กรมกิจการเด็กและเยาวชน

แนวทางการตรวจสอบและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

ของกรมกิจการเด็กและเยาวชน

ประจำปี 2569

กองยุทธศาสตร์และแผนงาน
กรมกิจการเด็กและเยาวชน

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญและมีบทบาทอย่างมากสำหรับองค์กร ซึ่งจะช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพและประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ เช่น การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่าง ๆ และการรับ – ส่งจดหมายอิเล็กทรอนิกส์ เป็นต้น และถึงแม้ว่าระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และช่วยอำนวยความสะดวกในด้านต่าง ๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง ซึ่งอาจก่อให้เกิดความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้บริการเชื่อมโยงข้อมูลผ่านเครือข่ายคอมพิวเตอร์จากที่ต่าง ๆ ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น และอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการสิ่งเหล่านี้ล้วนเป็นการสร้างความเสียหายต่อระบบเทคโนโลยีสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้น ผู้ใช้งาน ผู้ดูแลระบบ และผู้พัฒนาระบบเทคโนโลยีสารสนเทศของกรมกิจการเด็กและเยาวชน จึงต้องตระหนักและให้ความสำคัญ ในการควบคุม ดูแล และรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการเด็กและเยาวชน ร่วมกัน

แนวทางการตรวจสอบ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมกิจการเด็กและเยาวชน ฉบับนี้ ได้จัดทำขึ้นเพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง อย่างไรก็ตามการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือและถือปฏิบัติอย่างเคร่งครัดจากทุกหน่วยงาน ซึ่งต้องมีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงให้สอดคล้องกับการพัฒนางานด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไปอย่างรวดเร็ว กองยุทธศาสตร์และแผนงาน จึงหวังเป็นอย่างยิ่งว่า แนวทางการตรวจสอบและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมกิจการเด็กและเยาวชนฉบับนี้ จะเป็นประโยชน์กับผู้ใช้งาน ผู้ดูแลระบบ และผู้พัฒนา รวมถึงผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมกิจการเด็กและเยาวชน ทุกคน เพื่อใช้เป็นเครื่องมือและแนวปฏิบัติในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานต่อไป

กรมกิจการเด็กและเยาวชน

ตุลาคม 2568

สารบัญ

สารบัญ

แนวทางการตรวจสอบและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมกิจการเด็กและเยาวชน ประจำปี พ.ศ. 2569

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลบังคับใช้เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ เพื่อให้สามารถป้องกัน หรือรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ซึ่งกรมกิจการเด็กและเยาวชนมีภารกิจเกี่ยวกับการส่งเสริมและพัฒนาศักยภาพของเด็ก เยาวชน การคุ้มครองและพิทักษ์สิทธิเด็ก การส่งเสริมสวัสดิการเด็กและครอบครัว ดังนั้นเพื่อให้การดำเนินงานตามภารกิจของหน่วยงานสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง และเพื่อเป็นการสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐและเอกชนให้บรรลุตามเป้าหมายที่กำหนดไว้ รวมทั้งให้สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวง เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งช่วยลดโอกาสที่จะเกิดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากรของหน่วยงาน

ดังนั้น กรมกิจการเด็กและเยาวชน (ดย.) จึงได้จัดทำแผนการตรวจสอบและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ดย. ประจำปี พ.ศ. 2569 ฉบับนี้ขึ้น เพื่อใช้เป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ ดย. ซึ่งบุคลากรของ ดย. และหน่วยงานภายนอกที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด ทั้งนี้ ได้กำหนดมาตรการ แนวทางและขั้นตอนการปฏิบัติในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ได้อย่างปลอดภัยและคุ้มค่า

วัตถุประสงค์

1. เพื่อให้มีวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ ดย. ซึ่งสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อถือปฏิบัติอย่างเคร่งครัด

2. เพื่อสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ให้แก่เจ้าหน้าที่ทุกระดับของ ดย. และบุคคลที่เกี่ยวข้อง

3. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของ ดย.

การกำกับดูแล
(Govern)

1. นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management System Policy)

อ้างอิง : พรบ. ไซเบอร์ (ม.43, ม.44, ม.45, ม.46, ม.54, ม.56), นโยบาย [ข้อ 1.1, ข้อ 1.3, ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2], ประมวลและกรอบ [ข้อ 18]

1.1 วัตถุประสงค์ (Objective)

นโยบายนี้จัดทำขึ้นเพื่อกำหนดกรอบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ในองค์กรโดยมีวัตถุประสงค์เพื่อปกป้องทรัพย์สินสารสนเทศ โครงสร้างพื้นฐาน และข้อมูลที่มีความสำคัญจากภัยคุกคามทางไซเบอร์รวมถึงการสร้างความมั่นใจในการให้บริการประชาชนขององค์กรอย่างต่อเนื่องและปลอดภัย

1.2 ขอบเขต (Scope)

นโยบายนี้ครอบคลุมทุกระบบ ข้อมูล โครงสร้างพื้นฐานสารสนเทศ และกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในองค์กร รวมถึงพนักงาน ผู้บริหาร ผู้ใช้งาน ผู้ให้บริการ และผู้ที่มีส่วนเกี่ยวข้องทั้งหมดในองค์กร

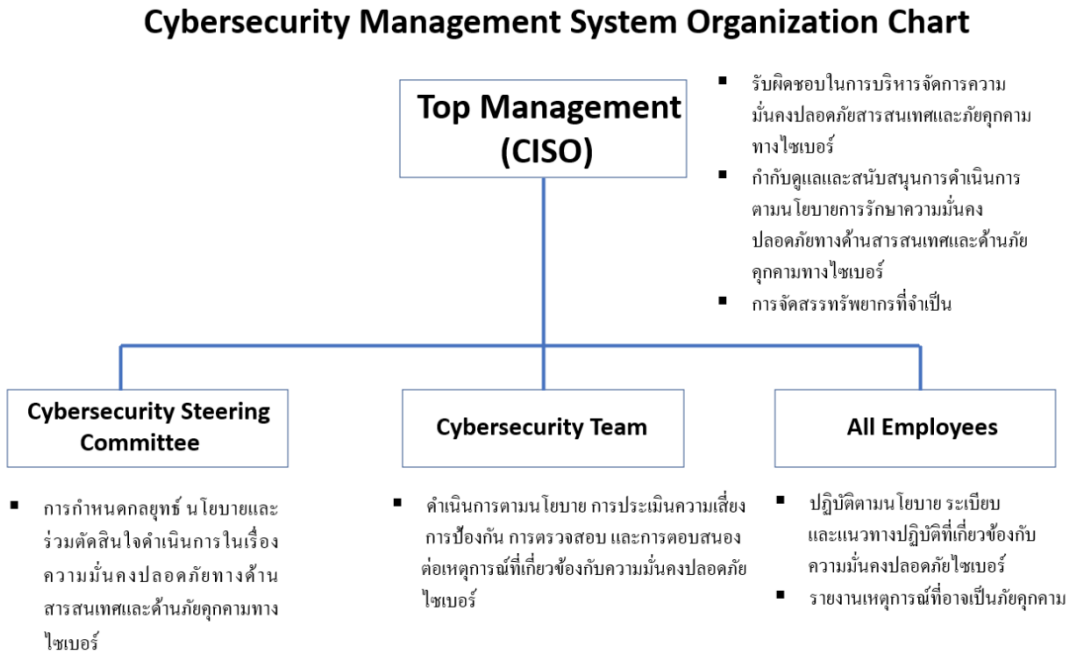
1.3 ความสอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (Alignment with Cybersecurity Policy and Plan)

1) องค์กรจะดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้มั่นใจว่าการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สอดคล้องกับกฎหมาย ข้อบังคับ และมาตรการที่เกี่ยวข้อง

2) นโยบายนี้ได้รับการออกแบบมาเพื่อสนับสนุนและเสริมสร้างมาตรการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจส่งผลกระทบต่อการดำเนินงานและความมั่นคงปลอดภัยของหน่วยงานที่รับผิดชอบ

1.4 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

โครงสร้างคณะทำงานระบบการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSMS Organization Structure Chart)



1) ผู้บริหารระดับสูง (Top Management - CISO) : รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์ พร้อมทั้งกำกับดูแลและสนับสนุนการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศและด้านภัยคุกคามทางไซเบอร์ รวมถึงการ จัดสรรทรัพยากรที่จำเป็น,CISO - Chief Information Security Officer มีความเป็นอิสระจากงานด้านการปฏิบัติงาน (IT Operation) และงานด้านพัฒนาระบบสารสนเทศ (IT Development)

2) คณะกรรมการบริหารจัดการและกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Steering Committee): รับผิดชอบในการกำหนดกลยุทธ์ นโยบาย และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยทางด้านสารสนเทศและด้านภัยคุกคามทางไซเบอร์

3) ทีมรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Team): รับผิดชอบในการดำเนินการ ตามนโยบาย การประเมินความเสี่ยง การป้องกัน การตรวจสอบ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

4) พนักงานทุกคน (All Employees): มีหน้าที่ในการปฏิบัติตามนโยบาย ระเบียบ และแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงการรายงานเหตุการณ์ที่อาจเป็นภัยคุกคาม

1.5 การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management)

1) การประเมินความเสี่ยง (Risk Assessment) : องค์กรจะดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อระบุ วิเคราะห์ และประเมินค่าความเสี่ยงที่อาจเกิดขึ้น

2) การจัดการความเสี่ยง (Risk Treatment) : องค์กรจะดำเนินการควบคุมและลดความเสี่ยงโดยใช้มาตรการป้องกันที่เหมาะสม เพื่อให้ความเสี่ยงเหลืออยู่ในระดับที่ยอมรับได้

1.6 มาตรการการป้องกัน รับมือ และลดความเสี่ยง (Prevention, Response, and Risk Mitigation Measures)

1) การป้องกัน (Prevention) : องค์กรจะนำมาตรการป้องกันที่ทันสมัยและเหมาะสมมาใช้เพื่อปกป้องข้อมูลและโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์ เช่น การใช้ไฟร์วอลล์ การเข้ารหัส ข้อมูล และการควบคุมการเข้าถึง

2) การรับมือ (Incident Response) : องค์กรจะพัฒนาและนำแผนตอบสนองต่อเหตุการณ์ทาง ไซเบอร์มาใช้ เพื่อให้สามารถรับมือและจัดการกับเหตุการณ์ทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ

3) การลดความเสี่ยง (Risk Mitigation) : องค์กรจะดำเนินการลดความเสี่ยงที่ระบุไว้ให้เหลือน้อยที่สุดโดยการปรับปรุงมาตรการป้องกันและการฝึกอบรมพนักงานอย่างสม่ำเสมอ

1.7 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

1) การเข้าถึงข้อมูล (Data Access Control) : องค์กรจะกำหนดมาตรการควบคุมการเข้าถึงข้อมูลให้เป็นไปตามหลักการสิทธิ์น้อยที่สุด (Least Privilege) และจำเป็นต้องทราบ (Need to Know) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2) การเข้ารหัสข้อมูล (Data Encryption) : ข้อมูลที่มีความสำคัญและข้อมูลส่วนบุคคลจะต้องถูกเข้ารหัสทั้งขณะเก็บรักษาและขณะส่งผ่านเครือข่าย เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

1.8 การรักษาความมั่นคงปลอดภัยของระบบ (System Security)

1) การป้องกันระบบ (System Protection): องค์กรจะดำเนินการติดตั้งและบำรุงรักษามาตรการ ป้องกันระบบ เช่น ไฟร์วอลล์ การตรวจจับและป้องกันการบุกรุก (IDS/IPS) และซอฟต์แวร์ป้องกันมัลแวร์

2) การจัดการแพตช์และอัปเดต (Patch Management and Updates) : ระบบและซอฟต์แวร์ทั้งหมดจะต้องได้รับการอัปเดตแพตช์และการรักษาความปลอดภัยอย่างสม่ำเสมอ เพื่อลดช่องโหว่ที่อาจถูกใช้ในการโจมตี

1.9 การบริหารจัดการเหตุการณ์ทางไซเบอร์ (Cyber Incident Management)

1) การตรวจจับเหตุการณ์ (Incident Detection) : องค์กรจะใช้เครื่องมือและระบบตรวจสอบเพื่อเฝ้าระวังและตรวจจับเหตุการณ์ทางไซเบอร์ที่อาจเกิดขึ้นอย่างต่อเนื่อง

2) การตอบสนองต่อเหตุการณ์ (Incident Response) : องค์กรจะพัฒนาและดำเนินการตามแผนตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response Plan) ซึ่งรวมถึงการกักกัน การวิเคราะห์ และการฟื้นฟูระบบที่ได้รับผลกระทบ

3) การรายงานเหตุการณ์ (Incident Reporting) : เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไซเบอร์จะต้องถูกรายงานต่อผู้บริหารและหน่วยงานที่เกี่ยวข้องตามขั้นตอนที่กำหนด

1.10 การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

1) การฝึกอบรมพนักงาน (Employee Training): องค์กรจะจัดฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้กับพนักงานทุกคนอย่างสม่ำเสมอ เพื่อให้พนักงานมีความรู้และทักษะในการปฏิบัติ ตามนโยบายและการป้องกันภัยคุกคามทางไซเบอร์

2) การฝึกอบรมพนักงาน (Employee Training): องค์กรจะจัดฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้กับพนักงานทุกคนอย่างสม่ำเสมอ เพื่อให้พนักงานมีความรู้และทักษะในการปฏิบัติตามนโยบายและการป้องกันภัยคุกคามทางไซเบอร์

1.11 การปฏิบัติตามกฎหมายและมาตรฐาน (Compliance with Laws and Standards)

1) การปฏิบัติตามข้อกำหนด (Regulatory Compliance) : องค์กรจะปฏิบัติตามกฎหมาย ข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด

2) การประเมินและตรวจสอบ (Assessment and Audits) : องค์กรจะดำเนินการประเมินและตรวจสอบภายในเป็นระยะเพื่อให้มั่นใจว่าการปฏิบัติตามข้อกำหนดและนโยบายด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างเหมาะสม

1.12 การจัดทำเอกสารและการจัดเก็บข้อมูล (Documentation and Record Keeping)

1) การจัดทำเอกสาร (Documentation) : องค์กรจะดำเนินการจัดทำเอกสารที่เกี่ยวข้องกับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์อย่างครบถ้วนและถูกต้อง

2) การจัดเก็บและเข้าถึงข้อมูล (Record Keeping and Access) : เอกสารและข้อมูลทั้งหมดจะถูกจัดเก็บอย่างปลอดภัย และจะต้องสามารถเข้าถึงได้เมื่อจำเป็นสำหรับการตรวจสอบหรือใช้งานในอนาคต

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

2. นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.54), นโยบาย (ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ3.2), ประมวลและกรอบ [ข้อ 18, ข้อ 18.1(ก), ข้อ 18.1(ข), ข้อ 18.1(ค), ข้อ 18.2, ข้อ 18.2(ข), ข้อ 18.3, ข้อ 18.4, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1]

2.1 วัตถุประสงค์ (Objective)

วัตถุประสงค์ของนโยบายนี้คือเพื่อกำหนดกรอบการทำงานสำหรับการระบุ ประเมิน และบริหารความเสี่ยงด้าน ความมั่นคงปลอดภัยไซเบอร์ เพื่อให้แน่ใจว่าโครงสร้างพื้นฐานและบริการที่สำคัญได้รับการปกป้องจากภัย คุกคามไซเบอร์ นโยบายนี้สอดคล้องกับนโยบายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย โดยเฉพาะ **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** และ **นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**

2.2 ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงหน่วยงาน สำนัก กอง กลุ่ม และพันธมิตรภายนอกทั้งหมดที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งรวมถึง

1. โครงสร้างพื้นฐานสำคัญด้านสารสนเทศ
2. ข้อมูลและเครือข่ายที่สำคัญ
3. ผู้ให้บริการและผู้จำหน่ายภายนอก

2.3 หลักการบริหารความเสี่ยง (Risk Management Principle)

องค์กรจะใช้หลักการดังต่อไปนี้ในการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

1. การระบุความเสี่ยงเชิงรุก : การระบุความเสี่ยงด้านไซเบอร์ผ่านการประเมินอย่างสม่ำเสมอและการวิเคราะห์ข้อมูลภัยคุกคาม

2. การประเมินความเสี่ยง : การประเมินผลกระทบและความเป็นไปได้ของความเสี่ยงที่ระบุโดยเน้นที่ภัยคุกคามที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานหรือข้อมูลสำคัญ

3. การลดความเสี่ยง : ดำเนินการลดหรือขจัดความเสี่ยงโดยจัดลำดับความสำคัญของภัยคุกคาม

4. การติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง: การติดตามและทบทวนความเสี่ยงด้านไซเบอร์มีการกระทำอย่างต่อเนื่อง หรืออย่างน้อยปีละ 1 ครั้ง โดยผ่านระบบอัตโนมัติและการตรวจสอบด้วยตนเองอย่างสม่ำเสมอ

2.4 ความสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

นโยบายนี้จะสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 : ปฏิบัติตามข้อกำหนดในการปกป้อง โครงสร้างพื้นฐานสำคัญและการรายงานเหตุการณ์

2. นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) : เป็นการพัฒนาความมั่นคงปลอดภัยทางทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติและเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศ

2.5 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1. ทีมงานด้านความมั่นคงปลอดภัยไซเบอร์ : รับผิดชอบในการดำเนินการประเมินความเสี่ยงดำเนิน มาตรการแก้ไข และติดตามความเสี่ยงอย่างต่อเนื่อง

2. ฝ่ายบริหาร : ต้องมั่นใจว่าการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ถูกรวมเข้ากับกรอบการบริหารจัดการทั่วไปและรายงานความสอดคล้องกับหน่วยงานที่เกี่ยวข้อง

3. เจ้าหน้าที่กำกับดูแล : รับผิดชอบในการตรวจสอบและให้แน่ใจว่าปฏิบัติตามกฎหมายและระเบียบ ข้อบังคับตามที่ระบุในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.6 กระบวนการระบุและประเมินความเสี่ยง (Risk Identification and Risk Assessment)

1. ทะเบียนความเสี่ยง : จะมีการบันทึกความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ทั้งหมดในทะเบียน ความเสี่ยง โดยจะมีการประเมินแต่ละความเสี่ยง เช่น

- ความเป็นไปได้ : ความน่าจะเป็นที่ความเสี่ยงจะเกิดขึ้น
- ผลกระทบ : ความเสียหายหรือการรบกวนที่อาจเกิดขึ้นจากความเสี่ยง
- มาตรการควบคุม : ขั้นตอนที่มีอยู่ในปัจจุบัน สามารถเพื่อบรรเทาความเสี่ยงนั้นๆ

2. การจัดประเภทความเสี่ยง : ความเสี่ยงจะถูกจัดหมวดหมู่ตามระดับ เช่น สูง กลาง ต่ำ ตามความรุนแรงที่ประเมิน

2.7 การจัดการความเสี่ยง (Risk Treatment)

1. การหลีกเลี่ยง : ความเสี่ยงที่สามารถหลีกเลี่ยงได้จะถูกขจัดออกโดยการเปลี่ยนแปลงระบบหรือกระบวนการในการปฏิบัติ

2. การลดความเสี่ยง : ลดความเสี่ยงโดยการดำเนินมาตรการควบคุมเพิ่มเติม เช่น การเข้ารหัสไฟล์ วางไฟร์วอลล์ และฝึกอบรมพนักงาน

3. การยอมรับ : มีการกำหนดความเสี่ยงในระดับต่ำที่ยอมรับได้โดยไม่ต้องมีมาตรการเพิ่มเติม

4. การโอนความเสี่ยง : โอนความเสี่ยงให้หน่วยงานหรือองค์กรภายนอกโดยการทำสัญญาหรือประกันภัยในกรณีที่เหมาะสม

2.8 การตอบสนองและรายงานเหตุการณ์ (Response and Incident Reporting)

1. ทุกเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์จะต้องรายงานต่อทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ทันที

2. เหตุการณ์ที่รุนแรงที่ส่งผลต่อโครงสร้างพื้นฐานสำคัญจะถูกส่งต่อไปยังผู้บริหารระดับสูงและหน่วยงานควบคุมหรือกำกับดูแลตาม**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

