืนยันความถูกต้องหรือความสมบูรณ์ของข้อมูลที่มีความอ่อนไหวซึ่งถูกจัดเก็บหรือส่งหรือข้อมูลที่มีความสำคัญ
- การห้ามปฏิเสธความรับผิด โดยการใช้เทคนิคการเข้ารหัสเพื่อแสดงหลักฐานกิจกรรมหรือเหตุการณ์ต่างๆ ของผู้ใช้ทั้งที่เกิดขึ้นหรือไม่เกิดขึ้น
- การรับรองความถูกต้อง โดยการใช้เทคนิคการเข้ารหัสเพื่อตรวจสอบผู้ใช้และหน่วยงานระบบอื่น ๆ ที่ขอเข้าถึงหรือทำธุรกรรมกับผู้ใช้งานระบบหน่วยงาน และทรัพยากรต่างๆ

การตัดสินใจว่าโซลูชันการเข้ารหัสลับมีความเหมาะสมหรือไม่ ควรมองว่าเป็นส่วนหนึ่งของกระบวนการประเมินความเสี่ยงและการเลือกการควบคุมในวงกว้าง ซึ่งการประเมิน

นี้สามารถใช้เพื่อพิจารณาว่าการควบคุมการเข้ารหัสมีความเหมาะสมหรือไม่ ควรใช้การควบคุมประเภทใด และเพื่อวัตถุประสงค์และกระบวนการทางธุรกิจใด

3.7.5 การทดสอบซอฟต์แวร์ (Software test)

วัตถุประสงค์ คือ เพื่อให้แน่ใจว่าการรักษาความปลอดภัยของข้อมูลเป็นส่วนสำคัญของระบบข้อมูลตลอดอายุการใช้งาน รวมถึง

- ต้องมีการทดสอบซอฟต์แวร์ทั้งภายในและภายนอกหน่วยงาน เช่น หน่วยงานของรัฐ บริษัทภายนอก เป็นต้น
- ต้องกำหนดแผนฉุกเฉินในกรณีเกิดการโจมตีทางไซเบอร์ ซึ่งบุคคลากรและเครือข่ายควรมีการตั้งรับเพื่อที่จะเผชิญทุกเมื่อ

3.7.5.1 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

การทดสอบเพื่อยอมรับระบบควรรวมถึงการทดสอบความต้องการด้านความปลอดภัยข้อมูลและการปฏิบัติตามแนวทางการพัฒนาระบบที่ปลอดภัย ซึ่งควรดำเนินการบนส่วนประกอบที่ได้รับมาและระบบแบบบูรณาการ

องค์กรสามารถใช้ประโยชน์จากเครื่องมืออัตโนมัติ เช่น เครื่องมือวิเคราะห์รหัสหรือเครื่องสแกนช่องโหว่ และควรตรวจสอบการแก้ไขข้อบกพร่องที่เกี่ยวข้องกับความปลอดภัย

การทดสอบเพื่อยอมรับระบบควรทำในสภาพแวดล้อมการทดสอบจริงเพื่อให้แน่ใจว่าระบบจะไม่นำช่องโหว่มาสู่สภาพแวดล้อมขององค์กรและเพื่อพิสูจน์ความน่าเชื่อถือของระบบ ซึ่งมักจะต้องใช้ข้อมูลการทดสอบจำนวนมากที่มีความใกล้เคียงกับข้อมูลการปฏิบัติงาน

3.7.5.2 การทดสอบความมั่นคงปลอดภัยของระบบ (System security testing)

ระบบใหม่ๆและที่มีการอัปเดตจำเป็นต้องผ่านการทดสอบและการตรวจสอบอย่างละเอียดระหว่างกระบวนการพัฒนาระบบ รวมถึงการจัดทำตารางกิจกรรมอย่างละเอียด ผลลัพธ์ของการทดสอบ และผลลัพธ์ที่คาดหวังภายใต้เงื่อนไขที่หลากหลาย

การทดสอบการบุกรุกด้านความปลอดภัยเป็นมาตรการหลักที่มีการตรวจสอบและการรับรองมาตรฐานเพื่อตรวจสอบความเสถียรภาพของเครือข่ายไอที การทดสอบเหล่านี้ต้องได้รับการดูแลและตรวจสอบโดยบุคคลที่มีความสามารถและได้รับการรับรองและควรดำเนินการทดสอบอย่างเหมาะสมโดยการใช้อุปกรณ์ไวต์บ็อกซ์ (white box)

สำหรับการพัฒนาภายในองค์กร การทดสอบดังกล่าวควรดำเนินการในขั้นต้นโดยทีมพัฒนา จากนั้นจึงควรทำการทดสอบการยอมรับแบบอิสระ (ทั้งการพัฒนาภายในและภายนอกองค์กร) เพื่อให้แน่ใจว่าระบบทำงานตามที่คาดไว้ รวมถึงควรกำหนดสัดส่วนของขอบเขตของการทดสอบให้สัมพันธ์กับความสำคัญและลักษณะของระบบ

3.8 การจัดหาและการบำรุงรักษาระบบ (System acquisition and maintenance)

3.8.1. ข้อกำหนดด้านความปลอดภัยของระบบข้อมูลอาณัติสัญญาณ (Security requirements of signaling information systems)

วัตถุประสงค์ คือ เพื่อให้แน่ใจว่าการรักษาความมั่นคงปลอดภัยเป็นส่วนสำคัญของระบบสารสนเทศการส่งสัญญาณซึ่งรวมถึงระบบปฏิบัติการ โครงสร้างพื้นฐาน ผลิตภัณฑ์ที่ไม่มีวางจำหน่ายทั่วไป โทรคมนาคม แอปพลิเคชันทางรถไฟ และแอปพลิเคชันที่ผู้ใช้พัฒนาขึ้น

การออกแบบและการใช้งานระบบรางที่รองรับการทำงานของตัวรถไฟนั้น มีความสำคัญต่อความมั่นคงปลอดภัยอย่างยิ่ง ควรมีการจัดทำข้อกำหนดด้านความปลอดภัยและมีการยอมรับก่อนการพัฒนาและหรือการนำระบบข้อมูลสัญญาณไปใช้งาน

ข้อกำหนดของระบบด้านความมั่นคงปลอดภัยของสารสนเทศและการนำกระบวนการในการดำเนินการด้านความปลอดภัยไปใช้ ควรถูกรวมไว้ในระยะเริ่มต้นของโครงการระบบสารสนเทศและคำชี้แจงความต้องการทางธุรกิจสำหรับการปรับปรุงระบบสารสนเทศที่มีอยู่ ควรระบุข้อกำหนดสำหรับการควบคุมความปลอดภัย

3.8.2 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยของข้อมูล (Information security requirements analysis and specification)

วัตถุประสงค์ คือ เพื่อให้มั่นใจว่าการรักษาความมั่นคงปลอดภัยของข้อมูล เป็นส่วนสำคัญของระบบสารสนเทศตลอดอายุการใช้งาน รวมถึงข้อกำหนดสำหรับระบบสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะด้วย

ควรมีการระบุข้อกำหนดด้านความปลอดภัยของข้อมูลโดยใช้วิธีการต่างๆ เช่น การปฏิบัติตามข้อกำหนดจากนโยบายและข้อบังคับ การสร้างแบบจำลองภัยคุกคาม การตรวจสอบเหตุการณ์หรือการใช้เกณฑ์ประเมินความเสี่ยง และควรมีการจัดทำผลของการระบุข้อกำหนดเป็นลายลักษณ์อักษรและทำการทบทวนโดยผู้มีส่วนได้ส่วนเสียทั้งหมด

ข้อกำหนดและการควบคุมความมั่นคงปลอดภัยของสารสนเทศควรสะท้อนถึงมูลค่าทางธุรกิจของสารสนเทศที่เกี่ยวข้อง และผลกระทบทางธุรกิจในเชิงลบที่อาจเกิดขึ้น ซึ่งเป็นผลมาจากการขาดการรักษาความมั่นคงปลอดภัยที่เพียงพอ

การระบุและการบริหารจัดการข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูลและกระบวนการที่เกี่ยวข้องควรถูกรวมไว้ในระยะเริ่มต้นของโครงการระบบสารสนเทศ

การพิจารณาข้อกำหนดด้านความปลอดภัยของข้อมูลตั้งแต่ระยะเริ่มต้น เช่น พิจารณาตั้งแต่ขั้นตอนการออกแบบ สามารถนำไปสู่โซลูชันที่มีประสิทธิภาพและคุ้มค่ามากขึ้นได้

ข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศควรพิจารณาด้วย:

- ระดับของความน่าเชื่อถือที่จำเป็นต่อการยืนยันตัวตนที่อ้างสิทธิของผู้ใช้ เพื่อให้ได้มาซึ่งข้อกำหนดในการตรวจสอบสิทธิ์ผู้ใช้
- กระบวนการจัดเตรียมการเข้าถึงและการอนุญาต สำหรับผู้ใช้ในเชิงธุรกิจตลอดจนสำหรับผู้ใช้ที่มีสิทธิพิเศษหรือเชิงเทคนิค
- แจ้งให้ผู้ใช้และผู้ปฏิบัติงานทราบถึงหน้าที่และความรับผิดชอบของตนเอง
- ความต้องการการป้องกันที่จำเป็นของทรัพย์สินที่เกี่ยวข้อง โดยเฉพาะความพร้อมใช้งาน การรักษาความลับ และความสมบูรณ์ของทรัพย์สิน

- ข้อกำหนดที่ได้มาจากกระบวนการทางธุรกิจ เช่น การบันทึกและการตรวจสอบธุรกรรม ข้อกำหนดของการห้ามปฏิเสธความรับผิดชอบ
- ข้อกำหนดที่กำหนดโดยการควบคุมความมั่นคงปลอดภัยอื่นๆ เช่น อินเตอร์เฟสในการบันทึกและติดตามหรือระบบตรวจจับการรั่วไหลของข้อมูล

ควรปฏิบัติตามกระบวนการทดสอบและการจัดหาอย่างเป็นทางการหากได้รับผลิตภัณฑ์มาแล้ว และควรเพิ่มข้อกำหนดด้านความปลอดภัยที่มีการระบุไว้ลงในสัญญาที่จัดทำขึ้นกับผู้ผลิต

ในกรณีที่ฟังก์ชันการรักษาความมั่นคงปลอดภัยในผลิตภัณฑ์ที่เสนอไม่เป็นไปตามข้อกำหนดที่ระบุไว้ ควรพิจารณาการนำมาซึ่งความเสี่ยงและการควบคุมที่เกี่ยวข้องอีกครั้งก่อนตัดสินใจซื้อผลิตภัณฑ์นั้นๆ

ควรกำหนดเกณฑ์ในการยอมรับผลิตภัณฑ์ เช่น ในแง่ของฟังก์ชันการทำงาน ซึ่งควรตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย และควรประเมินผลิตภัณฑ์ตามเกณฑ์ที่กำหนดขึ้นก่อนมีการรับผลิตภัณฑ์นั้นๆ รวมถึงควรตรวจสอบฟังก์ชันการทำงานเพิ่มเติมเพื่อให้แน่ใจว่าจะไม่มีความเสี่ยงเพิ่มเติมที่ไม่สามารถยอมรับได้

3.8.3. หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

ต้องคำนึงถึงความปลอดภัยในระหว่างการออกแบบสถาปัตยกรรมของระบบอาณัติสัญญาณและบูรณาการกับการพัฒนาวงจรตั้งแต่เริ่มต้น

ระบบตรวจสอบการทำงานแบบเรียลไทม์ คือ ลักษณะการทำงานที่ถูกต้องสำหรับแต่ละระบบบังคับสัมพันธ์ ซึ่งถูกกำหนดด้วยภาษาที่ใช้งานได้

ระบบบังคับสัมพันธ์ จะตรวจสอบคำสั่งที่ได้รับแต่ละคำสั่งว่าตรงตามลักษณะการทำงานที่มีการกำหนดไว้ล่วงหน้าหรือไม่ ซึ่งปัจจุบันฟังก์ชั่นนี้ไม่ค่อยถูกใช้ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระบบรางนัก แต่ถูกใช้หลักๆในประเด็นด้านความปลอดภัยเพื่อที่ความปลอดภัยอาจมีเพิ่มมากขึ้น

ควรตรวจสอบคำสั่งที่ได้รับจากหน่วยออนบอร์ดซ้ำอีกครั้ง

การตรวจสอบซ้ำของคำสั่งนั้น ไม่ใช่วิธีการด้านความปลอดภัยที่มีการบังคับใช้ ซึ่งวิธีนี้สามารถนำมาใช้เป็นส่วนหนึ่งของแนวทางหรือเครื่องเพื่อเปรียบเทียบความมั่นคงปลอดภัย

การใช้โซลูชัน ระบบตรวจจับการบุกรุกบนเครือข่าย (NIDS) หรือ ระบบตรวจจับการบุกรุกโฮสต์ (HIDS) มาตรวจสอบการรับส่งข้อมูลสัญญาณจากมุมมองการทำงานและการแจ้งเตือนจากรูปแบบการจราจรที่ผิดปกติ

ยังไม่มีการนำมาปรับใช้ แต่อาจเป็นแนวคิดสำหรับการทำงานในอนาคตของ UIC โดยใช้คำอธิบายของฟังก์ชันการส่งสัญญาณอย่างเป็นทางการ และในทางกลับกัน คุณสมบัติของการทำงานและความปลอดภัย หรือ ค่าคงที่ ที่เคยเกี่ยวข้องกับกับระบบภายในของการส่งสัญญาณโดยอุปกรณ์โมดูล

การประเมินประกอบด้วยสองวิธีการ ดังนี้: ระดับสาขา โดยใช้วิธีตรวจจับการบุกรุกโฮสต์ (HIDS) ในแต่ละโมดูล และระดับศูนย์กลาง โดยใช้วิธีตรวจจับการบุกรุกบนเครือข่าย(NIDS) ในแต่ละเครือข่าย

ต้องนำแนวทางการรักษาความมั่นคงปลอดภัยมาใช้เพื่อหลีกเลี่ยงวิสัยทัศน์ด้านความปลอดภัย และเพื่อครอบคลุมความเสี่ยงด้านสิทธิเท่านั้น

3.8.3.1. ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

ควรมีการตรวจสอบความปลอดภัยของแอปพลิเคชันที่ให้บริการแบบเปิดเผยผ่านเครือข่ายภายในหรือเครือข่ายสาธารณะ และความปลอดภัยในการใช้งาน และควรมีการปกป้องข้อมูลที่เกี่ยวข้องกับบริการของแอปพลิเคชันที่ส่งผ่านเครือข่ายภายในหรือเครือข่ายสาธารณะจากการฉ้อโกง ข้อพิพาทในสัญญา และการเปิดเผยและแก้ไขโดยไม่ได้รับอนุญาต

สำหรับความเสี่ยงที่เกิดขึ้นบนแอปพลิเคชันที่มีความอ่อนไหวพร้อมการบริการแบบเปิดเผย ควรได้รับการระบุ ประเมิน และยอมรับโดยเจ้าของแอปพลิเคชันนั้นๆ

3.8.3.2. การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

ควรมีการป้องกันข้อมูลที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์เพื่อป้องกันการส่งข้อมูลที่ไม่สมบูรณ์ เส้นทางในการส่งผิดพลาด การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การทำซ้ำข้อความโดยไม่ได้รับอนุญาต หรือการเล่นซ้ำ

ข้อควรพิจารณาด้านความปลอดภัยประกอบด้วย:

- การใช้ลายเซ็นอิเล็กทรอนิกส์ของแต่ละฝ่ายที่เกี่ยวข้องในการทำธุรกรรม
- ทุกด้านของการทำธุรกรรม เช่น การทำให้มั่นใจว่า:
  - ข้อมูลประจำตัวของผู้ใช้ทุกฝ่ายถูกต้องและมีการตรวจสอบ
  - ธุรกรรมยังคงไว้ซึ่งความลับ
  - มีการคงไว้ซึ่งความเป็นส่วนตัวที่เกี่ยวข้องกับทุกฝ่ายที่เกี่ยวข้อง
- การใช้วิธีเข้ารหัสกับเส้นทางการสื่อสารระหว่างฝ่ายที่เกี่ยวข้องทั้งหมด
- การรักษาความมั่นคงปลอดภัยของโปรโตคอลที่ใช้ในการสื่อสารระหว่างฝ่ายที่เกี่ยวข้อง
- ตรวจสอบให้แน่ใจว่าการจัดเก็บรายละเอียดธุรกรรมอยู่นอกเหนือการเข้าถึงแบบสาธารณะได้ เช่น อยู่บนแพลตฟอร์มการจัดเก็บข้อมูลที่มีอยู่บนอินทราเน็ตขององค์กร และไม่ถูกเก็บรักษาหรือเปิดเผยบนสื่อจัดเก็บข้อมูลที่เข้าถึงได้โดยตรงจากอินเทอร์เน็ต
- เมื่อมีการใช้หน่วยงานที่เชื่อถือได้ (เช่น เพื่อวัตถุประสงค์ในการออกและบำรุงรักษาลายเซ็นดิจิทัลและหรือใบรับรองดิจิทัล) การรักษาความมั่นคงปลอดภัยควรถูกรวมและฝังไว้ตลอดกระบวนการจัดการออกใบรับรองหรือลายเซ็นแบบ end-to-end

ขอบเขตของการควบคุมที่นำมาใช้จะต้องสอดคล้องกับระดับความเสี่ยงที่เกี่ยวข้องกับธุรกรรมออนไลน์แต่ละรูปแบบ

การทำธุรกรรมต่างๆ อาจจำเป็นต้องปฏิบัติตามกฎหมาย ข้อบังคับ และระเบียบในเขตอำนาจศาลโดยตรวจสอบว่ามีการสร้างธุรกรรมจากที่ใด ดำเนินการผ่านอะไร ดำเนินการเสร็จสิ้นที่ใด และหรือจัดเก็บอยู่ที่ใด

การทำธุรกรรมนั้น สามารถทำได้ในลักษณะออนไลน์ด้วยหลายรูปแบบ เช่น สัญญาการเงิน ฯลฯ

3.8.3.3. ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

ซอฟต์แวร์ควรได้รับการวิเคราะห์ไวรัสและทดสอบก่อนใช้เพื่ออัปเดตระบบของอุปกรณ์

ควรมีการทดสอบองค์ประกอบภายในของฮาร์ดแวร์ใหม่ในพื้นที่แยกต่างหากเพื่อตรวจหาความล้มเหลวด้านความปลอดภัยในลักษณะการทำงาน

นโยบายไวต์บ๊อกซ์ (White box policy) ได้ระบุไว้ว่า ไม่มีการได้มาซึ่งซอฟต์แวร์หรือฮาร์ดแวร์หากมีการจัดเตรียมข้อมูลจำเพาะของอุปกรณ์และซอร์สโค้ดไว้ครบถ้วนแล้ว ซึ่งโซลูชันนี้เชื่อมโยงกับปัญหาห่วงโซ่อุปทานด้านความปลอดภัย ในบริบทของมาตรฐานฯนี้ ห่วงโซ่อุปทานไม่ได้อยู่ภายใต้การควบคุมด้านความปลอดภัยอย่างแท้จริง แต่อาจจำเป็นต้องส่งออกในบางประเทศ

3.8.4. การปกป้องข้อมูลการทดสอบ (Protection of test data)

ควรเลือกข้อมูลการทดสอบอย่างรอบคอบ และควรมีการป้องกันและควบคุม

ควรหลีกเลี่ยงการใช้ฐานข้อมูลการปฏิบัติงานที่มีข้อมูลส่วนบุคคลหรือข้อมูลอื่นๆ ที่มีความอ่อนไหว เพื่อใช้ในการทดสอบ หากข้อมูลส่วนบุคคลหรือข้อมูลที่มีความอ่อนไหวถูกใช้เพื่อวัตถุประสงค์ในการทดสอบ รายละเอียดและเนื้อหานั้นควรถูกลบออกหรือแก้ไขนอกเหนือการบันทึกกิจกรรมก่อนเริ่มใช้งาน

ควรใช้แนวทางต่อไปนี้เพื่อปกป้องข้อมูลการปฏิบัติงานเมื่อถูกนำไปใช้ในการทดสอบ:

- ก) ควรนำกระบวนการของการควบคุมการเข้าใช้ที่ใช้กับระบบแอปพลิเคชันในการปฏิบัติงานไปใช้กับระบบแอปพลิเคชันทดสอบด้วย
- ข) ควรมีการอนุมัติแยกต่างหากในแต่ละครั้งที่คัดลอกข้อมูลการปฏิบัติงานไปยังระบบแอปพลิเคชันทดสอบ
- ควรลบข้อมูลการปฏิบัติงานออกจากระบบแอปพลิเคชันทดสอบทันทีหลังจากการทดสอบเสร็จสิ้น
- ควรบันทึกการคัดลอกและการใช้ข้อมูลการปฏิบัติงานเพื่อให้มีหลักฐานสำหรับการตรวจสอบ

3.9 การบริหารจัดการการเปลี่ยนแปลง (Change management)

ควรมีการควบคุมการเปลี่ยนแปลงของอุปกรณ์และระบบประมวลผลสารสนเทศ และควรจัดให้ระบบปฏิบัติการและซอฟต์แวร์แอปพลิเคชันอยู่ภายใต้การควบคุมการบริหารจัดการการเปลี่ยนแปลงที่เข้มงวด

โดยเฉพาะอย่างยิ่ง ควรพิจารณาประเด็นต่อไปนี้:

- การระบุและการบันทึกการเปลี่ยนแปลงที่มีลักษณะสำคัญ
- การวางแผนการทดสอบและการเปลี่ยนแปลงต่างๆ
- การประเมินผลกระทบที่อาจเกิดขึ้น รวมถึงผลกระทบด้านความปลอดภัยของการเปลี่ยนแปลงดังกล่าว
- ขั้นตอนการอนุมัติอย่างเป็นทางการของการเปลี่ยนแปลงที่นำเสนอ
- การตรวจสอบที่เป็นไปตามข้อกำหนดด้านความปลอดภัย
- การสื่อสารส่งต่อรายละเอียดการเปลี่ยนแปลงไปยังบุคคลที่เกี่ยวข้องทั้งหมด
- ขั้นตอนการใช้ทางเลือก รวมถึงขั้นตอนและความรับผิดชอบในการยกเลิกและการกู้คืนจากการเปลี่ยนแปลงที่ล้มเหลวและเหตุการณ์ที่คาดไม่ถึง
- การจัดเตรียมกระบวนการเปลี่ยนแปลงฉุกเฉินเพื่อให้สามารถดำเนินการเปลี่ยนแปลงได้อย่างรวดเร็วและควบคุมได้ซึ่งจำเป็นในการแก้ไขสถานการณ์ฉุกเฉิน

การอัปเดตซอฟต์แวร์ในระบบอุตสาหกรรมไม่สามารถดำเนินการได้ตามเวลาที่กำหนดเสมอไป เนื่องจากการอัปเดตเหล่านี้จำเป็นต้องได้รับการทดสอบอย่างละเอียดโดยทั้งผู้จำหน่ายสินทรัพย์ที่ใช้ในการควบคุมทางอุตสาหกรรม (อุปกรณ์หรือแอปพลิเคชัน) และผู้ใช้บริการก่อนที่จะมีการดำเนินการ

ควรมีการกำหนดความรับผิดชอบและขั้นตอนการจัดการอย่างเป็นทางการเพื่อให้แน่ใจว่าสามารถควบคุมการเปลี่ยนแปลงของอุปกรณ์ ซอฟต์แวร์ หรือขั้นตอนทั้งหมดได้อย่างน่าพอใจเมื่อมีการเปลี่ยนแปลงเกิดขึ้น ควรเก็บบันทึกการตรวจสอบที่มีข้อมูลที่เกี่ยวข้องไว้ทั้งหมด

