กรมการแพทย์แผนไทยและการแพทย์ทางเลือก
Department of Thai Traditional and Alternative Medicine

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมการแพทย์แผนไทยและการแพทย์ทางเลือก (DTAM Guideline and Cybersecurity Framework)

โดย
ศูนย์เทคโนโลยีดิจิทัล กองวิชาการและแผนงาน
(๒๘ พฤศจิกายน ๒๕๖๗)

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางโซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล กรมการแพทย์แผนไทยและการแพทย์ทางเลือก โดย ศูนย์เทคโนโลยีดิจิทัล กองวิชาการและแผนงาน จึงได้จัดทำเอกสารฉบับนี้ เพื่อให้กรมการแพทย์แผนไทยและการแพทย์ทางเลือกมีรูปแบบรวมถึงขั้นตอนปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ทั้งนี้ เพื่อใช้เป็นแนวทางสำหรับ ผู้ใช้งานข้อมูล ระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน ให้ตระหนักถึงความมั่นคงปลอดภัยไซเบอร์และปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ที่กำหนด

(นายแพทย์สมฤกษ์ จึงสมาน)
อธิบดีกรมการแพทย์แผนไทยและการแพทย์ทางเลือก

สารบัญ

เนื้อหา **หน้า**

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

(DTAM Guideline and Cybersecurity Framework)

๑. หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคาม ทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ ของกรมการแพทย์แผนไทยและการแพทย์ทางเลือก

๒. วัตถุประสงค์

เพื่อกำหนดกรอบแนวคิดและวิธีปฏิบัติของระบบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ นำไปใช้กับการดำเนินงานและการจัดการระบบเทคโนโลยีดิจิทัล ให้มีการปฏิบัติได้อย่างถูกต้อง รวดเร็ว และมีประสิทธิภาพ

๓. ขอบเขต

กำหนดกรอบและวิธีปฏิบัติสำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) สำหรับสารสนทศที่สำคัญของกรมการแพทย์แผนไทยและการแพทย์ทางเลือก

๔. คำนิยาม

หน่วยงาน หมายถึง กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

คณะกรรมการ หมายถึง คณะกรรมการควบคุมและกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

สำนักงาน หมายถึง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายถึง คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็น ประโยชน์สาธารณะ

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายถึง หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หน่วยงานควบคุมหรือกำกับดูแล หมายถึง หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของ หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

บริการที่สำคัญ หมายถึง ภารกิจหรือบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ตัวชี้วัดความเสี่ยงที่สำคัญ หมายถึง เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้หน่วยงานมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยง พร้อมทั้งเป็นสัญญาณเตือนให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

บุคคลภายนอก (Third Party) หมายถึง บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานหรือข้อมูลของลูกค้าที่ควบคุมโดยหน่วยงานได้

Interface หมายถึง การเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์ สามารถถ่ายโอนข้อมูลซึ่งกันและกันได้

Compiler หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

Patch หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของ ไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนา ซอฟต์แวร์หลายรายเผยแพร่ patch ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่ patch ที่แก้ไขช่อง โหว่ของซอฟต์แวร์ผ่านระบบ Windows update

Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืน

Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ระบบหยุดชะงัก เพื่อรองรับการดำเนินงานอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

Asset Management หมายถึง การจัดการสินทรัพย์ เช่น ข้อมูล บุคลากร อุปกรณ์ ระบบและสิ่งอำนวยความสะดวกที่ช่วยให้หน่วยงานบรรลุวัตถุประสงค์ การระบุและจัดการให้สอดคล้องกับความสำคัญที่ สัมพันธ์กับวัตถุประสงค์และกลยุทธ์ความเสี่ยงของหน่วยงาน

Business Environment หมายถึง สภาพแวดล้อมการดำเนินงาน ภารกิจ วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสีย และกิจกรรมของหน่วยงานได้รับการเข้าใจและจัดลำดับความสำคัญ ข้อมูลนี้ใช้เพื่อแจ้งบทบาทความปลอดภัยทางไซเบอร์ ความรับผิดชอบ และการตัดสินใจในการจัดการความเสี่ยง

Governance หมายถึง นโยบาย ขั้นตอน และกระบวนการในการจัดการและติดตามข้อกำหนดของหน่วยงาน กฎหมาย ความเสี่ยง สิ่งแวดล้อม และการดำเนินงาน เป็นที่เข้าใจและแจ้งการจัดการความเสี่ยง ด้านความปลอดภัยทางไซเบอร์

Risk Assessment หมายถึง การประเมินความเสี่ยง หน่วยงานเข้าใจถึงความเสี่ยงด้านความปลอดภัยทางไซเบอร์ต่อการดำเนินงานของหน่วยงาน (รวมถึงภารกิจ หน้าที่ ภาพลักษณ์หรือชื่อเสียง) ทรัพย์สินของหน่วยงาน และบุคคล