2.9 การปรับปรุงอย่างต่อเนื่อง (Continuously Improvement)

1) จะมีการตรวจสอบและประเมินผลนโยบายฯอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ากรอบการบริหารความเสี่ยงนั้นยังคงมีประสิทธิภาพ

2) นโยบายฯนี้จะได้รับการปรับปรุงเพื่อให้ทันกับการเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์

2.10 การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

นโยบายฯนี้จะได้รับการตรวจสอบอย่างต่อเนื่องเพื่อให้สอดคล้องกับยุทธศาสตร์ไซเบอร์แห่งชาติหรือนโยบาย ความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) รวมถึงข้อกำหนดของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) การไม่ปฏิบัติตามนโยบายนี้จะมีบทลงโทษตามข้อกำหนดขององค์กร

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

การตรวจสอบ
(Audit)

1. กระบวนการแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.44, ม.54), ประมวลและกรอบ [ข้อ 17.1, ข้อ 17.1(ก), ข้อ 17.1(ข), ข้อ 17.1(ค),ข้อ 17.2, ข้อ 17.3, ข้อ 17.4, ข้อ 17.5]

1.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่ามีการตรวจสอบและประเมินความมั่นคงปลอดภัยไซเบอร์ในองค์กรอย่างต่อเนื่องและมีประสิทธิภาพ โดยเป็นไปตามมาตรฐานและข้อกำหนดที่กำหนดไว้เพื่อป้องกันและ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

1.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับองค์กร รวมถึงการตรวจสอบกระบวนการวิเคราะห์ผลกระทบทางธุรกิจ บริการที่สำคัญ และการปฏิบัติตามข้อกำหนด ของกฎหมายและมาตรฐานที่เกี่ยวข้อง

1.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1. ผู้ตรวจสอบทางด้านไซเบอร์ (Cybersecurity Auditors) : รับผิดชอบในการดำเนินการตรวจสอบทั้งภายในและภายนอก โดยตรวจสอบการรักษาความมันคงปลอดภัยของระบบทางด้านไซเบอร์และกระบวนการต่าง ๆ ตามขอบเขตที่กำหนด

2. คณะกรรมการขององค์กรที่ได้รับการมอบหมาย (Cybersecurity Management Committee: CMC) : รับผิดชอบในการอนุมัติแผนการตรวจสอบ ติดตามผลการตรวจสอบ และกำหนดแนวทางในการดำเนินการแก้ไขหากพบข้อบกพร่อง

3. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII): รับผิดชอบในการดำเนินการตามแผนการตรวจสอบที่ได้รับการ อนุมัติ และดำเนินการแก้ไขข้อบกพร่องที่พบจากการตรวจสอบ

1.4 ขั้นตอนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Process Steps)

1. การวางแผนการตรวจสอบ (Audit Planning)

1) การกำหนดขอบเขตการตรวจสอบ

ขั้นตอน : กำหนดขอบเขตของการตรวจสอบตามที่ระบุไว้ในแนวปฏิบัติ รวมถึงกระบวนการ จัดทำและบริการที่สำคัญ และการปฏิบัติตามกฎหมาย พรบ ไซเบอร์และมาตรฐานที่เกี่ยวข้อง

2) การแต่งตั้งผู้ตรวจสอบ

ขั้นตอน : แต่งตั้งผู้ตรวจสอบที่มีความรู้และความเชี่ยวชาญในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ทั้งจากภายในหรือภายนอกองค์กรเพื่อร่วมดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ประจำปี

2. การดำเนินการตรวจสอบ (Audit Execution)

1) การตรวจสอบกระบวนการและบริการที่สำคัญ

ขั้นตอน : ผู้ตรวจสอบดำเนินการตรวจสอบกระบวนการจัดทำการตรวจสอบพร้อมวิเคราะห์ ผลกระทบ (BIA) และบริการที่สำคัญขององค์กรตามขอบเขตที่กำหนดไว้

2) การตรวจสอบการปฏิบัติตามกฎหมาย พรบ ไซเบอร์ และมาตรฐานอื่นๆ ที่เกี่ยวข้อง

ขั้นตอน : ผู้ตรวจสอบตรวจสอบการปฏิบัติตาม พรบ ไซเบอร์ และมาตรฐานการปฏิบัติงานที่ เกี่ยวข้อง รวมถึงการปฏิบัติตามข้อกำหนดขององค์กรและหน่วยงานควบคุมหรือกำกับดูแล

3. การรายงานผลการตรวจสอบ (Audit Reporting)

1) การจัดทำรายงานการตรวจสอบ

ขั้นตอน : ผู้ตรวจสอบจัดทำรายงานสรุปผลการตรวจสอบ รวมถึงข้อบกพร่องที่พบและข้อเสนอแนะในการปรับปรุง

2) การส่งรายงานผลการตรวจสอบ

ขั้นตอน : หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการ ตรวจสอบต่อสำนักงานภายในกำหนด 30 วันหลังจากที่ดำเนินการตรวจสอบเสร็จสิ้น และส่งสำเนาให้กับหน่วยงานควบคุมหรือกำกับดูแล

4. การดำเนินการแก้ไขข้อบกพร่อง (Corrective Action Implementation)

1) การจัดทำแผนการดำเนินการแก้ไข

ขั้นตอน : หากพบข้อบกพร่องหรือการไม่ปฏิบัติตามในการตรวจสอบองค์กรจะต้องจัดทำแผนการดำเนินการแก้ไขโดยระบุรายละเอียดการแก้ไขและระยะเวลาที่จะดำเนินการ

2) การติดตามและรายงานผลการแก้ไข

ขั้นตอน : ติดตามผลการดำเนินการแก้ไข และรายงานผลการแก้ไขต่อคณะกรรมการขององค์กรที่ได้รับมอบหมายเป็นประจำ และหน่วยงานควบคุมหรือกำกับดูแลภายในระยะเวลาที่กำหนด

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปี หรือตามความจำเป็นเพื่อให้มันใจในประสิทธิภาพ และถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนงานการตรวจสอบ (Audit Program / Plan)
2. รายงานการตรวจสอบ (Audit Reporting), NIST SP 800-53A Rev. 5
3. ผลการดำเนินการแก้ไข และรายงานผลการแก้ไข
4. แผนการตรวจสอบระยะเวลา 1 ปี (Annual Audit Plan) หรือ เกินกว่า 1 ปี (Multi-Year Audit Plan)
5. รายงานหรือเอกสารแสดงการจัดทำ BIA

2. กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) Procedure

อ้างอิง : พรบ ไซเบอร์ (ม.44, ม.54), ประมวลและกรอบ [ข้อ 17.1, ข้อ 17.1(ก), ข้อ 17.1(ข), ข้อ 17.1(ค),ข้อ 17.2, ข้อ 17.3, ข้อ 17.4, ข้อ 17.5]

2.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อระบุและวิเคราะห์ผลกระทบทางธุรกิจที่อาจเกิดขึ้นจากเหตุการณ์ที่ไม่คาดคิดรวมถึงการหยุดชะงักในการดำเนินงาน เพื่อกำหนดลำดับความสำคัญของกระบวนการและระบบที่สำคัญ และเพื่อกำหนดกลยุทธ์ในการรักษาความต่อเนื่องทางธุรกิจ

2.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมการวิเคราะห์ผลกระทบทางธุรกิจของทุกกระบวนการ ระบบ และทรัพยากรที่ เกี่ยวข้องกับการดำเนินงานขององค์กร เพื่อประเมินระดับผลกระทบและกำหนดกลยุทธ์ ในการจัดการความเสี่ยง และการฟื้นฟูการดำเนินงาน

2.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1. ผู้จัดการโครงการ BIA (BIA Project Manager) : รับผิดชอบในการจัดทำแผนการวิเคราะห์ผลกระทบทางธุรกิจ ควบคุมการดำเนินงาน และรายงานผลการวิเคราะห์

2. ทีมวิเคราะห์ผลกระทบ (Impact Analysis Team) : รับผิดชอบในการรวบรวมข้อมูลวิเคราะห์ผลกระทบ และจัดทำรายงาน BIA

3. ผู้บริหารองค์กร (Senior Management) : รับผิดชอบในการอนุมัติผลการวิเคราะห์ BIA และสนับสนุนการดำเนินการตามกลยุทธ์ที่กำหนด

2.4 ขั้นตอนการจัดทำและวิเคราะห์ผลกระทบทางธุรกิจ (BIA Process Steps)

1. การวางแผนและการเริ่มต้น (Planning and Initiation)

1) กำหนดวัตถุประสงค์และขอบเขต

ขั้นตอน : กำหนดวัตถุประสงค์ ขอบเขต และเกณฑ์ในการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงทรัพยากรที่เกี่ยวข้อง ซึ่งวัตถุประสงค์คือการประเมินผลกระทบจากการหยุดชะงักของระบบเครือข่ายที่ใช้ในการบริการลูกค้า ขอบเขตครอบคลุมกระบวนการทั้งหมดที่เกี่ยวข้องกับ การให้บริการลูกค้าและการจัดการข้อมูลลูกค้า

2) การจัดตั้งทีมวิเคราะห์ผลกระทบ

ขั้นตอน : แต่งตั้งทีมวิเคราะห์ผลกระทบที่ประกอบด้วยบุคลากรจากหน่วยงานต่าง ๆ ในองค์กรที่มีความเชี่ยวชาญในกระบวนการที่เกี่ยวข้อง เช่น ฝ่าย IT, ฝ่ายการเงิน, ฝ่าย ปฏิบัติการ, และฝ่ายบริหารความเสี่ยง

2. การรวบรวมข้อมูล (Data Collection)

1) การระบุและจัดลำดับความสำคัญของกระบวนการ

ขั้นตอน : ระบุและจัดลำดับความสำคัญของกระบวนการทางธุรกิจที่สำคัญ โดยพิจารณาจากผลกระทบที่อาจเกิดขึ้นต่อองค์กรโดยกระบวนการเหล่านี้ถูกจัดเป็นกระบวนการที่มีความสำคัญสูงสุด

2) การรวบรวมข้อมูลจากหน่วยงานที่เกี่ยวข้อง

ขั้นตอน : รวบรวมข้อมูลจากหน่วยงานที่เกี่ยวข้องเกี่ยวกับกระบวนการระบบและทรัพยากรที่ ใช้ในกระบวนการ เพื่อประเมินผลกระทบจากการหยุดชะงัก

3. การวิเคราะห์และประเมินผลกระทบ (Analysis and Impact Evaluation)

1) การประเมินผลกระทบที่อาจเกิดขึ้น (Impact Analysis)

ขั้นตอน : วิเคราะห์ผลกระทบทางการเงิน ด้านชื่อเสียง ด้านกฎหมาย และผลกระทบอื่น ๆ ที่ อาจเกิดขึ้นจากการหยุดชะงักของกระบวนการและระบบ หากระบบการประมวลผลธุรกรรม การเงินล่ม อาจส่งผลให้บริษัทสูญเสียรายได้และเกิดความเสียหายด้านชื่อเสียง

2) การกำหนดเกณฑ์เวลาที่สำคัญ (Critical Timeframes)

ขั้นตอน : กำหนดเกณฑ์เวลาที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), และ Recovery Point Objective (RPO) สำหรับกระบวนการที่สำคัญ ซึ่งหมายความว่าระบบต้องฟื้นฟู ให้ใช้งานได้ภายในเวลาที่กำหนดไว้

4. การจัดทำรายงานและข้อเสนอแนะ (Reporting and Recommendations)

1) การจัดทำรายงาน BIA

ขั้นตอน : จัดทำรายงานสรุปผลการวิเคราะห์ BIA ที่รวมถึงผลกระทบที่ประเมินได้ ข้อสังเกต และข้อเสนอแนะในการจัดการความเสี่ยงและการฟื้นฟูกระบวนการเช่นรายงาน BIA ต้อง ระบุว่าการหยุดชะงักของระบบเครือข่ายหลักจะส่งผลกระทบทางการเงินอย่างมีนัยสำคัญ และ เสนอให้จัดตั้งระบบสำรองเพื่อให้สามารถฟื้นฟูการทำงานได้ภายใน 2 ชั่วโมงเป็นต้น

2) การนำเสนอผลการวิเคราะห์

ขั้นตอน : นำเสนอผลการวิเคราะห์ต่อผู้บริหารองค์กรและคณะกรรมการที่เกี่ยวข้องเพื่อพิจารณาและอนุมัติแผนการดำเนินการตามข้อเสนอแนะเนื่องจากบางอย่างต้องมีการอนุมัติการลงทุนด้วย

5. การดำเนินการตามข้อเสนอแนะ (Implementation of Recommendations)

1) การดำเนินการตามแผนการฟื้นฟู

ขั้นตอน : ดำเนินการตามแผนการฟื้นฟูที่ได้รับอนุมัติ รวมถึงการจัดตั้งระบบสำรอง การ ทดสอบระบบ และการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ

2) การติดตามและประเมินผล

ขั้นตอน : ติดตามและประเมินผลการดำเนินการตามแผน BIA เพื่อปรับปรุงและปรับแผนให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลง

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปี หรือตามความจำเป็นเพื่อให้มันใจในประสิทธิภาพ และถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. เอกสารแสดงการจัดทำ BIA
2. รายงานผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)

การระบุ
(Identify)

1. กระบวนการจัดการทรัพย์สิน (Asset Management Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.1.1, ข้อ 21.1.2, ข้อ 21.1.3, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ21.2.2, ข้อ 21.3.1, ข้อ 21.3.2, ข้อ 21.3.3, ข้อ 21.3.9]

1.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าทรัพย์สินของบริการที่สำคัญขององค์กรได้รับการจัดการอย่างเหมาะสมและมีการบันทึกข้อมูลที่ครบถ้วนและเป็นปัจจุบัน รวมถึงการระบุ การติดตาม และการประเมินความเสี่ยงของทรัพย์สินเหล่านี้อย่างสม่ำเสมอ

1.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมทรัพย์สินทุกประเภทที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร รวมถึง ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ระบบเครือข่าย และทรัพยากรทางเทคโนโลยีสารสนเทศอื่น ๆ ที่มีความสำคัญต่อการดำเนินงานขององค์กร

1.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1. ผู้บริหาร (Top Management) : รับผิดชอบในการกำกับดูแลและสนับสนุนการดำเนินการตามกระบวนการจัดการทรัพย์สิน

2. ทีม IT (IT Team): รับผิดชอบในการจัดทำ ดูแลรักษา และอัปเดตทะเบียนทรัพย์สิน รวมถึงการ ตรวจสอบและประเมินความเสี่ยงของทรัพย์สิน

3. ผู้ใช้งานระบบ (System Users): มีหน้าที่ในการรายงานการเปลี่ยนแปลงที่เกิดขึ้นกับทรัพย์สินที่ ใช้งานต่อทีม IT เพื่อให้มีการอัปเดตข้อมูลในทะเบียนทรัพย์สิน

1.4 การจัดทำและดูแลทะเบียนทรัพย์สิน (Inventory Management)

1. การจัดทำทะเบียนทรัพย์สิน (Asset Inventory List)

ขั้นตอน

1) จัดทำทะเบียนทรัพย์สินที่ระบุรายละเอียดของทรัพย์สินทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร

2) ข้อมูลที่ต้องบันทึกในทะเบียนทรัพย์สิน ได้แก่

- ชื่อหรือคำอธิบายของทรัพย์สิน
- ฟังก์ชันที่สำคัญของทรัพย์สิน
- การจัดลำดับความสำคัญของทรัพย์สิน
- เจ้าของหรือผู้ดำเนินการทรัพย์สิน
- ตำแหน่งทางกายภาพของทรัพย์สิน
- การเชื่อมต่อและการพึ่งพาของทรัพย์สินบนระบบ/เครือข่าย

2. การดูแลและอัปเดตทะเบียนทรัพย์สิน

ขั้นตอน : ดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยมีการตรวจสอบและอัปเดตข้อมูลทุกครั้งที่มีการเปลี่ยนแปลง เช่น การเพิ่ม การย้าย หรือการกำจัดทรัพย์สิน

1.5 การระบุขอบเขตเครือข่ายและระบบคอมพิวเตอร์ (Network and System Scope Identification)

ขั้นตอน : ระบุและกำหนดขอบเขตของเครือข่ายที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน รวมถึง ระบบคอมพิวเตอร์ที่มีการเชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

1.6 การตรวจสอบและปรับปรุงทะเบียนทรัพย์สิน (Inventory Review and Update)

1. การตรวจสอบประจำปี

ขั้นตอน : ดำเนินการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าข้อมูลใน ทะเบียนเป็นปัจจุบันและถูกต้อง

2. การปรับปรุงทะเบียนเมื่อมีการเปลี่ยนแปลง

ขั้นตอน : หากมีการเปลี่ยนแปลงทรัพย์สินหรือบริการที่สำคัญ ต้องทำการอัปเดตข้อมูลในทะเบียนทรัพย์สินทันที

1.7 การประเมินความเสี่ยงของทรัพย์สินและบริการที่สำคัญ (Asset and System service Risk Assessment)

ขั้นตอน : ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของทรัพย์สินและของบริการที่สำคัญในทะเบียนอย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบและระบุความเสี่ยงที่อาจเกิดขึ้น รวมถึง การพิจารณามาตรการการจัดการความเสี่ยงที่เหมาะสม

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปี หรือตามความจำเป็นเพื่อให้มันใจในประสิทธิภาพ และถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. รายการทรัพย์สินทั้งหมด (Asset Inventory List
2. ทะเบียนทรัพย์สิน (Asset Register)
3. เอกสารการประเมินความเสี่ยงของทรัพย์สิน (Risk Assessment of Critical Asset Inventory List)

2. กระบวนการการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.54), นโยบาย (ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ3.2), ประมวลและกรอบ [ข้อ 18, ข้อ 18.1(ก), ข้อ 18.1(ข), ข้อ 18.1(ค), ข้อ 18.2, ข้อ 18.2(ข), ข้อ 18.3, ข้อ 18.4, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1]

2.1 วัตถุประสงค์ (Objective)

กระบวนการนี้มีวัตถุประสงค์เพื่อระบุ วิเคราะห์ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซ เบอร์ที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญขององค์กร และเพื่อกำหนดกลยุทธ์ในการจัดการความเสี่ยง เพื่อป้องกันหรือลดผลกระทบจากความเสี่ยงเหล่านั้น

2.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับ ทรัพย์สิน ข้อมูล ระบบ โครงสร้างพื้นฐาน และบริการที่สำคัญขององค์กร รวมถึงการจัดทำและปรับปรุงทะเบียนความเสี่ยง

2.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1. ผู้จัดการความเสี่ยง (Risk Manager) : รับผิดชอบในการกำกับดูแลการดำเนินการตามกระบวนการประเมินและจัดการความเสี่ยง รวมถึงการตัดสินใจเกี่ยวกับกลยุทธ์การจัดการความเสี่ยงที่สำคัญ

2. ทีมจัดการความเสี่ยง (Risk Management Team) : รับผิดชอบในการดำเนินการประเมินความเสี่ยง การจัดทำทะเบียนความเสี่ยง และการพัฒนากลยุทธ์ในการจัดการความเสี่ยง

3. เจ้าของความเสี่ยง (Risk Owner) : รับผิดชอบในการติดตามและจัดการความเสี่ยงที่ตนรับผิดชอบตามที่ระบุไว้ในทะเบียนความเสี่ยง

2.4 การประเมินความเสี่ยง (Risk Assessment))

1. การระบุความเสี่ยง (Risk Identification)

1) การระบุภัยคุกคามและช่องโหว่

ขั้นตอน : ระบุภัยคุกคามทางไซเบอร์และช่องโหว่ที่อาจส่งผลกระทบต่อระบบและกระบวนการที่สำคัญ รวมถึงความเสี่ยงที่เกิดจากกระบวนการปฏิบัติงาน บุคลากร หรือปัจจัยภายนอก โดยการระบุว่ามีความเสี่ยง จากการโจมตีทางไซเบอร์ต่างๆ ต่อระบบเครือข่ายหลัก หรือช่องโหว่จากการใช้งานซอฟต์แวร์ที่ไม่ได้รับการอัปเดต