ควรกำหนดโปรแกรมการจัดการการเปลี่ยนแปลงและขั้นตอนที่ใช้อย่างเป็นทางการเพื่อให้แน่ใจว่าการปรับเปลี่ยนทั้งหมดในเครือข่ายการส่งสัญญาณเป็นไปตามข้อกำหนดด้านความปลอดภัยเช่นเดียวกันกับส่วนประกอบดั้งเดิมที่มีการระบุไว้ในการประเมินสินทรัพย์ และแผนการประเมินและการบรรเทาความเสี่ยงที่เกี่ยวข้อง

การควบคุมการเปลี่ยนแปลงบนอุปกรณ์และระบบประมวลผลข้อมูลที่ไม่เพียงพอเป็นสาเหตุที่พบบ่อยในความล้มเหลวหรือความมั่นคงปลอดภัยของระบบ

การเปลี่ยนแปลงสภาพแวดล้อมในการปฏิบัติงาน โดยเฉพาะอย่างยิ่งเมื่อถ่ายโอนระบบจากการพัฒนาไปสู่ขั้นตอนการปฏิบัติงาน อาจส่งผลต่อความน่าเชื่อถือของแอปพลิเคชันได้

3.10 การแสวงหาประโยชน์ด้านความปลอดภัย (Security exploitation)

3.10.1 การป้องกันจากมัลแวร์ (Protection from malware)

วัตถุประสงค์ คือ เพื่อปกป้องความสมบูรณ์ของซอฟต์แวร์และสารสนเทศ ควรใช้ความระมัดระวังในการป้องกันและตรวจจับการนำมาซึ่งโค้ดที่เป็นอันตรายและรหัสมือถือที่ไม่ผ่านการรับรอง

ซอฟต์แวร์และอุปกรณ์ด้านการส่งสัญญาณและโทรคมนาคมอาจจะเสี่ยงต่อการนำมาซึ่งโค้ดที่เป็นอันตราย เช่น ไวรัสคอมพิวเตอร์(ผ่านกุญแจ USB ที่ไม่รู้จัก) ไวรัสหนอนคอมพิวเตอร์(network worms) ไวรัสโทรจัน(Trpjan horses) และ ไวรัสระเบิดเวลา(logic bombs)

ผู้ใช้ควรตระหนักถึงภัยของโค้ดที่เป็นอันตราย ผู้ที่มีหน้าที่ในการจัดการส่วนนี้ควรแนะนำการควบคุมเพื่อป้องกัน ตรวจจับ และลบโค้ดที่เป็นอันตรายเหล่านี้และควบคุมโค้ดมือถือตามความเหมาะสม

3.10.2 มาตรการการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

ควรดำเนินควบคุมการตรวจหา การป้องกัน และการกู้คืนเพื่อป้องกันมัลแวร์ ร่วมกับการสร้างความตระหนักของผู้ใช้งานที่เหมาะสม

การป้องกันมัลแวร์ควรขึ้นอยู่กับซอฟต์แวร์ที่ใช้ในการตรวจจับและซ่อมแซมมัลแวร์ การตระหนักถึงความปลอดภัยของข้อมูล การเข้าถึงระบบที่เหมาะสม และการควบคุมการจัดการการเปลี่ยนแปลง

การสร้างมาตรการป้องกันมัลแวร์นั้น ควรพิจารณาด้วยแนวทางต่อไปนี้:

- กำหนดนโยบายอย่างเป็นทางการที่ห้ามมิให้ใช้ซอฟต์แวร์ที่ไม่ผ่านการรับรอง
- ใช้การควบคุมที่ป้องกันหรือตรวจจับการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต เช่น การใช้ระบบ Application Whitelisting)
- ใช้วิธีการควบคุมที่ป้องกันหรือตรวจจับการใช้งานที่น่าสงสัย หรือเว็บไซต์ที่เป็นอันตราย เช่น การขึ้นบัญชีดำ (blacklisting)
- กำหนดนโยบายที่เป็นทางการเพื่อป้องกันความเสี่ยงที่เกี่ยวข้องกับการรับไฟล์และซอฟต์แวร์ต่างๆ ไม่ว่าจากหรือผ่านเครือข่ายภายนอกหรือบนสื่ออื่นใด โดยควรระบุว่าควรใช้มาตรการป้องกันใด
- ลดช่องโหว่ที่ปรแกรมไม่ประสงค์ดีหรือมัลแวร์อาจใช้ประโยชน์ได้ เช่น ผ่านการจัดการช่องโหว่ทางเทคนิค
- ดำเนินการตรวจสอบซอฟต์แวร์และเนื้อหาข้อมูลของระบบที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญเป็นประจำ และควรตรวจสอบการปรากฏตัวของไฟล์ที่ไม่ผ่านการอนุมัติหรือการแก้ไขที่ไม่ได้รับอนุญาตอย่างเป็นทางการ
- ติดตั้งและอัปเดตซอฟต์แวร์สำหรับตรวจจับและซ่อมแซมมัลแวร์เป็นประจำเพื่อสแกนคอมพิวเตอร์และสื่อต่างๆ เป็นการควบคุมไว้ล่วงหน้าหรือกระทำเป็นประจำ การสแกนที่ดำเนินการควรรวมถึง:
  - สแกนไฟล์ที่ได้รับผ่านเครือข่ายหรือผ่านสื่อจัดเก็บข้อมูลรูปแบบใดๆ เพื่อหามัลแวร์หรือโปรแกรมไม่ประสงค์ดีก่อนใช้งาน
  - สแกนไฟล์ที่แนบมากับอีเมลและดาวน์โหลดมัลแวร์ก่อนใช้งาน การดำเนินการดังกล่าวควรดำเนินการในสถานที่ที่แตกต่างกัน เช่น ที่เซิร์ฟเวอร์อีเมล พื้นหลังของจอภาพคอมพิวเตอร์ และเมื่อเข้าสู่เครือข่ายขององค์กร

- สแกนหน้าเว็บเพื่อหามัลแวร์

- กำหนดขั้นตอนและความรับผิดชอบในการจัดการกับการป้องกันมัลแวร์ในระบบ ฝึกอบรมการใช้งาน การรายงานและการกู้คืนระบบจากการโจมตีของมัลแวร์
- เตรียมแผนความต่อเนื่องทางธุรกิจที่เหมาะสมสำหรับการกู้คืนระบบ และข้อมูลที่จำเป็นจากการโจมตีของมัลแวร์ รวมถึงเตรียมการสำรองและกู้คืนซอฟต์แวร์
- การดำเนินการตามขั้นตอนเพื่อรวบรวมข้อมูลอย่างสม่ำเสมอ เช่น การสมัครรับจดหมายข่าวหรือตรวจสอบเว็บไซต์ที่ให้ข้อมูลเกี่ยวกับมัลแวร์ใหม่
- นำขั้นตอนการตรวจสอบข้อมูลที่เกี่ยวข้องกับมัลแวร์ไปปรับใช้ และตรวจสอบแน่ใจว่ารายการแจ้งเตือนต่างๆนั้นถูกต้องและเป็นประโยชน์ ผู้จัดการในส่วนที่เกี่ยวข้องควรตรวจสอบให้แน่ใจว่าแหล่งข้อมูลที่ผ่านการรับรอง เช่น วารสารที่มีชื่อเสียง เว็บไซต์อินเทอร์เน็ตที่เชื่อถือได้ หรือซัพพลายเออร์ที่ผลิตซอฟต์แวร์ป้องกันมัลแวร์ ถูกนำมาใช้เพื่อแยกความแตกต่างระหว่างมัลแวร์จริงหรือหลอกลวง ซึ่งควรสร้างความตระหนักของผู้ใช้งานทุกคนถึงปัญหาของการหลอกลวงและสิ่งที่ควรทำเมื่อเจอปัญหาเหล่านี้
- แยกสภาพแวดล้อมที่อาจส่งผลกระทบร้ายแรงออกจากกัน

3.10.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์ คือ เพื่อรักษาความสมบูรณ์และความพร้อมใช้งานของข้อมูลและอุปกรณ์ส่งสัญญาณ

ควรกำหนดขั้นตอนปฏิบัติงานประจำเพื่อดำเนินการตามนโยบายและกลยุทธ์การสำรองข้อมูลที่มีการตกลงไว้และซักซ้อมการกู้คืนในเวลาที่เหมาะสม

3.10.3.1 การสำรองข้อมูลสารสนเทศ (Information backup)

สำเนาของการสำรองข้อมูลและซอฟต์แวร์ควรได้รับการทดสอบอย่างสม่ำเสมอตามนโยบายการสำรองข้อมูลที่มีการตกลงไว้

การเตรียมการสำรองข้อมูลสามารถทำได้โดยอัตโนมัติเพื่อให้กระบวนการสำรองและกู้คืนข้อมูลง่ายขึ้น การแก้ปัญหาอัตโนมัติดังกล่าวควรผ่านการทดสอบอย่างเพียงพอก่อนนำไปใช้งานในช่วงเวลาปกติ

ควรกำหนดระยะเวลาการเก็บรักษาข้อมูลทางธุรกิจที่มีความสำคัญ และข้อกำหนดต่างๆ เพื่อการสำเนาเก็บถาวร โดยต้องสอดคล้องกับกฎหมายและระเบียบข้อบังคับท้องถิ่น

ควรมีการพิจารณาแนวทางต่อไปนี้สำหรับการสำรองข้อมูล:

- ควรกำหนดระดับความจำเป็นของข้อมูลสำรอง
- ควรจัดทำสำเนาสำรองและขั้นตอนการกู้คืนข้อมูลเป็นลายลักษณ์อักษรอย่างถูกต้องและครบถ้วน
- ขอบเขตของการสำรองข้อมูล (เช่น สำรองข้อมูลทั้งหมดหรือเฉพาะบางส่วน) และความถี่ของการสำรองข้อมูลควรสะท้อนถึงข้อกำหนดทางธุรกิจขององค์กร ข้อกำหนดด้านความปลอดภัยของข้อมูลที่เกี่ยวข้อง และความสำคัญของข้อมูลต่อการดำเนินงานอย่างต่อเนื่องขององค์กร

- ควรเก็บการสำรองข้อมูลไว้ในสถานที่ห่างไกล ในระยะที่เพียงพอเพื่อหลีกเลี่ยงความเสียหายจากภัยอันตรายที่สถานที่ดำเนินงานหลัก
- ควรมีการคุ้มครองข้อมูลสำรองทั้งทางกายภาพและสิ่งแวดล้อมในระดับที่เหมาะสม ซึ่งสอดคล้องกับมาตรฐานที่ใช้ที่เว็บไซต์หลัก และควรขยายการควบคุมที่ใช้กับสื่อที่เว็บไซต์หลักให้ครอบคลุมเว็บไซต์สำรองเช่นกัน
- สื่อสำรองควรได้รับการทดสอบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าสามารถใช้ในกรณีฉุกเฉินได้เมื่อจำเป็น
- ควรตรวจสอบและทดสอบขั้นตอนการกู้คืนเป็นประจำเพื่อให้แน่ใจว่าขั้นตอนเหล่านั้นยังคงมีประสิทธิภาพและสามารถดำเนินการให้เสร็จสิ้นภายในระยะเวลาที่กำหนดไว้ในขั้นตอนการปฏิบัติงานสำหรับการกู้คืน
- ในสถานการณ์ที่การรักษาความลับมีความสำคัญ ควรมีการปกป้องข้อมูลสำรองโดยใช้การเข้ารหัส
- ควรทดสอบการเตรียมการสำรองข้อมูลสำหรับแต่ละระบบเป็นประจำเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดของแผนความต่อเนื่องทางธุรกิจ

ในส่วนของระบบสำคัญ การเตรียมการสำรองข้อมูลนั้นควรครอบคลุมไปถึงส่วนของสารสนเทศ แอปพลิเคชันต่างๆ และข้อมูลที่จำเป็น เพื่อกู้คืนระบบทั้งหมดในกรณีที่เกิดภัยอันตราย

3.10.4 การบันทึกข้อมูลและการเฝ้าระวัง (Logging and monitoring)

ควรใช้การบันทึกและการตรวจสอบที่เหมาะสมเพื่อเปิดใช้งานการบันทึกของการดำเนินการที่เกี่ยวข้องกับความปลอดภัย

3.10.4.1 การบันทึกข้อมูลล็อกเหตุการณ์ (Event logging)

บันทึกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้ ข้อยกเว้น ข้อบกพร่องและเหตุการณ์ความปลอดภัยของข้อมูลควรจัดทำ เก็บรักษา และตรวจสอบอย่างสม่ำเสมอ บันทึกเหตุการณ์สามารถมีข้อมูลที่ละเอียดอ่อนและข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ควรใช้มาตรการป้องกันความเป็นส่วนตัวที่เหมาะสม

บันทึกเหตุการณ์ควรรวมถึง เมื่อมีความเกี่ยวข้อง:

- รหัสผู้ใช้
- กิจกรรมของระบบหรือผลิตภัณฑ์
- วันที่ เวลา และรายละเอียดของเหตุการณ์สำคัญต่างๆ เช่น การเข้าสู่ระบบและการออกจากระบบ
- ข้อมูลประจำตัวอุปกรณ์หรือตำแหน่งและตัวกำหนดระบบ
- บันทึกของความพยายามในการเข้าถึงระบบที่สำเร็จและถูกปฏิเสธ
- บันทึกของความพยายามในการเข้าถึงข้อมูลและทรัพยากรอื่นๆที่สำเร็จและถูกปฏิเสธ
- การเปลี่ยนแปลงการกำหนดค่าระบบ
- การใช้สิทธิพิเศษ

- การใช้ยูทิลิตี้ระบบและแอปพลิเคชัน
- ไฟล์ที่ถูกเข้าถึงและประเภทการเข้าถึง
- ที่อยู่และโปรโตคอลของเครือข่าย
- สัญญาณเตือนที่เกิดขึ้นโดยระบบควบคุมการเข้าถึง
- การเปิดและปิดการใช้งานของระบบป้องกันต่างๆ เช่น ระบบป้องกันไวรัส และระบบตรวจจับการบุกรุก
- บันทึกการทำธุรกรรมที่ดำเนินการโดยผู้ใช้ในแอปพลิเคชัน

การบันทึกเหตุการณ์เป็นพื้นฐานของระบบตรวจสอบอัตโนมัติที่สามารถสร้างรายงานรวมและการแจ้งเตือนเกี่ยวกับความปลอดภัยของระบบได้

ผู้ดูแลระบบไม่ควรได้รับอนุญาตให้ลบหรือปิดการใช้งานการบันทึกกิจกรรมของตนเองหากเป็นไปได้

3.10.4.2 การป้องกันข้อมูลบันทึก (Protection of log information)

วัตถุประสงค์ คือ เพื่อป้องกันการปลอมแปลงอุปกรณ์ที่ใช้ในการบันทึกข้อมูลและข้อมูลที่ถูกบันทึก รวมถึงการเข้าถึงโดยไม่ได้รับอนุญาต

การควบคุมควรมีวัตถุประสงค์เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตในข้อมูลที่มีการบันทึกและปัญหาการดำเนินการกับอุปกรณ์ที่ใช้ในการบันทึก ซึ่งประกอบด้วย:

- การเปลี่ยนแปลงประเภทข้อความที่บันทึกไว้
- ไฟล์บันทึกที่ถูกแก้ไขหรือลบ
- พื้นที่ความจุของสื่อบันทึกไฟล์เต็ม ทำให้ไม่สามารถบันทึกเหตุการณ์หรือบันทึกทับเหตุการณ์ที่บันทึกไว้ในอดีตได้

บันทึกการตรวจสอบบางรายการอาจจำเป็นต้องเก็บถาวรโดยเป็นส่วนหนึ่งของนโยบายการเก็บรักษาบันทึก หรือเนื่องจากข้อกำหนดในการรวบรวมและเก็บรักษาหลักฐาน

บันทึกของระบบมักประกอบด้วยข้อมูลจำนวนมาก ซึ่งส่วนใหญ่ไม่เกี่ยวข้องกับการตรวจสอบความปลอดภัยของข้อมูล

ควรพิจารณาการคัดลอกประเภทข้อความที่เหมาะสมโดยอัตโนมัติไปยังบันทึกที่สองหรือการใช้ยูทิลิตี้ระบบที่เหมาะสมหรือเครื่องมือตรวจสอบเพื่อดำเนินการสอบสวนไฟล์และอธิบายด้วยหลักแห่งเหตุผล เพื่อช่วยระบุเหตุการณ์ที่สำคัญสำหรับวัตถุประสงค์ในการตรวจสอบความปลอดภัยของข้อมูล

จำเป็นต้องมีการปกป้องบันทึกต่างๆของระบบ เพราะหากสามารถข้อมูลแก้ไขได้หรือข้อมูลในบันทึกถูกลบ บันทึกเหล่านั้นอาจสร้างความปลอดภัยที่ผิดพลาดได้ ดังนั้นจึงสามารถใช้วิธีการคัดลอกบันทึกแบบเรียลไทม์ไปยังระบบที่อยู่นอกการควบคุมของผู้ดูแลระบบหรือผู้ปฏิบัติงานเพื่อปกป้องบันทึกข้อมูลไว้

3.10.4.3. ข้อมูลบันทึกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administration and operator logs)

ข้อกำหนดการลงทะเบียนและการบันทึก คือ ควรมีการลงทะเบียนทุกการเข้าสู่ระบบและออกจากระบบ การโหลดระบบปฏิบัติการ การเริ่มต้นทำงานหรือการหยุดทำงานของโปรแกรม

พารามิเตอร์การบันทึกควรประกอบด้วย วันที่และเวลาที่ผู้ใช้งานเข้าสู่ระบบและออกจากระบบ หรือการโหลดและหยุดระบบ และผลลัพธ์ของการพยายามเข้าสู่ระบบทั้งสำเร็จและไม่สำเร็จ

ไม่ควรมีการลงทะเบียนการออกจากระบบในกรณีของการปิดระบบฮาร์ดแวร์รถไฟอัตโนมัติและการควบคุมระยะไกล

3.10.4.4 การตั้งนาฬิการะบบให้ถูกต้อง (Clock synchronization)

นาฬิกาของระบบประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดภายในองค์กรหรือโดเมนความปลอดภัยควรซิงค์ให้ตรงกันกับแหล่งอ้างอิงเวลาแห่งหนึ่ง

การตั้งค่าอุปกรณ์นาฬิกาที่ถูกต้องเป็นสิ่งสำคัญในการยืนยันความแม่นยำของบันทึกการตรวจสอบ ซึ่งอาจจำเป็นสำหรับการสอบสวนหรือใช้เป็นหลักฐานในทางกฎหมาย หรือทางวินัย

บันทึกการตรวจสอบที่ไม่ถูกต้องอาจขัดขวางการสอบสวนดังกล่าวและทำลายความน่าเชื่อถือของหลักฐานดังกล่าวเช่นกัน

การตั้งค่าอุปกรณ์นาฬิกาที่ถูกต้องเป็นสิ่งสำคัญในการยืนยันความแม่นยำของบันทึกการตรวจสอบ ซึ่งอาจจำเป็นสำหรับการสอบสวนหรือใช้เป็นหลักฐานในทางกฎหมาย หรือทางวินัย

บันทึกการตรวจสอบที่ไม่ถูกต้องอาจขัดขวางการสอบสวนดังกล่าวและทำลายความน่าเชื่อถือของหลักฐานดังกล่าวเช่นกัน

นาฬิกาที่เชื่อมโยงกับเวลาที่วิทยุออกอากาศจากนาฬิกาอะตอมสากลสามารถใช้เป็นนาฬิกาหลักสำหรับระบบบันทึกได้ รวมถึงสามารถใช้โปรโตคอลเวลาเครือข่ายเพื่อให้เซิร์ฟเวอร์ระบบทั้งหมดซิงค์กับนาฬิกาหลัก

ควรมีการจัดทำข้อกำหนดภายนอกและภายในสำหรับการแสดงเวลา การซิงโครไนซ์และความถูกต้องเป็นลายลักษณ์อักษร ซึ่งข้อกำหนดดังกล่าวอาจจัดทำขึ้นเป็นกฎหมาย ข้อบังคับ ข้อกำหนดตามสัญญา การปฏิบัติตามมาตรฐาน หรือข้อกำหนดสำหรับการตรวจสอบภายใน รวมถึงควรกำหนดเวลาอ้างอิงมาตรฐานสำหรับการใช้งานภายในองค์กร

แนวทางขององค์กรในการขอรับเวลาอ้างอิงจากแหล่งภายนอกและวิธีการซิงโครไนซ์นาฬิกาภายในอย่างน่าเชื่อถือควรจัดทำเป็นลายลักษณ์อักษรและนำไปปฏิบัติใช้

3.10.5 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical vulnerability management)

วัตถุประสงค์ คือ เพื่อลดความเสี่ยงที่เกิดจากการใช้ประโยชน์จากช่องโหว่ทางเทคนิคที่มีการเผยแพร่

การจัดการช่องโหว่ทางเทคนิคควรดำเนินการอย่างมีประสิทธิภาพ เป็นระบบ และทำซ้ำได้ โดยใช้การวัดเพื่อยืนยันประสิทธิผล ซึ่งข้อควรพิจารณาเหล่านี้ควรรวมถึงระบบปฏิบัติการและแอปพลิเคชันอื่นๆ ที่ใช้งานอยู่

3.10.5.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

ควรทราบถึงข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของสารสนเทศที่ถูกใช้งานอย่างทันท่วงที และนำวิธีการประเมินระดับการเปิดเผยขององค์กรต่อความเสี่ยงดังกล่าว รวมถึงมาตรการที่เหมาะสมมาปรับใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง

ผู้ให้บริการระบบราง/องค์กรการรถไฟควรเขียนกระบวนการและขั้นตอนการจัดการช่องโหว่ โดยกำหนดบทบาทและความรับผิดชอบที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค และรวมถึงการตรวจสอบช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ การแก้ไขช่องโหว่ที่เกิดขึ้น การติดตามทรัพย์สิน และหน้าที่ผิดชอบในการประสานงานที่จำเป็น

- กระบวนการจัดการช่องโหว่ทางเทคนิคควรสอดคล้องกับกิจกรรมของแผนการจัดการเหตุการณ์ที่ไม่ปกติ เพื่อสามารถส่งข้อมูลเกี่ยวกับช่องโหว่ไปยังฟังก์ชันการตอบสนองต่อเหตุการณ์ที่ไม่ปกติ และจัดเตรียมขั้นตอนเชิงเทคนิคที่จะนำไปปฏิบัติหากเหตุการณ์ไม่ปกติเกิดขึ้น
- ขั้นตอนการจัดการช่องโหว่ควรระบุสถานการณ์ที่มีช่องโหว่แต่ไม่มีมาตรการรับมือที่เหมาะสม ในสถานการณ์เช่นนี้ องค์กรการรถไฟควรประเมินความเสี่ยงที่เกี่ยวข้องกับช่องโหว่ที่พบและดำเนินการตรวจสอบและการแก้ไขตามเหมาะสม

ควรปฏิบัติตามคำแนะนำต่อไปนี้เพื่อสร้างกระบวนการจัดการที่มีประสิทธิภาพสำหรับช่องโหว่ทเทคนิค:

- รายการทรัพย์สินที่เกี่ยวข้องกับการระบบอาณัติสัญญาณที่ใช้ในปัจจุบันและมีความสมบูรณ์เป็นสิ่งพื้นฐานที่จำเป็นสำหรับการจัดการช่องโหว่ทางเทคนิคอย่างมีประสิทธิภาพ
- รายการทรัพย์สินที่เกี่ยวข้องกับระบบอาณัติสัญญาณที่ใช้ในปัจจุบันและมีความสมบูรณ์เป็นสิ่งพื้นฐานที่จำเป็นสำหรับการจัดการช่องโหว่ทางเทคนิคอย่างมีประสิทธิภาพ
- ควรมีการกำหนดแหล่งข้อมูลที่จะใช้เพื่อระบุช่องโหว่ทางเทคนิคที่เกี่ยวข้องและเพื่อรักษาความตระหนักถึงสิ่งเหล่านี้สำหรับซอฟต์แวร์และเทคโนโลยีอื่นๆ รวมถึงแหล่งข้อมูลเหล่านี้ควรได้รับการปรับปรุงตามการเปลี่ยนแปลงของรายการทรัพย์สิน หรือเมื่อพบแหล่งข้อมูลใหม่หรือแหล่งข้อมูลที่เป็นประโยชน์แล้ว
- ควรกำหนดระยะเวลาในการตอบสนองต่อการแจ้งเตือนของช่องโหว่ทางเทคนิคที่อาจเกี่ยวข้อง
- เมื่อพบช่องโหว่ทางเทคนิคที่อาจเกิดขึ้นแล้ว องค์กรควรระบุความเสี่ยงที่เกี่ยวข้องและกำหนดการดำเนินการแก้ไข ซึ่งการกระทำดังกล่าวอาจเกี่ยวข้องกับการแก้ไขระบบที่มีช่องโหว่หรือใช้การควบคุมอื่นๆ

- เมื่อพบช่องโหว่ทางเทคนิค ควรดำเนินการตามมาตรการควบคุมที่เกี่ยวข้องกับการจัดการการเปลี่ยนแปลงหรือโดยปฏิบัติตามขั้นตอนการตอบสนองต่อเหตุการณ์ไม่ปกติด้านความปลอดภัยของข้อมูล โดยขึ้นอยู่กับความจำเป็นเร่งด่วนในการแก้ไขช่องโหว่นั้นๆ
- หากมีแพตซ์จากแหล่งที่ถูกต้องตามกฎหมาย ควรประเมินความเสี่ยงที่เกี่ยวข้องกับการติดตั้งโปรแกรมนั้นๆ โดยเปรียบเทียบความเสี่ยงที่เกิดจากช่องโหว่กับความเสี่ยงในการติดตั้งแพตซ์
- แพตซ์ต่างๆควรผ่านการทดสอบและประเมินก่อนที่จะติดตั้งเพื่อให้แน่ใจว่ามีประสิทธิภาพและก่อให้เกิดผลข้างเคียงร้ายแรง หากแพตซ์ไม่สามารถใช้งานได้ ควรนำการควบคุมอื่นๆ มาพิจารณา เช่น
  1) การปิดบริการหรือความสามารถที่เกี่ยวข้องกับช่องโหว่
  2) การปรับหรือเพิ่มมาตรการควบคุมการเข้าถึง เช่น การเข้าถึงไฟร์วอลล์หรือการเข้าถึงที่พรมแดนเครือข่าย
  3) เพิ่มการตรวจสอบเพื่อตรวจจับการโจมตีจริง
  4) สร้างความตระหนักรู้ถึงช่องโหว่
- ควรเก็บบันทึกการตรวจสอบไว้สำหรับขั้นตอนทั้งหมดที่ดำเนินการ
- กระบวนการจัดการช่องโหว่ทางเทคนิคควรได้รับการตรวจสอบและประเมินผลอย่างสม่ำเสมอ เพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผล
- ควรแก้ไขปัญหาบนระบบที่มีความเสี่ยงสูงก่อน
- ข้อมูลเฉพาะที่จำเป็นเพื่อสนับสนุนการจัดการช่องโหว่ทางเทคนิค ได้แก่ ผู้จำหน่ายซอฟต์แวร์ หมายเลขเวอร์ชันซอฟต์แวร์ สถานะปัจจุบันของการใช้งานและบุคลากรภายในองค์กรที่รับผิดชอบซอฟต์แวร์

ผู้จำหน่ายมักอยู่ภายใต้แรงกดดันอย่างมากในการปล่อยแพทช์โดยเร็วที่สุด ดังนั้นจึงมีความเป็นไปได้ที่แพตซ์อาจไม่สามารถแก้ไขปัญหาได้เพียงพอและมีผลข้างเคียงเชิงลบ

นอกจากนี้ ในบางกรณี การถอนการติดตั้งแพตซ์ไม่สามารถทำได้ง่ายๆ เมื่อใช้งานแพตซ์แล้ว

หากไม่สามารถทดสอบแพตซ์ได้เพียงพอ อาจพิจารณาการเลื่อนการแก้ไขช่องโหว่ออกไปเพื่อประเมินความเสี่ยงที่เกี่ยวข้อง โดยพิจารณาจากประสบการณ์ที่ผู้ใช้รายอื่นรายงาน ซึ่งการใช้ ISO/IEC 27031[14] จะเป็นประโยชน์

3.10.5.2 ข้อจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

ผู้ให้บริการระบบรางควรกำหนดและบังคับใช้นโยบายที่เข้มงวดเกี่ยวกับประเภทของซอฟต์แวร์ที่ผู้ใช้อาจสามารถติดตั้งได้เอง โดยดำเนินการตามหลักการจำกัดสิทธิตามความจำเป็น (Least Privilege)

องค์กรควรกำหนดประเภทของการติดตั้งซอฟต์แวร์ที่อนุญาตให้ติดตั้งได้ เช่น การอัปเดตแพตช์ความมั่นคงปลอดภัยสำหรับซอฟต์แวร์ที่มีอยู่ และประเภทของการติดตั้ง

ที่ไม่อนุญาต เช่น ซอฟต์แวร์สำหรับใช้ส่วนบุคคลเท่านั้นและซอฟต์แวร์ที่ไม่ทราบที่มาซึ่งอาจเป็นอันตรายหรือน่าสงสัย ซึ่งควรมอบสิทธิเหล่านี้โดยคำนึงถึงบทบาทของผู้ใช้ที่เกี่ยวข้อง

การติดตั้งซอฟต์แวร์ที่ไม่มีการควบคุมบนอุปกรณ์คอมพิวเตอร์นั้น อาจทำให้เกิดช่องโหว่ซึ่งทำให้ข้อมูลเกิดการรั่วไหล การสูญเสียความสมบูรณ์ เหตุการณ์ไม่ปกติด้านความปลอดภัยของข้อมูลอื่นๆ หรือการละเมิดสิทธิในทรัพย์สินทางปัญญา

3.10.6 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information systems audit considerations)

วัตถุประสงค์ คือ เพื่อเพิ่มประสิทธิผลสูงสุดและลดการแทรกแซงจากกระบวนการตรวจสอบระบบสารสนเทศ

ควรมีการควบคุมเพื่อปกป้องระบบปฏิบัติการและเครื่องมือตรวจสอบระหว่างการตรวจสอบระบบสารสนเทศ การคุ้มครองจำเป็นต้องมีเพื่อรักษาความสมบูรณ์และป้องกันการใช้เครื่องมือตรวจสอบในทางที่ผิด

3.10.7 มาตรการการตรวจประเมินระบบ (Information systems audit controls)

ข้อกำหนดและกิจกรรมการตรวจสอบที่เกี่ยวข้องกับการตรวจสอบระบบปฏิบัติการควรได้รับการวางแผนอย่างรอบคอบและตกลงกันเพื่อลดความเสี่ยงของการหยุดชะงักของกระบวนการทางธุรกิจ

โดยควรปฏิบัติตามแนวทางต่อไปนี้:

- ข้อกำหนดในการตรวจประเมินสำหรับการเข้าถึงระบบและข้อมูลควรสอดคล้องกับหลักการบริหารจัดการที่เหมาะสม
- ขอบเขตของการทดสอบการตรวจประเมินเชิงเทคนิคควรผ่านการเห็นชอบและได้รับการควบคุม
- การทดสอบการตรวจประเมินควรถูกจำกัดการเข้าถึงซอฟต์แวร์และข้อมูลในรูปแบบการเข้าถึงแบบอ่านอย่างเดียว (read-only access)
- ควรอนุญาตการเข้าถึงอื่นๆที่นอกจากการเข้าถึงแบบอ่านอย่างเดียว (read-only access) สำหรับสำเนาไฟล์ระบบที่แยกต่างหากเท่านั้นซึ่งควรถูกลบทันทีเมื่อการตรวจสอบเสร็จสิ้น หรือควรมีการป้องกันที่เหมาะสมหากมีข้อผูกมัดในการก็บไฟล์ดังกล่าวไว้ภายใต้ข้อกำหนดด้านเอกสารของการตรวจประเมิน
- ควรมีการระบุข้อกำหนดสำหรับการประมวลผลพิเศษหรือเพิ่มเติม และควรผ่านการเห็นชอบ
- ควรดำเนินการทดสอบการตรวจประเมินที่อาจกระทบต่อความพร้อมในการใช้งานของระบบในช่วงเวลานอกเวลาทำการ
- ควรมีการตรวจสอบการเข้าถึงทั้งหมดและบันทึกไว้เพื่อใช้เป็นหลักฐานอ้างอิงในการตรวจสอบ

3.10.8 ความมั่นคงปลอดภัยสำหรับสื่อสารข้อมูล (Communications security)

3.10.8.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network security management)

3.10.8.1.1 มาตรการเครือข่าย (Network controls)

ระบบตรวจจับการบุกรุก(Intrusion Detection Systems) และระบบป้องกันการบุกรุก(Intrusion Prevention System) ใช้เพื่อตรวจจับผู้บุกรุกในเครือข่ายและตอบสนองต่อกิจกรรมที่น่าสงสัย

ระบบเหล่านี้ประกอบด้วยเซ็นเซอร์ต่างๆ(sensors) ที่ใช้ในการวิเคราะห์การรับส่งข้อมูลผ่านเครือข่ายและตรวจจับรูปแบบการรับส่งข้อมูลที่น่าสงสัย ในกรณีที่ตรวจพบกิจกรรมที่น่าสงสัย เซ็นเซอร์จะสามารถส่งสัญญาณเตือนไปยังศูนย์ควบคุมและหรือรีเซ็ตไฟร์วอลล์เพื่อตอบสนองต่อการโจมตีทางไซเบอร์

เป็นที่น่าสังเกตว่ารูปแบบความเสี่ยงด้านความปลอดภัยเหล่านี้อาจมาจากการตรวจจับการโจมตีก่อนหน้านี้ อย่างไรก็ตาม กิจกรรมเครือข่ายที่มีความถูกต้องและไม่เป็นอันตรายอาจมีพฤติกรรมเครือข่ายที่คล้ายคลึงกันและส่งผลให้ระบบตรวจจับและป้องกันการบุกรุกแสดงผลว่าเป็นการโจมตี ทำให้เกิดความผิดพลาดในการตรวจจับ (false-positive)

แม้ว่าทางการจะเริ่มกำหนดให้มีการใช้ระบบตรวจจับที่กล่าวถึงไปข้างต้น เช่น สำนักงานรักษาความปลอดภัยทางไซเบอร์แห่งชาติของประเทศฝรั่งเศส (ANSSI) โดยกำหนดใช้ใน Operators of Vital Importance (OIV) ในบริบทภาษาฝรั่งเศสและความปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญ

แต่ก็มีผู้ให้บริการเพียงไม่กี่รายที่ยังคงติดตั้งและพัฒนาเทคโนโลยีของระบบเหล่านี้ ในขณะที่เทคโนโลยีนี้จะถูกนำมาใช้ในโดเมนรถไฟมากขึ้นเรื่อยๆ

3.10.8.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

Demilitarized Zones (DMZ) หรือ เขตปลอดทหาร คือ เครือข่ายย่อยทางกายภาพหรือเชิงตรรกะที่ทำหน้าที่เก็บและเปิดเผยการบริการจากภายนอกองค์กรไปยังเครือข่ายที่ใหญ่กว่าและไม่น่าเชื่อถือ เช่น อินเทอร์เน็ต

จุดประสงค์ของกลไกเขตปลอดทหาร(DMZ) คือ การเพิ่มระดับความปลอดภัยโดยการจำกัดและควบคุมพื้นที่ที่บุคคลภายนอกอาจสามารถเข้าถึงได้

การรับส่งข้อมูลระหว่างเครือข่ายภายในและเขตปลอดทหาร (DMZ)มักจะเป็นไปในทิศทางเดียวกัน ซึ่งหมายความว่าอุปกรณ์ในเขตปลอดทหาร (DMZ)สามารถรับข้อมูลจากเครือข่ายภายในได้ แต่ไม่สามารถเข้าถึงเครือข่ายภายในได้ และในขณะเดียวกันผู้ใช้จากอินเทอร์เน็ตก็สามารถเข้าถึงเขตปลอดทหาร (DMZ)เพื่อศึกษาข้อมูลนี้ได้

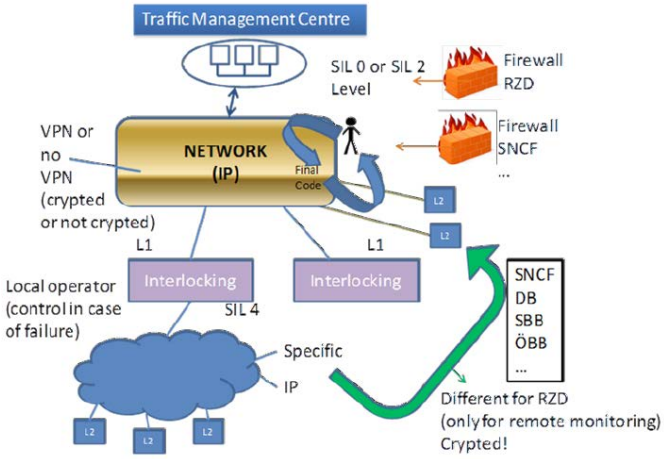
องค์ประกอบความปลอดภัยนี้มีบทบาทสำคัญในการจัดเตรียมฟังก์ชันการตรวจสอบในขณะที่การแยกเครือข่ายจะถูกเก็บไว้

ซึ่งเทคโนโลยีนี้ไม่ค่อยถูกนำมาใช้มากนัก แต่มีผู้ใช้จำนวนไม่น้อยเริ่มวางแผนที่จะนำมาปรับใช้

3.10.8.1.3 การแแบ่งแยกเครือข่าย (Segregation in networks)

การแบ่งแยกเครือข่ายสามารถทำได้ผ่าน เครือข่ายส่วนตัวเสมือน (VPN) ไฟร์วอลล์ และ การถอน (WDN) ซึ่งส่วนใหญ่การแยกเครือข่ายระหว่างบริการต่างๆ จะทำโดยใช้ เครือข่ายส่วนตัวเสมือน(VPN) ผ่าน IP/ MPLS

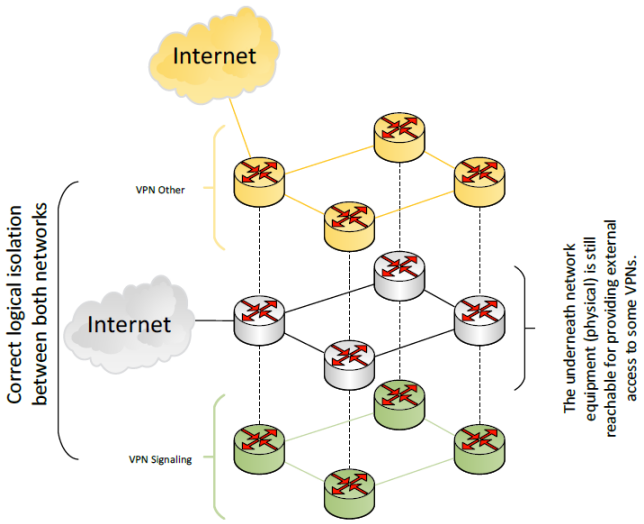
Network Security « VPN » Fig. 3



เครือข่ายส่วนตัวเสมือน(VPN) มักจะถือว่าเป็นเครือข่ายแบบปิด ดังนั้นตามมาตรฐาน EN 50159แล้ว จึงไม่มีการใช้การเข้ารหัสเพื่อปกป้องข้อมูลที่แลกเปลี่ยนผ่านเครือข่าย

อย่างไรก็ตาม ข้อสันนิษฐานนี้ไม่มีการบังคับใช้ เพราะแม้ว่าเครือข่ายส่วนตัวเสมือน(VPN) อาจทำให้เครือข่ายสามารถเป็นนามธรรมและจำกัดการเข้าถึงเครือข่ายส่วนตัวเสมือน(VPN)สำหรับบริการบางอย่าง และอุปกรณ์เครือข่ายทางกายภาพที่อยู่ด้านล่างตามรูปจะต้องเข้าถึงได้จากภายนอกเพื่ออนุญาตการเข้าถึงเครือข่ายส่วนตัวเสมือน(VPN) จากภายนอก

ซึ่งหมายความว่าแม้แต่เครือข่ายส่วนตัวเสมือน(VPN) เพียงเครือข่ายเดียวก็ไม่สามารถเข้าถึงได้โดยตรง หากอุปกรณ์ด้านล่างถูกโจมตีและตารางเส้นทางของอุปกรณ์นั้นๆเกิดความเสียหาย ส่งผลให้การแยกเครือข่ายส่วนตัวเสมือน(VPN) ที่สันนิษฐานไว้ก็จะถูกเลี่ยงออกไป



รูปที่ 4 แสดงเครือข่ายในรูปแบบนามธรรมที่สร้างขึ้นโดยเครือข่ายส่วนตัวเสมือน(VPN)

ดังจะเห็นได้ว่ามีเครือข่ายส่วนตัวเสมือน(VPN)ที่มีและไม่มีการเข้าถึงอินเทอร์เน็ตโดยใช้เครือข่ายทางกายภาพด้านล่างที่เหมือนกัน อย่างไรก็ตาม หากผู้โจมตีสามารถบุกรุกได้ถึงตัวเราเตอร์จริงที่จัดเก็บตารางเส้นทางของเครือข่ายส่วนตัวเสมือน(VPN)หลายเครือข่าย การแยกเครือข่าย "เสมือน" นี้จะไร้ประโยชน์โดยสิ้นเชิง

โดยสรุป การรักษาความปลอดภัยที่เครือข่ายส่วนตัวเสมือน(VPN)จัดเตรียมให้นั้นเป็นการรักษาความปลอดภัยของอุปกรณ์จริงซึ่งถูกใช้ร่วมกันสำหรับบริการต่างๆ ซึ่งหมายความว่าเครือข่ายส่วนตัวเสมือน(VPN)เหล่านี้ไม่ควรถือว่าเป็นเครือข่ายปิด ดังนั้นจึงควรแยกเครือข่ายออกจากบริการที่เหลือ

เทคโนโลยีมัลติเพล็กซ์แบบแบ่งความยาวคลื่น(WDM) คือ การใช้ความถี่ต่างกันเพื่อสร้างเครือข่ายแยกทางกายภาพบนใยแก้วนำแสงเดียวกัน

เทคโนโลยี WDM ยังไม่มีการใช้กันอย่างแพร่หลายในโดเมนการรถไฟสำหรับการแยกเครือข่ายจนถึงขณะนี้ แต่รัฐมนตรีบางประเทศกำลังให้การสนับสนุนเพื่อนำมาปรับใช้ในอนาคตอันใกล้

ไฟร์วอลล์ มีบทบาทสำคัญในการแยกเครือข่ายที่แตกต่างกัน เพราะสามารถลดการเข้าและออกของข้อมูลที่จำเพาะได้ เพื่ออนุญาตให้ส่วนอื่นๆ ดำเนินการต่อ

อย่างไรก็ตาม ไฟร์วอลล์ยังทำให้เกิดความล่าช้าในหลายกรณีและไม่สามารถให้การรับประกันสูงสุดในเวลานั้นได้ รวมถึงไฟร์วอลล์ยังต้องมีการอัปเดตบ่อยๆ ซึ่งโดยปกติจะทำการอัปเดตเมื่อมีการตรวจพบช่องโหว่หรือการโจมตี

ควรนำทางเลือกอื่นที่มีอัตราความล่าช้าต่ำและมีประสิทธิภาพที่มากขึ้น และการไดโอดข้อมูลมาใช้ในระบบควบคุมอุตสาหกรรม

3.10.8.2 การถ่ายโอนสารสนเทศ (Information transfer)

3.10.8.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

การถ่ายโอนข้อมูลที่ปลอดภัยสามารถใช้ฟังก์ชันการโหลดข้อมูลได้ ซึ่งช่วยให้ปรับใช้การกำหนดค่ารวมถึงการอัปเดตหรือการปรับแต่งไฟล์เมื่อเปิดใช้งานโหมดการโหลดข้อมูลได้ นอกจากนี้ยังสามารถถ่ายโอนข้อมูลการดำเนินงานผ่านลิงค์นี้ในโหมดสองทิศทาง

ควรนำการรับรองความถูกต้องของข้อมูลที่ถูกส่งออกไปและการตรวจสอบความถูกต้องซึ่งกันและกันมาปรับใช้ โดยใช้ใบรับรอง Pre-Shared Key (PSK) หรือ X509 ที่ออกจากการตรวจสอบสิทธิ์ของเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI)

เพื่อรักษาความปลอดภัยของช่องทาง ควรดูบทที่ 3.9.1 เรื่องการจัดการความปลอดภัยเครือข่าย (Network security management)

3.10.8.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

วัตถุประสงค์ คือ เพื่อให้มีการระบุการถ่ายโอนข้อมูลทางรถไฟที่ปลอดภัยระหว่างองค์กรกับบุคคลภายนอกลงในข้อตกลงระหว่างฝ่ายที่เกี่ยวข้องในการถ่ายโอนข้อมูล

ตรวจสอบให้แน่ใจว่ามีการป้องกันข้อมูลในเครือข่ายและอุปกรณ์ประมวลผลข้อมูลสนับสนุน

ข้อตกลงควรระบุถึงการถ่ายโอนข้อมูลทางธุรกิจที่ปลอดภัยระหว่างองค์กรและบุคคลภายนอก

ข้อตกลงการถ่ายโอนข้อมูลควรประกอบด้วย:

ก) หน้าที่รับผิดชอบในการบริหารจัดการการควบคุมและการแจ้งเตือนของการถ่ายโอนข้อมูล รวมถึงการจัดส่งและรับข้อมูล

ข) ขั้นตอนปฏิบัติเพื่อให้แน่ใจว่าการถ่ายโอนข้อมูลสามารถตรวจสอบย้อนกลับได้และไม่มีการปฏิเสธ

ค) มาตรฐานทางเทคนิคขั้นต่ำสำหรับการบรรจุและการถ่ายโอนข้อมูล

ง) สัญญาจ้าง

จ) มาตรฐานของการระบุ/กำหนดผู้จัดส่ง

ฉ) ความรับผิดชอบและความรับผิดในกรณีที่เกิดเหตุการณ์ด้านความปลอดภัยของข้อมูล เช่น การสูญหายของข้อมูล

ช) การใช้ระบบการบ่งชี้ข้อมูลกับข้อมูลที่มีความอ่อนไหวหรือมีความสำคัญ รวมถึงตรวจสอบให้แน่ใจว่าสามารถเข้าใจความหมายของการบ่งชี้ข้อมูลได้ในทันทีและข้อมูลนั้นๆได้รับการคุ้มครองอย่างเหมาะสม (ดูบทที่ 8.2)

ซ) มาตรฐานทางเทคนิคสำหรับการบันทึกและการอ่านข้อมูลและซอฟต์แวร์

ฌ) การควบคุมพิเศษใดๆ ที่จำเป็นในการป้องกันโปรแกรมหรือข้อมูลที่มีความอ่อนไหวง่าย เช่น การเข้ารหัส (ดูข้อ 10)