Risk Management Strategy หมายถึง ลำดับความสำคัญของหน่วยงาน ข้อจำกัด ความเสี่ยงที่ยอมรับได้ และข้อสมมติของหน่วยงานได้รับการกำหนดและใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงด้านปฏิบัติการ

Access Control หมายถึง การควบคุมการเข้าถึงทรัพย์สินและสิ่งอำนวยความสะดวกที่เกี่ยวข้องนั้นจำกัดเฉพาะผู้ใช้ กระบวนการ หรืออุปกรณ์ที่ได้รับอนุญาต และเฉพาะกิจกรรมและธุรกรรมที่ได้รับอนุญาต

Awareness and Training หมายถึง การรับรู้และการฝึกอบรม บุคลากรและพันธมิตรของหน่วยงานได้รับการศึกษาด้านความตระหนักด้านความปลอดภัยทางไซเบอร์และได้รับการฝึกอบรมอย่างเพียงพอเพื่อปฏิบัติหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล โดยสอดคล้องกับนโยบาย ขั้นตอน และข้อตกลงที่เกี่ยวข้อง

Data Security หมายถึง การรักษาความปลอดภัยข้อมูลและการบันทึก (ข้อมูล) โดยได้รับการจัดการที่สอดคล้องกับกลยุทธ์ความเสี่ยงของหน่วยงานเพื่อปกป้องความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล

Information Protection Processes and Procedures หมายถึง กระบวนการและขั้นตอนการคุ้มครองข้อมูล นโยบายความปลอดภัย (ที่กล่าวถึงวัตถุประสงค์ ขอบเขต บทบาท ความรับผิดชอบ ความมุ่งมั่นในการจัดการและการประสานงานระหว่างหน่วยงานขององค์กร) กระบวนการและขั้นตอนต่าง ๆ ได้รับการดูแลและใช้เพื่อจัดการการป้องกันระบบข้อมูลและทรัพย์สิน

Maintenance หมายถึง การบำรุงรักษาและการซ่อมแซมการควบคุมระบบสารสนเทศและส่วนประกอบระบบสารสนเทศ ดำเนินการให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติ

Protective Technology หมายถึง การรักษาความปลอดภัยทางเทคนิคได้รับการจัดการเพื่อให้มั่นใจในความปลอดภัยและความยืดหยุ่นของระบบและทรัพย์สิน สอดคล้องกับนโยบาย ขั้นตอนและข้อตกลงที่เกี่ยวข้อง

Anomalies and Events หมายถึง การตรวจพบกิจกรรมผิดปกติในเวลาที่เหมาะสมและเข้าใจผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์

Security Continuous Monitoring หมายถึง การตรวจสอบความปลอดภัยอย่างต่อเนื่องของระบบข้อมูลและทรัพย์สินได้รับการตรวจสอบเป็นระยะเพื่อระบุเหตุการณ์ความปลอดภัยทางไซเบอร์และตรวจสอบประสิทธิภาพของมาตรการป้องกัน

Detection Processes หมายถึง กระบวนการและขั้นตอนการตรวจจับได้ การบำรุงรักษาและทดสอบเพื่อให้แน่ใจว่ามีการรับรู้เหตุการณ์ผิดปกติในเวลาที่เหมาะสมและเพียงพอ

Response Planning หมายถึง กระบวนการและขั้นตอนการตอบสนองจะได้รับการดำเนินการเพื่อให้แน่ใจว่าตอบสนองต่อเหตุการณ์การรักษาความปลอดภัยทางไซเบอร์ที่ตรวจพบได้ทันท่วงที

