กรอบดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์
กรมกิจการเด็กและเยาวชน

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์กรมกิจการเด็กและเยาวชน

๑. วัตถุประสงค์

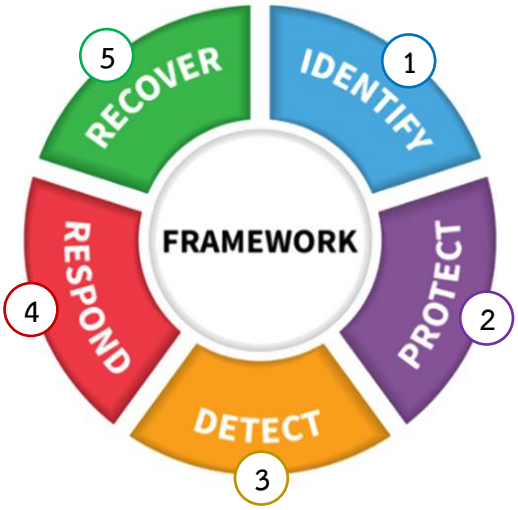
เพื่อกำหนดกรอบแนวคิด รวมถึงวิธีปฏิบัติของระบบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Management) สำหรับนำไปใช้กับการดำเนินงานและการจัดการด้านเทคโนโลยีและสารสนเทศของกรมกิจการเด็กและเยาวชน

๒. ขอบเขต

เพื่อกำหนดกรอบและวิธีปฏิบัติสำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) สำหรับบริหารจัดการเทคโนโลยีและสารสนเทศของกรมกิจการเด็กและเยาวชน

๓. กรอบดำเนินการ

กรอบดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) จัดทำขึ้นตามประกาศคณะกรรมการกำกับดูด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ซึ่งสามารถสรุปกิจกรรมที่ต้องดำเนินการได้ดังต่อไปนี้



ภาพที่ ๑ กรอบดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework)

กรอบดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework)

๑. ความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๑.๑ รูปแบบภัยคุกคาม

๑) Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบ คอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบ คอมพิวเตอร์ และอาจแชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมี พฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการ ผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus) เวิร์ม (worms) โทรจัน (Trojans)

๒) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ ที่มีช่องโหว่เพื่อแก้ไข เว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมาย ปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๓) Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดย ใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔) Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์ และ Web Server หรือ Database Server

๕) Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาต ไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

๖) DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบกาให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๗) Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูล ของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการ ระบบ ไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๘) Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือ ไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิด การโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

๙) Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบ แฝงตัว อยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ ถูกโปรแกรมไว้ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐) Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่อง คอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๑๑) Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการ ติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อ ประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

๑๒) ผู้บุกรุก (Hacker) ผู้ที่ไม่ได้รับอนุญาตในหารใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหาย จากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๑.๒ การจัดการทรัพย์สิน (Asset Management)

๑) ระบุและตรวจสอบ “ทะเบียนทรัพย์สินสารสนเทศ” ของหน่วยงาน โดยรายการทรัพย์สินสารสนเทศ ประกอบไปด้วย สารสนเทศและอุปกรณ์สารสนเทศ ซึ่งจัดแบ่งตามประเภท ดังนี้

- สารสนเทศ (Information) เช่น ข้อมูลในฐานข้อมูล ไฟล์ข้อมูล สัญญา เอกสาร/คู่มือระบบ ข้อมูลการวิจัย คู่มือผู้ใช้งาน ทรัพยากรในการฝึกอบรม ขั้นตอนการปฏิบัติงานหรือสนับสนุน แผน ความต่อเนื่องทางธุรกิจ แผนการกู้คืนสภาพ ประวัติการตรวจสอบสารสนเทศที่สำคัญอื่น ๆ
- ทรัพย์สินทางซอฟต์แวร์ (Software Assets) เช่น ซอฟต์แวร์สำเร็จรูป โปรแกรมระบบเครื่องมือสำหรับพัฒนา โปรแกรมประเภทยูทิลิตี้ (System Utilities)
- ทรัพย์สินทางฮาร์ดแวร์ (Hardware Assets) เช่น อุปกรณ์สารสนเทศ อุปกรณ์ติดต่อสื่อสาร อุปกรณ์เครือข่าย สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้
- การบริการด้านการประมวลผล การติดต่อสื่อสาร และสาธารณูปโภคอื่น ๆ (Services) เช่น บริการอินเตอร์เน็ต บริการควบคุมการเข้าถึงอาคาร บริการระบบควบคุมความร้อน บริการแสง สว่าง บริการไฟฟ้าและพลังงาน บริการควบคุมความชื้น