ญ) การรักษาห่วงโซ่การดูแลข้อมูลในระหว่างการถ่ายโอน

ฎ) ระดับการควบคุมการเข้าถึงที่ยอมรับได้

ควรมีการกำหนดนโยบาย ขั้นตอน และมาตรฐานและคงไว้ซึ่งการปกป้องข้อมูลและสื่อทางกายภาพระหว่างมีการถ่ายโอนข้อมูล และควรมีการระบุในข้อตกลงการถ่ายโอนข้อมูลดังกล่าว

เนื้อหาการรักษาความปลอดภัยของข้อมูลในข้อตกลงใดๆควรสะท้อนถึงความละเอียดอ่อนของข้อมูลในทางธุรกิจที่เกี่ยวข้อง อาจมีการจัดทำข้อตกลงอาจแบบอิเล็กทรอนิกส์หรือการเขียนด้วยลายมือ และอาจอยู่ในรูปแบบของสัญญาที่เป็นทางการ สำหรับข้อมูลที่เป็นความลับ กลไกเฉพาะที่ใช้สำหรับการถ่ายโอนข้อมูลดังกล่าวควรสอดคล้องกันในทุกหน่วยงานและข้อตกลงทุกประเภท

3.10.8.2.3 การส่งข้อความอิเล็กทรอนิกส์ (Electronic massaging)

ข้อควรพิจารณาด้านความปลอดภัยของข้อมูลสำหรับการส่งข้อความทางอิเล็กทรอนิกส์คต้องได้รับการปกป้องอย่างเหมาะสมและรวมถึงสิ่งต่อไปนี้:

- การปกป้องข้อความจากการเข้าถึงโดยไม่ได้รับอนุญาต การปรับเปลี่ยน หรือการปฏิเสธบริการ ที่สอดคล้องกับรูปแบบการจัดหมวดหมู่ที่องค์กรนำมาใช้
- การยืนยันความถูกต้องของที่อยู่ผู้รับและวิธีการส่งข้อความ
- ความน่าเชื่อถือและความพร้อมใช้งานของบริการ
- ข้อพิจารณาทางกฎหมาย เช่น ข้อกำหนดสำหรับลายเซ็นอิเล็กทรอนิกส์
- การขออนุมัติก่อนที่จะใช้บริการสาธารณะภายนอก เช่น การส่งข้อความโต้ตอบแบบทันที เครือข่ายสังคมออนไลน์ หรือการแชร์ไฟล์
- ระดับการตรวจสอบที่เข้มงวดยิ่งขึ้นซึ่งควบคุมการเข้าถึงจากเครือข่ายที่เข้าถึงได้แบบสาธารณะ

3.10.8.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

จุดประสงค์ของข้อตกลงในการรักษาความลับและการไม่เปิดเผยข้อมูลคือ เพื่อปกป้องข้อมูลขององค์กรและเพื่อแจ้งผู้ลงนามถึงหน้าที่ในการปกป้องการใช้ และการเปิดเผยข้อมูลด้วยลักษณะที่รับผิดชอบและผ่านการอนุญาต

หน่วยงานอาจจำเป็นต้องปรับการใช้รูปแบบของข้อตกลงการรักษาความลับหรือการไม่เปิดเผยข้อมูลในสถานการณ์ที่แตกต่างกัน

3.11 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

การรักษาความปลอดภัยทางกายภาพและการป้องกันระบบรางอัตโนมัติและการควบคุมระยะไกลควรต้องเป็นไปตามการใช้งานทางวิศวกรรมและวิธีการทางเทคนิคที่กำหนดไว้ในคู่มือกำกับดูแลของผู้ให้บริการระบบราง

การตรวจสอบการสื่อสารอย่างต่อเนื่องควรมีการดำเนินการภายนอกระบบ เช่นเดียวกับในสถานที่ติดตั้งอุปกรณ์และซอฟต์แวร์ระบบรางอัตโนมัติและการควบคุมระยะไกล

การเข้าถึงระบบควรมีข้อกำหนดดังต่อไปนี้:

- ควรมีรายชื่อบุคคลที่ได้รับอนุญาตให้เข้าถึงอุปกรณ์และหรือสถานที่ติดตั้งอุปกรณ์ซอฟต์แวร์ของระบบรางอัตโนมัติและการควบคุมระยะไกล ซึ่งหนังสือรับรองควรออกตามกฎที่ระบุไว้ในระเบียบข้อบังคับ
- พนักงานที่เกี่ยวข้องต้องตรวจสอบและอนุมัติรายชื่อผู้ขอทำการเข้าถึงระบบและออกหนังสือรับรอง
- ควรมีการตรวจสอบรายชื่อผู้ขอทำการเข้าถึงระบบเป็นระยะ ตามที่มีการกำหนดไว้ในระเบียบข้อบังคับ
- จำเป็นต้องผ่านกระบวนการคัดกรองก่อนจึงจะสามารถเข้าถึงส่วนของระบบรางอัตโนมัติและการควบคุมระยะไกลได้

อุปกรณ์และซอฟต์แวร์ของระบบรางอัตโนมัติและการควบคุมระยะไกลจะสามารถใช้ได้เฉพาะอุปกรณ์ที่มีเอกสารยืนยันว่าอุปกรณ์และซอฟต์แวร์ดังกล่าวเป็นไปตามเงื่อนไขที่ระบุไว้ในเอกสารทางเทคนิค

ผลิตภัณฑ์ฮาร์ดแวร์และซอฟต์แวร์การป้องกันข้อมูล (Data protection) สามารถใช้งานได้เฉพาะผลิตภัณฑ์ที่ยังอยู่ในช่วงเวลาที่ได้รับการรับรองเท่านั้น

ควรออกแบบช่องสัญญาณเคเบิลและระบบเชื่อมโยงต่างๆของระบบรางอัตโนมัติและการควบคุมระยะไกลตลอดจนเครือข่ายท้องถิ่นที่เป็นส่วนหนึ่งของระบบเหล่านี้ให้สอดคล้องกับเกณฑ์มาตรฐานที่ตั้งขึ้นมาเพื่อการออกแบบทางเทคนิคสำหรับอุปกรณ์อัตโนมัติและอุปกรณ์ควบคุมระยะไกลโดยเฉพาะ

เมื่ออยู่ในกระบวนการสร้างช่องทางและสายสื่อสาร การออกแบบเครือข่ายท้องถิ่นนั้นจะไม่สามารถเบี่ยงเบนไปจากคู่มือสำหรับการออกแบบได้

อุปกรณ์วิทยุที่ใช้ในระบบรางอัตโนมัติและการควบคุมระยะไกลต้องมีการลงทะเบียนตามที่ระเบียบข้อบังคับกำหนดไว้ รวมถึงอุปกรณ์และสิ่งอำนวยความสะดวกที่กล่าวมาทั้งหมดจะต้องปราศจากความเสียหาย

สิ่งอำนวยความสะดวกควรมีสิ่งอำนวยความสะดวกดังต่อไปนี้:

- ระบบจ่ายไฟที่มีระบบสำรองและมีขนาดที่เหมาะสมในการจ่ายพลังงานให้แก่ระบบรางอัตโนมัติและการควบคุมระยะไกล ในกรณีที่เกิดเหตุฉุกเฉิน แหล่งจ่ายไฟดังกล่าวจะต้องสามารถยกเลิกการจ่ายพลังงานให้กับส่วนใดส่วนหนึ่งของระบบรางอัตโนมัติและการควบคุมระยะไกลได้
- กระบวนการของระบบดับเพลิงอัตโนมัติและระบบแจ้งเตือนเพลิงไหม้อัตโนมัติ

ควรมีกระบวนการเพื่อตรวจสอบการปฏิบัติตามเงื่อนไขการทำงานของระบบรางอัตโนมัติและการควบคุมระยะไกลว่าเป็นไปตามข้อกำหนดที่ระบุไว้ในเอกสารทางเทคนิคที่เกี่ยวข้องกับระบบดับเพลิงอัตโนมัติและระบบแจ้งเตือนเพลิงไหม้อัตโนมัติ โดยมีข้อกำหนดการทำงานที่แนะนำดังนี้:

- ควรตรวจสอบการติดตั้งและถอนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และเฟิร์มแวร์ทั้งหมด
- การใช้ฮาร์ดแวร์การประมวลผลข้อมูลใหม่ต้องได้รับอนุญาตตามผลการประเมินจากผู้เชี่ยวชาญที่เกี่ยวข้อง
- การใช้การประมวลผลหรือฮาร์ดแวร์การจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการเข้าถึงหรือแทรกแซงระบบรางอัตโนมัติและการควบคุมระยะไกลต้องมีการอนุญาตหรือปฏิเสธการกระทำนั้นๆ

การเปลี่ยนแปลงการกำหนดค่าซอฟต์แวร์และฮาร์ดแวร์สำหรับการประมวลผลข้อมูลควรดำเนินการอย่างสอดคล้องกับคู่มือการปฏิบัติงานที่กำหนดไว้ซึ่งมีลายเซ็นและตราประทับที่จำเป็นทั้งหมดและต้องมีการลงทะเบียนในบันทึกประวัติการปฏิบัติงานด้วย (logbook)

3.11.1 พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure areas)

พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ประกอบด้วย สถานที่ อาคาร สำนักงาน หรือห้องต่างๆ ที่สามารถล็อคได้ ซึ่งต้องถูกล้อมรอบด้วยสิ่งกีดกั้นเพื่อความมั่นคงปลอดภัยทางกายภาพอย่างต่อเนื่อง

อุปกรณ์ประมวลผลข้อมูลที่สำคัญหรือมีความอ่อนไหวควรตั้งอยู่ในพื้นที่ที่ปลอดภัยที่ล้อมรอบด้วยส่วนกั้นที่มีควาปลอดภัยที่เหมาะสม รวมถึงระบบควบคุมการเข้าออก นอกจากนี้ยังอาจเป็นพื้นที่ชั่วคราวที่จัดตั้งขึ้นเพื่อปกป้องพื้นที่ริมรางรถไฟหรือที่จอดรถไฟได้

วัตถุประสงค์ คือ เพื่อป้องกันมิให้ผู้ไม่ได้รับอนุญาตเข้าถึง สร้างความเสียหาย และรบกวนสถานที่ปฏิบัติงานและข้อมูลของหน่วยงาน ซึ่งการเตรียมการป้องกันดังกล่าวควรสอดคล้องกับความเสี่ยงต่างๆ ที่สามารถระบุได้

3.11.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

ควรมีการกำหนดขอบเขตความปลอดภัยเพื่อปกป้องพื้นที่ที่มีข้อมูลและอุปกรณ์อาณัติสัญญาณ โดยการติดตั้งสิ่งกีดกั้น เช่น กำแพงหรือแผงกั้น ประตูควบคุมการเข้าออกโดยบัตรผ่าน หรือจุดคัดกรองการเข้าสถานที่ที่มีผู้ดูแล

ควรพิจารณาแนวทางต่อไปนี้และดำเนินการตามความเหมาะสมในการกำหนดขอบเขตการรักษาความปลอดภัยทางกายภาพ:

- ควรกำหนดขอบเขตความปลอดภัยให้ชัดเจน ตำแหน่งและความแข็งแกร่งของแต่ละขอบเขตควรขึ้นอยู่กับความต้องการความปลอดภัยของทรัพย์สินที่อยู่ภายในขอบเขตนั้นๆ และขึ้นอยู่กับผลลัพธ์ของการประเมินความเสี่ยง
- บริเวณโดยรอบของอาคารหรือสถานที่ที่มีการติดตั้งอุปกรณ์ส่งสัญญาณ/อาณัติสัญญาณควรมีความมั่นคงปลอดภัย
- ควรมีจุดคัดกรองบุคคลที่ต้องการเข้าในสถานที่หรือวิธีการอื่นเพื่อควบคุมการเข้าถึงสถานที่หรืออาคาร และต้องจำกัดการเข้าถึงสถานที่นั้นๆ ให้แก่บุคคลที่ได้รับอนุญาตเท่านั้น
- กำแพงภายนอกของสถานที่ควรมีโครงสร้างที่แข็งแรง และควรมีระบบป้องกันติดตั้งที่ประตูทางเข้าทั้งหมดเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น สัญญาณเตือนการเข้าออก ตัวล็อค ฯลฯ

- ประตูหนีไฟ/ป้องกันอัคคีภัยทั้งหมดในพื้นที่รักษาความปลอดภัยต้องมีการเตือนเฝ้าระวัง และทดสอบร่วมกับผนังเพื่อตั้งระดับความต้านทานให้เหมาะสมตามมาตรฐานระดับภูมิภาค ระดับประเทศ และระดับสากล รวมถึงระบบป้องกันอัคคีภัยต้องดำเนินการให้เป็นไปตามข้อกำหนดด้านอัคคีภัยในการใช้อุปกรณ์ป้องกันภัย
- ควรติดตั้งระบบตรวจจับผู้บุกรุกที่เหมาะสมตามมาตรฐานระดับภูมิภาค ระดับประเทศ หรือระดับสากล และต้องมีการทดสอบกับประตูทางเข้าและหน้าต่างสามารถเปิดได้อย่างสม่ำเสมอ
- ในกรณีที่มีผู้ไม่ได้รับอนุญาตพยายามเข้าถึงพื้นที่ควบคุมเหล่านี้ จะต้องรายงานไปยังศูนย์เตือนภัยส่วนกลางซึ่งมีการเฝ้าระวังตลอด 24 ชั่วโมง และควรมีทีมที่เข้าไปจัดการภัยดังกล่าว
- อุปกรณ์อาณัติสัญญาณหรือพื้นที่ควบคุมความปลอดภัยอื่นๆ ที่ดำเนินการโดยผู้ให้บริการด้านระบบรางควรแยกออกจากส่วนที่ดำเนินการโดยบุคคลภายนอก

การป้องกันทางกายภาพสามารถทำได้โดยการสร้างส่วนกั้นทางกายภาพอย่างน้อยหนึ่หรือหลายอันรอบๆสถานที่ดำเนินการและอุปกรณ์ประมวลผลข้อมูล การใช้ส่วนกั้นหลายๆอันจะช่วยเพิ่มการป้องกัน ซึ่งหากส่วนกั้นอันใดอันหนึ่งถูกคุกคามไม่ได้หมายความว่าจะเกิดช่องโหว่ของการรักษาความมั่นคงปลอดภัยในทันที

พื้นที่ที่ต้องการความมั่นคงปลอดภัยอาจเป็นสำนักงานที่ล็อคได้ หรือห้องหลายห้องที่ล้อมรอบด้วยส่วนกั้นที่ต่อเนื่องกันภายในเพื่อสร้างความปลอดภัย ซึ่งอาจจำเป็นต้องมีส่วนกั้นและขอบเขตเพิ่มเติมเพื่อควบคุมการเข้าถึงทางกายภาพระหว่างพื้นที่ที่มีข้อกำหนดด้านความปลอดภัยที่แตกต่างกันภายในพื้นที่ที่มีการควบคุมความปลอดภัย

3.11.1.2 มาตรการควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

พื้นที่รักษาความปลอดภัย (ยกเว้นบริเวณภายนอก) ควรต้องมีการป้องกันด้วยมาตรการควบคุมการเข้าออกอย่างเหมาะสม (เช่น บริเวณประตูล็อคระบบไฟฟ้า ประตูนิรภัย บริเวณทางเข้าอาคาร เครื่องอ่านการ์ดแบบกำหนดสิทธิในการเข้าถึงได้ แผนกต้อนรับ ระบบอินเตอร์คอม โทรศัพท์ที่เชื่อมต่อกับห้องควบคุมความปลอดภัย ประตูกั้นคน ระบบป้องกันการวนบัตร) เพื่อให้มั่นใจว่ามีเพียงบุคลากรและอุปกรณ์ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถเข้าถึงภายในพื้นที่ที่มีการรักษาความปลอดภัยได้โดยมีกระบวนการเฝ้าระวัง (เช่น เจ้าหน้าที่รักษาความปลอดภัย วีดิโอกล้องวงจรปิด และสัญญาณเตือนภัย) รวมถึงแสงสว่างที่เหมาะสม

ควรพิจารณาแนวทางต่อไปนี้ในการกำหนดมาตรการควบคุมการเข้าออก:

- ควรบันทึกวันที่และเวลาที่เข้าและออกของผู้เยี่ยมชม และต้องมีการเฝ้าระวังผู้เยี่ยมชมทุกคนเว้นแต่จะได้รับการอนุญาติให้เข้าถึงมาก่อนแล้ว โดยควรให้อนุญาตในเรื่องที่เฉพาะเจาะจงที่ผ่านการรับรองแล้ว และควรมีการแนะนำถึงข้อกำหนดด้านความปลอดภัยของพื้นที่นั้นๆ และวิธีการปฏิบัติในกรณีฉุกเฉิน

- ควรมีการควบคุมการเข้าถึงพื้นที่ที่มีการประมวลผลหรือจัดเก็บข้อมูลที่มีความสำคัญและจำกัดการเข้าถึงเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น รวมถึงแนวทางการตรวจสอบการเข้าถึงทั้งหมดควรได้รับการบำรุงรักษาอย่างปลอดภัย
- จุดทางเข้าพื้นที่ที่มีการรักษาความปลอดภัยควรมีแสงสว่างเพียงพอเพื่อให้แน่ใจสามารถมองเห็นได้อย่างชัดเจนตลอดเวลาและสามารถบันทึกภาพจากกล้องได้อย่างมีประสิทธิภาพ
- พนักงาน ลูกจ้าง ผู้ใช้งานที่เป็นบุคคลภายนอก และผู้เยี่ยมชมทุกคน เมื่ออยู่ในพื้นที่รักษาความปลอดภัยของผู้ให้บริการระบบราง (ยกเว้นพื้นที่ภายนอก) ควรติดบัตรระบุตัวตนที่สามารถเห็นได้ชัดเจน และควรแจ้งให้เจ้าหน้าที่รักษาความปลอดภัยทราบทันทีหากพบผู้เยี่ยมชมที่ไร้ผู้ดูแลและใครก็ตามที่ไม่สวมป้ายระบุตัวตน
- บุคลากรสนับสนุนจากหน่วยงานภายนอกควรได้รับอนุญาตให้เข้าถึงพื้นที่รักษาความปลอดภัยหรือสิ่งอุปกรณ์ประมวลผลข้อมูลที่สำคัญเมื่อจำเป็นเท่านั้น การเข้าถึงนี้ควรได้รับอนุญาตและติดตาม
- ควรมีการบำรุงรักษาบันทึกหรือหลักฐานการตรวจสอบทางอิเล็กทรอนิกส์ของการเข้าถึงทั้งหมดอย่างปลอดภัยและตรวจสอบอย่างสม่ำเสมอ
- ควรมีการตรวจสอบสิทธิในการเข้าถึงพื้นที่ที่มีการรักษาความปลอดภัยและปรับปรุงเป็นประจำ และเพิกถอนสิทธินั้นๆ เมื่อจำเป็น

3.11.1.3 สิทธิการเข้าถึง (Access rights)

ควรมีการจัดทำขั้นตอน/กระบวนการภายใต้ความรับผิดชอบของหน่วยงานรักษาความปลอดภัยในพื้นที่และนำมาใช้ในการให้สิทธิในการเข้าถึง

หมายเหตุ: สำหรับพื้นที่ควบคุมระดับประเทศ ตามกฎของพื้นที่ท้องถิ่นนั้น หน่วยงานกำกับดูแลในพื้นที่อาจมีส่วนร่วมในขั้นตอนการให้สิทธิการเข้าถึงได้

- ควรให้สิทธิการเข้าถึงเฉพาะในกรณีที่จำเป็นสำหรับการปฏิบัติงานตามนโยบายความจำเป็นในการเข้าถึง
- ควรมีการจำกัดการเข้าถึงห้องทำงานและอุปกรณ์ว้เฉพาะที่เกี่ยวข้องกับการทำงาน รวมถึงบุคลากรสนับสนุนเฉพาะเมื่อต้องการเข้าถึง
- ควรมีการกำหนดรายชื่อบุคคลที่ได้รับอนุญาตให้เข้าไปในพื้นที่และบังคับใช้โดยเจ้าหน้าที่รักษาความปลอดภัยในท้องที่ควรตรวจสอบรายชื่อดังกล่าวเป็นประจำและทำการปรับปรุงหากจำเป็น
- พนักงานทุกคนควรได้รับอนุญาตในการเข้าถึงพื้นที่ควบคุมทุกส่วน เว้นแต่พื้นที่หรือสถานที่อื่นๆ ที่นอกเหนือการกำหนดไว้ในกฎหมายและระเบียบข้อบังคับใช้
- การเข้าถึงพื้นที่ที่ปลอดภัยและมีการจำกัดจะต้องทำการอนุญาตการเข้าถึงเป็นครั้งๆไป

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

ความปลอดภัยทางกายภาพสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์อาณัติสัญญาณควรได้รับการออกแบบและใช้งาน

ควรพิจารณาแนวทางต่อไปนี้เพื่อรักษาความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และอุปกรณ์ต่างๆ:

- ควรคำนึงถึงกฎระเบียบและมาตรฐานด้านสุขภาพและความปลอดภัยที่เกี่ยวข้อง
- ควรติดตั้งอุปกรณ์สำคัญในการดำเนินงานให้หลีกเลี่ยงการเข้าถึงโดยบุคคลทั่วไป
- สถานที่ทำงานและอาคารไม่ควรจะโดดเด่นและควรมีสิ่งบ่งชี้จุดประสงค์การทำงานให้น้อยที่สุดและไม่ควรมีป้ายที่บ่งบอกอย่างชัดเจนเกี่ยวกับกระบวนการทำงานทั้งภายนอกและภายในอาคาร
- ควรมีการตั้งค่าอุปกรณ์เพื่อป้องกันไม่ให้ภายนอกรับรู้หรือเห็นข้อมูลเกี่ยวกับกิจกรรมที่เป็นความลับ รวมถึงควรพิจารณาการป้องกันทางสนามแม่เหล็กไฟฟ้าตามความเหมาะสม

สมุดรายชื่อและสมุดโทรศัพท์ภายในที่ระบุตำแหน่งของอุปกรณ์ประมวลผลข้อมูลที่มีความสำคัญไม่ควรที่จะเปิดเผยแก่ประชาชนทั่วไป

3.11.1.5 การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อมแวดล้อม (Protecting against External and Environmental Threats)

ควรมีการออกแบบการป้องกันทางกายภาพจากความเสียหายจากธรรมชาติ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว ฟ้าผ่า การรบกวนทางแม่เหล็ก ฯลฯ หรือจากการกระทำของมนุษย์ เช่น การบุกรุก การโจมตี การก่อวินาศกรรม การโจรกรรมหรือการก่อความไม่สงบ และนำการออกแบบนั้นๆ ไปใช้

ควรมีการตระหนักถึงการป้องกันภัยคุกคามจากพื้นที่ใกล้เคียง เช่น ไฟไหม้ในอาคารข้างเคียง น้ำรั่วซึมจากหลังคาหรือจากพื้นที่ต่ำกว่าระดับพื้นดิน หรือการเกิดระเบิดบนถนน

ควรพิจารณาแนวทางต่อไปนี้เพื่อหลีกเลี่ยงความเสียหายจากไฟไหม้ น้ำท่วม แผ่นดินไหว เหตุระเบิด การก่อความไม่สงบ และภัยที่เกิดจากธรรมชาติหรือจากมนุษย์ในรูปแบบอื่นๆ:

- ควรเก็บวัตถุอันตรายหรือวัตถุระเบิดไว้ให้ห่างจากพื้นที่ที่มีการรักษาความปลอดภัย ไม่ควรจัดเก็บวัสดุสิ้นเปลือง เช่น เครื่องเขียน ไว้ในพื้นที่ที่มีการรักษาความปลอดภัย
- อุปกรณ์กู้ระบบและข้อมูลสำรองควรถูกติดตั้งในระยะที่มีความปลอดภัย เพื่อหลีกเลี่ยงความเสียหายจากภัยอันตรายที่ส่งผลกระทบต่อพื้นที่ดำเนินการหลัก
- ควรมีการติดตั้งอุปกรณ์ดับเพลิงในพื้นที่ที่มีการรักษาความปลอดภัยอย่างเหมาะสม