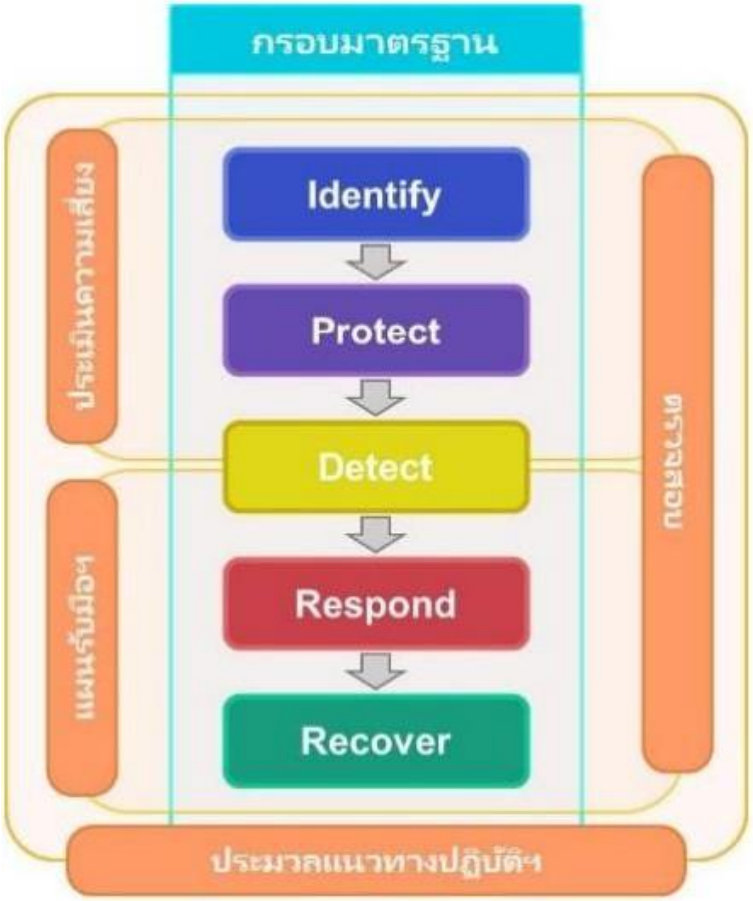
Communications หมายถึง กิจกรรมตอบสนองได้รับการประสานงานกับผู้มีส่วนได้ส่วนเสียภายในและภายนอกตามความเหมาะสมเพื่อรวมการสนับสนุนภายนอกจากหน่วยงานบังคับใช้กฎหมาย

Mitigation หมายถึง มีการดำเนินกิจกรรมเพื่อป้องกันการขยายเหตุการณ์ ลดผลกระทบ และกำจัดเหตุการณ์

Recovery Planning หมายถึง กระบวนการและขั้นตอนการกู้คืนจะได้รับการดำเนินการและบำรุงรักษาเพื่อให้แน่ใจว่าระบบหรือทรัพย์สินที่ได้รับผลกระทบจากเหตุการณ์ความปลอดภัยทางไซเบอร์สามารถกู้คืนได้ทันเวลา

๕. กรอบการดำเนินงาน

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ สามารถสรุปกิจกรรมการดำเนินการต่าง ๆ ดังต่อไปนี้



รูปที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กิจกรรมตามกรอบมาตรฐาน

รายละเอียดของแต่ละกิจกรรมมีดังนี้

๑) Identify คือ การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยงที่จะเกิดขึ้นแก่ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

๒) Protect คือ การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน

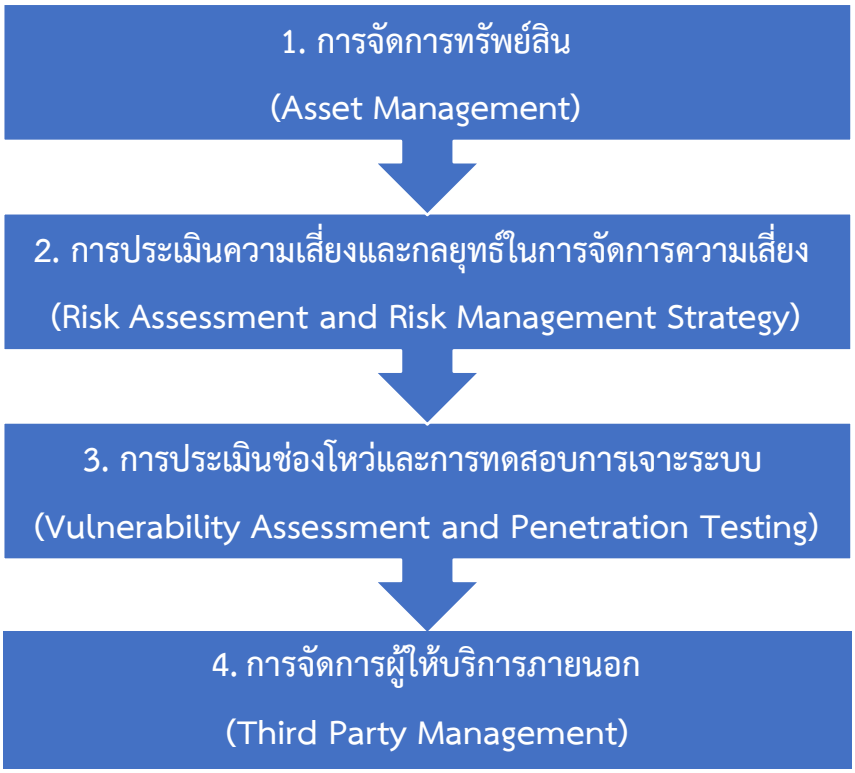
๓) Detect คือ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

๔) Response คือ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

๕) Recover คือ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

๕.๑ <u>กิจกรรมการระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)</u>

เพื่อให้หน่วยงานสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน ให้ครอบคลุมเรื่องโครงสร้างองค์การและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงบลอดภัยไซเบอร์ของหน่วยงาน โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง รายละเอียดของกิจกรรม ประกอบด้วยกระบวนการ ๔ ขั้นตอน ดังนี้