๒) ทบทวนทะเบียนทรัพย์สินสารสนเทศของหน่วยงานและปรับปรุงให้ทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง

๓) กำหนดผู้รับผิดชอบในทรัพย์สินสารสนเทศ หรือ จัดการให้สิทธิการใช้งานทรัพย์สินสารสนเทศ

๔) กำหนดกระบวนการจัดการให้สิทธิการใช้งานทรัพย์สินสารสนเทศ โดยแบ่งแยกหน้าที่ให้เหมาะสมเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาตหรือโดยไม่ได้ ตั้งใจ เช่น แบ่งแยกบุคคลที่มีหน้าที่ในขั้นตอนการร้องขอ (Request) และขั้นตอนการอนุมัติ (Approve) ออกจากกัน

๕) จัดหมวดหมู่ทรัพย์สินสารสนเทศตามข้อกำหนดของกฎหมาย คุณค่า ความสำคัญ และความอ่อนไหวต่อการเปิดเผยหรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๖) จัดทำขั้นตอนปฏิบัติสำหรับการทำป้ายบ่งชี้ทรัพย์สินสารสนเทศ และนำไปปฏิบัติให้สอดคล้องกับรูปแบบการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

๗) ทรัพย์สินสารสนเทศที่อยู่ในระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” ให้มีการจัดทำป้ายบ่งชี้ทรัพย์สินสารสนเทศ โดยจัดทำเป็นรหัสและระบุรหัสลงในทะเบียนทรัพย์สินสารสนเทศ เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงสารสนเทศดังกล่าวได้

๘) จัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ เพื่อป้องกันความเสียหายต่อทรัพย์สิน

๙) เก็บสารสนเทศที่อยู่ในระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ที่อยู่ในรูปแบบเอกสารหรือสื่อ บันทึกข้อมูลอิเล็กทรอนิกส์ โดยใส่กุญแจ (วิธีที่ดีที่สุด คือ เก็บไว้ในตู้นิรภัย หรือตู้ใส่ของ หรือครุภัณฑ์รูปแบบอื่น ๆ ที่รักษาความปลอดภัยได้)

๑๐) ทบทวนแผนการบำรุงรักษาทรัพย์สินสารสนเทศของหน่วยงานอย่างน้อยปีละ 1 ครั้ง

๑๑) กรณีมีความจำเป็นต้องมีการแลกเปลี่ยนข้อมูลที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ให้ ส่งผ่านช่องทางระบบบริการจัดส่งข้อมูลหรือระบบจดหมายอิเล็กทรอนิกส์ของ ดย.

๑๒) ตรวจสอบอายุของสื่อบันทึกข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้คงสภาพความสามารถในการเก็บข้อมูลบนอุปกรณ์

๑๓) ควบคุมและตรวจสอบการถอดถอนหรือทำลายสารสนเทศของ ดย. ออกจากอุปกรณ์ดังกล่าวเมื่อ เลิกใช้งานสื่อบันทึกข้อมูลหรือโอนให้หน่วยงานอื่นหรือจำหน่ายออกจากองค์กร

๑๔) ตรวจสอบโปรแกรมไม่พึงประสงค์ก่อนนำสื่อบันทึกข้อมูลมาใช้งาน และตรวจสอบข้อมูลภายในสื่อบันทึกข้อมูลเป็นประจำ