3.11.1.5.1 ห้องปฏิบัติการเทคโนโลยีสารสนเทศ (IT rooms)

ห้องที่ติดตั้งอุปกรณ์เซิร์ฟเวอร์ควรอยู่ในพื้นที่ที่มีการรักษาความปลอดภัย(หรือพื้นที่ปลอดภัย) ซึ่งควรมีผนังกันไฟ ล้อมรอบด้วยห้องที่มีโอกาสเกิดเพลงไหม้ต่ำ ห่างจากที่เก็บวัสดุอันตราย ท่อน้ำ ท่อแก๊สและห้องเก็บแก๊ส

เครื่องพิมพ์ ตู้เก็บของ เครื่องกำเนิดไฟฟ้า และเครื่องปรับอากาศควรอยู่ในที่ที่ต่างกัน

3.11.1.6 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

ควรมีการออกแบบการป้องกันทางกายภาพและแนวทางนำสำหรับการทำงานในพื้นที่ที่มีการรักษาปลอดภัยและนำไปปรับใช้ โดยควรพิจารณาแนวทางต่อไปนี้:

- ผู้ปฏิบัติงานควรต้องรู้ถึงอุปกรณ์และกิจกรรมภายในพื้นที่ที่มีการรักษาความปลอดภัยตามหลักความจำเป็นในการทราบข้อมูลเท่านั้น
- หลีกเลี่ยงการทำงานแบบไม่มีผู้ดูแลในพื้นที่มีการรักษาความปลอดภัยด้วยเหตุผลด้านความปลอดภัยและเพื่อป้องกันโอกาสในการเกิดเหตุอันตราย
- พื้นที่ควบคุมควรถูกล็อคและมีการตรวจสอบเป็นระยะ
- ไม่ควรอนุญาตให้มีการบันทึกภาพ วิดีโอ เสียง หรืออุปกรณ์บันทึกอื่นๆ เช่น กล้องในโทรศัพท์มือถือ เว้นแต่จะได้รับอนุญาต

การเตรียมการสำหรับการทำงานในพื้นที่ปลอดภัยนั้น รวมถึงการควบคุมพนักงาน ลูกจ้าง และบุคคลภายนอกที่ทำงานในพื้นที่ควบคุม ตลอดจนกิจกรรมของบุคคลภายนอกทั้งหมดที่เกิดขึ้นในพื้นที่ดังกล่าว

3.11.2 อุปกรณ์ (Equipment)

วัตถุประสงค์ คือ เพื่อป้องกันการสูญเสีย ความเสียหาย การโจรกรรม หรือการเกิดอันตรายต่อทรัพย์สินและทำให้การดำเนินงานของผู้ให้บริการระบบรางหยุดชะงัก

ควรมีการป้องกันอุปกรณ์จากภัยคุกคามทั้งทางกายภาพและสิ่งแวดล้อม

การป้องกันอุปกรณ์ (รวมไปถึงอุปกรณ์ที่ใช้นอกสถานที่และที่เคลื่อนย้ายได้) มีความจำเป็นเพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและเพื่อป้องกันไม่ให้เกิดกาสูญเสียหรือความเสียหายต่ออุปกรณ์ โดยควรพิจารณาการจัดตั้งและการถอนอุปกรณ์ออกด้วย ซึ่งอาจจำเป็นต้องมีการควบคุมพิเศษเพื่อป้องกันภัยคุกคามทางกายภาพ และเพื่อปกป้องอุปกรณ์สนับสนุนอื่นๆ เช่น ระบบจ่ายไฟฟ้า สายสัญญาณ และสายไฟฟ้าต่างๆ

3.11.2.1 การติดตั้งและป้องกันอุปกรณ์ (Equipment siting and protection)

ควรมีการติดตั้งหรือป้องกันอุปกรณ์เพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายจากสิ่งแวดล้อม และความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

ควรพิจารณาแนวทางต่อไปนี้ในการป้องกันอุปกรณ์:

- อุปกรณ์ประมวลผลอาณัติสัญญาณที่ทำหน้าที่ประมวลผลข้อมูลที่มีความสำคัญควรถูกติดตั้งในตำแหน่งที่มีค่าองศาของมุมมองที่จำกัดเพื่อลดความเสี่ยง

ของข้อมูลที่จะถูกแก้ไขโดยบุคคลที่ไม่ได้รับอนุญาต และสถานที่จัดเก็บอุปกรณ์ต้องมีความปลอดภัยเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

- อุปกรณ์ที่ต้องการการป้องกันเป็นพิเศษ ควรติดตั้งแยกจากอุปกรณ์อื่นๆ เพื่อลดระดับการป้องกันทั่วไปที่ต้องการ
- ควรใช้การมาตรการการควบคุมเพื่อลดความเสี่ยงของภัยคุกคามทางกายภาพที่อาจเกิดขึ้น เช่น การโจรกรรม ไฟไหม้ การระเบิด ควัน น้ำ ฝุ่น การสั่นสะเทือน ผลกระทบจากสารเคมี ไฟฟ้าดับ การรบกวนการสื่อสาร การรบกวนจากคลื่นแม่เหล็กไฟฟ้า และการทำลายทรัพย์สิน
- ควรมีการตรวจวัดสภาพแวดล้อมที่อาจส่งผลกระทบต่อการดำเนินงานของอุปกรณ์ประมวลผลข้อมูล
- ควรติดตั้งอุปกรณ์ป้องกันฟ้าผ่ากับอาคารทุกหลัง และควรติดตั้งฟิลเตอร์ป้องกันฟ้าผ่าที่สายไฟหลักและสายสื่อสารหลักทุกเส้น
- ควรพิจารณาการใช้วิธีการป้องกันพิเศษ เช่น คีย์บอร์ดแผ่นยาง กับอุปกรณ์ที่อยู่ในสภาพแวดล้อมทางอุตสาหกรรม
- ควรมีการป้องกันอุปกรณ์การประมวลผลข้อมูลที่มีสำคัญเพื่อลดความเสี่ยงที่ข้อมูลจะรั่วไหลอันเนื่องมาจากการแพร่กระจายของคลื่นแม่เหล็กไฟฟ้า

3.11.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

ควรมีการป้องกันอุปกรณ์ที่สนับสนุนการทำงานจากเหตุไฟฟ้าขัดข้องและจากสาเหตุอื่นๆ ที่เกิดจากความล้มเหลวในการสนับสนุนการทำงานของอุปกรณ์

ระบบและอุปกรณ์ที่สนับสนุนการทำงาน เช่น ระบบไฟฟ้า ระบบสื่อสาร ระบบน้ำ ระบบแก๊ซ ระบบบำบัดน้ำเสีย ระบบระบายอากาศ และระบบปรับอากาศ ควรจะ:

- สอดคล้องกับข้อกำหนดของผู้ผลิตอุปกรณ์และข้อกำหนดทางกฎหมายในพื้นที่
- ได้รับการประเมินอย่างเป็นประจำว่ามีความสามารถในการรองรับการเติบโตของธุรกิจอย่างเพียงพอและสามารถเชื่อมต่อกับอุปกรณ์สนับสนุนการทำงานอื่นๆได้ดี
- ได้รับการตรวจสอบและทดสอบอย่างเป็นประจำเพื่อให้มั่นใจว่ามีการทำงานที่เหมาะสมและถูกต้อง
- ควรมีระบบแจ้งเตือนเมื่อตรวจพบการทำงานที่ผิดปกติหากจำเป็น
- หากจำเป็น ควรมีระบบแหล่งจ่ายพลังงานหลายทางที่แยกเส้นทางกันทางกายภาพ

ควรมีการติดตั้งระบบไฟและการสื่อสารฉุกเฉิน และควรติดตั้งสวิตช์และวาล์วฉุกเฉินสำหรับปิดระบบไฟฟ้า ระบบน้ำ ระบบแก๊ส หรือระบบสาธารณูปโภคอื่นๆ ไว้ใกล้ทางออกฉุกเฉินหรือห้องอุปกรณ์ นอกจากนี้การเพิ่มระบบสำรองสำหรับการเชื่อมต่อเครือข่ายสามารถทำได้โดยการใช้บริการระบบสาธารณูปโภคจากผู้ให้บริการมากกว่าหนึ่งราย

3.11.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

สายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ควรได้รับการป้องกันจากการเกิดความเสียหายหรือการดักรับข้อมูลโดยผู้ที่มิได้รับอนุญาต

ควรพิจารณาแนวทางต่อไปนี้ในการรักษาความมั่นคงปลอดภัยของสายสัญญาณและสายสื่อสาร:

- สายไฟฟ้าและสายสื่อสารที่ใช้ในระบบอาณัติสัญญาณควรเดินสายใต้ดินหากเป็นไปได้ หรือมีการป้องกันอื่นๆ ที่เหมาะสม
- ควรติดตั้งสายไฟฟ้าแยกออกจากสายสื่อสารเพื่อป้องกันการรบกวนซึ่งกันและกัน
- ควรมีการป้องกันสายสัญญาณเครือข่ายจากการดักรับข้อมูลหรือความเสียหายโดยผู้ที่มิได้รับอนุญาต
- จุดตรวจสอบและจุดต่อสายต่างๆ ควรติดตั้งในห้องหรือกล่องรวมถึงควรใช้ฉนวนห่อหุ้มสายสัญญาณและสายสื่อสารต่างๆ
- ควรติดตั้งอุปกรณ์กั้นคลื่นสนามแม่เหล็กไฟฟ้าเพื่อป้องกัน สายเคเบิล
- ควรตรวจสอบระบบสายเพื่อตรวจจับอุปกรณ์แปลกปลอม
- ควรควบคุมการเข้าถึงแผงพักปลายสาย (Patch Panel) และห้องเคเบิล

3.11.2.4 การบำรุงรักษาและซ่อมบำรุงอุปกรณ์ (Equipment Maintenance)

ควรมีการบำรุงรักษาอุปกรณ์อย่างถูกต้องเพื่อให้มั่นใจถึงความพร้อมใช้งานและความสมบูรณ์อย่างต่อเนื่องของอุปกรณ์

ควรพิจารณาแนวทางต่อไปนี้ในการซ่อมบำรุงและดูแลอุปกรณ์:

- ควรมีการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ หรือตามช่วงเวลาที่ระบุในคู่มือการใช้งานของอุปกรณ์ อุปกรณ์ที่สำคัญควรต้องอยู่ในการรับประกันของผู้ผลิตหรือต้องสามารถดำเนินการบำรุงรักษาอย่างครอบคลุมได้เองภายในองค์กร
- เฉพาะเจ้าหน้าที่บำรุงรักษาที่ได้รับอนุญาตเท่านั้นที่สามารถดำเนินการซ่อมแซมและบำรุงอุปกรณ์ได้
- ควรมีการระบุข้อกำหนดของการบำรุงรักษาอุปกรณ์ทุกชิ้นไว้อย่างชัดเจนอยู่ก่อนแล้ว
- ควรมีการลบข้อมูลที่เป็นความลับอย่างปลอดภัย หรือถอดที่จัดเก็บข้อมูลออกจากอุปกรณ์ก่อนดำเนินการบำรุงรักษา
- ควรเก็บบันทึกข้อมูลที่เกี่ยวกับการเสียหรือเหตุผิดปกติบนอุปกรณ์ รวมถึงข้อมูลการซ่อมแซมและการบำรุงรักษาอุปกรณ์นั้นๆ
- ก่อนนำอุปกรณ์กลับคืนสู่การทำงานหลังการบำรุงรักษา ควรตรวจสอบให้แน่ใจว่าอุปกรณ์ไม่ได้ผ่านการดัดแปลงและสามารถทำงานได้ปกติ
- ควรบำรุงรักษาอุปกรณ์ตามข้อกำหนดของนโยบายประกันภัย

3.11.2.5 การนำทรัพย์สินขององค์กรออกนอกสถานที่ (Removal of Assets)

อุปกรณ์ ข้อมูล หรือซอฟแวร์ไม่ควรถูกนำออกนอกสถานที่ก่อนได้รับอนุญาต

- ไม่ควรนำทรัพย์สินขององค์กรหรือหน่วยงานออกนอกสถานที่ ก่อนได้รับอนุญาต
- ควรกำหนดระยะเวลาในการส่งคืนทรัพย์สินที่ถูกนำออกไปโดยปฏิบัติตามคู่มือการคืนทรัพย์สินเพื่อยืนยันความถูกต้อง
- จุดตรวจสอบตามกฎหมายและข้อบังคับใช้ ควรมีหน้าที่รับผิดชอบในการตรวจสอบการนำสินทรัพย์ออกจากสถานที่โดยไม่ได้รับอนุญาต และตรวจสอบอุปกรณ์บันทึกต่างๆที่ไม่ได้รับอนุญาต อาวุธ ฯลฯ รวมถึงป้องกันการเข้าและออกจากสถานที่ของบุคคลที่ไม่ได้รับอนุญาต

3.11.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสถานที่ (Security of equipment and assets off premises)

ควรใช้การรักษาความมั่นคงปลอดภัยกับทรัพย์สินที่ใช้งานอยู่ภายนอกสถานที่โดยคำนึงถึงความเสี่ยงต่างๆ ของการปฏิบัติงานนอกสถานที่ขององค์กร และการใช้อุปกรณ์จัดเก็บและประมวลผลข้อมูลการส่งสัญญาณภายนอกสถานที่ปฏิบัติการ ควรต้องได้รับอนุญาตจากผู้จัดการเสียก่อน

ข้อกำหนดนี้ใช้กับอุปกรณ์ที่องค์กรเป็นเจ้าของ และอุปกรณ์ที่ใช้ในนามขององค์กร ควรพิจารณาแนวทางต่อไปนี้ในการปกป้องอุปกรณ์ที่ใช้งานอยู่ภายนอกสถานที่:

- อุปกรณ์และสื่อที่นำออกนอกสถานที่ไม่ควรถูกปล่อยทิ้งไว้ในที่สาธารณะโดยไม่มีผู้ดูแล
- ควรปฏิบัติตามคำแนะนำของผู้ผลิตในการป้องกันความเสียหายอุปกรณ์ตลอดเวลาที่ใช้งาน
- ควรมีการควบคุมการใช้งานอุปกรณ์นอกสถานที่ เช่น การทำงานที่บ้าน การทำงานนอกสำนักงาน และการทำงานในสถานที่ชั่วคราวโดยต้องมีการประเมินความเสี่ยงและมีการควบคุมที่เหมาะสม
- เมื่ออุปกรณ์ที่ใช้ภายนอกสถานที่มีการเปลี่ยนมือระหว่างหน่วงงานหรือกับบุคคลภายนอก ควรมีการบันทึกข้อมูลของผู้นำอุปกรณ์ไปใช้ หรืออย่างน้อยควรมีชื่อและหน่วยงานของผู้รับผิดชอบอุปกรณ์ดังกล่าว รวมถึงควรระมัดระวังและควบคุมความเสี่ยงที่อาจเกิดขึ้น เช่น ความเสียหาย การโจรกรรม หรือการดักฟังในระหว่างการขนย้ายไปอีกสถานที่

อุปกรณ์จัดเก็บและประมวลผลข้อมูลนั้นรวมไปถึง คอมพิวเตอร์ส่วนบุคคลหรือของหน่วยงาน โทรศัพท์มือถือ บัตรอัจฉริยะ กระดาษ หรือรูปแบบอื่นๆ ทุกรูปแบบซึ่งใช้สำหรับทำงานที่บ้านหรือเคลื่อนย้ายออกจากสถานที่ทำงานปกติด้วยเช่นกัน

3.11.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

ควรมีการตรวจสอบอุปกรณ์ที่มีสื่อจัดเก็บข้อมูลทั้งหมดเพื่อให้มั่นใจว่าข้อมูลที่เป็นความลับและซอฟต์แวร์ที่มีใบอนุญาตมีการลบทิ้งอย่างปลอดภัยก่อนกำจัดอุปกรณ์หรือนำกลับมาใช้ใหม่ มิฉะนั้นควรทำลายสื่อเก็บข้อมูลทิ้ง

อุปกรณ์ที่บันทึกข้อมูลสำคัญของระบบอาณัติสัญญาณควรถูกทำลายทิ้ง หรือข้อมูลนั้นๆ ควรถูกทำลายทิ้ง ลบ หรือเขียนข้อมูลทับโดยใช้เทคนิคที่ทำให้ข้อมูลเดิมไม่สามารถเรียกคืนได้ ซึ่งไม่แนะนำให้ใช้วิธีการลบแบบธรรมดา

อุปกรณ์บันทึกข้อมูลที่สำคัญที่มีความเสียหายอาจต้องมีการประเมินความเสี่ยงเพื่อพิจารณาว่าอุปกรณ์ดังกล่าวควรถูกทำลายทิ้งแทนที่จะส่งไปซ่อมแซมหรือทิ้งลงถังขยะหรือไม่

3.11.2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)

ผู้ใช้งานทุกคนควรตระหนักถึงข้อกำหนดและขั้นตอนด้านความมั่นคงปลอดภัยในการปกป้องอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแลตลอดจนความรับผิดชอบในการดำเนินการป้องกันดังกล่าว

ผู้ใช้ควรปิดโปรแกรมเมื่อใช้งานเสร็จแล้ว ทำการออกจากระบบจากแอปพลิเคชันหรือบริการเครือข่าย และสร้างระบบป้องกันคอมพิวเตอร์หรือโทรศัพท์มือถือด้วยการล็อครหัสหรือวิธีอื่นๆที่เทียบเท่าได้เมื่อไม่ได้ใช้งาน

3.11.2.9 นโยบายควบคุมทรัพย์สินสารสนเทศและโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

ควรนำนโยบายโต๊ะทำงานปลอดเอกสารสำคัญมาปรับใช้กับเอกสารต่างๆ และสื่อเก็บข้อมูลแบบถอดได้ และนำนโยบายป้องกันหน้าจอคอมพิวเตอร์มาปรับใช้กับอุปกรณ์ประมวลผลข้อมูล

ควรห้ามการใช้เครื่องถ่ายเอกสารและเครื่องมือชนิดอื่นที่ใช้ในการทำสำเนาโดยไม่ได้รับอนุญาต เช่น สแกนเนอร์ กล้องดิจิตอล เข้ามาในพื้นที่ที่มีการรักษาความปลอดภัย

ควรใช้เครื่องพิมพ์ที่มีฟังก์ชันการใส่รหัส(PIN code) หากเป็นไปได้ ซึ่งจะทำให้ผู้สั่งงานเป็นเพียงผู้เดียวที่สามารถรับงานพิมพ์ได้เมื่อยืนอยู่ข้างเครื่องพิมพ์เท่านั้น รวมถึงควรถอดอุปกรณ์ที่มีข้อมูลสำคัญออกจากเครื่องพิมพ์ในทันทีที่ใช้งานเสร็จ

3.12 การบริหารจัดการเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์ของการบริหารจัดการเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศควรผ่านการตกลงกับฝ่ายบริหาร และควรตรวจสอบให้แน่ใจว่าผู้ที่รับผิดชอบการบริหารจัดการดังกล่าวเข้าใจถึงลำดับความสำคัญของหน่วยงานด้านระบบรางในการจัดการเหตุการณ์ไม่พึงประสงค์ด้านความปลอดภัยของสารสนเทศ

หมายเหตุ: รายละเอียดเพิ่มเติมดูได้ที่ มาตรฐาน ISO 27035

3.12.1 การบริหารจัดการและการปรับปรุงแก้ไขเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Management of information security incidents and improvements)

ควรมีการตรวจสอบให้แน่ใจว่าการบริหารจัดการเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศมีวิธีการจัดการที่สอดคล้องกันและมีประสิทธิภาพ โดยควรนำวิธีการดังต่อไปนี้มาปรับใช้:

1. ช่วงการบริหารจัดการเหตุการณ์ไม่พึงประสงค์ (Incident management phases)

1.1 การสืบหาและการรายงาน (Detection and reporting)

1.1.1 การสืบหาเหตุการณ์ (Event detection)

1.1.2 การรายงานเหตุการณ์ (Event reporting)

1.2 การประเมินและการตัดสินใจ (Assessment and decision)

1.2.1 การประเมินและการตัดสินใจเบื้องต้น (Assessment and initial decision)

1.2.2 การประเมินและการยืนยันเหตุการณ์ (Assessment and incident confirmation)

1.3 การตอบสนอง (Responses)

1.3.1 การตอบสนองในทันที (Immediate responses)

1.3.2 การประเมินระดับการควบคุมเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Assessment of control over information security incidents)

1.3.3 การตอบสนองในภายหลัง (Later responses)

1.3.4 การตอบสนองต่อสถานการณ์วิกฤต (Responses to crisis situations)

1.3.5 การวิเคราะห์หลักฐานการรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information security forensics analysis)

1.3.6 การติดต่อสื่อสาร (Communications)

1.3.7 การยกระดับ (Escalation)

1.3.8 การควบคุมการบันทึกและการเปลี่ยนแปลงของกิจกรรม (Activity logging and change control)

นอกจากนี้ การร่วมมือและการแบ่งปันข้อมูลกับหน่วยงานที่รับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (CERT) เป็นสิ่งที่ควรกระทำเพื่อคงไว้ซึ่งความปลอดภัยทางไซเบอร์อย่างต่อเนื่อง ซึ่งประเด็นนี้สำคัญมากสำหรับการจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการเหตุวิกฤต การตอบสนอง และการพิสูจน์หลักฐาน และยังเป็นสิ่งสำคัญในเรื่องของการแจ้งเตือนถึงสิ่งที่อาจจะเกิดขึ้นได้

3.12.2 ขั้นตอนปฏิบัติและความรับผิดชอบ (Responsibilities and procedures)

ควรกำหนดขั้นตอนปฏิบัติและความรับผิดชอบในการจัดการเพื่อให้มั่นใจว่ามีการตอบสนองต่อเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศอย่างรวดเร็ว มีประสิทธิภาพ

และเป็นระเบียบ ซึ่งพนักงาน ลูกจ้าง และบุคคลภายนอกทุกคนควรรับทราบถึงขั้นตอนปฏิบัติดังกล่าวที่กำหนดไว้

ควรมีการพัฒนาและการสื่อสารภายในหน่วยงานผู้ให้บริการระบบรางตามขั้นตอนต่อไปนี้:

- การวางแผนและเตรียมพร้อมตอบสนองต่อเหตุการณ์ไม่พึงประสงค์
- การเฝ้าระวัง ตรวจจับ วิเคราะห์ และรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ
- การบันทึกกิจกรรมของการบริหารจัดการเหตุการณ์ไม่พึงประสงค์
- การตรวจพิสูจน์หลักฐาน
- การประเมินและการตัดสินใจเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศและการประเมินจุดอ่อนของการรักษาความมั่นคงปลอดภัยของสารสนเทศ
- การตอบสนองรวมถึงการยกระดับ การควบคุมการกู้คืนระบบจากเหตุการณ์ไม่พึงประสงค์ และการสื่อสารระหว่างบุคคลหรือระหว่างหน่วยงานทั้งภายในและภายนอก

ซึ่งขั้นตอนที่กล่าวข้างต้นควรมีการตรวจสอบให้แน่ใจว่า:

- มีบุคลากรที่มีความสามารถในการรับมือกับปัญหาที่เกี่ยวข้องกับเหตุการณ์ไม่พึงประสงค์ด้านความปลอดภัยของสารสนเทศภายในหน่วยงานระบบรางได้
- มีการแต่งตั้งผู้รับผิดชอบสำหรับการตรวจจับและการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย และให้พนักงานทุกคนทำการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศใดๆ แก่ผู้รับผิดชอบอย่างรวดเร็วที่สุด
- มีการเก็บรักษารายชื่อติดต่อเจ้าหน้าที่ กลุ่มผลประโยชน์ที่เป็นหน่วยงานภายนอก หรือกลุ่มที่มีหน้าที่จัดการปัญหาที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศ

3.12.3 การประเมินและตัดสินใจต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

ผู้ติดต่อควรประเมินแต่ละเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศ โดยใช้ข้อตกลงด้านเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศและการจัดแบ่งประเภทของเหตุการณ์ และทำการตัดสินใจว่าเหตุการณ์ดังกล่าวควรถูกจัดเป็นเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศหรือไม่ ซึ่งการจัดประเภทและจัดลำดับความสำคัญของเหตุการณ์ไม่พึงประสงค์สามารถช่วยระบุผลกระทบและขอบเขตของเหตุการณ์ได้

ในกรณีที่องค์กรมีทีมรับมือต่อเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Response Team หรือ ISIRT) การประเมินและการตัดสินใจจะถูกส่งต่อไปยังทีมดังกล่าวเพื่อยืนยันหรือประเมินเหตุการณ์ใหม่

ผลของการประเมินและการตัดสินใจควรถูกบันทึกไว้อย่างละเอียดเพื่อวัตถุประสงค์ในการอ้างอิงและการทวนสอบในอนาคต

3.12.4 การตอบสนองต่อเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Response to information security incidents)

วัตถุประสงค์ คือ เพื่อลดความเสียหายที่เกิดจากเหตุการณ์ไม่พึงประสงค์

การตอบสนองต่อเหตุการณ์หมายถึงกิจกรรมต่างๆ ประกอบด้วย การเตรียมการตอบสนองล่วงหน้า การตั้งนโยบายการตอบสนองจากการวิเคราะห์ และการวางแผนกลยุทธ์ด้านความมั่นคงปลอดภัยร่วมกับทีมเฝ้าระวัง ทีมรับมือ และทีมวิเคราะห์

ควรมีการตอบสนองเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศโดยผู้รับผิดชอบที่ได้รับการแต่งตั้งขึ้นและบุคคลภายในหน่วยงานหรือบุคคลภายนอกที่เกี่ยวข้อง

3.12.4.1 หลักเกณฑ์การตัดสินเหตุการณ์ไม่พึงประสงค์ (Determine incident criteria)

วัตถุประสงค์ คือ เพื่อการตอบสนองและการดำเนินการกับเหตุการณ์ไม่พึงประสงค์อย่างมีประสิทธิภาพ

ควรมีการกำหนดเกณฑ์ในการพิจารณาการจัดการเหตุการณ์ไม่พึงประสงค์ นอกเหนือจากนี้ ควรมีการกำหนดแนวปฏิบัติอ้างอิงสำหรับเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยตามลำดับความสำคัญของข้อมูลและระบบสารสนเทศ ผลกระทบจากการบุกรุกแต่ละประเภท ระดับความเสียหาย ระดับการแจ้งเตือนการบุกรุก และความรุนแรงของเหตุการณ์

โดยทั่วไปเหตุการณ์ไม่พึงประสงค์สามารถจำแนกได้ดังต่อไปนี้โดยขึ้นอยู่กับคุณลักษณะของงาน ขนาดของหน่วยงาน และความสำคัญของข้อมูล:

1. เหตุการณ์ไม่รุนแรง
   - ก. เหตุการณ์ที่เกิดจากซอฟต์แวร์ที่เป็นอันตราย(มัลแวร์) เช่น ไวรัส หนอน ไวรัสทั่วไป ไวรัสbackdoor ไวรัสโทรจัน ฯลฯ
   - ข. การบุกรุกเครือข่ายหรือระบบโดยไม่ได้รับอนุญาต
   - ค. การโจรกกรม การสูญเสีย และการทำลายทรัพย์สินทั่วไป
   - ง. การทำงานที่ผิดปกติของระบบที่เกิดจากช่องโหว่ของระบบการป้องกัน
   - จ.การเข้าถึงโดยไม่ได้รับอนุญาต หรือการอนุญาตให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้
   - ฉ. การพยายามเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
   - ช. การให้บริการที่ผิดปกติที่เกิดจากการดัดแปลงและหรือความเสียหายเนื่องจากการเข้าถึงโดยไม่ได้รับอนุญาต
2. เหตุการณ์รุนแรง

ก. การหยุดบริการโดยการเข้าถึงระบบแบบไม่ได้รับอนุญาต ซึ่งทำให้เกิดการดัดแปลงและหรือทำลายข้อมูลหรือระบบ

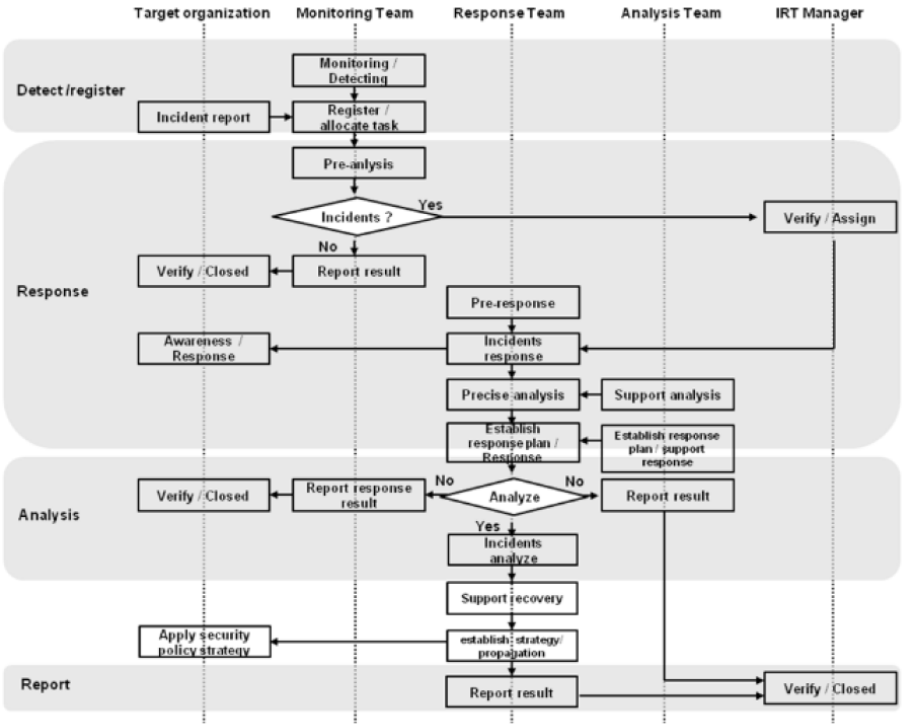
ข. การเปิดเผยข้อมูลที่เป็นความลับหรือการเกิดความเสียหายรุนแรงต่อชื่อเสียงหรือแบรนด์

ค. การเกิดความเสียหายอย่างรุนแรงต่อการดำเนินงานของหน่วยงานที่เกิดจากความตั้งใจและหรือความผิดพลาด

ง. การดัดแปลงและหรือการทำลายอุปกรณ์รักษาความมั่นคงปลอดภัย เช่น ระบบควบคุมการเข้าถึง ระบบตรวจจับการบุกรุก ระบบล็อค กล้องวงจรปิด ฯลฯ

3.12.4.2 การกำหนดกระบวนการรับมือต่อเหตุการณ์ไม่พึงประสงค์ (Define incident response processes)

กระบวนการตอบสนองเหตุการณ์ไม่พึงประสงค์อย่างทันทีจะดำเนินการตามลำดับ ได้แก่ การตรวจจับหรือการบันทึกการพบเหตุการณ์ การตอบสนอง การวิเคราะห์ และการรายงานผล ดังภาพที่แสดกระบวนการด้านล่าง



การตอบสนองควรรวมถึงกระบวนการดังต่อไปนี้

- การรวบรวมหลักฐานโดยเร็วที่สุดหลังจากเหตุการณ์เกิดขึ้น
- ดำเนินการวิเคราะห์พิสูจน์หลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศตามความจำเป็น
- ตรวจสอบให้แน่ใจว่ากิจกรรมที่เกี่ยวข้องกับการตอบสนองทั้งหมดได้ถูกบันทึกอย่างเหมาะสมสำหรับการวิเคราะห์ในภายหลัง

- ควรมีการการสื่อสารการเกิดขึ้นของเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศหรือรายละเอียดที่เกี่ยวข้องใดๆ กับบุคลากรหรือหน่วยงานทั้งภายในและภายนอกที่จำเป็นต้องทราบ
- มีการรับมือกับจุดอ่อนด้านความปลอดภัยของสารสนเทศที่พบว่าเป็นสาเหตุหรือมีส่วนทำให้เกิดเหตุการณ์ไม่พึงประสงค์
- เมื่อจัดการเหตุการณ์สำเร็จแล้ว ให้ปิดและบันทึกเหตุการณ์นั้นอย่างเป็นทางการ

การวิเคราะห์หลังเกิดเหตุการณ์ไม่พึงประสงค์ควรทำตามความจำเป็น เพื่อระบุสาเหตุของเหตุการณ์ดังกล่าว

3.12.5 การรายงานเหตุการณ์และช่องโหว่ด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Reporting information security events and weaknesses)

ควรมีการรายงานเหตุการณ์อย่างเป็นทางการและควรนำขั้นตอนการยกระดับและรายงานผ่านช่องทางการจัดการที่เหมาะสมมาปรับใช้

ตรวจสอบให้มั่นใจว่ามีการสื่อสารถึงเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศและจุดอ่อนที่เกี่ยวข้องกับระบบอาณัติสัญญาณ เพื่อให้สามารถดำเนินการแก้ไขได้อย่างทันท่วงที

พนักงาน ลูกจ้าง และผู้ใช้งานระบบที่เป็นบุคคลภายนอกทุกคนควรรายงานเหตุการณ์และจุดอ่อนด้านความปลอดภัยของข้อมูลที่อาจมีผลกระทบต่อความปลอดภัยของทรัพย์สินของ หน่วยงานไปยังผู้รับผิดชอบที่มีการแต่งตั้งโดยเร็วที่สุดเท่าที่เป็นไปได้ เพื่อป้องกันเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ

กลไกการรายงานควรเข้าใจได้ง่าย เข้าถึงได้ และพร้อมใช้งานมากที่สุด ควรมีแจ้งพนักงานถึงข้อห้ามที่ไม่ควรกระทำหรือการพยายามพิสูจน์จุดอ่อนที่น่าสงสัยในแต่ละสถานการณ์

ควรรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศผ่านช่องทางบริหารจัดการที่เหมาะสม ควรมีการกำหนดขั้นตอนการรายงานอย่างเป็นทางการ พร้อมกับการตอบสนองต่อเหตุการณ์และขั้นตอนการยกระดับการตอบสนอง รวมถึงกำหนดวิธีการดำเนินการเมื่อได้รับรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ

ขั้นตอนการรายงานควรรวมถึง:

- การเตรียมแบบฟอร์มสำหรับการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อช่วยให้ผู้รายงานจดจำการการปฏิบัติที่จำเป็นทั้งหมดในกรณีเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ เช่น
  - การควบคุมความปลอดภัยที่ไม่มีประสิทธิภาพ
  - การละเมิดต่อความถูกต้องสมบูรณ์ของข้อมูลสารสนเทศ การเก็บรักษาความลับ หรือความคาดหวังในการพร้อมใช้งาน
  - ความผิดพลาดของผู้ปฏิบัติงาน
  - การไม่ปฏิบัติตามนโยบายหรือแนวทางปฏิบัติ
  - การละเมิดข้อตกลงด้านความปลอดภัยทางกายภาพ

- การเปลี่ยนแปลงระบบปฏิบัติการหรือชุดคำสั่งที่ควบคุมระบบโดยไม่ได้รับอนุญาต
- การทำงานผิดพลาดของโปรแกรมหรืออุปกรณ์คอมพิวเตอร์
- การเข้าถึงโดยไม่ได้รับอนุญาต

➢ การอ้างอิงถึงกระบวนการทางวินัยที่กำหนดขึ้นอย่างเป็นทางการ เพื่อใช้ในการจัดการกับพนักงานที่ละเมิดความปลอดภัย

➢ ขั้นตอนการตอบกลับที่เหมาะสม เพื่อให้มั่นใจว่าผู้ที่รายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศจะได้รับการแจ้งผลหลังจากที่จัดการกับปัญหาแล้วเสร็จ

การทดสอบจุดอ่อนของระบบอาจถูกตีความว่าเป็นการใช้ระบบในทางที่ผิด ซึ่งอาจทำให้เกิดความเสียหายต่อระบบข้อมูลสารสนเทศหรือการให้บริการ และส่งผลให้เกิดความรับผิดทางกฎหมายสำหรับผู้ที่ทำการทดสอบ

ควรมีกลไกเพื่อให้สามารถตรวจสอบประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหายจากเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศได้

ควรใช้ข้อมูลที่ได้รับจากการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศเพื่อระบุถึงเหตุการณ์ที่เกิดซ้ำหรือมีผลกระทบสูง

3.12.6 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

ต้องบันทึกเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย ข้อมูลที่ได้รับจากการประเมินเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศควรถูกใช้เพื่อระบุถึงเหตุการณ์ที่เกิดซ้ำหรือเหตุการณ์ที่มีผลกระทบสูง

การประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศอาจนำมาบ่งชี้ถึงความจำเป็นในการเตรียมการป้องกันหรือการปรับปรุงเพิ่มเติม เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ที่จะเกิดขึ้นในอนาคต หรืออาจนำมาพิจารณาในการทบทวนนโยบายด้านความมั่นคงปลอดภัย

3.12.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)

หน่วยงานต้องกำหนดขั้นตอนปฏิบัติสำหรับการระบุ การรวบรวม การเก็บรักษาข้อมูลสารสนเทศ ซึ่งสามารถใช้เป็นหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง

ขั้นตอนโดยทั่วไปสำหรับหลักฐานนั้น ควรจัดให้มีการระบุ การรวบรวม การรับหลักฐานและการเก็บรักษาหลักฐานตามแต่ละประเภทของสื่อ อุปกรณ์ และสถานะของอุปกรณ์ เช่น ใช้งานอยู่หรือปิดอยู่

ควรคำนึงถึงหัวข้อต่อไปนี้ในการกำหนดขั้นตอนการเก็บรวบรวมหลักฐาน:

➢ ห่วงโซ่ผู้ครอบครองพยานหลักฐาน (chain of custody)

➢ ความปลอดภัยของพยานหลักฐาน (safety of evidence)

➢ ความปลอดภัยของบุคลากร (safety of personnel)

- บทบาทและความรับผิดชอบของบุคลากรที่เกี่ยวข้อง (roles and responsibilities of personnel involved)
- สมรรถนะของบุคลากร (competency of personnel)
- การเตรียมเอกสารคู่มือ (documentation)
- การบรรยายสรุป (briefing)

ควรต้องมีใบรับรองหรือเอกสารอื่นๆ ที่เกี่ยวข้องในการรับรองคุณสมบัติของบุคลากรและเครื่องมือเพื่อเพิ่มความเชื่อมั่นของหลักฐานที่ถูกเก็บรักษาไว้

การตรวจพิสูจน์หลักฐานใดๆ ควรทำเฉพาะกับสำเนาของหลักฐานเท่านั้น ต้องมีการป้องกันความสมบูรณ์ของวัสดุหลักฐานทุกชิ้น การสำเนาหรือคัดลอกวัสดุหลักฐานควรอยู่ภายใต้การดูแลของบุคลากรที่เชื่อถือได้ และควรบันทึกข้อมูลเกี่ยวกับขั้นตอน เวลา สถานที่ ผู้ดำเนินการ รวมถึงเครื่องมือและโปรแกรมที่ใช้ในการคัดลอกวัสดุหลักฐาน

การตรวจพิสูจน์หลักฐานในบางครั้งอาจอยู่เหนือขอบเขตของหน่วยงานหรืออำนาจศาล ในกรณีเช่นนี้ ควรตรวจสอบให้แน่ใจว่าหน่วยงานให้บริการระบบรางมีสิทธิ์ในการรวบรวมข้อมูลที่จำเป็นเพื่อใช้ในการตรวจพิสูจน์หลักฐาน ควรพิจารณาข้อกำหนดทางกฎหมายที่แตกต่างกันเพื่อเพิ่มโอกาสในการได้รับอนุญาตในขอบเขตอำนาจศาลที่เกี่ยวข้อง

3.13 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

ในบทนี้จะให้ความสนใจเมื่อผู้ให้บริการภายนอกมาจากประเทศใดประเทศหนึ่ง หรือเมื่อมีข้อจำกัดหรือคำเตือนเกี่ยวกับห่วงโซ่อุปทานของการจ้างบุคคลภายนอก(outsourcing)

ตรวจสอบให้แน่ใจว่าผู้ให้บริการภายนอกสามารถเข้าถึงการคุ้มครองทรัพย์สินของหน่วยงานได้ รวมถึงการจัดการความมั่นคงปลอดภัยสำหรับห่วงโซ่อุปทานเป็นปัญหาเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะอย่างยิ่งเกี่ยวกับการพัฒนาฮาร์ดแวร์และซอฟต์แวร์

ข้อมูลเพิ่มเติมสำหรับแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอกดูได้จากมาตรฐาน ISO/IEC 270036

3.13.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

ควรมีการพิจารณาการรักษาความมั่นคงปลอดภัยในขั้นตอนการจ้างบุคคลภายนอก

หน่วยงานผู้ให้บริการระบบรางต้องมีการกำหนดและคงไว้ซึ่งนโยบายเกี่ยวกับขั้นตอนของวงจรการดำเนินการ รูปแบบของวงจรการดำเนินการ และระเบียบการดำเนินการ รวมถึงตรวจสอบให้แน่ใจถึงความพร้อมในการดำเนินการ

หน่วยงานผู้ให้บริการระบบรางควรระบุและจัดตั้งข้อกำหนดพื้นฐานของมาตรการการควบคุมความมั่นคงปลอดภัยสารสนเทศ โดยต้องมีการตกลงกับผู้ให้บริการภายนอกที่จะเข้าถึงข้อมูลของหน่วยงานให้ทำตามนโยบายที่มีการจัดตั้งไว้

3.13.1.1 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)

ความสัมพันธ์ระหว่างหน่วยงานผู้ให้บริการระบบรางกับผู้ให้บริการภายนอกต้องมีการกำหนดและตกลงกันเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าจะไม่เกิดการเข้าใจผิดระหว่างกันในเรื่องของหน้าที่รับผิดชอบของทั้งสองฝ่ายในการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศที่เกี่ยวข้อง ซึ่งข้อตกลงของผู้ให้บริการภายนอกนี้อาจเกี่ยวข้องกับฝ่ายอื่นๆได้เช่นกัน เช่น บริษัทคู่ค้ารายย่อยของผู้ให้บริการภายนอก

เมื่อผู้ให้บริการภายนอกอยู่ในหน่วยงานเดียวกัน แนะนำให้ยังคงใช้กระบวนการจัดทำข้อตกลงแต่ลดความเป็นทางการลง

ข้อกำหนดต่อไปนี้ควรถูกพิจารณารวมไว้ในข้อตกลงเพื่อให้เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ:

- คำอธิบายของข้อมูลสารสนเทศที่จะได้รับและอนุญาตให้เข้าถึง รวมถึงวิธีการจัดหาให้หรือการเข้าถึงข้อมูลสารสนเทศ
- การจัดประเภทของข้อมูลสารสนเทศตามรูปแบบที่หน่วยงานกำหนด หรือในกรณีจำเป็นสามารถจัดประเภทโดยผสมผสานกันระหว่างการแบ่งประเภทของหน่วยงานเองกับการแบ่งประเภทของผู้ให้บริการภายนอก
- ข้อกำหนดทางกฎหมายและการกำกับดูแล ซึ่งรวมถึงการปกป้องข้อมูล สิทธิบัตร และลิขสิทธิ์ และคำอธิบายว่าจะถูกต้องตามข้อกำหนดอย่างไร
- ภาระผูกพันของคู่สัญญาแต่ละฝ่ายในการดำเนินการตามข้อกำหนดที่มีการตกลงกันไว้ รวมถึงมาตรการควบคุมการเข้าถึง การทบทวนด้านประสิทธิภาพ การเฝ้าระวัง การรายงานและการตรวจสอบ
- กฎการใช้งานข้อมูลสารสนเทศที่ยอมรับได้ รวมถึงการใช้งานที่ไม่เป็นที่ยอมรับในกรณีจำเป็น
- รายชื่อบุคลากรของผู้ให้บริการภายนอกที่ได้รับอนุญาตให้เข้าถึงหรือสามารถรับข้อมูลสารสนเทศของหน่วยงานได้ รวมถึงขั้นตอนหรือเงื่อนไขสำหรับการอนุญาตและการถอนการอนุญาตในการเข้าถึงหรือการรับข้อมูลของหน่วยงานโดยบุคลากรของผู้ให้บริการภายนอก
- นโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศที่เกี่ยวข้องกับข้อสัญญา
- ข้อกำหนดและขั้นตอนในการจัดการเหตุการณ์ไม่พึงประสงค์ โดยเฉพาะการแจ้งเตือนและการทำงานร่วมกันในระหว่างการแก้ไขเหตุการณ์ไม่พึงประสงค์
- การฝึกอบรมและการตระหนักถึงข้อกำหนดของกระบวนการและข้อกำหนดเฉพาะในด้านความมั่นคงปลอดภัยของสารสนเทศ เช่น ข้อกำหนดสำหรับการตอบสนองต่อเหตุการณ์ไม่พึงประสงค์ ขั้นตอนการอนุญาต
- กฎระเบียบที่เกี่ยวข้องกับผู้รับเหมาช่วง รวมถึงมาตรการต่างๆ ที่จำเป็นต้องนำไปปฏิบัติตาม
- ข้อตกลงที่เกี่ยวข้องกับคู่ค้า รวมถึงผู้รับผิดชอบเมื่อเกิดปัญหาด้านความปลอดภัยของข้อมูล

- ข้อกำหนดในการคัดกรองสำหรับบุคลากรของผู้ให้บริการภายนอก รวมถึงความรับผิดชอบในการดำเนินการตามขั้นตอนการคัดกรองและการแจ้งเตือนหากการคัดกรองยังไม่สมบูรณ์ หรือหากผลลัพธ์ที่ได้มามีข้อสงสัยหรือข้อกังวล
- สิทธิในการตรวจสอบและควบคุมกระบวนการของผู้ให้บริการภายนอกที่เกี่ยวข้องกับข้อตกลง
- กระบวนการแก้ไขข้อบกพร่องและข้อขัดแย้ง
- หน้าที่ของผู้ให้บริการภายนอกในการส่งมอบรายงานที่เกี่ยวข้องกับประสิทธิผลของการควบคุมและข้อตกลงในการแก้ไขปัญหาตามเวลาที่ระบุในรายงานอย่างทันท่วงที
- หน้าที่ของผู้ให้บริการภายนอกในการปฏิบัติตามข้อกำหนดด้านความปลอดภัยขององค์กร

ข้อตกลงอาจแตกต่างกันไปสำหรับการนำไปปรับใช้ในองค์กรและผู้ให้บริการภายนอกที่แตกต่างกัน ดังนั้นควรพิจารณาถึงความเสี่ยงและข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศที่เกี่ยวข้องทั้งหมด