2) การจัดทำรายการความเสี่ยง

ขั้นตอน : จัดทำรายการความเสี่ยงที่ระบุได้ โดยจัดลำดับความสำคัญตามความรุนแรงและโอกาสที่ความ เสี่ยงจะเกิดขึ้น โดยจัดลำดับความเสี่ยงที่สูงสุดเป็นความเสี่ยงจากการโจมตีทางไซเบอร์ ที่อาจทำให้ระบบ เครือข่ายล่มเป็นเวลานาน

1. การระบุความเสี่ยง (Risk Identification)

1) การระบุภัยคุกคามและช่องโหว่

ขั้นตอน : ระบุภัยคุกคามทางไซเบอร์และช่องโหว่ที่อาจส่งผลกระทบต่อระบบและกระบวนการที่สำคัญ รวมถึงความเสี่ยงที่เกิดจากกระบวนการปฏิบัติงาน บุคลากร หรือปัจจัยภายนอก โดยการระบุว่ามีความเสี่ยง จากการโจมตีทางไซเบอร์ต่างๆ ต่อระบบเครือข่ายหลัก หรือช่องโหว่จากการใช้งานซอฟต์แวร์ที่ไม่ได้รับการอัปเดต

2) การจัดทำรายการความเสี่ยง

ขั้นตอน : จัดทำรายการความเสี่ยงที่ระบุได้ โดยจัดลำดับความสำคัญตามความรุนแรงและโอกาสที่ความ เสี่ยงจะเกิดขึ้น โดยจัดลำดับความเสี่ยงที่สูงสุดเป็นความเสี่ยงจากการโจมตีทางไซเบอร์ ที่อาจทำให้ระบบ เครือข่ายล่มเป็นเวลานาน

2. การวิเคราะห์ความเสี่ยง (Risk Analysis)

1) การวิเคราะห์ผลกระทบและโอกาส

ขั้นตอน : วิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงที่ระบุและโอกาสที่ความเสี่ยงจะเกิดขึ้น รวมถึง ผลกระทบทางการเงิน ด้านชื่อเสียง ด้านกฎหมาย และอื่น ๆ โดยการวิเคราะห์ว่าการโจมตีทางไซเบอร์ อาจ ทำให้เว็บไซต์ขององค์กรไม่สามารถให้บริการได้ และเกิดความเสียหายทางการเงินและชื่อเสียงอย่างมาก

2) การจัดลำดับความสำคัญของความเสี่ยง

ขั้นตอน : จัดลำดับความสำคัญของความเสี่ยงตามผลกระทบและโอกาสที่เกิดขึ้น เพื่อกำหนดลำดับการ ดำเนินการจัดการความเสี่ยง โดยความเสี่ยงจากการโจมตีทางไซเบอร์ ถูกจัดลำดับเป็นความเสี่ยงสูงสุด เนื่องจากมีผลกระทบทางการเงินและชื่อเสียงสูง

3. การประเมินค่าความเสี่ยง (Risk Evaluation)

1) การประเมินโอกาสและผลกระทบ

ขั้นตอน : ประเมินโอกาสที่ความเสี่ยงจะเกิดขึ้นและผลกระทบต่อการดำเนินงานและธุรกิจรวมถึงกำหนด ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) โดยประเมินว่าโอกาสที่การโจมตีทางไซเบอร์จะเกิดขึ้นมีสูง และผลกระทบที่เกิดขึ้นอาจทำให้ระบบหยุดทำงานเป็นเวลานาน ซึ่งเกินกว่าระดับความเสี่ยงที่ยอมรับได้ขององค์กร

4. การจัดการความเสี่ยง (Risk Treatment)

1) การกำหนดแนวทางการจัดการความเสี่ยง

ขั้นตอน : กำหนดแนวทางจัดการความเสี่ยง เช่น การหลีกเลี่ยงความเสี่ยง การลดความเสี่ยง การโอนความเสี่ยง หรือการยอมรับความเสี่ยง โดยคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยง และผลประโยชน์ที่คาดว่าจะได้รับ

2) การกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (KRI)

ขั้นตอน : กำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (KRI) เพื่อใช้ติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง

5. การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

1) การติดตามความเสี่ยงอย่างต่อเนื่อง

ขั้นตอน : มีกระบวนการที่มีประสิทธิภาพในการติดตามความเสี่ยง และทบทวนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อให้แน่ใจว่าความเสี่ยงยังคงอยู่ภายใต้ระดับที่ยอมรับได้ และมีรายงานผลให้กับคณะทำงานที่เกี่ยวข้องรับทราบ

2) การทบทวนและปรับปรุงแนวทางการจัดการความเสี่ยง

ขั้นตอน : ทบทวนแนวทางการจัดการความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ เพื่อให้แน่ใจว่ายังคงมีประสิทธิภาพในการจัดการความเสี่ยง หรือหลังจากเกิดการโจมตีทางไซเบอร์ให้ทำการทบทวนแนวทางการป้องกัน และเสนอแนะการปรับปรุงแนวทางป้องกันเพิ่มเติม

6. การรายงานความเสี่ยง (Risk Assessment Reporting)

1) การรายงานระดับความเสี่ยงและผลการจัดการความเสี่ยง

ขั้นตอน : รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ

2) การทบทวนและปรับปรุงระเบียบวิธีปฏิบัติ

ขั้นตอน : ทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์อย่างมีนัยสำคัญ

2.5 การจัดทำทะเบียนความเสี่ยง (Risk Register)

ขั้นตอน : จัดทำและปรับปรุงทะเบียนความเสี่ยงหลังการประเมินความเสี่ยงทุกครั้ง โดยรายละเอียดที่ต้องบันทึกในทะเบียนความเสี่ยง ได้แก่

- วันที่ระบุความเสี่ยง (Date the Risk is Identified)

- คำอธิบายของความเสี่ยง (Description of the Risk)
- โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- การจัดการความเสี่ยง (Risk Treatment)
- เจ้าของความเสี่ยง (Risk Owner)
- สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
- ความเสี่ยงที่เหลือ (Residual Risk)

2.6 การพัฒนากลยุทธ์เพื่อจัดการความเสี่ยง (Risk Management Strategy)

1. การพัฒนากลยุทธ์การเพื่อจัดการความเสี่ยง

ขั้นตอน : พัฒนากลยุทธ์ในการจัดการความเสี่ยงที่เหมาะสมเพื่อลดผลกระทบจากความเสี่ยงให้ อยู่ในระดับที่ยอมรับได้ โดยอาจใช้วิธีการต่าง ๆ เช่น การป้องกันความเสี่ยง (Risk Avoidance) การลดความเสี่ยง (Risk Reduction) การถ่ายโอนความเสี่ยง (Risk Transfer) หรือการยอมรับความเสี่ยง (Risk Acceptance) โดยการใช้ การเข้ารหัสข้อมูลเพื่อลดความเสี่ยงจากการถูกโจมตีแบบ Man-in-the-Middle6.2 การปรับปรุงทะเบียนเมื่อมีการเปลี่ยนแปลง

2. การติดตามและปรับปรุงกลยุทธ์การจัดการความเสี่ยง

ขั้นตอน : ติดตามผลการจัดการความเสี่ยงและปรับปรุงกลยุทธ์การจัดการความเสี่ยงตามความเหมาะสม โดยพิจารณาจากสถานะของการจัดการความเสี่ยงและความเสี่ยงที่เหลือ (Residual Risk) และดำเนินการปรับปรุงมาตรการความปลอดภัยเพิ่มเติม หลังจากพบว่าการควบคุมความเสี่ยงที่ใช้อยู่ยังไม่เพียงพอ

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปี หรือตามความจำเป็นเพื่อให้มันใจในประสิทธิภาพ และถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ทะเบียนความเสี่ยง (Risk Register)
2. เอกสารการประเมินความเสี่ยงและการจัดการความเสี่ยง (Risk Assessment and Risk Treatment)
3. ดัชนีวัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI)
4. รายงานการประเมินความเสี่ยง (Risk Assessment Report), NIST SP 800-30

3. กระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.3.1, ข้อ 21.3.3, ข้อ 21.3.4, ข้อ 21.3.5, ข้อ 21.3.6, ข้อ 21.3.7, ข้อ 21.3.8, ข้อ 21.3.9, ข้อ 21.3.10]

3.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อระบุและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศ (IT) และระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS) ที่เกี่ยวข้องกับบริการที่สำคัญของ องค์กร รวมถึงการดำเนินการทดสอบเจาะระบบเพื่อประเมินความเสี่ยงและการควบคุมความปลอดภัย

3.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมการประเมินช่องโหว่และการทดสอบเจาะระบบสำหรับระบบเทคโนโลยี สารสนเทศและระบบควบคุมเครื่องจักรในอุตสาหกรรมที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร โดยรวมถึง การตรวจสอบความมั่นคงปลอดภัยของโฮสต์ เครือข่าย สถาปัตยกรรม และแอปพลิเคชัน

3.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1. ทีมความมั่นคงปลอดภัยสารสนเทศ (IT Security Team) : รับผิดชอบในการดำเนินการประเมินช่องโหว่และการทดสอบเจาะระบบ รวมถึงการติดตามและแก้ไขช่องโหว่ที่พบ

2. ผู้ให้บริการทดสอบเจาะระบบ (Penetration Testing Service Providers): รับผิดชอบในการดำเนินการทดสอบเจาะระบบตามขอบเขตที่กำหนด โดยต้องมีการรับรองและได้รับ ประกาศนียบัตรที่เป็นที่ยอมรับในอุตสาหกรรม

3. ผู้บริหาร (Top Management): รับผิดชอบในการอนุมัติและสนับสนุนการดำเนินการตามกระบวนการ รวมถึงการตรวจสอบและประเมินผล

3.4 การประเมินช่องโหว่ (Vulnerability Assessment)

1. การประเมินช่องโหว่ตามหลักการบริหารความเสี่ยง

ขั้นตอน : ดำเนินการประเมินช่องโหว่ของระบบเทคโนโลยีสารสนเทศและระบบควบคุมเครื่องจักรในอุตสาหกรรมตามหลักการบริหารความเสี่ยงที่องค์กรกำหนด เพื่อระบุจุดอ่อนและ การควบคุมที่จำเป็น โดยการประเมินความเสี่ยงความมั่นคงปลอดภัยของโฮสต์เพื่อหาช่องโหว่ ที่อาจถูกโจมตีได้

2. การตรวจสอบขอบเขตของการประเมินช่องโหว่

ขั้นตอน : ตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่ครอบคลุมถึงการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม โดยการตรวจสอบว่าได้ทำการประเมินความมั่นคงปลอดภัยของเครือข่ายทั้งหมดที่เชื่อมต่อกับระบบที่สำคัญ

3. การประเมินช่องโหว่ก่อนการเปลี่ยนแปลงระบบสำคัญ

ขั้นตอน : ทำการประเมินช่องโหว่ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบที่สำคัญหรือเชื่อมต่อระบบใหม่ รวมถึงการเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ และการปรับเปลี่ยน เทคโนโลยี โดยการประเมินช่องโหว่ก่อนการอัปเกรดซอฟต์แวร์ในระบบควบคุมเครื่องจักรใน อุตสาหกรรม

3.5 การทดสอบเจาะระบบ (Penetration Testing)

1. การดำเนินการทดสอบเจาะระบบตามความเสี่ยง

ขั้นตอน : พิจารณาดำเนินการทดสอบเจาะระบบสำหรับบริการที่สำคัญ โดยเฉพาะอย่างยิ่ง ระบบที่เชื่อมต่อกับอินเทอร์เน็ต ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบ ที่อาจเกิดขึ้นจากการทดสอบ โดยเฉพาะการทดสอบเจาะระบบของแอปพลิเคชันที่มีการเข้าถึง จากภายนอกผ่านอินเทอร์เน็ต

2. การตรวจสอบขอบเขตของการทดสอบเจาะระบบ

ขั้นตอน : ตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบครอบคลุมถึงโฮสต์ เครือข่าย และแอปพลิเคชันของระบบที่เป็นบริการที่สำคัญ โดยเฉพาะระบบที่เชื่อมต่อกับ อินเทอร์เน็ตโดยตรง

3. ความถี่ในการทดสอบเจาะระบบ

ขั้นตอน : พิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่สำคัญ เพื่อประเมินความถูกต้องของระบบรักษาความมั่นคงปลอดภัย ตัวอย่างเช่น การทดสอบเจาะระบบของระบบควบคุมเครื่องจักรหลังการปรับปรุงเทคโนโลยีใหม่

4. การรับรองผู้ทดสอบเจาะระบบ

ขั้นตอน : ตรวจสอบให้แน่ใจว่าผู้ทดสอบเจาะระบบมีการรับรองและประกาศนียบัตรที่เป็นที่ ยอมรับในอุตสาหกรรม และผู้ทดสอบต้องเป็นอิสระจากระบบที่ทำการทดสอบ เช่น การใช้ผู้ ทดสอบเจาะระบบที่ได้รับการรับรองจากองค์กรมาตรฐานสากล เช่น CEH – Certificated Ethical Hacker, OSCP - Offensive Security Certificated Professional

5. การควบคุมการทดสอบเจาะระบบโดยองค์กร/หน่วยงานที่รับผิดชอบ

ขั้นตอน : ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดดำเนินการภายใต้การดูแลขององค์กร/หน่วยงานที่รับผิดชอบ โดยต้องมีทีมงานภายในองค์กรควบคุมและตรวจสอบการทดสอบเจาะระบบที่ดำเนินการโดยผู้ให้บริการภายนอก

3.6 การติดตามและจัดการช่องโหว่ (Vulnerability Management)

1. การติดตามและจัดการช่องโหว่

ขั้นตอน : สร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่าง เพียงพอ ซึ่งมีการใช้ระบบติดตามการแก้ไขช่องโหว่ (Vulnerability Management System) เพื่อรับประกันว่าช่องโหว่ทั้งหมดถูกแก้ไขตามกำหนดเวลา

3.7 การรายงานผลการทดสอบเจาะระบบ (Penetration Testing Reporting)

ขั้นตอน : หากได้รับการร้องขอจากหน่วยงานควบคุมหรือกำกับดูแล ทางหน่วยงานโครงสร้างพื้นฐาน สำคัญต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบภายใน 30 วันหลังจากได้รับการร้องขอโดยรูปแบบของรายงานให้เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนด

ต่อไปนี้เป็นกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Process)

1. การประเมินช่องโหว่ (Vulnerability Assessment)

1.1 ขอบเขตของการประเมินช่องโหว่

- ประเมินช่องโหว่ของระบบเทคโนโลยีสารสนเทศ (IT System) ที่ให้บริการสำคัญ
- ประเมินช่องโหว่ของระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

1.2 รายการที่ต้องตรวจสอบ

- การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
- การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
- การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

1.3 ระยะเวลาในการดำเนินการ

- ดำเนินการประเมินอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่สำคัญ

2. การทดสอบเจาะระบบ (Penetration Testing)

2.1 ขอบเขตของการทดสอบเจาะระบบ

- ทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ
- ทดสอบเจาะระบบของระบบที่เชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing Systems)

2.2 การทดสอบเจาะระบบเป็นประจำ

- พิจารณาดำเนินการทดสอบเจาะระบบ ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ หรือการเปลี่ยนเทคโนโลยี

2.3 การรับรองผู้ทดสอบเจาะระบบ

- ผู้ทดสอบเจาะระบบต้องมีการรับรองและได้รับประกาศนียบัตรที่เป็นที่ยอมรับในอุตสาหกรรม

2.4 การดำเนินการทดสอบเจาะระบบ

- ทดสอบเจาะระบบทั้งหมดดำเนินการภายใต้การดูแลขององค์กร/หน่วยงาน และควบคุมโดยผู้ทดสอบที่เป็นอิสระจากระบบที่ถูกทดสอบ

3. การติดตามและจัดการกับช่องโหว่ (Vulnerability Management)

3.1 กระบวนการติดตาม

- สร้างกระบวนการเพื่อติดตามและจัดการช่องโหว่ที่ระบุในผลการประเมินและการทดสอบเจาะระบบ

3.2 การแก้ไขช่องโหว่

- ตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

3.3 รายงานผลการทดสอบ

- หากได้รับการร้องขอจาก กกม. หรือสำนักงาน หน่วยงานโครงสร้างพื้นฐานสำคัญต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบภายใน 30 วัน หลังจากได้รับหนังสือร้องขอ

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. รายงาน/ผลการทดสอบเจาะระบ
2. รายงาน/ผลการประเมินช่องโหว่
3. เอกสารการประเมินความเสี่ยง ทั้ง 3 ด้าน (Host Security, Network Security, Architecture Security)
4. Vulnerability Management System

4. กระบวนการการเจาะระบบ (Penetration Testing Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.3.1, ข้อ 21.3.3, ข้อ 21.3.4, ข้อ 21.3.5, ข้อ 21.3.6, ข้อ 21.3.7, ข้อ 21.3.8, ข้อ 21.3.9, ข้อ 21.3.10]

4.1 วัตถุประสงค์ (Objective)

การทดสอบเจาะระบบมีวัตถุประสงค์เพื่อระบุและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ (IT System) และระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS) เพื่อให้สามารถ ดำเนินการแก้ไขปัญหาเหล่านั้นได้ก่อนที่จะถูกโจมตีจริง

4.2 ขอบเขตของการทดสอบ (Scope of Testing)

การทดสอบจะครอบคลุมระบบและส่วนประกอบต่อไปนี้

- ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) Systems)
- ระบบควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control Systems: ICS)
- โครงสร้างพื้นฐานทางเครือข่าย (Network Infrastructure)
- แอปพลิเคชันและบริการที่เชื่อมต่ออินเทอร์เน็ต (Internet-facing Applications and Services)
- ฐานข้อมูล (Database)
- ระบบควบคุมการเข้าถึง (Access Control System)

4.3 ทีมที่รับผิดชอบ (Responsibility)

1) ผู้ทดสอบเจาะระบบ (Penetration Tester) : ทีมความมั่นคงปลอดภัยหรือผู้ให้บริการภายนอกที่ได้รับการรับรอง

2) ผู้ประสานงาน (Coordinator) : ผู้จัดการหรือหัวหน้าทีมที่มีหน้าที่ดูแลและประสานงานกับทีมต่าง ๆ

3) เจ้าของระบบ (System Owner) : เจ้าของหรือผู้ดูแลระบบที่ได้รับการทดสอบ

4.4 ขั้นตอนการทดสอบ (Testing Procedure)

1. การวางแผนและการเตรียมการ (Planning and Preparation)

1) กำหนดขอบเขตการทดสอบ (Define Scope): ระบุระบบและส่วนประกอบที่ต้องการทดสอบ เช่น ระบบฐานข้อมูล, ระบบควบคุมเครื่องจักร, หรือระบบเครือข่าย โดยในการ ทดสอบนี้ ขอบเขตครอบคลุมถึงระบบฐานข้อมูลของลูกค้า ระบบเครือข่ายที่ใช้ในการสื่อสาร และแอปพลิเคชันที่เชื่อมต่อกับอินเทอร์เน็ต

2) จัดทำเอกสารการอนุญาต (Obtain Authorization): ขอกำหนดการอนุญาตจากเจ้าของระบบหรือผู้บริหารที่เกี่ยวข้องเพื่อดำเนินการทดสอบ ซึ่งต้องได้รับอนุญาตจากฝ่าย IT และผู้จัดการฝ่ายความมั่นคงสารสนเทศในการดำเนินการทดสอบเจาะระบบ

3) เตรียมเครื่องมือและทรัพยากร (Prepare Tools and Resources): ตรวจสอบเครื่องมือที่จะใช้ในการทดสอบให้มีความพร้อมใช้ เช่น เครื่องมือสำหรับการสแกนช่องโหว่ (Nessus) และเครื่องมือสำหรับการทดสอบการเจาะระบบ (Metasploit)

2. การสแกนและการรวบรวมข้อมูล (Scanning and Information Gathering)