๑.๓ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้า ขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบ เครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่ มีประสิทธิภาพเพียงพอ

๒) ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการ ดำเนินงานด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงานการ มอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่าง ละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยี สารสนเทศและการสื่อสาร รวมทั้งบุคลากร ภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความ เสี่ยงทั้งสิ้น

๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การ ติดตั้งอุปกรณ์ในพื้นที่ไม่ เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ malware, Trojan, Adware เป็นต้น ทั้งที่ เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือ จากคอมพิวเตอร์ โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของ โปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของ ซอฟต์แวร์นั้น ๆ หรือการถูกผูกไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่ง สำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิด ลิขสิทธิ์ เป็นต้น

๕) ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบ สารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลายความเสี่ยงจากผู้บุกรุก ข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาด ความน่าเชื่อถือและสร้างความ เสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหาร จัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูล สารสนเทศและการสื่อสารเป็น ปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีสาวนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความ ปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจาก ธรรมชาติ หรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อ ระบบข้อมูลสารสนเทศและเทคโนโลยี

๖) ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบ สารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลายความเสี่ยงจากผู้บุกรุก ข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาด ความน่าเชื่อถือและสร้างความ เสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหาร จัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูล สารสนเทศและการสื่อสารเป็น ปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความ ปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจาก ธรรมชาติ หรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อ ระบบข้อมูลสารสนเทศและเทคโนโลยี

๗) ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่ เพียงพอ และต่อการเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลา

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้น ทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของ แผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการ พิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขต ของระดับความเสี่ยงที่สามารถยอมรับได้ **ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของ เหตุการณ์ต่าง ๆ** ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง
1-5	ต่ำ	ยอมรับความเสี่ยง
6-10	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)
11-16	ปานกลางค่อนข้างสูง	ยอมรับความเสี่ยง
17-24	สูง	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)
25	สูงมาก	ยอมรับความเสี่ยง

การจัดการความเสี่ยง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
1. การนำเครื่องส่วนบุคคลเข้ามาใช้ในองค์กร	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร	1. จัดทำทะเบียนประวัติ เครื่องคอมพิวเตอร์ส่วนบุคคล 2. จัดทำทะเบียนเครื่องด้วย Mac address
2. เครื่องคอมพิวเตอร์ของพนักงานไม่มี password ในการป้องกัน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร	จัดทำระบบควบคุมการใช้งานคอมพิวเตอร์ เช่น ติดตั้งระบบ Active Directory ของ Microsoft Window
3. ระบบที่ใช้ในองค์กรบางระบบไม่สามารถเปลี่ยน password ได้	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	ประสานงานกับ Vendor ที่เป็นเจ้าของระบบแต่ละระบบ เพื่อให้มี การปรับปรุงระบบให้รองรับการเปลี่ยน password ได้
4. ลิขสิทธิ์โปรแกรมที่ใช้ในองค์กร	ความเสี่ยงด้าน โปรแกรมคอมพิวเตอร์	จัดซื้อและจัดหาโปรแกรมให้ถูกต้องตามลิขสิทธิ์
5. การประกาศนโยบายการใช้งานระบบสารสนเทศ	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจาก ผู้ปฏิบัติงาน	ประกาศนโยบายให้พนักงานได้รับทราบ
6. การตรวจสอบช่องโหว่บนระบบ Server และระบบ Network	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร	1. ปรับแก้ไข Config ของโปรแกรม เพื่อปิดช่องโหว่ 2. แจ้ง Vendor ให้ทำการปรับแก้ไขโปรแกรม 3. จัดซื้อและจัดหาระบบป้องกันความปลอดภัยทางคอมพิวเตอร์