ในข้อตกลงต้องมีการพิจารณาถึงกระบวนการในการดำเนินงานอย่างต่อเนื่องในกรณีที่ผู้ให้บริการภายนอกไม่สามารถจัดหาผลิตภัณฑ์หรือบริการของตนได้ เพื่อหลีกเลี่ยงความล่าช้าในการจัดหาผลิตภัณฑ์หรือบริการทดแทน

3.13.1.2 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

ควรมีการจัดตั้งนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อกำหนดข้อกำหนดด้านความสัมพันธ์กับผู้ให้บริการภายนอกในการนำไปปรับใช้

ผู้ให้บริการภายนอกควรปฏิบัติตามกระบวนการและขั้นตอนที่ผู้ให้บริการระบบรางกำหนด ซึ่งรวมถึง:

- การระบุและจัดทำเอกสารแบ่งประเภทของผู้ให้บริการภายนอก เช่น การให้บริการด้านเทคโนโลยีสารสนเทศ การขนส่ง การให้บริการทางการเงิน และบุคลากรที่หน่วยงานจะอนุญาตให้เข้าถึงข้อมูลสารสนเทศได้
- กระบวนการและวงจรชีวิตที่เป็นมาตรฐานสำหรับการจัดการความสัมพันธ์กับผู้ให้บริการภายนอก
- การระบุประเภทของข้อมูลสารสนเทศที่ผู้ให้บริการภายนอกแต่ละประเภทจะสามารถเข้าถึงได้ รวมถึงการเฝ้าระวังและควบคุมการเข้าถึงนั้นๆ
- ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยของสารสนเทศสำหรับข้อมูลสารสนเทศและการเข้าถึงแต่ละประเภท เพื่อใช้เป็นพื้นฐานสำหรับข้อตกลงกับผู้ให้บริการภายนอกแต่ละรายบนพื้นฐานของความต้องการและข้อกำหนดทางธุรกิจ รวมถึงความเสี่ยงต่อหน่วยงาน

- กระบวนการและขั้นตอนการตรวจติดตาม เพื่อจัดทำข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศสำหรับผู้ให้บริการภายนอกและการเข้าถึงแต่ละประเภท รวมถึงการทบทวนโดยบุคคลที่สาม และการตรวจสอบการใช้งานของผลิตภัณฑ์
- การควบคุมความถูกต้องและความสมบูรณ์เพื่อให้แน่ใจว่าข้อมูลสารสนเทศหรือการประมวลผลข้อมูลที่ได้รับจากฝ่ายใดฝ่ายหนึ่งมีความสมบูรณ์
- ประเภทของภาระผูกพันที่ใช้กับผู้ให้บริการภายนอกเพื่อปกป้องข้อมูลสารสนเทศของหน่วยงาน
- การรับมือกุเหตุการณ์ไม่พึงประสงค์และเหตุฉุกเฉินที่เกี่ยวข้องกับการเข้าถึงผู้ให้บริการภายนอก รวมถึงความรับผิดชอบของทั้งหน่วยงานและผู้ให้บริการภายนอก
- การเตรียมตัวและการตอบสนองในกรณีที่เกิดเหตุฉุกเฉินหรือกู้คืนระบบ เพื่อให้มั่นใจในความพร้อมใช้งานของข้อมูลสารสนเทศหรือการประมวลผลข้อมูลที่จัดหาให้โดยฝ่ายใดฝ่ายหนึ่ง
- การฝึกอบรมเพื่อสร้างความตระหนักรู้ถึงนโยบาย กระบวนการและขั้นตอนปฏิบัติที่เกี่ยวข้องแก่บุคลากรของหน่วยงาน
- การฝึกอบรมเพื่อสร้างความตระหนักรู้สำหรับบุคลากรขององค์กรที่มีปฏิสัมพันธ์กับบุคลากรของผู้ให้บริการภายนอกเกี่ยวกับกฎเกณฑ์ของการมีส่วนร่วมและพฤติกรรมตามประเภทของผู้ให้บริการภายนอก และระดับของการเข้าถึงระบบและสารสนเทศของผู้ให้บริการภายนอก
- มีการบันทึกเงื่อนไขภายใต้ข้อกำหนดและมาตรการควบคุมความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษรไว้ในข้อตกลงที่ลงนามโดยทั้งสองฝ่าย
- การจัดการการถ่ายโอนที่จำเป็นของข้อมูล อุปกรณ์ประมวลผลข้อมูลและอุปกรณ์อื่นๆ ที่จำเป็นต้องมีการเคลื่อนย้าย เพื่อมั่นใจว่ามีความมั่นคงปลอดภัยของสารสนเทศตลอดช่วงการถ่ายโอน

3.13.1.3 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

การจัดการความมั่นคงปลอดภัยของสารสนเทศของแต่ละองค์กรนั้น ไม่เพียงพอต่อการรักษาความปลอดภัยของสารสนเทศสำหรับผลิตภัณฑ์และการให้บริการด้านระบบสื่อสารและระบบอาณัติสัญญาณตลอดทั้งห่วงโซ่การให้บริการได้

หัวข้อต่อไปนี้ควรถูกพิจารณารวมอยู่ในข้อตกลงของผู้ให้บริการภายนอกในเรื่องความมั่นคงปลอดภัยของห่วงโซ่การให้บริการ:

- การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศเพื่อนำไปใช้กับผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร หรือใช้กับการจัดหาบริการที่นอกเหนือจากข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศโดยทั่วไปสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก

- การกำหนดให้ผู้ให้บริการภายนอกเผยแพร่ข้อกำหนดด้านความมั่นคงปลอดภัยของหน่วยงานตลอดห่วงโซ่การให้บริการ ในกรณีที่เป็นผู้รับช่วงต่อจากผู้ให้บริการภายนอกเป็นผู้ให้บริการเทคโนโลยีสารสนเทศและการสื่อสารแก่หน่วยงาน
- การกำหนดให้ผู้ให้บริการภายนอกเผยแพร่ข้อกำหนดด้านความมั่นคงปลอดภัยของหน่วยงานตลอดห่วงโซ่การให้บริการ ในกรณีที่ผลิตภัณฑ์เหล่านี้มีส่วนประกอบที่ซื้อจากผู้ให้บริการภายนอกรายอื่น
- การนำกระบวนการตรวจติดตามไปใช้และวิธีการที่ยอมรับได้สำหรับการตรวจสอบว่าผลิตภัณฑ์และบริการด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ถูกส่งมอบนั้นเป็นไปตามข้อกำหนดด้านความปลอดภัยที่มีการระบุไว้
- การใช้กระบวนการเพื่อระบุส่วนประกอบของผลิตภัณฑ์หรือการบริการที่มีความสำคัญต่อการรักษาฟังก์ชันการทำงาน และต้องมีการตรวจสอบที่เข้มงวดขึ้นเมื่อผลิตภัณฑ์หรือการบริการนั้นๆ ถูกผลิตหรือสร้างขึ้นภายนอกองค์กร โดยเฉพาะในกรณีที่ผู้ให้บริการภายนอกชั้นนำจ้างบริษัทอื่นให้ผลิตส่วนประกอบของผลิตภัณฑ์หรือการบริการ
- มีการรับรองว่าสามารถตรวจสอบแหล่งที่มาของส่วนประกอบที่สำคัญได้ตลอดห่วงโซ่การให้บริการ
- มีการรับรองว่าผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสารที่ส่งมอบนั้นสามารถทำงานตามที่คาดไว้โดยไม่มีข้อผิดพลาดทางเทคนิค
- มีการกำหนดกฎสำหรับการแบ่งปันข้อมูลเกี่ยวกับห่วงโซ่การให้บริการและปัญหาที่อาจเกิดขึ้น รวมถึงการประนีประนอมระหว่างหน่วยงานและผู้ให้บริการภายนอก

มีการนำกระบวนการเฉพาะเจาะจงไปใช้ในการจัดการวงจรการดำเนินงานและความพร้อมใช้งานของชิ้นส่วนอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารและความเสี่ยงด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง ซึ่งรวมถึงการจัดการความเสี่ยงของชิ้นส่วนที่ไม่สามารถใช้งานได้เนื่องจากผู้ให้บริการภายนอกปิดกิจการ หรือไม่สามารถจัดหาชิ้นส่วนได้อีกต่อไปเนื่องจากชิ้นส่วนนั้นตกรุ่นไปแล้ว

3.13.2 การบริหารจัดการการให้บริการของผู้ให้บริการภายนอก (Supplier service delivery management)

ควรมีการตรวจติดตาม ทบทวน และตรวจสอบบริการ รายงาน และบันทึกที่จัดหาโดยหน่วยงานภายนอกอย่างเป็นประจำ นอกจากนี้หน่วยงานควรตรวจสอบให้แน่ใจว่าหน่วยงานภายนอกมอบหมายผู้รับผิดชอบในการตรวจสอบการปฏิบัติตามและการบังคับใช้ข้อกำหนดที่มีการตกลงไว้

3.13.2.1 การติดตามและการทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier series)

ควรมีการตรวจสอบ ติดตาม และทบทวนบริการของผู้ให้บริการภายนอกเพื่อให้มั่นใจว่ามีการปฏิบัติตามข้อตกลงและเงื่อนไขในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงมี

การจัดการเหตุการณ์ไม่พึงประสงค์และปัญหาด้านความมั่นคงปลอดภัยของสารสนเทศได้อย่างเหมาะสม ซึ่งควรเกี่ยวข้องกับความสัมพันธ์และกระบวนการจัดการบริการระหว่างหน่วยงานและผู้ให้บริการภายนอกเพื่อ:

- ติดตามระดับประสิทธิภาพในการบริการเพื่อตรวจสอบการปฏิบัติตามข้อตกลง
- ตรวจสอบรายงานการให้บริการจากหน่วยงานภายนอก และมีการประชุมเพื่อติดตามความคืบหน้าเป็นประจำตามที่มีการกำหนดในข้อตกลง
- ให้ข้อมูลเกี่ยวกับเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ และให้ผู้ให้บริการภายนอกและหน่วยงานทำการทบทวนข้อมูลดังกล่าวที่กำหนดไว้ในข้อตกลงหรือกระบวนการสนับสนุนใดๆ
- ทบทวนรายงานและบันทึกการตรวจประเมินเหตุการณ์ด้านความมั่นคงปลอดภัย ปัญหาในการดำเนินงาน ความล้มเหลว การติดตามข้อผิดพลาดและการหยุดชะงักของการให้บริการโดยผู้ให้บริการภายนอก
- แก้ไขและจัดการปัญหาต่างๆ ที่พบ
- ทบทวนมุมมองในเรื่องของความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ให้บริการภายนอกกับผู้ให้บริการรายย่อย
- ตรวจสอบว่าผู้ให้บริการภายนอกสามารถรักษาความสามารถในการให้บริการที่เพียงพอพร้อมกับการออกแบบแผนการดำเนินงาน เพื่อให้แน่ใจว่าสามารถรักษาระดับความต่อเนื่องในการบริการที่ตกลงไว้ได้ หากเกิดความล้มเหลวในการบริการหรือเกิดภัยอันตรายครั้งใหญ่
- มอบหมายให้มีบุคลากรหรือทีมการจัดการบริการในการรับผิดชอบการจัดการความสัมพันธ์กับหน่วยงานผู้ให้บริการภายนอก โดยควรมีทักษะทางเทคนิคและทรัพยากรข้อมูลที่เพียงพอสำหรับการตรวจติดตามให้เป็นไปตามข้อกำหนดของข้อตกลง (ดูเพิ่มเติมได้ที่หัวข้อ 3.13.1.2 นโยบายความมั่นคงปลอดภัยของสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก) โดยเฉพาะข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และควรดำเนินการแก้ไขอย่างเหมาะสมเมื่อพบข้อบกพร่องในการให้บริการ
- หน่วยงานควรมีมาตรการควบคุมโดยภาพรวมและควบคุมการมองเห็นที่เพียงพอสำหรับการรักษาความมั่นคงปลอดภัยทุกด้านสำหรับข้อมูลที่มีความอ่อนไหวหรือมีความสำคัญ หรือสิ่งอุปกรณ์ประมวลผลข้อมูลที่มีการเข้าถึง ประมวลผล หรือจัดการโดยผู้ให้บริการภายนอก

องค์กรควรจัดให้มีการควบคุมการมองเห็นกิจกรรมด้านความปลอดภัยต่างๆ เช่น การจัดการการเปลี่ยนแปลง การระบุช่องโหว่ และการรายงานเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศ และการตอบสนองผ่านกระบวนการรายงานที่มีการกำหนดไว้

3.13.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)

การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอก รวมถึงการรักษาและปรับปรุงนโยบาย ขั้นตอนปฏิบัติ และมาตรการควบคุมการรักษาความมั่นคงปลอดภัยสารสนเทศที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยคำนึงถึงความสำคัญของระบบธุรกิจและกระบวนการที่เกี่ยวข้อง รวมถึงการประเมินความเสี่ยงที่เกิดใหม่

ควรพิจารณาประเด็นต่อไปนี้ในการบริหารจัดการการเปลี่ยนแปลงของผู้ให้บริการภายนอก:

- การเปลี่ยนแปลงข้อตกลงกับผู้ให้บริการภายนอก
- การเปลี่ยนแปลงที่หน่วยงานนำไปประยุกต์ใช้กับ
  - การปรับปรุงบริการปัจจุบัน
  - การพัฒนาระบบและโปรแกรมใหม่
  - การปรับเปลี่ยนหรือปรับปรุงนโยบายและกระบวนการขอหน่วยงาน
  - การเปลี่ยนแปลงหรือสร้างมาตรการควบคุมใหม่เพื่อแก้ไขเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยของสารสนเทศและเพื่อปรับปรุงความมั่นคงปลอดภัย
- การเปลี่ยนแปลงการให้บริการของผู้ให้บริการภายนอกเพื่อนำไปประยุกต์ใช้กับ:
  - การเปลี่ยนแปลงและการปรับปรุงระบบเครือข่าย
  - การใช้เทคโนโลยีใหม่
  - การนำผลิตภัณฑ์ใหม่หรือเวอร์ชันล่าสุดมาปรับใช้
  - เครื่องมือและสภาพแวดล้อมที่ใช้ในการพัฒนารูปแบบใหม่
  - การเปลี่ยนแปลงตำแหน่งของอุปกรณ์
  - การเปลี่ยนผู้ให้บริการภายนอก
  - การเปลี่ยนผู้รับเหมาช่วง

3.14 การบริหารจัดการความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Aspects of Business Continuity Management)

3.14.1 ความต่อเนื่องของการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

วัตถุประสงค์ คือ เพื่อหลีกเลี่ยงการหยุดชะงักของระบบอาณัติสัญญาณและการสื่อสาร และเพื่อปกป้องกระบวนการทำงานที่สำคัญจากผลกระทบของความล้มเหลวที่เกิดในระบบข้อมูลสารสนเทศหรือภัยอันตราย และเพื่อให้แน่ใจว่าระบบจะเริ่มกลับมาทำงานได้ใหม่ในเวลาที่เหมาะสม

ควรใช้กระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจเพื่อลดผลกระทบต่อระบบรางอัตโนมัติและการควบคุมทางไกลให้น้อยที่สุด และเพื่อกู้คืนระบบจากการสูญเสียของทรัพย์สินสารสนเทศ ซึ่งอาจเป็นผลจากการเกิดภัยธรรมชาติ อุบัติเหตุ อุปกรณ์ขัดข้อง และการกระทำโดยเจตนา

เพื่อให้ยังสามารถให้บริการในระดับที่ยอมรับได้ ผ่านมาตรการควบคุมทั้งการป้องกันและการกู้คืนระบบ ซึ่งกระบวนการนี้ควรมีการจำแนกกระบวนการที่สำคัญ และมีการบูรณาการข้อกำหนดการจัดการความมั่นคงปลอดภัยสารสนเทศของความต่อเนื่องทางธุรกิจร่วมกับข้อกำหนดด้านความต่อเนื่องอื่นๆ ที่เกี่ยวข้อง เช่น การดำเนินงาน บุคลากร วัสดุ การขนส่ง และอุปกรณ์สนับสนุนต่างๆ

ควรมีการศึกษาวิเคราะห์ผลกระทบของภัยอันตราย ความล้มเหลวของระบบป้องกันการสูญเสียการให้บริการ และความพร้อมในการให้บริการที่มีต่อการดำเนินธุรกิจ และมีการพัฒนาแผนความต่อเนื่องทางธุรกิจและนำไปปรับใช้เพื่อให้มั่นใจสามารถกู้คืนระบบที่สำคัญได้อย่างทันท่วงที

ความมั่นคงปลอดภัยสารสนเทศควรเป็นส่วนสำคัญของกระบวนการความต่อเนื่องทางธุรกิจโดยรวม และกระบวนการจัดการอื่นๆ ภายในองค์กร

ควรมีมาตรการควบคุมการบริหารจัดการความต่อเนื่องทางธุรกิจเพื่อระบุและลดความเสี่ยงที่นอกเหนือจากกระบวนการประเมินความเสี่ยงทั่วไป เพื่อจำกัดกระทบที่เกิดขึ้นจากเหตุการณ์ไม่พึงประสงค์ที่สร้างความเสียหาย และตรวจสอบให้แน่ใจว่าข้อมูลที่จำเป็นในการดำเนินธุรกิจนั้นพร้อมใช้งาน

3.14.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

แผนความต่อเนื่องทางธุรกิจควรรักษาไว้เพื่อให้แน่ใจว่าแผนทั้งหมดมีความสอดคล้องกันและให้การดำเนินการเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงเพื่อระบุลำดับความสำคัญในการทดสอบและการบำรุงรักษา

ควรมีการกำหนดข้อกำหนดด้านความมมั่นคงปลอดภัยสารสนเทศเมื่อมีการวางแผนสำหรับความต่อเนื่องทางธุรกิจและการกู้คืนระบบหลังเกิดความเสียหาย

องค์กรควรตัดสินใจว่าความต่อเนื่องของการรักษาความมั่นคงปลอดภัยสารสนเทศควรถูกนำมาใช้ในกระบวนการจัดการความต่อเนื่องทางธุรกิจหรือในกระบวนการจัดการการกู้คืนระบบจากความเสียหาย

แต่ละแผนนั้นควรระบุผู้รับผิดชอบให้ชัดเจน ขั้นตอนฉุกเฉิน แผนรอบรับสำรอง และแผนการเริ่มต้นระบบใหม่ควรอยู่ภายใต้ความรับผิดชอบของผู้รับผิดชอบทรัพยากรทางธุรกิจหรือกระบวนการที่เกี่ยวข้อง

การจัดเตรียมแผนสำรองสำหรับบริการทางเลือกในเชิงเทคนิค เช่น การประมวลผลข้อมูลและอุปกรณ์ในการสื่อสาร โดยทั่วไป ควรเป็นความรับผิดชอบของผู้ให้บริการ

ในกรณีที่ไม่มีแผนความต่อเนื่องทางธุรกิจและแผนการกู้คืนระบบจากความเสียหายอย่างเป็นทางการ ผู้การจัดการความมั่นคงปลอดภัยสารสนเทศควรถือว่าข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศยังคงเดิมในสถานการณ์ที่ไม่พึงประสงค์ เมื่อเทียบกับสภาวะการดำเนินงานปกติ

การวางแผนความต่อเนื่องทางธุรกิจควรพิจารณาถึงประเด็นด้านความมั่นคงปลอดภัยสารสนเทศดังต่อไปนี้:

- เงื่อนไขสำหรับการใช้งานแผนต่างๆ ที่มีการอธิบายกระบวนการที่ต้องปฏิบัติตาม (เช่น ประเมินสถานการณ์อย่างไร ใครมีส่วนร่วมบ้าง) ก่อนแต่ละแผนจะมีการใช้งาน

- กระบวนการฉุกเฉินที่มีการอธิบายการปฏิบัติหลังเกิดเหตุการณ์ไม่พึงประสงค์ซึ่งเป็นอันตรายต่อการดำเนินธุรกิจ
- กระบวนการสำรองที่มีการอธิบายถึงการปฏิบัติเพื่อย้ายกิจกรรมสำคัญทางธุรกิจหรือบริการสนับสนุนไปยังสถานที่อื่นชั่วคราว และเพื่อนำกระบวนการทางธุรกิจกลับเข้าสู่การดำเนินงานในช่วงเวลาที่กำหนด
- ขั้นตอนการปฏิบัติงานชั่วคราวเพื่อติดตามการกู้คืนและการฟื้นฟูระบบที่กำลังรอดำเนินการให้เสร็จสมบูรณ์
- ขั้นตอนการเริ่มต้นระบบใหม่ที่มีการอธิบายการปฏิบัติเพื่อกลับไปสู่การดำเนินธุรกิจได้ตามปกติ
- กำหนดการบำรุงรักษาซึ่งมีการระบุว่าจะทำการทดสอบแผนอย่างไรและเมื่อใด รวมถึงกระบวนการในการเก็บรักษาแผน
- กิจกรรมเพิ่มความตระหนักรู้ ให้ความรู้ และฝึกอบรมซึ่งออกแบบมาเพื่อสร้างความเข้าใจในกระบวนการความต่อเนื่องทางธุรกิจ และเพื่อให้มั่นใจว่ากระบวนการจะดำเนินต่อไปได้มีประสิทธิภาพ
- ความรับผิดชอบของแต่ละบุคคล โดยมีการอธิบายว่าใครเป็นผู้รับผิดชอบการดำเนินการส่วนใดของแผนงาน ซึ่งสามารถเพิ่มรายชื่อบุคคลสำรองได้ตามความจำเป็น
- ทรัพย์สินและทรัพยากรที่สำคัญที่จำเป็นต้องนำมาใช้ในกระบวนการฉุกเฉิน แผนสำรอง และการเริ่มต้นระบบใหม่

3.14.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)

ควรมีการพัฒนาแผนและนำไปปรับใช้ เพื่อรักษาหรือกู้คืนการดำเนินการ และรับรองความพร้อมใช้งานของข้อมูลสารสนเทศในระดับที่จำเป็นและตามช่วงเวลาที่กำหนดหลังเกิดการหยุดชะงักหรือความล้มเหลวของกระบวนการทางธุรกิจที่สำคัญ

กระบวนการวางแผนความต่อเนื่องทางธุรกิจควรพิจารณาถึงหัวข้อต่อไปนี้:

- ข้อกำหนดและข้อตกลงของความรับผิดชอบทั้งหมด และขั้นตอนในการดำเนินธุรกิจอย่างต่อเนื่อง
- การระบุระดับการสูญเสียข้อมูลและบริการที่ยอมรับได้
- การดำเนินการตามขั้นตอนเพื่อให้สามารถกู้คืนและฟื้นฟูการดำเนินธุรกิจและความพร้อมของข้อมูลได้ในระยะเวลาที่กำหนด โดยเฉพาะการประเมินการพึ่งพาธุรกิจอื่นทั้งภายในและภายนอกหน่วยงาน รวมถึงสัญญาที่มีอยู่
- ขั้นตอนการปฏิบัติงานเพื่อติดตามการกู้คืนและการฟื้นฟูระบบที่รอดำเนินการ
- ขั้นตอนและกระบวนการที่ตกลงกันแบบเป็นลายลักษณ์อักษร
- การให้ความรู้เกี่ยวกับขั้นตอนและกระบวนการที่ผ่านการตกลงกันรวมถึงการจัดการในสภาวะวิกฤตที่เหมาะสมแก่พนักงาน

- การทดสอบและการปรับปรุงแผน

3.14.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องของความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

แผนความต่อเนื่องทางธุรกิจควรได้รับการทดสอบและปรับปรุงอย่างเป็นประจำ เพื่อให้แน่ใจว่าแผนมีความทันสมัยและมีประสิทธิภาพ