1) สแกนหาช่องโหว่ (Vulnerability Scanning): ใช้เครื่องมือสแกนหาช่องโหว่ (Nessus) ในระบบเครือข่ายหรือเซิร์ฟเวอร์ฐานข้อมูลเพื่อหาช่องโหว่ การตั้งค่าการเข้าถึง

2) รวบรวมข้อมูลเกี่ยวกับระบบเป้าหมาย (Information Gathering): รวบรวมข้อมูลที่จำเป็นเกี่ยวกับระบบที่กำลังทดสอบ เช่น ที่อยู่ IP, โดเมน, และบริการที่เปิดใช้งาน รวมถึงพอร์ตที่เปิดใช้งาน

3. การวิเคราะห์และการทดสอบช่องโหว่ (Analysis and Exploitation)

1) วิเคราะห์ผลการสแกน (Analyze Scan Results): ตรวจสอบผลการสแกนเพื่อระบุช่องโหว่ที่ควรดำเนินการทดสอบเพิ่มเติม เช่น มีช่องโหว่ในระบบฐานข้อมูลที่เปิดให้เข้าถึงได้ หรือไม่ โดยไม่ได้รับอนุญาตผ่านพอร์ตที่ไม่ได้เข้ารหัส

2) ทดสอบการเจาะระบบ (Exploitation Testing): ดำเนินการทดสอบเจาะระบบ โดยใช้เครื่องมือเฉพาะเพื่อยืนยันและประเมินความรุนแรงของช่องโหว่ที่พบ โดยใช้เครื่องมือMetasploit ในการเจาะระบบฐานข้อมูลผ่านช่องโหว่ที่พบ และดูว่าสามารถเข้าถึงข้อมูล สำคัญได้หรือไม่

4. การรายงานและการสรุปผล (Reporting and Conclusion)

1) จัดทำรายงานผลการทดสอบ (Create Testing Report): สรุปผลการทดสอบที่ดำเนินการ ช่องโหว่ที่พบ ความรุนแรง และแนวทางการแก้ไข ซึ่งการจัดทำรายงานนั้นต้องระบุว่าได้พบช่องโหว่ที่รุนแรงในระบบฐานข้อมูลหรืออื่นๆและพร้อมการนำเสนอการ ปรับปรุง ด้วย เช่น การตั้งค่าไฟร์วอลล์และการเข้ารหัสข้อมูล เป็นต้น

2) เสนอแนะการแก้ไข (Provide Remediation Recommendations): ให้ คำแนะนำเกี่ยวกับวิธีการแก้ไขช่องโหว่ที่พบในการทดสอบ

- สรุปผลการทดสอบกับผู้เกี่ยวข้อง (Conclude Testing with Stakeholders): สรุปผลการทดสอบและข้อเสนอแนะให้กับทีมงานที่เกี่ยวข้องและ เจ้าของระบบรับทราบ หรืออาจจัดประชุมสรุปผลการทดสอบกับทีม IT และผู้จัดการฝ่าย ความมั่นคงสารสนเทศ ก็ได้ เพื่อดำเนินการแก้ไขช่องโหว่ตามข้อเสนอแนะ

5. การติดตามผลการแก้ไข (Follow-Up on Remediation)

ตรวจสอบการแก้ไขช่องโหว่ (Verify Remediation): ทดสอบช่องโหว่ที่ได้รับการแก้ไขแล้วอีกครั้ง เพื่อยืนยันว่าได้ทำการแก้ไขอย่างถูกต้องและไม่มีความเสี่ยงอีกต่อไป

4.5 สรุปและการปิดโครงการ (Summary and Closure)

1. ปิดโครงการทดสอบเจาะระบบ (Project Closure): สรุปโครงการและปิดโครงการหลังจาก ได้ดำเนินการทดสอบเจาะระบบและแก้ไขช่องโหว่ทั้งหมดแล้ว

2. จัดเก็บเอกสาร (Documentation Storage): จัดเก็บรายงานผลการทดสอบและเอกสารที่เกี่ยวข้องอย่างปลอดภัย เพื่อใช้เป็นข้อมูลอ้างอิงในอนาคต

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนรวมถึงขอบเขตการทดสอบเจาะระบบ
2. เอกสารที่ได้รับการอนุญาตในการเจาะระบบ
3. ผลการทดสอบช่องโหว่
4. รายงานผลการทดสอบ
5. รายงานผลการติดตามการแก้ไข
6. เอกสารสรุปปิดโครงการ

5. กระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.4.1, ข้อ 21.4.2, ข้อ 21.4.3, ข้อ 21.4.4]

5.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าผู้ให้บริการภายนอกที่เข้ามาเกี่ยวข้องกับบริการที่สำคัญของ องค์กรสามารถปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด และเพื่อป้องกันหรือลด ความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการภายนอก

5.2 ขอบเขตของการทดสอบ (Scope of Testing)

กระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าผู้ให้บริการภายนอกที่เข้ามาเกี่ยวข้องกับบริการที่สำคัญขององค์กรสามารถปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด และเพื่อป้องกัน หรือลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการภายนอก

5.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1. ผู้บริหาร (Top Management) : รับผิดชอบในการกำกับดูแลและตรวจสอบให้แน่ใจว่ามีการจัดการผู้ให้ บริการภายนอกอย่างเหมาะสมและปฏิบัติ ตาม พรบ ไซเบอร์ รวมถึงการอนุมัติข้อตกลงและสัญญาที่เกี่ยวข้อง

2. ทีมจัดการผู้ให้บริการภายนอก (Third Party Management Team) : รับผิดชอบในการดำเนินการตาม กระบวนการทั้งหมดที่เกี่ยวข้องกับผู้ให้บริการภายนอก รวมถึงการกำหนดข้อกำหนดการตรวจสอบ และการเจรจาต่อรองสัญญา

3. ผู้ให้บริการภายนอก (Third Party Providers) : มีหน้าที่ในการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในสัญญาหรือข้อตกลงกับองค์กร

5.4 การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Requirements)

1. การกำหนดข้อกำหนดในข้อตกลงระดับการให้บริการ (SLA) หรือสัญญากับผู้ให้บริการภายนอก

ขั้นตอน : สร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่าง เพียงพอ ซึ่งมีการใช้ระบบติดตามการแก้ไขช่องโหว่ (Vulnerability Management System) เพื่อรับประกันว่าช่องโหว่ทั้งหมดถูกแก้ไขตามกำหนดเวลา

2. ประเภทของผู้ให้บริการภายนอก

ขั้นตอน : ระบุประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญขององค์กร โดยพิจารณาความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ด้วย เนื่องจากอาจมีการเข้าถึงข้อมูลที่มีความสำคัญสูงขององค์กร

3. ภาระหน้าที่ของผู้ให้บริการภายนอก

ขั้นตอน : ระบุภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญขององค์กร จากภัยคุกคามทางไซเบอร์ เช่น ผู้ให้บริการภายนอกต้องมีตรวจสอบระบบความปลอดภัยของตนเองอย่างสม่ำเสมอ หรือดำเนินการอัปเดตระบบรักษาความปลอดภัยทุกครั้งที่มีการเปลี่ยนแปลงเทคโนโลยีให้รับทราบ

4. การจัดการความเสี่ยงในห่วงโซ่อุปทาน (Supply Chain Risk Management)

ขั้นตอน : ระบุความเสี่ยงที่เกี่ยวข้องกับบริการ และห่วงโซ่อุปทานของผลิตภัณฑ์ และกำหนดมาตรการในการควบคุมความเสี่ยงเหล่านี้ โดยการการตรวจสอบแหล่งที่มาของการบริการในผลิตภัณฑ์ที่ผู้ให้บริการภายนอกจัดหามาให้ เพื่อป้องกันการใช้ส่วนประกอบหรือส่วนที่เกี่ยวข้องที่ไม่ได้มาตรฐานหรือมีความเสี่ยง

5. สิทธิ์ในการตรวจสอบ (Audit Rights)

ขั้นตอน : ระบุสิทธิ์ขององค์กรในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการปฏิบัติตามข้อกำหนดที่ระบุไว้ในสัญญา

5.5 การตรวจสอบความถูกต้องและความสอดคล้อง (Verification and Compliance)

1. การตรวจสอบความถูกต้องของผู้ให้บริการภายนอก

ขั้นตอน : ระบุสิทธิ์ขององค์กรในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการปฏิบัติตามข้อกำหนดที่ระบุไว้ในสัญญา

2. การเจรจาต่อรองเงื่อนไขของสัญญาจ้าง

ขั้นตอน : พิจารณาเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับข้อกำหนดทางกฎหมายปัจจุบันหรือข้อบังคับใหม่ที่อาจเกิดขึ้นในอนาคต เช่น มีการประกาศใช้กฎหมายใหม่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

5.6 การติดตามและปรับปรุงกระบวนการ (Monitoring and Process Improvement)

ขั้นตอน : ดำเนินการติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างสม่ำเสมอ และปรับปรุงกระบวนการจัดการผู้ให้บริการตามความเหมาะสม เพื่อให้มั่นใจว่าการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ โดยต้องมีการจัดทำรายงานผลการตรวจสอบกับผู้ให้บริการภายนอกเป็นรายไตรมาส

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ข้อตกลงระดับการให้บริการ (SLA)
2. เงื่อนไขของสัญญากับผู้ให้บริการภายนอก
3. หลักฐานการทำการประเมินความเสี่ยงไซเบอร์ที่เกี่ยวข้องกับบริการและห่วงโซ่ อุปทานผลิตภัณฑ์
4. หลักฐานการทำการตรวจสอบระบบความมั่นคงปลอดภัยทางไซเบอร์ของผู้ให้บริการ ภายนอก
5. ใบรับรองตามมาตรฐานสากลต่างๆ เช่น ISO/IEC 27001 (ISMS), ISO/IEC 29110 (Software Engineer), ISO 9001 (Quality), ISO 14001 (Environment), ISO 45001 (Safety)
6. ใบรับรองทางไซเบอร์ เช่น NIST Cybersecurity Management System

การป้องกัน
(Protect)

กระบวนการการควบคุมการเข้าถึง
(Access Control Procedure)

1. กระบวนการการจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.43), ประมวลและกรอบ [ข้อ 22.1.1, ข้อ 22.1.2, ข้อ 22.1.3, ข้อ22.1.4]

1.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อการจัดการตัวตนและการควบคุมกำกับดูแลการเข้าถึงบริการที่สำคัญขององค์กร ทั้งนี้เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต รักษาความมั่นคงปลอดภัยไซเบอร์ และให้มั่นใจว่าการบริหาร จัดการตัวตนของบุคลากรเป็นไปอย่างมีประสิทธิภาพ

1.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการจัดการตัวตนและการควบคุมกำกับดูแลการเข้าถึง สำหรับบุคลากร อุปกรณ์ และอินเทอร์เฟซ รวมถึงการตรวจสอบและจัดเก็บบันทึกการเข้าถึงบริการที่สำคัญขององค์กร เพื่อให้แน่ใจว่า การเข้าถึงเหล่านี้เป็นไปตามข้อกำหนดที่กำหนดไว้ นอกจากนี้ยังรวมถึงการบริหารจัดการวงจรชีวิตของตัวตน ในระบบ (Identity Lifecycle Management)

1.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management) : กำกับดูแลให้มีนโยบายและแนวปฏิบัติในการจัดการตัวตน และการควบคุมการเข้าถึง

2) ผู้ดูแลระบบ (System Administrators) : รับผิดชอบการจัดการบัญชีผู้ใช้ กำหนดสิทธิ์และตรวจสอบการเข้าถึงระบบเป็นประจำ

3) พนักงาน (Employee) : ปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการเข้าถึงบริการที่สำคัญขององค์กร

1.4 การจัดการตัวตน (Identity Management)

1) การสร้างตัวตน (Identity Creation)

ขั้นตอน

- พิจารณาเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับข้อกำหนดทางกฎหมายปัจจุบันหรือข้อบังคับใหม่ที่อาจเกิดขึ้นในอนาคต เช่น มีการประกาศใช้กฎหมายใหม่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

- ใช้การตรวจสอบตัวตนสองปัจจัย (Two-Factor Authentication) ในการ ลงทะเบียนและเข้าใช้งานระบบที่มีข้อมูลสำคัญ

2) การบริหารวงจรชีวิตตัวตน (Identity Lifecycle Management)

ขั้นตอน

- มีการกำหนดวงจรชีวิตของตัวตนในระบบ ตั้งแต่การลงทะเบียน การใช้งาน การปรับเปลี่ยนสิทธิ์ จนถึงการยกเลิกการเข้าถึงเมื่อบุคลากรออกจากองค์กร
- ตรวจสอบสิทธิ์การเข้าถึงของพนักงานทุก 6 เดือนเพื่อให้แน่ใจว่าสอดคล้องกับหน้าที่งาน

3) การยกเลิกตัวตน (Identity Deactivation)

ขั้นตอน

- เมื่อพนักงานลาออกหรือไม่มีความจำเป็นต้องเข้าถึงระบบ ระบบต้องดำเนินการยกเลิกบัญชีผู้ใช้งานภายใน 24 ชั่วโมง
- ตรวจสอบให้แน่ใจว่าไม่มีบัญชีที่ไม่ได้ใช้งานหรือบัญชีซ้ำซ้อนในระบบ

1.5 การจำกัดการเข้าถึง (Access Restrictions)

1) การจำกัดการเข้าถึงบริการที่สำคัญ

ขั้นตอน

- การเข้าถึงบริการที่สำคัญถูกจำกัดเฉพาะบุคลากรที่ได้รับอนุญาต อุปกรณ์ และอินเทอร์เฟซที่ได้รับอนุญาตเท่านั้น
- ระบบต้องมีการตรวจสอบสิทธิ์การเข้าถึงเป็นระยะเพื่อให้แน่ใจว่าผู้ใช้ยังคงมีความจำเป็นในการเข้าถึง

2) การใช้เทคนิคการตรวจสอบสิทธิ์

ขั้นตอน

- กำหนดให้ใช้การตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-Factor Authentication, MFA) ในการเข้าถึงระบบที่สำคัญ
- ใช้มาตรการเข้ารหัสข้อมูลการยืนยันตัวตนเพื่อป้องกันการถูกดักฟังหรือขโมยข้อมูล

1.6 การบันทึกและตรวจสอบการเข้าถึง (Access Logging and Monitoring)

1) การเก็บรักษาบันทึกการเข้าถึง

ขั้นตอน

- เก็บรักษาบันทึกของการเข้าถึงทั้งหมดและตรวจสอบเป็นระยะเพื่อหากิจกรรมที่ผิดปกติ
- ใช้ระบบบันทึกการเข้าถึงอัตโนมัติและแจ้งเตือนเมื่อมีพฤติกรรมที่ผิดปกติ

2) ความสม่ำเสมอในการตรวจสอบบันทึก

ขั้นตอน

- ตรวจสอบบันทึกการเข้าถึงของระบบเครือข่ายภายในทุกวัน และการตรวจสอบบันทึกการเข้าถึงข้อมูลสำคัญอย่างน้อยรายสัปดาห์

1.7 การควบคุมการเข้าถึงอินเทอร์เฟซและการเข้าถึงทางลอจิคอล (Interface and Logical Access Control)

1) การควบคุมการเข้าถึงอินเทอร์เฟซ

ขั้นตอน

- ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ เช่น USB และพอร์ตอนุกรม ต้องถูกควบคุมและดำเนินการภายใต้การดูแลขององค์กรที่เกี่ยวข้องเท่านั้น
- ตั้งค่าข้อจำกัดในการใช้งานพอร์ต USB บนอุปกรณ์คอมพิวเตอร์ที่ใช้ในองค์กร

2) การเข้าถึงทางลอจิคอล

ขั้นตอน

- กำกับดูแลการเข้าถึงทางลอจิคอลของบริการที่สำคัญ โดยให้ดำเนินการในสถานที่ที่ได้รับอนุญาตและอยู่ภายใต้การควบคุมขององค์กร
- กำหนดให้การเข้าถึงระบบจัดการข้อมูลต้องทำจากภายในองค์กรเท่านั้น และห้ามเข้าถึงจากภายนอกองค์กร

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. หลักฐาน Logs of Access
2. หลักฐานสิทธิ์การเข้าถึงระบบ (User Permission Matrix)
3. หลักฐานการจัดการตัวตน (Identity Users)

กระบวนการการทำให้ระบบมีความแข็งแกร่ง
(System Hardening Procedure)

2. นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย
(Security Baseline Configuration Standards Policy)

อ้างอิง : นโยบาย (ข้อ 3.1), ประมวลและกรอบ [ข้อ 22.2.1, ข้อ 22.2.2, ข้อ 22.2.3, ข้อ22.2.4]

2.1 วัตถุประสงค์ (Objective)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับการกำหนดค่าระบบสารสนเทศเพื่อป้องกันความเสี่ยงและลดช่องโหว่ที่อาจเกิดขึ้นจากการกำหนดค่าระบบที่ไม่ปลอดภัย

2.2 ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงการกำหนดค่าระบบทั้งหมดในองค์กร รวมถึงเซิร์ฟเวอร์, คอมพิวเตอร์, อุปกรณ์ เครือข่าย และแอปพลิเคชันที่ใช้งานภายในองค์กร

2.3 หลักการรักษาความมั่นคงปลอดภัย (Security Principles)

องค์กรต้องปฏิบัติตามหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

1) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

- ระบบฐานข้อมูลขององค์กรจะต้องถูกกำหนดให้พนักงานแต่ละคนเข้าถึงข้อมูลเฉพาะส่วนที่เกี่ยวข้องกับหน้าที่ของตนเท่านั้น เช่น เจ้าหน้าที่ฝ่ายการเงินจะสามารถเข้าถึงข้อมูลการเงินแต่ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลของพนักงานได้

2) การแบ่งแยกหน้าที่ (Separation of Duties)

- ในองค์กรนั้นจะต้องมีการแบ่งแยกหน้าที่กันอย่างชัดเจน

3) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

- องค์กรกำหนดให้ผู้ใช้ทุกคนต้องตั้งรหัสผ่านที่ประกอบด้วยอักษรพิมพ์ใหญ่, อักษรพิมพ์เล็ก, ตัวเลข และอักขระพิเศษ และต้องมีความยาวอย่างน้อย 12 ตัวอักษร

4) การลบบัญชีที่ไม่ได้ใช้

- บัญชีของพนักงานที่ลาออกจะถูกลบออกจากระบบภายใน 24 ชั่วโมงหลังจากที่พนักงานคนนั้นออกจากองค์กร เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

5) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น

- เซิร์ฟเวอร์ขององค์กรจะถูกกำหนดค่าให้ลบคอมไพเลอร์ (Compiler) และแอปพลิเคชันที่ไม่จำเป็น เช่น แอปพลิเคชันที่ใช้สำหรับการทดสอบหรือสนับสนุนจากผู้ให้บริการภายนอก เพื่อป้องกันการโจมตีที่อาจเกิดขึ้นจากช่องโหว่ในแอปพลิเคชันเหล่านั้น

6) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

- ในการตั้งค่าเครือข่ายขององค์กร พอร์ตที่ไม่ได้ใช้งาน เช่น พอร์ต FTP จะถูกปิดเพื่อป้องกัน การโจมตีที่อาจเกิดขึ้นจากการเข้าถึงผ่านพอร์ตเหล่านั้น

7) การป้องกันมัลแวร์ (Malware Protection)

- คอมพิวเตอร์ทุกเครื่องในองค์กรจะต้องติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์เป็นประจำรวมถึงมีการสแกนระบบแบบอัตโนมัติทุกสัปดาห์

8) การปรับปรุงซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัยของระบบ

- เซิร์ฟเวอร์ขององค์กรจะได้รับการอัปเดตซอฟต์แวร์และติดตั้งแพตช์ความมั่นคงปลอดภัยที่ ปล่อยออกมาโดยผู้ผลิตซอฟต์แวร์ภายใน 48 ชั่วโมงหลังจากที่แพตช์เหล่านั้นถูกปล่อยออกมา เพื่อป้องกันการโจมตีจากช่องโหว่ที่เป็นที่รู้จัก

2.4 การตรวจสอบและการปฏิบัติตามนโยบาย (Audit and Compliance)