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๑) เมื่อมีแนวโน้มในการเกิดช่องโหว่ทางเทคนิค ต้องระบุถึงความเสี่ยงที่เกี่ยวข้องและการกระทาที่จะต้อง ดำเนินงาน ทั้งนี้การกระทำดังกล่าวอาจเกี่ยวข้องกับการปรับปรุงระบบ (Patch) ที่มีช่องโหว่ หรือการ ใช้การควบคุมอื่น ๆ ควรดำเนินงานตามมาตรการควบคุมที่เกี่ยวข้องกับการบริหารจัดการการ เปลี่ยนแปลง หรือตามขั้นตอนการตอบสนองต่อความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ โดยขึ้นอยู่กับความจำเป็นเร่งด่วนที่จะต้องจัดการช่องโหว่ทางเทคนิค

๒) ประเมินความเสี่ยงและทดสอบการปรับปรุงระบบ (Patch) ก่อนติดตั้งบนอุปกรณ์ที่ใช้งานจริง (Production) เพื่อให้มั่นใจได้ว่า การติดตั้งมีประสิทธิภาพและไม่ส่งผลกระทบข้างเคียงอย่างรุนแรง ในกรณีที่ไม่มีการปรับปรุงระบบ (Patch) ต้องจัดให้มีการควบคุมอื่น ๆ เช่น

- การปิดบริการที่เกี่ยวข้องกับช่องโหว่ทางเทคนิค
- การปรับเปลี่ยนหรือเพิ่มการควบคุมในการเข้าถึง เช่น Firewalls
- การเพิ่มการเฝ้าระวัง เพื่อตรวจจับหรือป้องกันการจู่โจม
- การเพิ่มความตระหนักถึงช่องโหว่ทางเทคนิค

๓) บันทึกเหตุการณ์เพื่อการตรวจสอบ (Audit Log) ในทุก ๆ ขั้นตอนปฏิบัติงาน

๔) ตรวจสอบและประเมินกระบวนการในการบริหารจัดการช่องโหว่ทางเทคนิคอย่างสม่ำเสมอ เพื่อให้ มั่นใจว่ากระบวนการดังกล่าวมีประสิทธิภาพและประสิทธิผล

๕) จัดการช่องโหว่ทางเทคนิคกับระบบที่มีความเสี่ยงสูงก่อน

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๑) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก (ถ้ามี)

๒) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก

๓) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร

๔) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตามข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าวได้

๕) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า

๖) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของบุคคลภายนอก

๗) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ

๘) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

๑) Discretionary access control (DAC) คือ การควบคุมการเข้าถึงทรัพยากรที่เจ้าของเป็นผู้ควบคุมอย่างสมบูรณ์ โดยผู้เป็นเจ้าของสามารถกำหนดสิทธิ์การเข้าถึงของผู้ใช้รายอื่น เช่น การอนุญาตให้เข้าไปอ่าน หรือแก้ไขข้อมูล และเมื่อมีการร้องขอเพื่อเข้ามาในระบบ เจ้าของทรัพยากรสามารถอนุญาตคำร้องของผู้ใช้รายนั้นได้ทันที นอกจากนี้ยังสามารถโอนสิทธิ์ความเป็นเจ้าของให้กับผู้อื่นได้อีกด้วย ทำให้ DAC เป็นวิธีการควบคุมที่มีความยืดหยุ่น แต่จะไม่เหมาะหากนำไปใช้กับการปกป้องข้อมูลที่เป็นความลับ หรือทรัพยากรที่ต้องการความปลอดภัยสูง

๒) Mandatory access control (MAC) คือ การควบคุมแบบส่วนกลาง ซึ่งจะกำหนดการเข้าถึงทรัพยากรตามนโยบาย หรือตามระดับชั้นความปลอดภัยที่วางไว้ เป็นการควบคุมโดยระบบไม่ใช่โดยเจ้าของ ทำให้ผู้ใช้ไม่สามารถเปลี่ยนแปลงนโยบายต่าง ๆ เหล่านั้นได้ วิธีการควบคุมแบบนี้มักใช้กับระบบที่มีความอ่อนไหวสูง เช่น ระบบของรัฐบาล