การทดสอบแผนความต่อเนื่องทางธุรกิจควรพิสูจน์ว่าสมาชิกทุกคนของทีมกู้คืนระบบและพนักงานที่เกี่ยวข้องตระหนักถึงแผนและความรับผิดชอบของตนเองในด้านความต่อเนื่องทางธุรกิจและความมั่นคงปลอดภัยของสารสนเทศ รวมถึงต้องรู้บทบาทของตนเองเมื่อมีการนำแผนมาปรับใช้

การกำหนดการทดสอบแผนความต่อเนื่องทางธุรกิจควรระบุว่า ควรทดสอบองค์ประกอบแต่ละส่วนของแผนอย่างไรและเมื่อใด รวมถึงแต่ละองค์ประกอบของแผนควรได้รับการทดสอบเป็นประจำ

ควรใช้วิธีการที่หลากหลายเพื่อให้เกิดความมั่นใจว่าแผนสามารถใช้งานได้จริง โดยควรรวมถึงประเด็นต่อไปนี้:

- มีการประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยงานที่เกี่ยวข้องในสถานการณ์ต่างๆ เช่น แลกเปลี่ยนความคิดเห็นเรื่องการจัดเตรียมการฟื้นฟูธุรกิจโดยจำลองสถานการณ์ขึ้นมา
- การจำลองสถานการณ์ โดยเฉพาะเพื่อฝึกอบรมบุคลากรในเรื่องการปฏิบัติตัวหลังเกิดเหตุการณ์ไม่พึงประสงค์หรือเกิดภัยวิกฤต
- การทดสอบการกู้คืนระบบเชิงเทคนิค เพื่อให้แน่ใจว่าระบบสารสนเทศสามารถกู้คืนได้อย่างมีประสิทธิภาพ
- การทดสอบการกู้คืนระบบที่สถานที่ดำเนินงานสำรอง โดยดำเนินการตามกระบวนการทางธุรกิจควบคู่ไปกับการดำเนินการกู้คืนระบบจากสถานที่ดำเนินงานหลัก
- การทดสอบอุปกรณ์และบริการของผู้ให้บริการภายนอก เพื่อให้แน่ใจว่าบริการและผลิตภัณฑ์ที่จัดหามาจะเป็นไปตามข้อตกลงสัญญา)
- มีการทดสอบแบบครบวงจร (การทดสอบว่าหน่วยงาน บุคลากร อุปกรณ์ สถานที่ และกระบวนการต่างๆ สามารถรับมือกับการหยุดชะงักของระบบได้)

เทคนิคเหล่านี้สามารถใช้ได้กับทุกหน่วยงาน โดยควรนำไปปรับใช้กับส่วนที่เกี่ยวข้องกับแผนการกู้คืนระบบเฉพาะ รวมถึงควรมีการบันทึกผลการทดสอบและการดำเนินการเพื่อปรับปรุงแผนหากจำเป็น

3.14.2 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

เนื่องจากเครือข่ายของระบบอาณัติสัญญาณนั้นจำเป็นต้องมีความมั่นคงปลอดภัย ระบบจึงต้องมีความคงทนและมีเสถียรภาพ ดังนั้นจึงมีต้องมีการรองรับระบบสำรองของอุปกรณ์และเครือข่าย

ยิ่งเครือข่ายสำรองมีความแตกต่างกันมากเท่าไร ยิ่งมีความเป็นไปได้ที่ระบบจะไม่เชื่อมต่อกันมากเท่านั้น ดังนั้นจึงทำให้ความยืดหยุ่นของระบบยิ่งสูงขึ้น โดยเกิดจากการรวมกันของเครือข่ายแบบคงที่(fixed networks) เครือข่ายวิทยุ(radio networks) และสายกระจายสัญญาณ(radiating cables) เช่นเดียวกับของ ยูโรลูป(Euroloop)

การใช้ระบบเครือข่ายไร้สายสำรองควรเป็นทางเลือกในการนำมาปรับใช้งานเมื่อเครือข่ายไร้สายหลักไม่พร้อมใช้งานเท่านั้น

ข้อเสนอนี้สามารถใช้เทคโนโลยีวิทยุกำหนดด้วยซอฟต์แวร์(Software Defined Radio) เพื่อตรวจสอบย่านความถี่อิสระที่สามารถใช้ได้ และกำหนดค่าโปรโตคอลเครือข่ายอัตโนมัติ ซึ่งวิธีนี้ผู้บุกรุกจะไม่มีทางรู้ได้ชัดว่าเครือข่ายสำรองจะใช้ความถี่ใด ทำให้ไม่สามารถโจมตีเครือข่ายสำรองได้ และวิธีนี้ยังช่วยเพิ่มความมั่นคงปลอดภัยของเครือข่ายด้วยเช่นกัน

การแก้ไขปัญหาบนระบบสำรองเพื่อความมั่นคงปลอดภัยอาจไม่มีประโยชน์สำหรับการรักษาความปลอดภัย หากระบบไม่มีการพัฒนาระบบสำรองให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัย

3.15 ความสอดคล้อง (Compliance)

ควรมีการกำหนดการปฏิบัติตามข้อกำหนดทางกฎหมาย ข้อบังคับ และสัญญาที่เกี่ยวข้องทั้งหมดและแนวทางของหน่วยงานในการปฏิบัติอย่างสอดคล้องกับข้อกำหนดดังกล่าวไว้อย่างชัดเจน โดยจัดทำเป็นลายลักษณ์อักษร และปรับปรุงแต่ละระบบสารสนเทศและองค์กรให้ทันสมัยอยู่เสมอ

3.15.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

วัตถุประสงค์ คือ เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันทางกฎหมาย ระเบียบข้อบังคับหรือสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดด้านความปลอดภัยใดๆ

3.15.1.1 การระบุกฎหมายที่บังคับใช้และข้อกำหนดในสัญญา (Identification of applicable legislation and constractual requirements)

ควรมีการกำหนดมาตรการควบคุมเฉพาะและความรับผิดชอบส่วนบุคคลเพื่อให้เป็นไปตามข้อกำหนดเหล่านี้และจัดทำเป็นลายลักษณ์อักษร

ระเบียบข้อบังคับทั้งหมดที่มีผลบังคับใช้กับผู้ให้บริการระบบรางควรถูกระบุโดยผู้จัดการเพื่อให้เป็นไปตามข้อกำหนดที่จำเป็นสำหรับระบบอาณัติสัญญาณและการสื่อสาร หากมีการดำเนินธุรกิจในประเทศอื่น ผู้จัดการควรพิจารณาถึงความสอดคล้องกับระเบียบบังคับทั้งหมดในประเทศที่เกี่ยวข้อง

3.15.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

ควรดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้มั่นใจว่ามีความสอดคล้องกับข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญาที่เว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์

ควรพิจารณาแนวทางต่อไปนี้เพื่อป้องกันผลิตภัณฑ์ใดๆ ที่ถือเป็นทรัพย์สินทางปัญญา:

- การเผยแพร่สิทธิในทรัพย์สินทางปัญญาที่สอดคล้องกับนโยบายที่ระบุถึงการใช้ผลิตภัณฑ์สารสนเทศและซอฟต์แวร์อย่างถูกกฎหมาย
- การจัดหาซอฟต์แวร์ผ่านแหล่งที่น่าเชื่อถือและมีชื่อเสียงเท่านั้น เพื่อให้แน่ใจว่าไม่มีการละเมิดลิขสิทธิ์
- การรักษาความตระหนักรู้ถึงนโยบายเพื่อป้องกันการละเมิดลิขสิทธิ์และแจ้งให้ทราบถึงการดำเนินการทางวินัยกับบุคลากรที่ทำการละเมิด
- การรักษาทะเบียนทรัพย์สินและการระบุทรัพย์สินทั้งหมดที่มีข้อกำหนดในการปกป้องสิทธิในทรัพย์สินทางปัญญาอย่างเหมาะสม
- การรักษาข้อพิสูจน์และหลักฐานถึงการเป็นเจ้าของใบอนุญาต มาสเตอร์ดิสก์ คู่มือ ฯลฯ
- มีมาตรการควบคุมจำนวนผู้ใช้ให้ไม่เกินที่ระบุในใบอนุญาต
- ดำเนินการตรวจสอบว่ามีการติดตั้งเฉพาะซอฟต์แวร์และผลิตภัณฑ์ที่ได้รับอนุญาตแล้วเท่านั้น
- จัดทำนโยบายสำหรับการรักษาเงื่อนไขของใบอนุญาตอย่างเหมาะสม
- มีนโยบายสำหรับการกำจัดหรือถ่ายโอนซอฟต์แวร์ไปยังผู้อื่น
- ปฏิบัติตามข้อกำหนดและเงื่อนไขของซอฟต์แวร์และข้อมูลสารสนเทศที่ได้รับจากเครือข่ายสาธารณะ
- ไม่ทำซ้ำ ดัดแปลง หรือแยกข้อมูลสารสนเทศออกจากสื่อต้นฉบับ(เช่น ภาพยนตร์ หรือ แผ่นบันทึกเสียง) นอกเหนือจากที่กฎหมายลิขสิทธิ์อนุญาต
- ห้ามคัดลอกทรัพย์สินทางปัญญาประเภท หนังสือ บทความ รายงาน หรือเอกสารอื่นๆ โดยวิธีการคัดลอกทั้งหมดหรือแค่บางส่วนที่นอกเหนือไปจากที่กฎหมายลิขสิทธิ์อนุญาต

สิทธิในทรัพย์สินทางปัญญานั้น รวมไปถึงซอฟต์แวร์หรือลิขสิทธิ์เอกสาร ลิขสิทธิ์การออกแบบ เครื่องหมายการค้า สิทธิบัตร และใบอนุญาตซอร์สโค้ด ด้วยเช่นกัน

3.15.1.3 การป้องกันข้อมูล (Protection of records)

ควรมีการปกป้องบันทึกข้อมูลที่สำคัญขององค์กร/หน่วยงานจากการสูญหาย การทำลาย และการปลอมแปลงโดยสอดคล้องกับตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง และข้อกำหนดทางธุรกิจ

บันทึกข้อมูลบางอย่างอาจต้องมีการเก็บรักษาไว้อย่างปลอดภัยเพื่อให้เป็นไปตามข้อกำหนดทางกฎหมาย ข้อบังคับ หรือสัญญา ตลอดจนเพื่อสนับสนุนกิจกรรมทางธุรกิจที่สำคัญ

ตัวอย่างเช่น บันทึกข้อมูลที่อาจต้องใช้เพื่อเป็นหลักฐานว่าหน่วยงานมีการดำเนินงานภายใต้กฎหมาย หรือระเบียบข้อบังคับ เพื่อให้มั่นใจว่าสามารถใช้เป็นหลักฐานเพื่อป้องกันหน่วยงานได้อย่างเพียงพอต่อการดำเนินคดีทางแพ่งหรือทางอาญาที่อาจเกิดขึ้น หรือเพื่อยืนยันสถานะทางการเงินของหน่วยงานในส่วนที่เกี่ยวกับผู้ถือหุ้น บุคคลภายนอก และผู้ตรวจ

สอบบัญชี รวมถึงอาจมีการออกกฎหมายหรือข้อบังคับของประเทศนั้นๆ ในเรื่องของช่วงเวลาและเนื้อหาข้อมูลสำหรับการจัดเก็บรักษาบันทึกข้อมูล

ควรมีการจัดแบ่งบันทึกในประเภทต่างๆ ตัวอย่างเช่น บันทึกทางบัญชี บันทึกฐานข้อมูล บันทึกทางธุรกรรม บันทึกการตรวจประเมิน และบันทึกขั้นตอนการปฏิบัติงาน โดยแต่ละบันทึกควรมีรายละเอียดเกี่ยวกับระยะเวลาในการจัดเก็บและประเภทของสื่อที่อนุญาตให้จัดเก็บ เช่น เอกสาร ไมโครฟิช แถบแม่เหล็ก สายออปติคัล เป็นต้น

ควรมีการจัดเก็บวิธีการเข้ารหัสและโปรแกรมใดๆ ที่เกี่ยวข้องกับไฟล์ที่ถูกจัดเก็บถาวรซึ่งมีการเข้ารหัสหรือมีการใช้ลายเซ็นดิจิทัล เพื่อใช้สำหรับการถอดรหัสของบันทึกข้อมูลตามระยะเวลาที่ถูกเก็บรักษาไว้

ควรมีการพิจารณาถึงความเป็นไปได้ของการเสื่อมสภาพของสื่อที่ใช้สำหรับจัดเก็บข้อมูล และควรมีการดำเนินการการจัดเก็บและจัดการข้อมูลตามคำแนะนำของผู้ผลิต

ควรมีการกำหนดระยะเวลาเก็บรักษาเพื่อให้แน่ใจว่าสามารถเข้าถึงข้อมูลได้เพื่อป้องกันการสูญเสียอันเนื่องมาจากพัฒนาการของเทคโนโลยีในอนาคต รวมถึงควรเลือกระบบจัดเก็บข้อมูลที่สามารถดึงข้อมูลที่ต้องการได้ในช่วงเวลาที่เหมาะสมโดยขึ้นอยู่กับข้อกำหนดที่ต้องปฏิบัติตาม

ควรตรวจสอบระบบการจัดเก็บและการจัดการข้อมูลให้แน่ใจว่าข้อมูลและระยะเวลาในการจัดเก็บเป็นไปตามที่กฎหมายหรือข้อบังคับระดับชาติหรือระดับภูมิภาคกำหนดไว้ ซึ่งระบบดังกล่าวควรมีการอนุญาตให้กำจัดหรือลบข้อมูลทิ้งได้อย่างเหมาะสมหากหน่วยงานไม่ต้องการข้อมูลเหล่านั้นแล้ว

เพื่อให้เป็นไปตามวัตถุประสงค์ในการปกป้องข้อมูล หน่วยงานควรดำเนินการตามขั้นตอนต่อไปนี้:

- ควรจัดทำแนวทางปฏิบัติในการจัดเก็บ การบันทึก การจัดการ และการกำจัดหรือลบบันทึกและข้อมูลทิ้ง
- ควรจัดทำตารางการเก็บรักษาเพื่อระบุบันทึกข้อมูลและระยะเวลาที่ควรทำการจัดเก็บ
- ควรเก็บรักษาแหล่งที่มาของบันทึกข้อมูลที่สำคัญไว้

3.15.1.4 ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)

การปกป้องข้อมูลและความเป็นส่วนตัวต้องดำเนินการให้สอดคล้องกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง รวมถึงสัญญาจ้างหากเป็นไปได้

ควรมีการพัฒนานโยบายความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคลและนำไปปรับใช้ รวมถึงควรแจ้งให้บุคลากรทุกท่านที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลทราบถึงนโยบายดังกล่าว

จำเป็นต้องมีโครงสร้างในการจัดการการปฏิบัติตามนโยบาย กฎหมาย และข้อบังคับทั้งหมดที่เกี่ยวข้องกับการปกป้องความเป็นส่วนตัวและข้อมูลส่วนบุคคลและการควบคุมที่เหมาะสม

เพื่อให้การปฏิบัติประสบผลสำเร็จ ควรมีการแต่งตั้งบุคคลที่รับผิดชอบเช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งควรทำหน้าที่ในการให้คำแนะนำแก่ผู้จัดการระบบ ผู้ใช้งาน และผู้ให้บริการด้านต่างๆ เกี่ยวกับความรับผิดชอบส่วนบุคคลและกระบวนการเฉพาะที่ควรปฏิบัติตาม

ควรมีการจัดการความรับผิดชอบในดูแลข้อมูลที่สามารถระบุตัวบุคคลได้ และสร้างความตระหนักรู้ถึงหลักการความเป็นส่วนตัวตามกฎหมายและข้อบังคับที่เกี่ยวข้อง

ควรนำมาตรการเชิงปฏิบัติของหน่วยงานในการปกป้องข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้มาปรับใช้อย่างเหมาะสม

3.15.1.5 ระเบียบข้อบังคับสำหรับมาตรการการเข้ารหัส (Regulation of cryptographic controls)

ควรพิจารณาหัวข้อต่อไปนี้เพื่อนำไปปรับใช้ให้สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง:

ก) ข้อจำกัดในการนำเข้าหรือส่งออกฮาร์ดแวร์และซอฟต์แวร์สำหรับการทำงานของฟังก์ชันเข้ารหัส

ข) ข้อจำกัดในการนำเข้าหรือส่งออกฮาร์ดแวร์และซอฟต์แวร์ที่ถูกออกแบบให้มีการเพิ่มฟังก์ชันการเข้ารหัสเข้าไป

ค) ข้อจำกัดในการใช้การเข้ารหัส

ง) การใช้ชุดคำสั่งหรือการใช้ดุลยพินิจในการเข้าถึงโดยหน่วยงานของประเทศต่างๆ เพื่อเข้ารหัสข้อมูลที่เข้ารหัสโดยฮาร์ดแวร์หรือซอฟต์แวร์เพื่อให้เนื้อหาเป็นความลับ

ควรขอคำแนะนำทางกฎหมายเพื่อให้แน่ใจว่าการปฏิบัตินั้นสอดคล้องกับกฎหมายและข้อบังคับที่เกี่ยวข้อง ก่อนที่ข้อมูลที่เข้ารหัสหรือมาตรการควบคุมการเข้ารหัสจะถูกโอนไปยังหน่วยงานอื่น

3.15.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

3.15.2.1 การทบทวนความมั่นคงปลอดภัยสารสนเทศอย่างอิสระ (Independent review of information security)

วัตถุประสงค์ คือ เพื่อให้แน่ใจว่าความมั่นคงปลอดภัยของสารสนเทศถูกนำไปปรับใช้และดำเนินการตามนโยบายและกระบวนการของหน่วยงาน โดยจัดให้ฝ่ายบริหารทำการทบทวนความมั่นคงปลอดภัยอย่างอิสระ

การทบทวนอย่างอิสระนั้นเป็นสิ่งจำเป็นต้องพึงกระทำ เพื่อให้แน่ใจว่าแนวทางการจัดการความมั่นคงปลอดภัยของสารสนเทศในหน่วยงานนั้นมีความเหมาะสมและมีประสิทธิภาพอย่างต่อเนื่อง

การทบทวนควรรวมถึงการประเมินโอกาสในการปรับปรุงและความจำเป็นในการเปลี่ยนแปลงแนวทางการรักษาความมั่นคงปลอดภัย รวมถึงนโยบายและวัตถุประสงค์ของการควบคุม

การทบทวนความมั่นคงปลอดภัยสารสนเทศควรดำเนินการโดยบุคคลภายนอกหรือบุคคลากรที่ไม่อยู่ภายใต้หน่วยงาน เช่น หน่วยงานตรวจสอบภายใน ผู้จัดการอิสระหรือหน่วยงานภายนอกที่เชี่ยวชาญในการทบทวนดังกล่าวซึ่งมีทักษะและประสบการณ์ที่เหมาะสม

ควรมีการบันทึกและเก็บรักษาผลของการทบทวนความมั่นคงปลอดภัยสารสนเทศอย่างอิสระ และรายงานไปยังฝ่ายบริหารที่ริเริ่มการทบทวนนี้

ฝ่ายบริหารควรพิจารณาดำเนินการแก้ไขให้ถูกต้องในกรณีที่การทบทวนอย่างอิสระมีการระบุว่าแนวทางของหน่วยงานและการปฏิบัติเพื่อจัดการความมั่นคงปลอดภัยของสารสนเทศนั้นยังเหมาะสมไม่เพียงพอ เช่น วัตถุประสงค์และข้อกำหนดที่จัดทำเป็นลายลักษณ์อักษร ไม่สอดคล้องหรือไม่เป็นไปตามทิศทางเดียวกันกับการรักษาความมั่นคงปลอดภัยสารสนเทศที่ระบุไว้ในนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

3.15.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

ตรวจสอบให้แน่ใจว่ามีการดำเนินการรักษาความมั่นคงปลอดภัยสารสนเทศตามนโยบายและกระบวนการของหน่วยงาน

การนำมาตรฐานการรักษาความมั่นคงปลอดภัยไปใช้: ระบบอาณัติสัญญาณทางระบบรางเป็นกระบวนการทางอุตสาหกรรมที่มีความเชื่อมโยงกับมาตรฐานระหว่างประเทศและระดับชาติหลายประการ ซึ่งจำเป็นต้องยึดเป็นหลักเพื่อให้สอดคล้องกับความต้องการด้านความมั่นคงปลอดภัย

ผู้ประกอบกิจการระบบรางส่วนใหญ่เชื่อมั่นในความจำเป็นของการประสานงานระดับสูงนานาชาติ ในด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งต้องมีการลดระดับความมั่นคงปลอดภัยด้านดังกล่าวลงตามกระบวนการอย่างเป็นทางการ และนำมาประยุกต์ใช้ร่วมกันระหว่างบริการภายใน

ผู้จัดการควรกำหนดวิธีการทบทวนข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศที่ระบุไว้ในนโยบาย มาตรฐาน และระเบียบข้อบังคับอื่นๆ ว่ามีความสอดคล้องกันหรือไม่ รวมถึงควรตรวจสอบวิธีการประเมินและการรายงานแบบอัตโนมัติเป็นประจำเพื่อให้การทบทวนเป็นไปอย่างมีประสิทธิภาพ

หากพบความไม่สอดคล้องอันเป็นผลมาจากการทบทวน ผู้จัดการควร:

จ) ระบุต้นเหตุของความไม่สอดคล้องกับข้อกำหนด
ฉ) ประเมินความจำเป็นในการดำเนินการเพื่อให้เป็นไปตามข้อกำหนด
ช) ดำเนินการแก้ไขอย่างเหมาะสม
ซ) ทบทวนการดำเนินการแก้ไขเพื่อตรวจสอบประสิทธิภาพและระบุข้อบกพร่องหรือจุดอ่อน

ควรมีการบันทึกผลของการทบทวนและการดำเนินการแก้ไขที่ดำเนินการโดยผู้จัดการและเก็บรักษาไว้

ผู้จัดการควรรายงานผลต่อบุคคลที่ดำเนินการทบทวนอย่างอิสระ (ดูหัวข้อ 3.15.2.1) เมื่อมีการทบทวนอย่างอิสระในส่วนที่บุคคลดังกล่าวรับผิดชอบ

3.15.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

ตรวจสอบให้แน่ใจว่ามีการนำความปลอดภัยของข้อมูลตามนโยบายและขั้นตอนขององค์กรมาปรับใช้และนำไปปฏิบัติ

รวมถึงควรมีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอเพื่อให้เป็นไปตามมาตรฐานการดำเนินงานด้านความมั่นคงปลอดภัย

ควรทบทวนการปฏิบัติตามข้อกำหนดทางเทคนิคโดยใช้เครื่องมืออัตโนมัติ ซึ่งเครื่องมืออัตโนมัติดังกล่าวจะช่วยสร้างรายงานเชิงเทคนิคสำหรับอธิบายในภายหลังโดยผู้เชี่ยวชาญด้านเทคนิค หรืออาจทำการทบทวนโดยวิศวกรระบบที่มีประสบการณ์ โดยใช้เครื่องมือซอฟต์แวร์ที่เหมาะสม

หากมีการใช้การทดสอบการเจาะระบบหรือการประเมินช่องโหว่ ควรทดสอบอย่างระมัดระวังเนื่องจากกิจกรรมดังกล่าวอาจนำไปสู่การลดทอนความมั่นคงปลอดภัยของระบบ ซึ่งการทดสอบดังกล่าวควรมีการวางแผน จัดทำเป็นลายลักษณ์อักษร และทำซ้ำได้

การทบทวนการปฏิบัติตามข้อกำหนดทางเทคนิคใดๆ ควรดำเนินการโดยผู้มีอำนาจ ผู้เชี่ยวชาญ หรือบุคคลอยู่ภายใต้การกำกับดูแลของบุคคลดังกล่าวเท่านั้น