องค์กรต้องดำเนินการตรวจสอบการปฏิบัติตามนโยบายนี้อย่างสม่ำเสมอ โดยการตรวจสอบการตั้งค่าระบบ และระบบ และการใช้งานสิทธิ์ต่าง ๆ และรายงานผลการตรวจสอบต่อผู้บริหารที่เกี่ยวข้องนโยบายนี้ต้องได้รับการทบทวนและปรับปรุงอย่างต่อเนื่องเพื่อให้สอดคล้องกับภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลงไป

2.5 การฝ่าฝืนนโยบาย (Policy Violations)

ผู้ใช้งานใดที่ฝ่าฝืนนโยบายนี้จะต้องได้รับการพิจารณาและอาจต้องรับโทษตามมาตรการที่กำหนดไว้ในกฎระเบียบขององค์กร

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามี การเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

3. กระบวนการการทำให้ระบบมีความแข็งแกร่ง (System Hardening Procedure)

อ้างอิง : นโยบาย (ข้อ 3.1), ประมวลและกรอบ [ข้อ 22.2.1, ข้อ 22.2.2, ข้อ 22.2.3, ข้อ22.2.4]

3.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อกำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่เกี่ยวข้องกับ บริการที่สำคัญขององค์กร เพื่อป้องกันภัยคุกคามทางไซเบอร์และรักษาความมั่นคงปลอดภัยของบริการที่สำคัญ

3.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการกำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่ เกี่ยวข้องกับบริการที่สำคัญขององค์กร

3.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management) : รับผิดชอบในการอนุมัติและกำกับดูแลการดำเนินการตามมาตรฐานการ กำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย

2) ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team) : รับผิดชอบในการพัฒนามาตรฐานการ กำหนดค่าขั้นต่ำ ตรวจสอบการปฏิบัติตามมาตรฐาน และดำเนินการตรวจสอบและปรับปรุงมาตรฐาน ตามความเหมาะสม

3) ผู้ใช้งานระบบ (System Users) : มีหน้าที่ในการปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการใช้ งานระบบตามมาตรฐานที่กำหนด

3.4 การกำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

1) การพัฒนามาตรฐานการกำหนดค่าขั้นต่ำ

ขั้นตอน: พัฒนามาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่เกี่ยวข้อง โดยให้สอดคล้องกับโปรไฟล์ ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยการกำหนดนโยบายการเข้าถึงที่ใช้หลักการ สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

2) องค์ประกอบหลักของมาตรฐานการกำหนดค่าขั้นต่ำ

ขั้นตอน: มาตรฐานการกำหนดค่าขั้นต่ำต้องครอบคลุมถึงองค์ประกอบความมั่นคงปลอดภัยที่สำคัญ เช่น

- สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

- การแบ่งแยกหน้าที่ (Separation of Duties)
- การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- การลบบัญชีที่ไม่ได้ใช้
- การลบบริการและแอปพลิเคชันที่ไม่จำเป็น
- การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
- การป้องกันมัลแวร์
- การอัปเดตซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัย

3) การใช้งานมาตรฐานการกำหนดค่าขั้นต่ำ

ขั้นตอน: ตรวจสอบให้แน่ใจว่ามาตรฐานการกำหนดค่าขั้นต่ำถูกใช้งานก่อนที่จะเชื่อมต่อทรัพย์สินใด ๆ หรือก่อนการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ โดยการตรวจสอบ มาตรฐานการกำหนดค่าของเซิร์ฟเวอร์ก่อนการนำไปใช้งานจริง

4) การตรวจสอบและปรับปรุงมาตรฐานการกำหนดค่าขั้นต่ำ

ขั้นตอน: ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ายังคงมี ประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ โดยการทบทวนและปรับปรุงมาตรฐานการ กำหนดค่าขั้นต่ำตามการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามใหม่ ๆ

3.5 การจัดการเปลี่ยนแปลง (Change Management Process)

การอนุญาตและตรวจสอบการเปลี่ยนแปลง

ขั้นตอน: จัดทำกระบวนการจัดการเปลี่ยนแปลงเพื่ออนุญาตและตรวจสอบความถูกต้องของ การเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน โดยการทบทวนการ เปลี่ยนแปลงระบบโดยคณะกรรมการความมั่นคงปลอดภัยก่อนที่จะอนุมัติการเปลี่ยนแปลง

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. นโยบายมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)
2. กระบวนการจัดการเปลี่ยนแปลง (Change Management Process)
3. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

4. กระบวนการจัดการเปลี่ยนแปลง (Change Management Process Procedure)

อ้างอิง : อ้างอิง : ประมวลและกรอบ [ข้อ 22.2.5]

4.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มี ต่อบริการที่สำคัญ รวมถึงการควบคุมการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นในระบบหรือกระบวนการขององค์กร เพื่อให้มั่นใจว่าการเปลี่ยนแปลงเหล่านั้นได้รับการดำเนินการอย่างเหมาะสม ลดความเสี่ยงที่อาจเกิดขึ้น และรักษาความมั่นคงปลอดภัยทางไซเบอร์ในการดำเนินงานขององค์กรหรือหน่วยงาน

4.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมการเปลี่ยนแปลงทุกประเภทสำหรับระบบปฏิบัติการ แอปพลิเคชัน และ อุปกรณ์เครือข่ายทั้งหมดในระบบ

4.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้ร้องขอการเปลี่ยนแปลง (Change Requester): รับผิดชอบในการระบุความจำเป็นในการเปลี่ยนแปลง และจัดทำเอกสารการร้องขอ

2) คณะกรรมการจัดการการเปลี่ยนแปลง (Change Advisory Board: CAB): รับผิดชอบในการประเมิน อนุมัติ หรือปฏิเสธการเปลี่ยนแปลง

3) ผู้ดำเนินการเปลี่ยนแปลง (Change Implementer): รับผิดชอบในการดำเนินการเปลี่ยนแปลงตามแผนที่ได้รับอนุมัติ

4.4 ขั้นตอนการจัดการเปลี่ยนแปลง (Change Management Process Steps)

1. การร้องขอการเปลี่ยนแปลง (Change Request)

1.1 ระบุความต้องการในการเปลี่ยนแปลง

ขั้นตอน : บุคลากรหรือหน่วยงานที่พบว่ามีความจำเป็นต้องเปลี่ยนแปลงระบบหรือกระบวนการจะต้องระบุความต้องการในการเปลี่ยนแปลง พร้อมเหตุผลและรายละเอียดที่ เกี่ยวข้อง เช่น ทีม IT ร้องขอการเปลี่ยนแปลงเพื่ออัปเดตซอฟต์แวร์ระบบให้เป็นเวอร์ชันล่าสุด เพื่อลดความเสี่ยงจากช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์

1.2 ส่งเอกสารการร้องขอ

ขั้นตอน : ผู้ร้องขอจัดทำเอกสารการร้องขอการเปลี่ยนแปลง (Change Request Document) ที่รวมถึงวัตถุประสงค์ของการเปลี่ยนแปลงรายละเอียดการเปลี่ยนแปลงผลกระทบที่คาดการณ์ และทรัพยากรที่จำเป็นแล้วส่งไปยังคณะกรรมการจัดการการเปลี่ยนแปลง (CAB) เช่น ทีม IT จัดทำเอกสารการร้องขออัปเดตซอฟต์แวร์ โดยระบุว่าอัปเดตนี้จะช่วยแก้ไขช่องโหว่ความ ปลอดภัยที่พบในระบบปัจจุบัน

2. การประเมินและอนุมัติการเปลี่ยนแปลง (Change Evaluation and Approval)

2.1 การประเมินการเปลี่ยนแปลง

ขั้นตอน : คณะกรรมการจัดการการเปลี่ยนแปลง (CAB) จะทำการประเมินความเสี่ยงผลกระทบต่อระบบและกระบวนการปัจจุบัน ต้นทุน และทรัพยากรที่จำเป็นในการดำเนินการ เช่น คณะกรรมการจัดการการเปลี่ยนแปลง (CAB) ประเมินว่าการอัปเดตซอฟต์แวร์จะใช้เวลา 4 ชั่วโมงในการดำเนินการ และอาจทำให้ระบบต้องหยุดให้บริการในช่วงเวลานั้น แต่จะช่วย ลดความเสี่ยงจากการถูกโจมตี

2.2 การอนุมัติหรือปฏิเสธการเปลี่ยนแปลง

ขั้นตอน : หลังจากการประเมิน คณะกรรมการจัดการการเปลี่ยนแปลง (CAB) จะทำการอนุมัติ หรือปฏิเสธการเปลี่ยนแปลง หากได้รับการอนุมัติ จะมีการกำหนดแผนการดำเนินการที่ชัดเจน เช่น กำหนดให้ดำเนินการในช่วงสุดสัปดาห์เมื่อมีผู้ใช้น้อยที่สุด

2.3 การจัดทำแผนการเปลี่ยนแปลง

ขั้นตอน : ผู้ร้องขอการเปลี่ยนแปลงและผู้ดำเนินการเปลี่ยนแปลงร่วมกันจัดทำแผนการ ดำเนินการเปลี่ยนแปลง ซึ่งรวมถึงเวลาที่จะดำเนินการ ทรัพยากรที่จำเป็น และการเตรียมการ สำรอง (Backup) ก่อนดำเนินการ เสมอ

3. การดำเนินการเปลี่ยนแปลง (Change Implementation)

3.1 การสื่อสารการเปลี่ยนแปลง

ขั้นตอน : ก่อนเริ่มดำเนินการเปลี่ยนแปลง ต้องมีการสื่อสารแผนการเปลี่ยนแปลงไปยังบุคลากรที่เกี่ยวข้องทุกคน เพื่อให้ทราบถึงการเปลี่ยนแปลงที่จะเกิดขึ้นและการเตรียมความ พร้อมโดยการส่งอีเมลแจ้งเตือนผู้ใช้งานทุกคนเกี่ยวกับการหยุดให้บริการระบบในที่กำหนด ไว้เพื่ออัปเดตซอฟต์แวร์ เป็นต้น

3.2 การดำเนินการตามแผน

ขั้นตอน : ผู้ดำเนินการเปลี่ยนแปลงจะดำเนินการเปลี่ยนแปลงตามแผนที่ได้รับอนุมัติ โดย ปฏิบัติตามขั้นตอนที่กำหนดอย่างเคร่งครัด และติดตามความคืบหน้าตามแผนที่วางไว้

3.3 การทดสอบและตรวจสอบผลการเปลี่ยนแปลง

ขั้นตอน : หลังจากดำเนินการเปลี่ยนแปลง จะต้องทำการทดสอบระบบหรือกระบวนการที่ เปลี่ยนแปลงเพื่อให้แน่ใจว่าไม่มีปัญหาเกิดขึ้นและการเปลี่ยนแปลงเป็นไปตามที่คาดหวัง โดย การทดสอบระบบเพื่อตรวจสอบว่าซอฟต์แวร์ทำงานได้อย่างถูกต้องและไม่มีข้อผิดพลาด

4. การติดตามและการรายงานผล (Monitoring and Reporting)

4.1 การติดตามผลหลังการเปลี่ยนแปลง

ขั้นตอน : ติดตามผลการเปลี่ยนแปลงในระยะเวลาที่กำหนด เพื่อให้แน่ใจว่าการเปลี่ยนแปลงไม่ มีผลกระทบเชิงลบต่อระบบหรือกระบวนการ โดยมีการติดตามผลการทำงานของซอฟต์แวร์ ที่อัปเดตใหม่เป็นเวลา 7 วันหลังจากการอัปเดต เพื่อให้แน่ใจว่าไม่มีปัญหาใด ๆ เกิดขึ้น

4.2 การรายงานผลการเปลี่ยนแปลง

ขั้นตอน : รายงานผลการเปลี่ยนแปลงให้กับคณะกรรมการจัดการการเปลี่ยนแปลง (CAB) และ ผู้บริหาร เพื่อประเมินผลการดำเนินการและตัดสินใจเพิ่มเติมหากมีปัญหาเกิดขึ้น

5. การปิดการเปลี่ยนแปลง (Change Closure)

5.1 การปิดเอกสารการเปลี่ยนแปลง

ขั้นตอน : เมื่อการเปลี่ยนแปลงเสร็จสมบูรณ์และผ่านการทดสอบและติดตามผลแล้ว ผู้ดำเนินการเปลี่ยนแปลงจะต้องปิดเอกสารการเปลี่ยนแปลง และบันทึกผลลัพธ์สุดท้ายลงในระบบการจัดการเอกสาร

5.2 การจัดเก็บเอกสารและบทเรียนที่ได้

ขั้นตอน : จัดเก็บเอกสารที่เกี่ยวข้องกับการเปลี่ยนแปลง และบันทึกกิจกรรมที่ได้จากการเปลี่ยนแปลงนี้ เพื่อนำไปใช้ในการปรับปรุงกระบวนการในอนาคต

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพ และและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ใบร้องขอการเปลี่ยนแปลง (Change Management Request Form)
2. รายงานผลการเปลี่ยนแปลง (Change Management report)

กระบวนการการเชื่อมต่อระยะไกล
(Remote Connection Procedure)

5. นโยบายการเชื่อมต่อระยะไกล (Remote Connection Policy)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 22.3.1, ข้อ 22.3.2]

5.1 วัตถุประสงค์ (Objective)

นโยบายนี้กำหนดแนวทางและข้อกำหนดสำหรับการเชื่อมต่อระยะไกลมายังบริการที่สำคัญขององค์กร เพื่อให้ มั่นใจว่าการเข้าถึงจากภายนอกมีความปลอดภัย ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และปฏิบัติตาม มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูล

5.2 ขอบเขต (Scope)

นโยบายนี้ใช้กับพนักงาน ผู้รับเหมา และบุคคลภายนอกที่ต้องการเชื่อมต่อเข้ามายังระบบสารสนเทศขององค์กร จากระยะไกล รวมถึงการเข้าถึงผ่าน VPN, Remote Desktop, และเครื่องมือการเข้าถึงระยะไกลอื่น ๆ ที่ได้รับ อนุญาต

5.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management) : กำกับดูแลให้มีการปฏิบัติตามนโยบายการเชื่อมต่อระยะไกล และอนุมัติแนวทางที่จำเป็นในการรักษาความมันคงปลอดภัย

2) ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team) : กำหนดและบังคับใช้นโยบาย รวมถึงตรวจสอบและบันทึกกิจกรรมที่เกี่ยวข้องกับการเข้าถึงระยะไกล

3) ผู้ใช้งานระบบ (Remote Users) : ปฏิบัติตามข้อกำหนดของนโยบายนี้และแจ้งเหตุการณ์ที่ผิดปกติแก่ ฝ่าย IT Security

5.4 แนวปฏิบัติในการเชื่อมต่อระยะไกล (Remote Connection Guidelines)

1) ข้อกำหนดทั่วไป

- ผู้ใช้ต้องได้รับการอนุมัติจากฝ่าย IT ก่อนการเข้าถึงระยะไกล
- อุปกรณ์ที่ใช้เชื่อมต่อระยะไกลต้องเป็นอุปกรณ์ที่ได้รับอนุญาตจากองค์กรและต้องติดตั้งซอฟต์แวร์ รักษาความปลอดภัย
- การเชื่อมต่อระยะไกลต้องใช้ VPN และการเข้ารหัสแบบ End-to-End

2) การพิสูจน์ตัวตนและการควบคุมการเข้าถึง

- ผู้ใช้ต้องใช้ Multi-Factor Authentication (MFA) ในการเข้าถึงระบบระยะไกล

- ใช้มาตรการ Least Privilege Access โดยกำหนดสิทธิ์การเข้าถึงเฉพาะส่วนที่จำเป็น
- มีการตรวจสอบสิทธิ์การเข้าถึงเป็นระยะ และต้องเพิกถอนสิทธิ์ทันทีเมื่อผู้ใช้ออกจากองค์กรหรือหมด หน้าที่ความรับผิดชอบ

3) การรักษาความมั่นคงปลอดภัยของข้อมูล

- ห้ามใช้เครือข่ายสาธารณะ (Public Wi-Fi) ในการเข้าถึงบริการที่สำคัญขององค์กร เว้นแต่มีมาตรการ ป้องกันที่เหมาะสม เช่น VPN
- ห้ามเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์กรบนอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อระยะไกล
- ระบบที่รองรับการเข้าถึงระยะไกลต้องมี Session Timeout เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4) การบันทึกและการติดตามการเข้าถึง

- ต้องมีการบันทึกกิจกรรมการเข้าถึงระยะไกลทั้งหมดใน Security Information and Event Management (SIEM)
- ทีม IT Security ต้องดำเนินการตรวจสอบบันทึกการเข้าถึงเป็นระยะ และมีการแจ้งเตือนเมื่อพบ กิจกรรมที่ผิดปกติ
- รายงานการเชื่อมต่อระยะไกลต้องถูกจัดเก็บและตรวจสอบอย่างน้อยปีละ 1 ครั้ง

5.5 การบังคับใช้และบทลงโทษ (Enforcement and Penalties)

1) ผู้ใช้ที่ฝ่าฝืนนโยบายนี้อาจถูกระงับสิทธิ์การเข้าถึงระยะไกล และอาจได้รับโทษทางวินัยตามระเบียบ ขององค์กร

2) องค์กรมีสิทธิ์ตรวจสอบและบังคับใช้นโยบายนี้โดยปรับปรุงให้สอดคล้องกับภัยคุกคามและข้อกำหนด ทางกฎหมายที่เปลี่ยนแปลง

นโยบายการเชื่อมต่อระยะไกล (Policy Review)

นโยบายการเชื่อมต่อระยะไกล นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

6. กระบวนการการเชื่อมต่อระยะไกล (Remote Connection Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.3.1, ข้อ 22.3.2]

6.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อควบคุมและรักษาความมั่นคงปลอดภัยของการเชื่อมต่อระยะไกลมายัง บริการที่สำคัญขององค์กร โดยให้แน่ใจว่ามีมาตรการที่เพียงพอในการป้องกันและตรวจจับการเข้าถึงที่ไม่ได้รับอนุญาต

6.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระยะไกลมายังบริการที่สำคัญ รวมถึงการกำหนดแนวทางปฏิบัติสำหรับการเชื่อมต่อและการควบคุมการไหลของข้อมูล

6.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management): รับผิดชอบในการอนุมัติและตรวจสอบมาตรการความมั่นคงปลอดภัย สำหรับการเชื่อมต่อระยะไกล

2) ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team): รับผิดชอบในการกำหนดและบังคับใช้ นโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล

3) ผู้ใช้งานระบบ (Remote Users): มีหน้าที่ปฏิบัติตามนโยบายและแนวทางปฏิบัติที่กำหนดไว้สำหรับการเชื่อมต่อระยะไกล

6.4 การรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล (Remote Connection Security)

1) มาตรการรักษาความมั่นคงปลอดภัย

ขั้นตอน : ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลมายังบริการที่สำคัญมีมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอ เช่น การใช้การเข้ารหัส การพิสูจน์ตัวตนที่แข็งแกร่ง และการ ควบคุมการไหลของข้อมูล โดยมีการใช้ VPN ที่เข้ารหัสการเชื่อมต่อและการยืนยันตัวตนด้วย สองปัจจัย (2FA) สำหรับการเข้าถึงระบบจากระยะไกล

2) การเปิดใช้งานการเชื่อมต่อ

ขั้นตอน : เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกลเมื่อจำเป็นเท่านั้น และปิดการเชื่อมต่อเมื่อไม่ใช้งาน โดยการตั้งค่าให้เซิร์ฟเวอร์เปิดใช้งานการเชื่อมต่อระยะไกลเฉพาะใน ช่วงเวลาทำงานเท่านั้น

3) การใช้เทคนิคการพิสูจน์ตัวตนที่แข็งแกร่ง

ขั้นตอน : ใช้เทคนิคการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยในการส่งข้อมูลและความสมบูรณ์ของข้อความที่แข็งแกร่ง เช่น การใช้โปรโตคอลที่ปลอดภัย SSH สำหรับการเชื่อมต่อระยะไกล เพื่อป้องกันการโจมตีแบบ Man-in-the-Middle