๓) Role-based access control (RBAC) คือ เป็นการจัดการสิทธิ์ในการเข้าถึงระบบ โดยจะเป็นตัวกำหนดบทบาทว่าผู้ใช้รายใดสามารถเข้าถึงส่วนใดได้บ้าง เช่น ผู้ใช้ A สามารถเข้าไปลบ แก้ไขข้อมูล และติดตั้งซอฟต์แวร์ใหม่ได้ ขณะที่ผู้ใช้ B ทำได้เพียงแค่ลบ หรือแก้ไขข้อมูล แต่ไม่สามารถติดตั้งซอฟต์แวร์ได้ ส่วนคนที่เหลืออาจได้สิทธิ์แค่เข้าไปอ่านข้อมูลเท่านั้น นอกจากนี้ผู้ใช้งานหนึ่งคนยังสามารถมีได้หลายบทบาท เช่น ได้บทบาทเป็น Admin ของระบบหนึ่ง แต่เป็นแค่ User ของอีกระบบหนึ่งก็ได้เช่นกัน นั่นทำให้วิธีการควบคุมแบบ RBAC มีการนำไปใช้อย่างกว้างขวาง และยังสามารถนำไปใช้ร่วมกับการควบคุมทั้งแบบ DAC และ MAC ได้อีกด้วย

๔) Attribute Based Access Control (ABAC) คือ เป็นการควบคุมการเข้าถึงทรัพยากรโดยการคัดกรองจากคุณสมบัติของผู้ใช้บางประการ เช่น หากผู้ใช้เป็นพนักงานของบริษัท และอยู่ฝ่าย IT ด้าน Security จะสามารถเข้าถึงอุปกรณ์ Firewall ได้ หรือกำหนดให้ผู้ใช้ที่เป็น Manager เท่านั้นที่มีสิทธิ์เข้าไปแก้ไขข้อมูลที่มีความอ่อนไหว

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๑) การใช้งาน SSH หรือเรียกว่า Secure Shell เป็น network protocol ที่เอาไว้ให้เราเชื่อมต่อระหว่าง Server กับ Server โดยที่ไม่ต้องใช้ Username หรือ Password แต่ใช้สิ่งที่เรียกว่า Public Key และ Private Key เพื่อยืนยันตัวตนแทน

๒) Strong Password Policy คือ การให้ความสำคัญกับพาสเวิร์ดรหัสผ่านยังคงเป็นเครื่องมืออันดับหนึ่งที่ใช้ยืนยันตัวตนของผู้ใช้ ซึ่งรหัสผ่านที่ดีควรมีความยาวไม่น้อยกว่า 10 ตัวอักษร และประกอบด้วยตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ หรืออีกทางเลือกหนึ่งคือใช้ Passphrase ความยาวประมาณ 15 ตัวอักษร เพื่อให้จดจำได้ง่าย

- กำหนดให้รหัสผ่านมีความยาวขั้นต่ำ 10 ตัวอักษร หรือ 15 ตัวอักษรสำหรับ Passphrases
- บังคับใช้ Password History โดยย้อนหลังไป 10 ครั้ง
- ตั้งค่า Password Age ไม่น้อยกว่า 3 วัน และสูงสุดไม่เกิน 90 วัน (180 วันสำหรับ Passphrases)
- กำหนดให้รหัสผ่านมีความซับซ้อน คือ ประกอบด้วยตัวพิมพ์ใหญ่และเล็ก ตัวเลข และอักขระ

๓) Encrypt the Data สำหรับการจัดเก็บข้อมูล หากเป็นข้อมูลที่มีความสำคัญและเป็นความลับควรจะ Encrypt ข้อมูล เพื่อความปลอดภัย

๔) การตั้งค่า Server Log ทุก ๆ Server ที่มีควรตั้งค่า Log ไปไว้ในที่เดียว ไม่ควรแยกกัน เนื่องจากหากต้องการจะตรวจสอบและข้อมูลอยู่คนละที่กันจะทำให้ตรวจสอบได้ยาก

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

Remote Access เป็นความสามารถในการเข้าถึงคอมพิวเตอร์หรือเครือข่ายจากระยะทางไกล ให้สามารถเข้าถึงเครือข่าย ผู้ใช้ตามบ้านที่เข้าถึงอินเตอร์เน็ต โดยผ่านการผู้ใช้บริการอินเตอร์เน็ต นอกจากนี้ Remote Access ครอบคลุมถึงการใช้สายพิเศษระหว่างคอมพิวเตอร์หรือ LAN ที่อยู่ระยะไกลกับศูนย์กลางหรือเครือข่ายหลัก สายพิเศษมักจะมีราคาแพง และความยืดหยุ่นน้อยแต่อัตราข้อมูลสูง ISDN เป็นวิธีหนึ่งในการติดต่อของสำนักงาน เนื่องจากได้รวมการหมุนด้วยอัตราข้อมูลสูง เทคโนโลยี wireless cable modem และ Digital Subscriber Line สามารถนำมาใช้การติดต่อแบบ Remote Access

๒.๔ เก็บข้อมูลแบบถอดได้ (Removable Storage Media)

อุปกรณ์จัดเก็บข้อมูลที่สามารถเคลื่อนย้ายไปต่อกับคอมพิวเตอร์เครื่องใดก็ได้ โดยการเชื่อมต่อเข้ากับสายนำสัญญาณชนิดต่าง ๆ หรือสอดใส่อุปกรณ์บันทึกข้อมูลเฉพาะเข้ากับตัวอุปกรณ์ส่วนควบหลัก เพื่อให้เปิดใช้งาน

ได้ เหมาะอย่างยิ่งสำหรับการโอนถ่ายข้อมูลจากเครื่องต้นทาง ไปยังเครื่องปลายทาง แต่ความสะดวกในการพกพาข้อมูลของแฟลชไดร์ฟมาพร้อมกับโอกาสที่มากขึ้นในการได้รับและแพร่กระจายไวรัสและมัลแวร์/แรนซัมแวร์ จากเครื่องสู่เครื่องและฝังรหัสอันตรายเข้าไปในเครือข่ายองค์กร โดยมาตรการป้อง และแก้ไขเบื้องต้น คือ การลงโปรแกรมป้องกันไวรัสเพื่อให้ USB Flash Drive ปราศจากไวรัส และสแกนไวรหัสทุกครั้งก่อนเปิดใช้งาน

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับบุคลากรภายในองค์กร โดยหัวข้อที่อบรม จะเป็นความรู้เกี่ยวกับ

๑) ความหมายของ Cybersecurity

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้นรวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

๒) รูปแบบภัยคุกคามของ Cybersecurity โดยข้อมูลเกี่ยวกับรูปแบบภัยคุกคามจะอยู่ในหัวข้อ **“การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)”**

๓) ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

◈ วันทำงาน ◈

(๑) Computer

- ควรมีการแยก user ใช้งานกันของแต่ละบุคคล
- ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด password และติด password ไว้ที่หน้าจอ
- มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น

(๒) Password

- มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ
- มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
- ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย
- มีการเปลี่ยน Password อย่างสม่ำเสมอ
- ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
- ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
- ไม่ควรบอก Password แก่ผู้อื่น

(๓) E-mail

- ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
- ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
- ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค
- เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

(๔) Website

- ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่าง ๆ
- ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser
- เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
- ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น google chrome mozilla firefox เป็นต้น
- ควรมีการอัพเดทเวอร์ชั่นของ Browser อย่างสม่ำเสมอ
- ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing
- ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

(๕) Messaging

- ไม่ควรบันทึก password ไว้ที่โปรแกรม
- กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง
- มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่าง ๆ ที่ได้รับมา
- มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ
- ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

(๖) Conference

- ใช้สถานที่เหมาะสมกับการ Conference
- ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
- แชร์เอกสารต่างๆ อย่างระมัดระวัง
- ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
- มีการอัพเดทเวอร์ชั่นของโปรแกรม Conference อย่างสม่ำเสมอ
- ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการ

(๗) Cloud Storage

- แยก User ในการใช้งานของแต่ละบุคคล
- ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
- ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
- ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ
- มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ
- มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

◈ วันพักผ่อน ◈

(๑) Computer

- ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
- ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ควรติดตั้ง anti-malware และมีการอัพเดตอย่างสม่ำเสมอ
- มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- มีการใช้ Password ที่ดีและไม่ควรบอก Password แก่ผู้อื่น

(๒) Free WIFI

- ไม่ควรใช้งาน WiFi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
- หลีกเลี่ยงการใช้งาน WiFi ที่ไม่รู้ที่มาในการให้บริการ

(๓) Mobile

- เปิดการใช้งาน PIN/Password,Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
- ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
- กำหนด Application permission ให้เหมาะสม
- มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างเหมาะสม
- มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

(๔) Internet Connection

- เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
- เปลี่ยน SSID และรหัสผ่านของ WiFi ที่กำหนดมาจากผู้ให้บริการ
- กำหนดผู้ที่สามารถเข้าใช้งานอินเทอร์เน็ตเท่าที่จำเป็น

(๕) IoT Devices

อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือ Application ต่าง ๆ ได้ เช่น หลอดไฟ,พัดลม,เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

- เปลี่ยน Default Password ที่มาจากโรงงาน
- ควรมีการอัพเดทเฟิร์มแวร์ให้เป็นเวอร์ชั่นล่าสุด
- ใช้ application ที่ใช้ในการคอนโทรลกับอุปกรณ์ต่าง ๆ ให้เป็นเวอร์ชั่นล่าสุด

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

Data Sharing คือ กระบวนการแบ่งปันข้อมูลจากผู้ถือข้อมูลต้นทาง ไปยังผู้รับข้อมูลปลายทางที่มีความต้องการนำข้อมูล นั้นไปใช้ประโยชน์ โดยกระบวนการแบ่งปันข้อมูลดังกล่าวควรมีความปลอดภัย และเป็นไปตามกฎหมายที่เกี่ยวข้อง เช่น หากมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล การแบ่งปันข้อมูลนั้นก็ควรสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งหัวใจสำคัญของการทำ Data Sharing คือต้องทำให้เกิดกระบวนการแบ่งปันข้อมูลที่มีความสะดวก (Convenience) ปลอดภัย (Secure) และเคารพสิทธิส่วนบุคคล (Privacy)

ในส่วนของการทำ Data Sharing จะประกอบด้วยผู้เล่นที่เกี่ยวข้องหลายส่วน ยกตัวอย่างเช่น ผู้ถือข้อมูลต้นทาง (Data Holder), ผู้รับข้อมูลปลายทาง (Data Recipient), เจ้าของข้อมูล (Data Owner), ผู้ให้บริการข้อมูลกลาง (Data Broker) และหน่วยงานกำกับดูแล (Regulator) โดยบทบาทหน้าที่ของแต่ละผู้เล่น ได้แก่

๑) ผู้ถือข้อมูลต้นทาง (Data Holder) : หน่วยงานหรือองค์กรที่มีข้อมูลของเจ้าของข้อมูล และจะส่งต่อข้อมูลนี้ไปให้ผู้รับข้อมูลปลายทางเมื่อได้รับความยินยอมจากเจ้าของข้อมูล

๒) ผู้รับข้อมูลปลายทาง (Data Recipient) : หน่วยงานหรือองค์กรที่รับข้อมูลจากผู้ถือข้อมูลต้นทาง โดยผู้รับข้อมูลปลายทางจะได้รับข้อมูลเท่าที่เจ้าของข้อมูลยินยอม และสามารถนำข้อมูลนั้นไปใช้ตามวัตถุประสงค์ที่เคยแจ้งให้เจ้าของข้อมูลทราบ