4) การเข้ารหัสการเชื่อมต่อ

ขั้นตอน : ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมดเพื่อป้องกันการดักฟังข้อมูลระหว่างทาง เช่น การใช้ HTTPS สำหรับการเข้าถึงเว็บไซต์ภายในองค์กรจากระยะไกล

5) การเปิดใช้งานการเชื่อมต่อ

ขั้นตอน : ไม่อนุญาตให้เชื่อมต่อระยะไกลเพื่อใช้งานคำสั่งระบบที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างชัดเจน โดยการจำกัดสิทธิ์ในการใช้คำสั่งที่เกี่ยวข้องกับการจัดการเซิร์ฟเวอร์ผ่านการเชื่อมต่อระยะไกล เว้นแต่จะได้รับการอนุมัติ จากผู้บริหาร

6) การจำกัดการไหลของข้อมูล

ขั้นตอน : จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ เพื่อป้องกันการรั่วไหลของข้อมูลที่ไม่จำเป็น โดยการกำหนดให้สามารถถ่ายโอนข้อมูลเฉพาะไฟล์ที่จำเป็น สำหรับการทำงานเท่านั้นในระหว่างการเชื่อมต่อระยะไกล

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. นโยบายแนวปฏิบัติในการเชื่อมต่อระยะไกล
2. หลักฐานการขออนุญาตเชื่อมต่อระยะไกล จากการใช้คำสั่งระบบ (Issuing System Commands)
3. รายงานการตรวจสอบการเชื่อมต่อที่มายังบริการที่สำคัญ

กระบวนการการใช้สื่อเก็บข้อมูลแบบถอดได้
(Removable Storage Media Procedure)

7. นโยบายการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Policy)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 2.4.1, ข้อ 22.4.2]

7.1 วัตถุประสงค์ (Objective)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดมาตรการและแนวปฏิบัติสำหรับการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ เช่น USB, External Hard Drive, SD Card และอุปกรณ์จัดเก็บข้อมูลอื่น ๆ เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลและการรั่วไหลของข้อมูลสำคัญขององค์กร

7.2 ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงพนักงานทุกระดับ ผู้รับเหมา และบุคคลภายนอกที่ต้องการใช้งานหรือเชื่อมต่ออุปกรณ์บันทึกข้อมูลแบบถอดได้กับระบบสารสนเทศขององค์กร

7.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management): กำกับดูแลให้มีการปฏิบัติตามนโยบายและสนับสนุนมาตรการด้านความมั่นคงปลอดภัย

2) ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team): บังคับใช้และตรวจสอบการใช้งานอุปกรณ์บันทึกข้อมูลแบบ ถอดได้ พร้อมดำเนินมาตรการรักษาความมั่นคงปลอดภัย

3) พนักงานและผู้ใช้งาน (Employees & Users): ปฏิบัติตามแนวทางของนโยบายนี้ และรายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับ การใช้งานสื่อบันทึกข้อมูลแบบถอดได้

7.4 แนวปฏิบัติในการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Guidelines)

1) การอนุญาตและข้อจำกัด

- อุปกรณ์บันทึกข้อมูลแบบถอดได้ต้องได้รับการอนุมัติจากฝ่าย IT ก่อนใช้งาน
- ห้ามใช้อุปกรณ์ส่วนตัวในการถ่ายโอนหรือจัดเก็บข้อมูลขององค์กร เว้นแต่ได้รับอนุญาตเป็นกรณีพิเศษ
- ต้องมีการเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลสำคัญที่จัดเก็บในอุปกรณ์บันทึกข้อมูลแบบถอดได้

2) การควบคุมการเข้าถึงและการใช้งาน

- จำกัดสิทธิ์การเข้าถึงสื่อบันทึกข้อมูลแบบถอดได้เฉพาะผู้ที่มีความจำเป็นต้องใช้งานเท่านั้น
- ระบบที่รองรับการใช้งานอุปกรณ์แบบถอดได้ต้องมีการเปิดใช้ Read-Only Mode เป็นค่าเริ่มต้น และอนุญาตให้เขียนข้อมูลได้ เฉพาะอุปกรณ์ที่ได้รับอนุญาต

- ห้ามใช้อุปกรณ์บันทึกข้อมูลแบบถอดได้ที่ไม่มีการตรวจสอบหรือมีแหล่งที่มาไม่แน่ชัด

3) มาตรการรักษาความมั่นคงปลอดภัย

- ต้องใช้ซอฟต์แวร์ป้องกันมัลแวร์เพื่อตรวจสอบอุปกรณ์ทุกครั้งก่อนใช้งาน
- อุปกรณ์ที่ไม่ได้ใช้งานเป็นเวลานานต้องถูกลบข้อมูลทั้งหมดก่อนนำมาใช้อีกครั้ง
- ต้องมีระบบบันทึกการใช้งานสื่อบันทึกข้อมูลแบบถอดได้เพื่อให้สามารถตรวจสอบย้อนหลังได้

4) การนำออกและการทำลายข้อมูล

- เมื่อเลิกใช้งานอุปกรณ์ ต้องมีการลบข้อมูลอย่างปลอดภัย (Secure Erasure) ตามมาตรฐานขององค์กร
- อุปกรณ์ที่ชำรุดหรือหมดอายุการใช้งานต้องถูกทำลายอย่างปลอดภัย โดยใช้เทคนิคการลบข้อมูลที่ไม่สามารถกู้คืนได้เช่น Data Wiping หรือ Physical Destruction

7.5 การตรวจสอบและบังคับใช้ (Monitoring and Enforcement)

1) การตรวจสอบและติดตาม

- ทีม IT Security ต้องมีระบบเฝ้าระวังและตรวจสอบการใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้
- ต้องมีการตรวจสอบบันทึกการใช้งานเป็นระยะ และดำเนินมาตรการตอบสนองหากพบพฤติกรรมที่ผิดปกติ

2) การตอบสนองต่อเหตุการณ์ (Incident Response)

- หากพบการใช้งานที่ไม่ได้รับอนุญาต ระบบต้องแจ้งเตือนฝ่าย IT Security ทันที
- ทีม IT มีอำนาจในการยกเลิกสิทธิ์การใช้งานของผู้ใช้ที่ละเมิดนโยบาย

3) การบังคับใช้ข้อกำหนด

- ผู้ใช้ที่ฝ่าฝืนนโยบายนี้อาจถูกระงับสิทธิ์การใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้และอาจได้รับโทษทางวินัยตามระเบียบขององค์กร
- องค์กรมีสิทธิ์ปรับปรุงนโยบายและกระบวนการนี้ให้สอดคล้องกับภัยคุกคามและกฎหมายที่เปลี่ยนแปลง

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามี การเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

8. กระบวนการการใช้สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.4.1, ข้อ 22.4.2]

8.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อควบคุมและรักษาความมั่นคงปลอดภัยทางไซเบอร์ในการใช้สื่อเก็บข้อมูล แบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการแพร่กระจาย ของมัลแวร์ไปยังบริการที่สำคัญขององค์กร

8.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการใช้ การควบคุม และการเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้และ อุปกรณ์คอมพิวเตอร์แบบพกพาที่เชื่อมต่อกับบริการที่สำคัญขององค์กร

8.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management) : รับผิดชอบในการอนุมัติและกำกับดูแลการดำเนินการตามกระบวนการ ควบคุมการใช้สื่อเก็บข้อมูลแบบถอดได้

2) ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team) : รับผิดชอบในการกำหนดและบังคับใช้ มาตรการควบคุม การตรวจสอบ และการเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้

3) ผู้ใช้งานระบบ (System Users) : มีหน้าที่ปฏิบัติตามนโยบายและแนวทางปฏิบัติที่กำหนดไว้สำหรับการ ใช้สื่อเก็บข้อมูลแบบถอดได้

8.4 การควบคุมการใช้สื่อเก็บข้อมูลแบบถอดได้ (Control of Removable Storage Media)

1) การปิดใช้งานพอร์ตเชื่อมต่อภายนอก

ขั้นตอน: ให้ทำการปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น โดยการตั้งค่าให้พอร์ต USB บนอุปกรณ์คอมพิวเตอร์ภายในองค์กรถูกปิดใช้งานโดยค่าเริ่มต้น และต้องได้รับการอนุญาตจากผู้ดูแลระบบก่อนการเปิดใช้งาน

2) การใช้งานสื่อเก็บข้อมูลที่ได้รับอนุญาต

ขั้นตอน : อนุญาตให้ใช้สื่อเก็บข้อมูลแบบถอดได้เฉพาะที่ได้รับอนุญาตและผ่านการตรวจสอบตามข้อกำหนดที่กำหนดไว้เท่านั้น โดยการจำกัดการใช้งานสื่อเก็บข้อมูลแบบถอดได้ที่ได้รับ การจัดหาโดยองค์กรเท่านั้น และป้องกันไม่ให้พนักงานใช้สื่อเก็บข้อมูลส่วนตัว

3) การตรวจสอบมัลแวร์ก่อนการเชื่อมต่อ

ขั้นตอน : ตรวจสอบว่าสื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญขององค์กร โดยการสแกนหามัลแวร์บนสื่อเก็บ ข้อมูลก่อนการเชื่อมต่อกับเครือข่ายองค์กร

8.5 การเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้ (Encryption of Data on Removable Storage Media)

1) การเข้ารหัสข้อมูลที่ละเอียดอ่อน

ขั้นตอน : เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญขององค์กรที่จัดเก็บบนสื่อเก็บข้อมูลแบบถอดได้ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยการใช้ซอฟต์แวร์ เข้ารหัสข้อมูลเพื่อเข้ารหัสไฟล์สำคัญก่อนที่จะถ่ายโอนข้อมูลไปยังสื่อเก็บข้อมูลแบบถอดได้

2) การตรวจสอบการปฏิบัติตาม

ขั้นตอน : ตรวจสอบให้แน่ใจว่าผู้ใช้งานปฏิบัติตามมาตรการการเข้ารหัสข้อมูลและการควบคุมสื่อเก็บข้อมูลแบบถอดได้ตามที่กำหนดไว้ในกระบวนการ มีการตรวจสอบเป็นระยะเพื่อให้ แน่ใจว่าสื่อเก็บข้อมูลที่ใช้งานในองค์กรมีการเข้ารหัสข้อมูลตามข้อกำหนด

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. หลักฐานหรือเอกสารที่ใช้ในการร้องขอการเปิด USB Port

9. กระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.5.1, ข้อ 22.5.2]

9.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อส่งเสริมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย ไซเบอร์แก่ พนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

9.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการจัดทำแผนงาน การเผยแพร่ และการทบทวนกิจกรรมต่าง ๆ ที่เกี่ยวข้อง กับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรที่เกี่ยวข้องในองค์กร

9.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management): รับผิดชอบในการสนับสนุนและกำกับดูแลการดำเนินการตามแผนงาน การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

2) ทีมรักษาความปลอดภัยไซเบอร์ (Cybersecurity Awareness Team): รับผิดชอบในการพัฒนาและ ดำเนินการตามแผนงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการจัดกิจกรรมและการเผยแพร่ข้อมูล

3) พนักงานและผู้ให้บริการภายนอก (Employees and External Service Providers): มีหน้าที่เข้าร่วม กิจกรรมและปฏิบัติตามนโยบายและแนวทางที่ได้รับการอบรมหรือเผยแพร่

9.4 การจัดทำแผนงานการสร้างความตระหนักรู้ (Development of Cybersecurity Awareness Plan)

1) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท

ขั้นตอน : จัดทำกิจกรรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกกลุ่ม รวมถึงพนักงานใหม่ ผู้ใช้และผู้บริหาร เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญ และผู้ขายหรือผู้รับเหมา โดยการจัดอบรมความมั่นคงปลอดภัยไซเบอร์สำหรับพนักงานใหม่เมื่อเริ่มงาน และ การจัดสัมมนาเชิงปฏิบัติการสำหรับเจ้าหน้าที่ IT เพื่อเรียนรู้เกี่ยวกับภัยคุกคามใหม่ ๆ

2) การเผยแพร่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

ขั้นตอน : เผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ โดยใช้ช่องทางต่าง ๆ เช่น อีเมล บอร์ดประกาศ และการ ประชุม โดยการส่งอีเมลแจ้งให้พนักงานทุกคนทราบถึงหน้าที่ในการรักษาความมั่นคง ปลอดภัยไซเบอร์ และการกำหนดหน้าที่เฉพาะสำหรับทีม IT

3) การตระหนักรู้กฎหมายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

ขั้นตอน : จัดทำและเผยแพร่ข้อมูลเกี่ยวกับกฎหมาย กฎ ระเบียบ นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับการใช้งานและการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อให้บุคลากร ทุกคนตระหนักถึงข้อกำหนดที่ต้องปฏิบัติตาม โดยการการจัดทำคู่มือการปฏิบัติตามนโยบาย ความมั่นคงปลอดภัยไซเบอร์ และการอบรมเกี่ยวกับกฎหมายความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง

4) การสื่อสารและเผยแพร่ข้อมูลอย่างสม่ำเสมอ

ขั้นตอน : สื่อสารข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามใหม่ ๆ อย่างสม่ำเสมอและทันท่วงทีผ่านช่องทางที่เหมาะสม เช่น อีเมล บอร์ดข่าวสารภายในองค์กร หรือระบบการจัดการเรียนรู้ โดยการส่งข่าวสารเกี่ยวกับภัยคุกคามไซเบอร์ล่าสุดให้กับพนักงานทุกสัปดาห์ และการจัดทำคอร์สออนไลน์เกี่ยวกับวิธีการบรรเทาผลกระทบจากภัยคุกคามทางไซเบอร์

9.5 การทบทวนแผนงานและการปรับปรุง (Review and Improvement of Awareness Plan)

1) การทบทวนแผนงานประจำปี

ขั้นตอน : ทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีความเกี่ยวข้องกับ สถานการณ์ปัจจุบัน

2) การปรับปรุงเนื้อหาและกิจกรรมตามผลการทบทวน

ขั้นตอน : ปรับปรุงเนื้อหาและกิจกรรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ตามผลการทบทวน เพื่อเพิ่มประสิทธิภาพในการตระหนักรู้และป้องกันภัยคุกคาม โดย การเพิ่มโมดูลการอบรมเกี่ยวกับการป้องกันการโจมตีในรูปแบบต่างๆ

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
2. หลักฐานหรือเอกสาร การจัดทำกิจกรรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากร

กระบวนการการแบ่งปันข้อมูล
(Information Sharing Procedure)

10. นโยบายการแบ่งปันข้อมูล (Information Sharing Policy)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 22.6.1]

10.1 วัตถุประสงค์ (Objective)

นโยบายนี้จัดทำขึ้นเพื่อกำหนดแนวทางในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ภัย คุกคามทางไซเบอร์ และมาตรการบรรเทาผลกระทบ เพื่อให้มั่นใจว่าการแบ่งปันข้อมูลเป็นไปอย่างปลอดภัย มีประสิทธิภาพ และสอดคล้องกับข้อกำหนดขององค์กรและกฎหมายที่เกี่ยวข้อง

10.2 ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงการแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคาม ทางไซเบอร์ให้กับบุคคลที่เกี่ยวข้อง เช่น หน่วยงานหรือองค์กรที่อยู่ในหน่วยงานควบคุมหรือกำกับดูแลเดียวกัน, ผู้ใช้บริการ, ผู้รับเหมา และเจ้าของระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญขององค์กร

10.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management) : อนุมัติและกำกับดูแลการแบ่งปันข้อมูลให้เป็นไปตามนโยบายและ ข้อกำหนดที่กำหนด

2) ทีมรักษาความปลอดภัยไซเบอร์ (Cybersecurity Team) : รวบรวม วิเคราะห์ และแบ่งปันข้อมูลเกี่ยวกับ เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคาม

3) ผู้ใช้บริการและผู้รับเหมา (Users and Contractors): รับทราบข้อมูลที่แบ่งปันและดำเนินการตาม มาตรการป้องกันที่ได้รับแจ้ง

10.4 แนวทางปฏิบัติในการแบ่งปันข้อมูล (Guidelines for Information Sharing)

1) การรวบรวมและวิเคราะห์ข้อมูล

- ทีมรักษาความปลอดภัยไซเบอร์ต้องรวบรวมข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามทางไซเบอร์ และ ดำเนินการวิเคราะห์เพื่อระบุผลกระทบที่อาจเกิดขึ้น
- การวิเคราะห์ข้อมูลต้องอ้างอิงจากแหล่งข้อมูลที่น่าเชื่อถือและดำเนินการตามมาตรฐานที่กำหนด

2) การแบ่งปันข้อมูลกับบุคคลที่เกี่ยวข้อง

- ข้อ มูลที่แบ่งปันต้องเป็นไปตามหลักการ ความถูกต้อง ครบถ้วน และทันเวลา (Accuracy, Completeness, and Timeliness)

- ต้องแบ่งปันข้อมูลให้กับบุคคลหรือหน่วยงานที่ได้รับผลกระทบโดยตรงและมีเหตุผลที่เหมาะสมในการรับข้อมูล
- ข้อมูลที่มีความอ่อนไหวต้องแบ่งปันโดยใช้ช่องทางที่ปลอดภัย เช่น การเข้ารหัสอีเมล หรือการใช้ระบบ ที่ได้รับการรับรองด้านความปลอดภัย

3) ข้อจำกัดและข้อกำหนดในการแบ่งปันข้อมูล

- ข้อมูลที่แบ่งปันต้องไม่ละเมิดความเป็นส่วนตัวของบุคคล หรือข้อกำหนดด้านการปกป้องข้อมูลตามกฎหมายที่เกี่ยวข้อง
- ต้องมีการกำหนดระดับของข้อมูลที่สามารถแบ่งปันได้ เช่น:
  - ข้อมูลสาธารณะ: สามารถเผยแพร่ได้โดยไม่ต้องได้รับอนุมัติ
  - ข้อมูลภายใน: ใช้ภายในองค์กรเท่านั้น
  - ข้อมูลจำกัด (Restricted): แบ่งปันเฉพาะบุคคลที่ได้รับอนุญาต
  - ข้อมูลลับ (Confidential): ต้องได้รับการอนุมัติเป็นพิเศษก่อนการแบ่งปัน

4) ข้อจำกัดและข้อกำหนดในการแบ่งปันข้อมูล

- ข้อมูลควรถูกแบ่งปันในรูปแบบที่สามารถใช้ได้อย่างมีประสิทธิภาพ เช่น รายงานการวิเคราะห์ เหตุการณ์, การแจ้งเตือนภัยคุกคาม หรือเอกสารแนวทางปฏิบัติ
- ควรใช้ช่องทางการสื่อสารที่ปลอดภัย เช่น Secure Email, VPN, หรือ ระบบภายในองค์กร
- องค์กรต้องมีระบบแจ้งเตือนภัยคุกคามทางไซเบอร์ เช่น การแจ้งเตือนผ่านอีเมลหรือแอปพลิเคชันมือถือ

10.5 การควบคุมและการรักษาความมั่นคงของข้อมูล (Security and Compliance Controls)

1) การควบคุมการเข้าถึงข้อมูลที่แบ่งปัน

- การเข้าถึงข้อมูลที่แบ่งปันต้องได้รับอนุญาตตามระดับของข้อมูลและข้อกำหนดด้านความมั่นคงปลอดภัย
- บุคคลที่ได้รับข้อมูลต้องปฏิบัติตามมาตรการรักษาความปลอดภัยขององค์กร

2) การตรวจสอบและติดตาม

- ต้องมีการบันทึกและติดตามการแบ่งปันข้อมูล รวมถึงบุคคลที่ได้รับข้อมูลเพื่อให้สามารถตรวจสอบย้อนหลังได้
- ทีมรักษาความปลอดภัยไซเบอร์ต้องทำการตรวจสอบเป็นระยะ เพื่อให้แน่ใจว่าการแบ่งปันข้อมูลเป็นไปตามข้อกำหนดที่กำหนด

3) การรับมือกับการละเมิดนโยบาย

- หากพบว่ามีการแบ่งปันข้อมูลที่ไม่ได้รับอนุญาต หรือมีการใช้ข้อมูลผิดวัตถุประสงค์ ต้องดำเนิน มาตรการตอบสนอง เช่น การแจ้งเตือน, การระงับสิทธิ์เข้าถึง หรือการดำเนินการทางกฎหมาย

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามี การเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

11. กระบวนการการแบ่งปันข้อมูล (Information Sharing Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 22.6.1]

11.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อกำหนดแนวทางในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัย ไซเบอร์และภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อให้บุคคลที่ได้รับ ผลกระทบหรืออาจได้รับผลกระทบสามารถใช้มาตรการป้องกันที่จำเป็นได้อย่างทันท่วงที

11.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ภัย คุกคามทางไซเบอร์ และมาตรการบรรเทาผลกระทบให้กับบุคคลที่เกี่ยวข้อง เช่น หน่วยงานหรือองค์กรที่อยู่ใน หน่วยงานควบคุมหรือกำกับดูแลเดียวกัน, ผู้ใช้บริการ ผู้รับเหมา และเจ้าของระบบคอมพิวเตอร์ที่จำเป็นต้อง เชื่อมต่อกับบริการที่สำคัญขององค์กร

11.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management): รับผิดชอบในการอนุมัติและกำกับดูแลการแบ่งปันข้อมูล และ ตรวจสอบให้แน่ใจว่าการแบ่งปันข้อมูลเป็นไปตามนโยบายและข้อกำหนดที่กำหนด

2) ทีมรักษาความปลอดภัยไซเบอร์ (Cybersecurity Team): รับผิดชอบในการรวบรวมข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามทางไซเบอร์ รวมถึงมาตรการบรรเทาผลกระทบ และแบ่งปันข้อมูลให้กับ บุคคลที่เกี่ยวข้องตามหลักเกณฑ์ที่กำหนด

3) ผู้ใช้บริการและผู้รับเหมา (Users and Contractors): มีหน้าที่รับทราบข้อมูลที่แบ่งปันและดำเนินการ ตามมาตรการป้องกันที่ได้รับแจ้ง

11.4 แนวทางและรูปแบบในการแบ่งปันข้อมูล (Guidelines and Formats for Information Sharing)

1) กำหนดแนวทางการแบ่งปันข้อมูล

ขั้นตอน : รวบรวมข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซ เบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดำเนินการวิเคราะห์เพื่อระบุผลกระทบที่อาจเกิดขึ้น โดยเน้นการรวบรวมข้อมูลเกี่ยวกับการโจมตีทางไซเบอร์ที่เกิดขึ้นและวิเคราะห์ผลกระทบต่อระบบที่สำคัญ

2) การแบ่งปันข้อมูลกับบุคคลที่เกี่ยวข้อง

ขั้นตอน : แบ่งปันข้อมูลเกี่ยวกับเหตุการณ์หรือภัยคุกคามที่เกิดขึ้น รวมถึงมาตรการบรรเทาผลกระทบที่ดำเนินการแล้ว ให้กับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ เช่น ผู้ใช้บริการ ผู้รับเหมา และเจ้าของระบบคอมพิวเตอร์ โดยการส่งอีเมลแจ้งเตือนผู้ใช้บริการ เกี่ยวกับการโจมตีทางไซเบอร์ที่เกิดขึ้น พร้อมแนวทางปฏิบัติเพื่อป้องกันตนเอง

11.5 แนวทางและรูปแบบในการแบ่งปันข้อมูล (Guidelines and Formats for Information Sharing)

1) กำหนดแนวทางการแบ่งปันข้อมูล

ขั้นตอน : กำหนดแนวทางในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคาม รวมถึงมาตรการบรรเทาผลกระทบ เพื่อให้มั่นใจว่าการแบ่งปันข้อมูลเป็นไป ตามมาตรฐานและมีประสิทธิภาพ โดยการกำหนดนโยบายการแจ้งเตือนภัยคุกคามที่ครอบคลุม ถึงการแจ้งเตือนผ่านช่องทางอีเมลและระบบข้อความภายในองค์กร

2) การกำหนดรูปแบบของข้อมูลที่แบ่งปัน

ขั้นตอน : กำหนดรูปแบบของข้อมูลที่แบ่งปัน เช่น รายงานการวิเคราะห์เหตุการณ์ รายงานการแจ้งเตือน หรือคู่มือการปฏิบัติตามมาตรการบรรเทาผลกระทบ เพื่อให้ข้อมูลสามารถใช้ได้อย่าง มีประสิทธิภาพ โดยการจัดทำรายงานสรุปเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ในรูปแบบ ไฟล์ PDF ที่มีรายละเอียดเกี่ยวกับเหตุการณ์ ภัยคุกคาม และแนวทางป้องกัน

11.6 การทบทวนและปรับปรุง (Review and Improvement)

1) **การทบทวนกระบวนการแบ่งปันข้อมูล**

ขั้นตอน : ทบทวนกระบวนการแบ่งปันข้อมูลเป็นระยะเพื่อให้แน่ใจว่ากระบวนการยังคงมีประสิทธิภาพและเป็นไปตามหลักเกณฑ์ที่กำหนด โดยการทบทวนและปรับปรุงกระบวนการ แบ่งปันข้อมูลทุกปีหรือหลังจากเกิดเหตุการณ์สำคัญที่ส่งผลกระทบต่อระบบ

2) **การปรับปรุงแนวทางการแบ่งปันข้อมูลตามผลการทบทวน**

ขั้นตอน : ปรับปรุงแนวทางและรูปแบบการแบ่งปันข้อมูลตามผลการทบทวน เพื่อเพิ่ม ประสิทธิภาพในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยการเพิ่มช่องทางการ แจ้งเตือนใหม่, ใช้แอปพลิเคชันมือถือในการแจ้งเตือนภัยคุกคามเพื่อเพิ่มความรวดเร็วในการ แบ่งปันข้อมูล

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. รายชื่อของเอกสารที่สามารถแบ่งปันข้อมูลได้

การตรวจจับ
(Detect)

1. กระบวนการการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม. 56), ประมวลและกรอบ [ข้อ 23.1.1, ข้อ 23.1.2]

1.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อกำหนดกลไกและกระบวนการในการตรวจจับ จัดประเภท วิเคราะห์ และ กวนการในการด ระบุภัยคุกคามทางไซเบอร์หรือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับบริการที่สำคัญขององค์กร

1.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับบริการที่ สำคัญขององค์กร การจัดประเภทและวิเคราะห์เหตุการณ์ที่ตรวจพบ และการระบุภัยคุกคามที่อาจเกิดขึ้นเพื่อดำเนินการป้องกันและตอบสนองอย่างทันท่วงที

1.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management) : รับผิดชอบในการกำกับดูแลและตรวจสอบความถูกต้องของกลไกและ กระบวนการตรวจจับและเฝ้าระวังภัยคุกคาม

2) ทีมรักษาความปลอดภัยไซเบอร์ (Cybersecurity Team) : รับผิดชอบในการพัฒนากลไกและ กระบวนการในการตรวจจับ จัดประเภท วิเคราะห์ และระบุภัยคุกคามทางไซเบอร์ รวมถึงการทบทวนและปรับปรุงกระบวนการตามความจำเป็น

3) เจ้าหน้าที่ตรวจสอบและเฝ้าระวัง (Cybersecurity Monitoring Officers) : มีหน้าที่ในการตรวจสอบ และเฝ้าระวังเหตุการณ์ความมั่นคงปลอดภัย ไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ และรายงานผลการ ตรวจสอบต่อผู้บริหาร

1.4 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) การสร้างกลไกและกระบวนการตรวจจับภัยคุกคาม

ขั้นตอน: พัฒนากลไกและกระบวนการในการตรวจจับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับบริการที่สำคัญ โดยใช้เครื่องมือและเทคโนโลยีที่เหมาะสม เช่น ระบบตรวจจับ การบุกรุก (Intrusion Detection Systems: IDS) รวมถึงการตั้งค่าและปรับแต่งระบบ IDS เพื่อตรวจจับพฤติกรรมที่น่าสงสัยและแจ้งเตือนผู้ดูแลระบบทันทีเมื่อพบกิจกรรมที่อาจเป็นภัยคุกคาม

2) การจัดประเภทและวิเคราะห์เหตุการณ์ที่ตรวจพบ

ขั้นตอน: จัดประเภทและวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ เพื่อระบุระดับความรุนแรงและความเร่งด่วนในการตอบสนอง โดยการวิเคราะห์เหตุการณ์ที่เกี่ยวข้อง กับการโจมตีแบบฟิชชิ่ง หรืออื่นๆ ที่พบ และจัดประเภทเหตุการณ์เป็นระดับความเสี่ยงสูงเพื่อตอบสนองอย่างเร่งด่วน

3) การระบุภัยคุกคามและการตอบสนอง

ขั้นตอน: ระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่อาจส่งผลกระทบต่อบริการที่สำคัญหรือไม่ และดำเนินการตอบสนองอย่างเหมาะสม ตามมาตรการที่กำหนดไว้ โดยการระบุว่าการโจมตีจากบุคคลภายนอกอาจส่งผลกระทบต่อบริการสำคัญขององค์กร และมีการดำเนินการตอบสนองตามแผนการรับมือภัยคุกคาม

1.5 การทบทวนและปรับปรุงกระบวนการ (Review and Improvement)

1) การทบทวนกลไกและกระบวนการตรวจจับภัยคุกคาม

ขั้นตอน: ทบทวนกลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ากระบวนการยังคงมีประสิทธิภาพในการตรวจจับและตอบสนองต่อภัยคุกคามที่ อาจเกิดขึ้น รวมถึงการทบทวนและปรับปรุงระบบ IDS (Intrusion Detection Systems) ให้ สามารถตรวจจับภัยคุกคามใหม่ ๆ ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

2) การปรับปรุงกระบวนการตามผลการทบทวน

ขั้นตอน: ปรับปรุงกลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามตามผลการทบทวน เพื่อเพิ่มประสิทธิภาพในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยการเพิ่ม ฟีเจอร์การวิเคราะห์พฤติกรรมผู้ใช้งาน (User Behavior Analytics: UBA) ในระบบตรวจจับภัย คุกคามเพื่อเพิ่มความแม่นยำในการตรวจจับ

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนงานการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
2. รายงานการตรวจจับเหตุการณ์ การจัดประเภทและวิเคราะห์เหตุการณ์

การตอบสนอง
(Respond)

1. กระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม. 43, ม. 44, ม. 45, ม. 56, ม. 57, ม. 58), ประมวลและกรอบ [ข้อ 24.1.1]

1.1 วัตถุประสงค์ (Objective)

แผนการรับมือภัยคุกคามทางไซเบอร์นี้จัดทำขึ้นเพื่อเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้อง กับความมั่นคงปลอดภัยไซเบอร์ โดยมีเป้าหมายเพื่อป้องกัน, จำกัดขอบเขตความเสียหาย , และฟื้นฟูระบบให้ กลับมาทำงานตามปกติได้อย่างรวดเร็ว

1.2 ขอบเขต (Scope)

แผนการรับมือภัยคุกคามทางไซเบอร์นี้ใช้สำหรับเหตุการณ์ภัยคุกคามที่ส่งผลกระทบต่อระบบสำคัญขององค์กร ทั้งระบบเทคโนโลยีสารสนเทศ (IT) และระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control Systems: ICS) โดยมีการครอบคลุมถึงการรับมือกับ

- การโจมตีทางไซเบอร์ เช่น Malware, Ransomware, Phishing, Distributed Denial of Service (DDoS) หรืออื่นๆ
- การโจมตีทางช่องโหว่ความปลอดภัยในระบบ
- การโจมตีการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

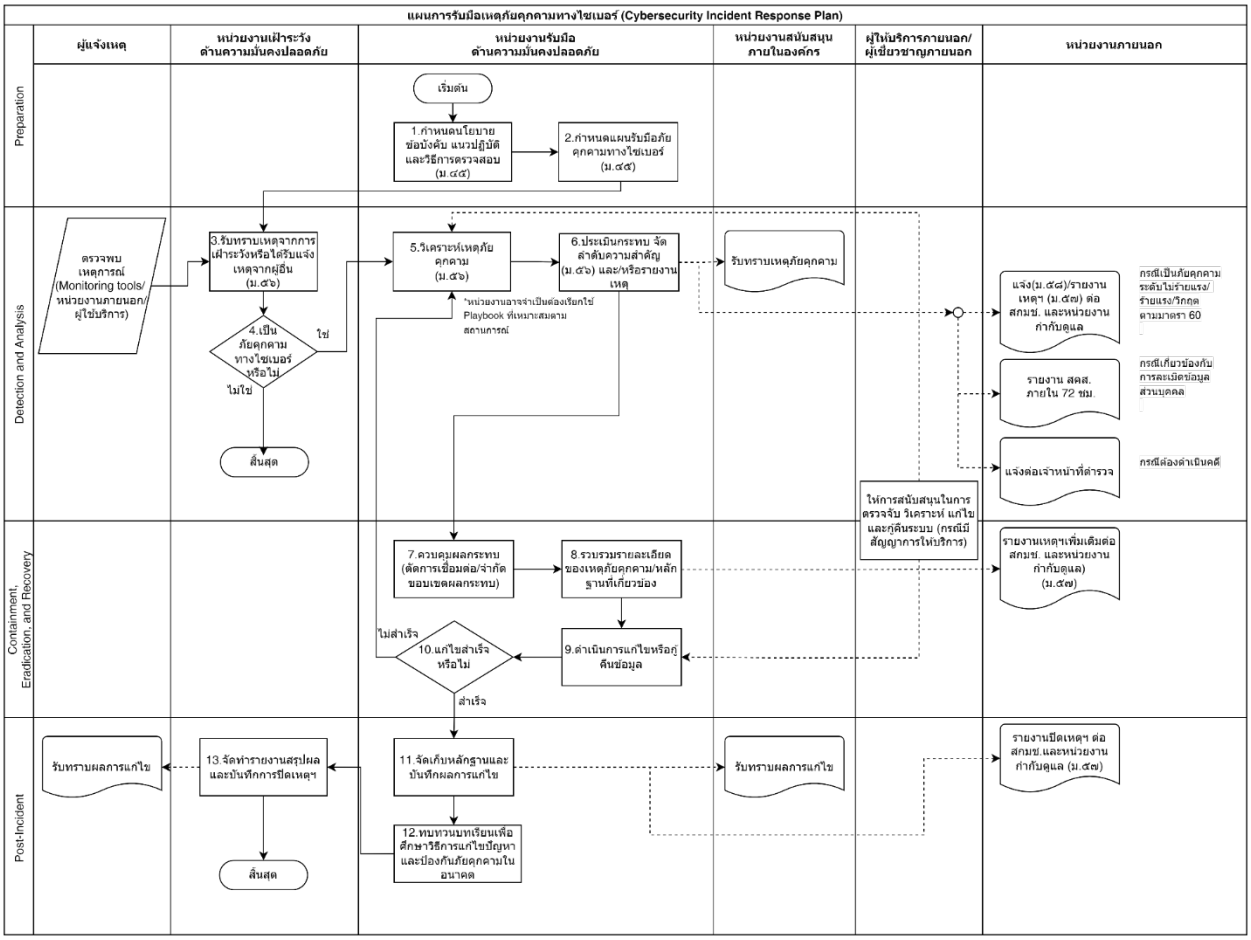
1.3 โครงสร้างทีมรับมือเหตุการณ์ทางไซเบอร์ (Incident Response Team Structure)

ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

	ตำแหน่ง	หน้าที่และความรับผิดชอบ	ข้อมูลการติดต่อ
1	นางเรณูบุญ วัฒน์พุฒิ หัวหน้าทีม (Team Leader)	รับผิดชอบการจัดการภาพรวมของเหตุการณ์, การตัดสินใจที่สำคัญ	โทร: 026516884 (262)
2	นาย สมศักดิ์ หนองจิก ผู้จัดการด้าน IT	รับผิดชอบการประเมินระบบ, การกู้คืนระบบ และการจำกัดขอบเขต	โทร: 026516884 (242)
3	นาย สมศักดิ์ หนองจิก ผู้จัดการด้านความปลอดภัย	รับผิดชอบการประเมินระบบ, การกู้คืนระบบ และการจำกัดขอบเขต	โทร: 026516884 (242)
4	นายณรงศักดิ์ ทองสุข ผู้จัดการด้านกฎหมาย	ให้คำปรึกษาด้านกฎหมายและจัดการด้านการรายงานภายใต้ พ.ร.บ. ไซเบอร์	โทร: 026516884 (271)
5	นายโอภาส ภูครองนาค เจ้าหน้าที่ด้านการสื่อสาร	สื่อสารภายในองค์กรและแจ้งข้อมูลต่อสื่อและหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงาน อื่นๆ ที่เกี่ยวข้อง	โทร: 026516884 (170)

6	นายโอภาส ภูครองนาค (Cyber Technical Expert)	สื่อสารภายในองค์กรและแจ้งข้อมูลต่อสื่อและหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงาน อื่นๆ ที่เกี่ยวข้อง	โทร: 026516884 (170)

- **1.4 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)**



1.5 เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activation Criteria and Procedures)

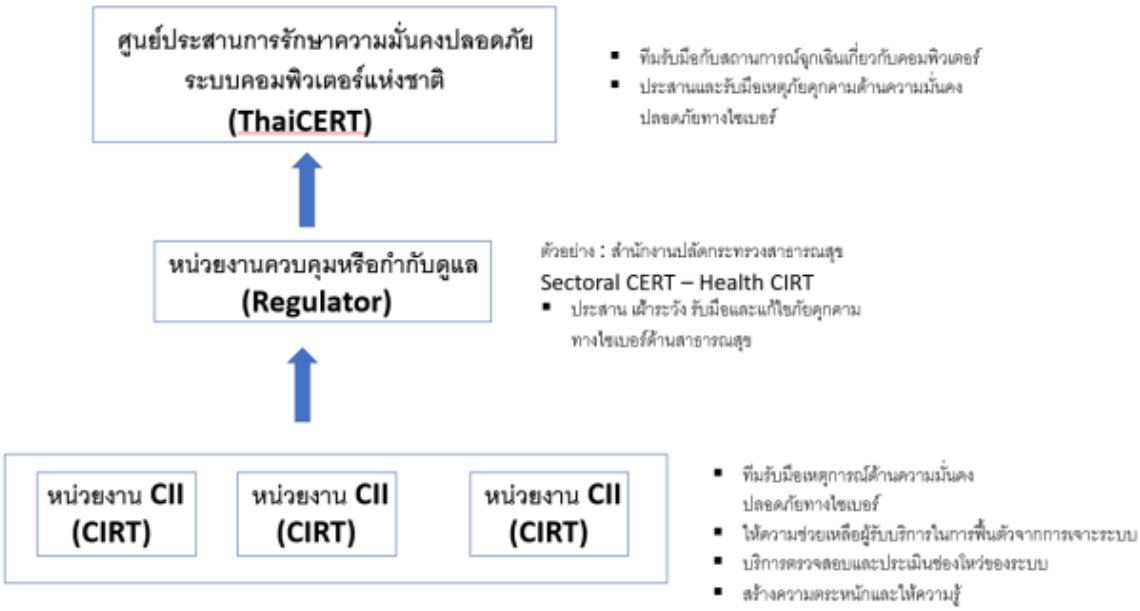
เกณฑ์การเรียกใช้งาน

แผนการรับมือภัยคุกคามทางไซเบอร์นี้จะถูกเรียกใช้งานเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคง ปลอดภัยของระบบที่สำคัญ เช่น

- การโจมตีทางไซเบอร์
- การรั่วไหลของข้อมูลสำคัญ
- การเข้าถึงระบบโดยไม่ได้รับอนุญาต

ขั้นตอนการเรียกใช้งาน

1. แจ้งเตือนทีม Cyber Incident Response Team (CIRT) ผ่านโทรศัพท์และอีเมล
2. เปิดใช้แผนการตอบสนอง โดยทีมรับมือเริ่มดำเนินการตามขั้นตอนที่กำหนด
3. แจ้งเตือนบุคลากรที่เกี่ยวข้องภายในองค์กรถึงสถานการณ์ฉุกเฉิน



1.6 ขั้นตอนจำกัดขอบเขต (Containment)