๓) เจ้าของข้อมูล (Data Owner) : เจ้าของข้อมูลจะเป็นผู้ให้ความยินยอมก่อนที่จะเกิดการส่งต่อข้อมูลระหว่างผู้ถือข้อมูลต้นทางและผู้รับข้อมูลปลายทาง ซึ่งเจ้าของข้อมูลจะอยู่ในฐานะผู้ใช้บริการหรือผู้บริโภค ในกรณีการทำ Data Sharing ที่เกี่ยวกับข้อมูลส่วนบุคคล

๔) ผู้ให้บริการข้อมูลกลาง (Data Broker) : หน่วยงานหรือองค์กรที่รวบรวมข้อมูลจากแหล่งต่าง ๆ นำมาประมวลผล ปรับรูปแบบข้อมูลให้อยู่ในสภาพที่พร้อมใช้งาน วิเคราะห์ข้อมูล และเป็นผู้ให้สิทธิการเข้าถึงข้อมูลแก่องค์กรหรือหน่วยงานอื่น

๕) หน่วยงานกำกับดูแล (Regulator) : หน่วยงานกำกับดูแลจะมีหน้าที่กำกับดูแลและให้การรับรองตามกรอบกฎหมายและมาตรฐานที่หน่วยงานต้องปฏิบัติ

๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๑) กำหนดช่องทางที่จะใช้ในการตรวจจับความผิดปกติได้อย่างเหมาะสมกับสภาพแวดล้อม ที่ดูแล โดยสามารถพิจารณา “การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident”

๒) ดำเนินการวิเคราะห์ Incident ได้อย่างรวดเร็วและเหมาะสม

๓) การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident การตรวจจับ Incidentจะขึ้นอยู่กับระบบที่ใช้งานอยู่และรูปแบบของ ความพยายามในการโจมตีประกอบกับกลไกต่าง ๆ ที่ทำการปกป้องระบบอยู่ เพราะโดยทั่วไประบบการป้องกันจะทำการแจ้งเตือน (Alert) หรือ เก็บบันทึกข้อมูล (Log) เพื่อ ใช้ในการวิเคราะห์หาความผิดปกติด้วย

๔) การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติควรมีความถูกต้องแม่นยำและ ประสิทธิภาพ เพื่อให้การ ดำเนินการในขั้นตอนต่อไปสามารถดำเนินการได้เร็ว

๕) การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม

๖) วิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident

๗) กรมกิจการเด็กและเยาวชนสามารถพิจารณาปัจจัยในเรื่องดังต่อไปนี้ประกอบการ พิจารณาเพื่อกำหนดแนวทางในการติดต่อประสานงานและแจ้งข้อมูลให้กับ ผู้ที่เกี่ยวข้อง

- เป็นผู้ได้รับผลกระทบจาก Incident
- เป็นผู้ที่มีหน้าที่ตัดสินใจในการดำเนินการที่เกี่ยวข้องกับ Incident
- เป็นผู้ที่มีหน้าที่รับผิดชอบกำหนดในนโยบายและแผน
- เป็นผู้ที่มีหน้าที่รับผิดชอบตามที่กฎหมายกำหนด

๘) แจ้งเตือนเหตุภัยคุกคามทางไซเบอร์แก่ผู้ที่เกี่ยวข้องหรือหน่วยงานที่ควรได้รับการแจ้งเหตุภัยคุกคาม

๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๑) จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์กรมกิจการเด็กและเยาวชน

๒) จัดทำแผนการจัดการและการสื่อสารในภาวะวิกฤต (Crisis Communication Management Plan) กรมกิจการเด็กและเยาวชน

๓) จัดให้หน่วยงานมีการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๕. การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์(Cybersecurity Resilience and Recovery)

๑) จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ

๒) มีการตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

เอกสารอ้างอิง

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔
- แผนการรับมือภัยคุกคามทางไซเบอร์กรมกิจการเด็กและเยาวชน
- แผนการจัดการและการสื่อสารในภาวะวิกฤต (Crisis Communication Management Plan) ดย.
- แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ดย.

กรมกิจการเด็กและเยาวชน
www.dcy.go.th