ขั้นตอนการจำกัดขอบเขต

1. แยกระบบที่ได้รับผลกระทบออกจากเครือข่ายหลักเพื่อป้องกันการแพร่กระจายไปยังระบบอื่น
2. ประเมินความเสียหายและระบุว่ามีระบบใดที่เกี่ยวข้อง
3. ดำเนินการแก้ไขเบื้องต้น เช่น การปิดพอร์ตที่ถูกโจมตีหรือการบล็อก IP ที่มีพฤติกรรมไม่พึงประสงค์
4. เก็บข้อมูลสำคัญจากระบบที่ได้รับผลกระทบเพื่อใช้ในกระบวนการสอบสวน

1.7 การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

ขั้นตอนการกู้คืน

1. ตรวจสอบและซ่อมแซมระบบที่ได้รับผลกระทบเพื่อให้แน่ใจว่าไม่มีช่องโหว่ที่ยังไม่ได้รับการแก้ไข
2. ฟื้นฟูระบบโดยการกู้คืนข้อมูลจากระบบสำรองล่าสุด (Backup)
3. ทดสอบระบบทั้งหมดเพื่อยืนยันว่าระบบปลอดภัยและสามารถทำงานได้ปกติ
4. ตรวจสอบการทำงานของระบบสำรองเพื่อให้แน่ใจว่าข้อมูลที่กู้คืนครบถ้วน

1.8 ขั้นตอนในการสอบสวน (Investigation)

ขั้นตอนการสอบสวน

1. เก็บหลักฐานทางดิจิทัลจากระบบที่ได้รับผลกระทบ เช่น ไฟล์ล็อก การจับภาพหน้าจอ การตรวจสอบ ข้อมูลเครือข่าย

2. วิเคราะห์สาเหตุของเหตุการณ์ เช่น ตรวจสอบวิธีการที่ผู้โจมตีใช้ในการเข้าถึงระบบ

3. ระบุผู้ที่อาจรับผิดชอบต่อเหตุการณ์ เช่น การระบุที่อยู่ IP หรือการตรวจสอบพฤติกรรมที่ผิดปกติ

4. จัดทำรายงานการสอบสวนและเสนอแนวทางการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

1.9 การเก็บรักษาหลักฐาน (Preservation of Evidence)

การจัดเก็บหลักฐาน

1. บันทึกข้อมูลจากระบบที่ได้รับผลกระทบ เช่น ล็อกไฟล์ การจับภาพหน้าจอ และอุปกรณ์เครือข่ายที่เกี่ยวข้อง

2. จัดเก็บอุปกรณ์ที่มีหลักฐานไว้ในที่ปลอดภัยเพื่อป้องกันการดัดแปลง เช่น จัดเก็บในตู้ที่มีการล็อกและ การควบคุมการเข้าถึง

3. ทำรายการหลักฐานทั้งหมดที่ถูกเก็บรวบรวม พร้อมระบุวันที่และเวลาที่ได้รับหลักฐาน

1.10 วิธีการมีส่วนร่วมกับบุคคลภายนอก (Engagement Protocols)

ผู้ที่เกี่ยวข้อง

บริษัทที่ปรึกษา : บริษัท A โทร. 02-111-XXXX

หน่วยงานบังคับใช้กฎหมาย: นาย C โทร. 02-111-XXXX

ขั้นตอนการมีส่วนร่วม

1. ติดต่อบุคคลภายนอกตามความจำเป็น เช่น บริษัทที่ปรึกษา สำหรับการวิเคราะห์หาสาเหตุ

2. ประสานงานกับหน่วยงานบังคับใช้กฎหมาย หากมีความจำเป็นในการดำเนินคดี

3. ส่งมอบหลักฐานที่เกี่ยวข้องให้กับผู้เชี่ยวชาญภายนอก พร้อมรายการหลักฐานทั้งหมดเพื่อใช้ในการตรวจสอบ

1.11 กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process)

ขั้นตอนการทบทวน

1. จัดประชุมทีม CIRT ภายใน 7 วันหลังจากเหตุการณ์สิ้นสุด เพื่อประเมินกระบวนการตอบสนอง

2. ประเมินผลการดำเนินการ เช่น ความเร็วในการตอบสนอง, การกู้คืนระบบ, และการจำกัดขอบเขตเหตุการณ์

3. ระบุข้อบกพร่องและข้อเสนอแนะสำหรับการปรับปรุงกระบวนการตอบสนอง

4. เสนอมาตรการปรับปรุงแผนรับมือภัยคุกคาม เพื่อให้มีประสิทธิภาพมากขึ้นในการป้องกันเหตุการณ์ในอนาคต

1.12 การสื่อสารและการทบทวนแผน (Communication and Plan Review)

การสื่อสารแผน

- สื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้กับบุคลากรที่เกี่ยวข้องทั้งหมดผ่านการอบรมและเอกสารแผน
- จัดอบรมพนักงานอย่างสม่ำเสมอเกี่ยวกับการตอบสนองต่อเหตุการณ์ฉุกเฉิน

การทบทวนแผน

- ทบทวนแผนการรับมือภัยคุกคามทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในสภาพแวดล้อมทางไซเบอร์
- ปรับปรุงแผนตามผลการทบทวนและการฝึกซ้อมแผนรับมือภัยคุกคาม

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. โครงสร้างทีมรับมือภัยคุกคามทางไซเบอร์
2. โครงสร้างทีมรับมือเหตุการณ์
3. รายงานสรุปเหตุการณ์
4. แผนการรับมือภัยคุกคามทางไซเบอร์

2. กระบวนการแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 24.2.1, ข้อ 24.2.2, ข้อ 24.2.3, ข้อ 24.2.4]

2.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าองค์กรมีแผนการสื่อสารที่มีประสิทธิภาพในภาวะวิกฤตที่เกิด จากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การสื่อสารและการเผยแพร่ข้อมูลเป็นไปอย่างทันท่วงที ประสานกัน และสอดคล้องกับทุกฝ่ายที่เกี่ยวข้อง

2.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการจัดทำ การทบทวน และการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตที่เกิด จากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ รวมถึงการกำหนดบทบาทหน้าที่และช่องทางการสื่อสารที่เหมาะสม

2.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management) : รับผิดชอบในการอนุมัติแผนการสื่อสารในภาวะวิกฤตและกำกับดูแล การดำเนินการในช่วงวิกฤต

2) ทีมสื่อสารในภาวะวิกฤต (Crisis Communication Team): รับผิดชอบในการดำเนินการตามแผนการสื่อสารในภาวะวิกฤต รวมถึงการจัดการการสื่อสารและการประสานงานกับทุกฝ่ายที่เกี่ยวข้อง

2.4 การจัดทำแผนการสื่อสารในภาวะวิกฤต (Development of Crisis Communication Plan)

1) การจัดตั้งทีมสื่อสารในภาวะวิกฤต

ขั้นตอน: จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต โดยประกอบด้วยบุคลากร ที่มีบทบาทสำคัญในการสื่อสารและการตัดสินใจ โดยการแต่งตั้งผู้บริหารระดับสูงเป็นหัวหน้า ทีมสื่อสารในภาวะวิกฤต และแต่งตั้งตัวแทนจากฝ่าย IT และฝ่ายอื่นๆ เป็นสมาชิกทีม

การจัดตั้งทีมสื่อสารในภาวะวิกฤต (Crisis Communication Team)

	ตำแหน่ง	หน้าที่รับผิดชอบ	ชื่อบุคคลที่รับผิดชอบ	ข้อมูลการติดต่อ
1	หัวหน้าทีมสื่อสารในภาวะวิกฤต (Crisis Communication Leader)	รับผิดชอบการตัดสินใจ หลักในการสื่อสาร และ ประสานงานกับผู้บริหาร ระดับสูง และควบคุม แผนการสื่อสารทั้งหมด	นาย A	โทร: 081-xxx-xxxx อีเมล: A@company.com
2	โฆษกหลัก (Primary Spokesperson)	เป็นตัวแทนองค์กรในการ แถลงข่าวและตอบคำถาม ต่อสื่อมวลชน	นาย B	โทร: 081-xxx-xxxx อีเมล: A@company.com

3	ผู้เชี่ยวชาญด้านเทคนิค (Technical Expert)	ให้ข้อมูลด้านเทคนิคที่ เกี่ยวข้องกับเหตุการณ์และ ให้คำแนะนำทางเทคนิคในการแก้ไขปัญหา	นาย C	โทร: 081-xxx-xxxx อีเมล: A@company.com
4	ผู้จัดการการสื่อสารกับสื่อมวลชน (Media Relations Manager)	จัดการสื่อมวลชนและ ประสานงานการเผยแพร่ข้อมูลผ่านช่องทางสื่อดั้งเดิมและโซเชียลมีเดีย	นาย D	โทร: 081-xxx-xxxx อีเมล: A@company.com
5	ผู้จัดการด้านการสื่อสารภายใน (Internal Communications Manager)	รับผิดชอบการสื่อสาร ภายในองค์กรและประสานงานกับพนักงาน	นาย E	โทร: 081-xxx-xxxx อีเมล: A@company.com
6	ผู้จัดการการประสานงานกับหน่วยงานภายนอก (External Coordination Manager)	ประสานงานกับหน่วยงาน ภายนอกที่เกี่ยวข้อง เช่น หน่วยงานรัฐและผู้มีส่วนได้ส่วนเสีย	นาย F	โทร: 081-xxx-xxxx อีเมล: A@company.com
7	ผู้ประสานงานฉุกเฉิน (Emergency Response Coordinator)	ดูแลการจัดการแผนฉุกเฉิน และการติดต่อประสานงาน กับหน่วยงานด้านความปลอดภัย	นาย G	โทร: 081-xxx-xxxx อีเมล: A@company.com

2) การระบุสถานการณ์จำลองและแผนการดำเนินการ

ขั้นตอน: ระบุสถานการณ์จำลองเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น เช่น กรณีที่มีการรั่วไหลของข้อมูลสำคัญ และกำหนดแผนการดำเนินการที่เกี่ยวข้องสำหรับแต่ละ สถานการณ์ ซึ่งต้องมีการกำหนดขั้นตอนการสื่อสารกับสาธารณชนและผู้มีส่วนได้ส่วนเสีย

3) การระบุกลุ่มเป้าหมายและผู้มีส่วนได้ส่วนเสีย

ขั้นตอน: ระบุกลุ่มเป้าหมายและผู้มีส่วนได้ส่วนเสีย พร้อมจัดทำรายชื่อผู้ใช้บริการหลักผู้รับเหมาและหน่วยงานรัฐบาลที่ต้องได้รับการแจ้งเตือนและข้อมูลในกรณีที่เกิดการโจมตีทาง ไซเบอร์ ในแต่ละสถานการณ์จำลอง เพื่อให้แน่ใจว่าการสื่อสารครอบคลุมทุกฝ่ายที่ได้รับผลกระทบ

4) การระบุช่องทางการเผยแพร่ที่เหมาะสม

ขั้นตอน: ระบุแพลตฟอร์มและช่องทางการเผยแพร่ข้อมูลที่เหมาะสม สำหรับการสื่อสาร ในช่วงวิกฤต โดยการใช้โซเชียลมีเดีย หรือเว็บไซต์ขององค์กร

2.5 การประสานงานและการฝึกซ้อม (Coordination and Drills)

1) การประสานงานระหว่างทุกฝ่ายที่เกี่ยวข้อง

ขั้นตอน : ตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้มีการตอบสนองที่สอดคล้องและมีประสิทธิภาพ โดยการจัด ประชุม

ระหว่างทีมสื่อสารในภาวะวิกฤตกับทีม IT และฝ่ายอื่นๆ ที่เกี่ยวข้อง รวมถึงหน่วยงาน ที่รับผิดชอบ ตามพรบ ไซเบอร์กำหนด

2) การฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต

ขั้นตอน : ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อทดสอบความพร้อมและความสามารถในการสื่อสารในช่วงวิกฤต

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ทีมสื่อสารในภาวะวิกฤต
2. แผนการสื่อสารในภาวะวิกฤต
3. หลักฐานหรือเอกสารแสดงการดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต

1. กระบวนการการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม. 43, ม. 44, ม. 45, ม. 56, ม. 57, ม. 58), ประมวลและกรอบ [ข้อ 24.3.1, ข้อ 24.3.2]

1.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อให้องค์กรมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งใน ระดับชาติและระดับภาคส่วน เพื่อเพิ่มความพร้อมและประสิทธิภาพในการตอบสนองต่อเหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์

1.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการวางแผน การดำเนินการ และการประเมินผลการฝึกซ้อมความมั่นคง ปลอดภัยไซเบอร์ รวมถึงการปฏิบัติตามคำขอของหน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่มีอำนาจตาม พรบ ไซเบอร์ กำหนด

1.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

1) ผู้บริหาร (Top Management): รับผิดชอบในการอนุมัติและสนับสนุนการมีส่วนร่วมในกระบวนการ ฝึกซ้อม รวมถึงการจัดสรรทรัพยากรที่จำเป็น

2) ทีมร่วมการฝึกซ้อม (Exercise Security Team): รับผิดชอบในการวางแผนและดำเนินการฝึกซ้อมความ มั่นคงปลอดภัยไซเบอร์ รวมถึงการประสานงานกับหน่วยงานภายนอก

3) บุคลากรที่เกี่ยวข้อง (Relevant Personnel): มีหน้าที่เข้าร่วมในการฝึกซ้อมตามที่ระบุไว้ในแผนการ รับมือภัยคุกคามทางไซเบอร์

1.4 การวางแผนและการเตรียมการฝึกซ้อม (Planning and Preparation for Cybersecurity Exercise)

1) การจัดตั้งทีมสื่อสารในภาวะวิกฤต

ขั้นตอน : องค์กร, หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้อง มีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งจากหน่วยงาน ควบคุมหรือกำกับดูแลหรือหน่วยงานที่มีอำนาจตาม พรบ ไซเบอร์ กำหนด

2) การระบุตัวบุคคลที่ต้องเข้าร่วมฝึกซ้อม

ขั้นตอน : ระบุบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์เพื่อให้เข้า ร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

1.5 การให้ข้อมูลและการประสานงาน (Providing Information and Coordination)

1) การให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ

ขั้นตอน : ปฏิบัติตามคำขอใด ๆ ของหน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่มีอำนาจ ตามพรบ ไซเบอร์ กำหนด โดยให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญขององค์กรหรือหน่วยงาน สำหรับการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์

2) การประสานงานระหว่างฝ่ายที่เกี่ยวข้อง

ขั้นตอน : ประสานงานระหว่างทีมรักษาความปลอดภัยสารสนเทศกับหน่วยงานภายนอกและผู้ มีส่วนได้ส่วนเสีย เพื่อให้แน่ใจว่าการฝึกซ้อมเป็นไปอย่างมีประสิทธิภาพและครอบคลุมทุก ฝ่ายที่เกี่ยวข้อง หรือมีการจัดการประชุมระหว่างหน่วยงานรัฐ หน่วยงานโครงสร้างพื้นฐาน สำคัญ และหน่วยงานระดับชาติ เพื่อประสานการฝึกซ้อมร่วมกัน

1.6 การดำเนินการฝึกซ้อมและการประเมินผล (Execution and Evaluation of Cybersecurity Exercise)

1) การดำเนินการฝึกซ้อม

ขั้นตอน : ดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ตามแผนที่กำหนด และติดตามการดำเนินงานของบุคลากรที่เกี่ยวข้อง รวมทั้งการดำเนินการฝึกซ้อมการตอบสนองต่อการโจมตี ทางไซเบอร์ที่จำลองขึ้น พร้อมสังเกตการณ์การตอบสนองของทีมรักษาความปลอดภัย สารสนเทศ

2) การประเมินผลการฝึกซ้อม

ขั้นตอน : ประเมินผลการฝึกซ้อมเพื่อวิเคราะห์ประสิทธิภาพในการตอบสนองต่อภัยคุกคาม และระบุจุดที่ต้องปรับปรุงในการฝึกซ้อมครั้งถัดไป หรืออาจจัดทำรายงานผลการฝึกซ้อมที่ สรุปจุดแข็งและจุดอ่อนที่ต้องปรับปรุง และนำเสนอให้กับผู้บริหารเพื่อวางแผนการปรับปรุง ในอนาคต

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนการฝึกซ้อม
2. ทีมร่วมการฝึกซ้อมและบทบาท รวมถึงหน้าที่ของทีมร่วมการฝึกซ้อม
3. รายงานผลการฝึกซ้อม

การกู้คืน
(Recover)

1. กระบวนการการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 25.1.1, ข้อ 25.1.2]

1.1 วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าบริการที่สำคัญขององค์กร สามารถให้บริการต่อไปได้อย่าง ต่อเนื่องในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้กระบวนการ ฟื้นฟูความเสียหายเป็นไปอย่างมีประสิทธิภาพและใช้เวลาสั้นในการฟื้นฟู

1.2 ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) การทบทวนแผน BCP ของผู้ให้บริการภายนอก และการฝึกซ้อมแผน BCP เพื่อประเมินความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

1.3 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- ผู้บริหาร (Top Management): รับผิดชอบในการอนุมัติและสนับสนุนการจัดทำและการทบทวนแผน BCP รวมถึงการจัดสรรทรัพยากรที่จำเป็นสำหรับการฟื้นฟูความเสียหาย
- ทีมรักษาความต่อเนื่องทางธุรกิจ (Business Continuity Team): รับผิดชอบในการพัฒนาแผน BCP และการประสานงานกับผู้ให้บริการภายนอกเพื่อให้แน่ใจว่าแผน BCP ของผู้ให้บริการภายนอกสอดคล้องกับแผนขององค์กร

1.4 การจัดทำและทบทวนแผนความต่อเนื่องทางธุรกิจ (Development and Review of Business Continuity Plan)

1) การจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP)

ขั้นตอน: จัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) เพื่อให้บริการที่สำคัญขององค์กรหรือหน่วยงานสามารถดำเนินการต่อไปได้ในกรณีที่เกิดการหยุดชะงักจากเหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์ โดยต้องมีการกำหนดขอบเขตของแผน BCP ที่ครอบคลุมทุกส่วนที่เกี่ยวข้อง กับบริการที่สำคัญ และการกำหนดระยะเวลาในการฟื้นฟู (RTO, RPO)

2) การระบุตัวบุคคลที่ต้องเข้าร่วมฝึกซ้อม

ขั้นตอน: ทบทวนแผน BCP ของผู้ให้บริการภายนอกเพื่อให้แน่ใจว่ามีความสอดคล้องกับแผนความต่อเนื่องทางธุรกิจ ขององค์กรหรือหน่วยงาน อีกทั้ง เพื่อให้แน่ใจว่าการฟื้นฟูระบบ สามารถดำเนินการได้ภายในระยะเวลาที่กำหนดในแผนความต่อเนื่องทางธุรกิจ ขององค์กร หรือหน่วยงาน

1.5 การฝึกซ้อมและการประเมินผล (Exercise and Evaluation)

1) การระบุตัวบุคคลที่ต้องเข้าร่วมฝึกซ้อม

ขั้นตอน: ดำเนินการฝึกซ้อมแผน BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ แผนในการรับมือกับภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซ เบอร์ โดยการการจำลองสถานการณ์การโจมตีทางไซเบอร์และการทดสอบความสามารถของ บุคลากรในการดำเนินการตามแผน BCP

2) การประเมินผลการฝึกซ้อม

ขั้นตอน: ประเมินผลการฝึกซ้อมแผน BCP เพื่อวิเคราะห์จุดแข็งและจุดอ่อนที่ต้องปรับปรุงใน การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ และต้องมีการจัดทำรายงานผลการฝึกซ้อมที่ สรุปผลการดำเนินงานพร้อมข้อเสนอแนะการปรับปรุงแผน BCP เพื่อเพิ่มประสิทธิภาพในการ ฟื้นฟูความเสียหายในอนาคต

การทบทวนกระบวนการดำเนินการ (Procedure Review)

กระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจใน ประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนความต่อเนื่องทางธุรกิจ
2. แผนการสอบทานแผนของผู้ให้บริการภายนอก
3. ผลการฝึกซ้อมแผนตามแผนความต่อเนื่องทางธุรกิจ