รูปที่ ๒ การระบุความเสี่ยง (Identify)

๕.๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑) ต้องจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และต้อง ทบทวนทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

- ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ
- ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ
- ตำแหน่งทางกายภาพของทรัพย์สิน ของบริการที่สำคัญ
- การระบุและการจัดลำดับความสำคัญของทรัพย์สิน ของบริการที่สำคัญ
- การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญ บนระบบเครือข่ายภายใน และ/หรือภายนอก

๒) ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๓) ต้องมีการตรวจสอบและปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สิน ของบริการที่สำคัญ

๔) ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สิน อย่างน้อยปีละ ๑ ครั้ง

๕.๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑) การประเมินความเสี่ยง (Risk Assessment)

- การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ รวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก
- การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการ รักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม
- การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงาน และการดำเนินงานของหน่วยงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒) ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคง ปลอดภัยไซเบอร์ที่คณะกรรมการฯ ประกาศกำหนด

๓) ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- 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 the Treatment)
- ความเสี่ยงที่เหลือ (Residual Risk)

๔) การจัดการความเสี่ยง (Risk Treatment ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง กับการดำเนินงาน ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและ ทบทวนความเสี่ยง

๕) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

๖) การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยงและผลกระทบการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการกำกับและดูแลหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมี นัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๕.๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๑) ดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยไซเบอร์และการควบคุม โดยครอบคลุมบริการที่สำคัญ

- Information Technology System
- Industrial Control System

๒) ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

- Host Security Assessment
- Network Security Assessment
- Architecture Security Assessment

๓) ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และควบคุมก่อนที่จะทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับ บริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๔) ควรดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต ให้สอดคล้องกับระดับของความเสี่ยงและพิจารณา ผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๕) ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ

๖) ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร ที่เป็นที่ยอมรับและเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้คุณสมบัติของผู้ ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

๗) ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

๘) ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

๙) หากได้รับการรับรองจาก กกม. หรือสำนักงาน ต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยซเบอร์ของหน่วยงาน ดังกล่าวไปยังสำนักงานภายในกำหนด ๓๐ วัน นับแต่วันที่ได้รับหนังสือ

๕.๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

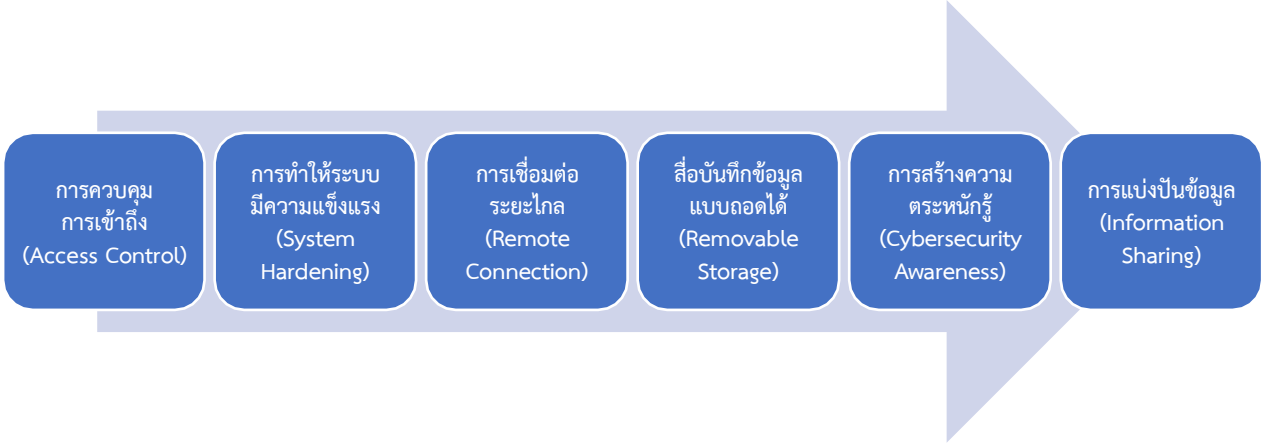
๑) ต้องรับผิดชอบ (Responsible) และมีการรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญ

๒) ต้องกำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียด ดังต่อไปนี้

- ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญ ตามความต้องการทางธุรกิจของหน่วยงานและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์
- ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของหน่วยงานจากภัยคุกคาม
- ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
- สิทธิ์ของหน่วยงาน ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๕.๒ <u>กิจกรรมการวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)</u>

รายละเอียดของกิจกรรมนี้ ประกอบด้วยกระบวนการ ๖ ขั้นตอน ดังต่อไปนี้



รูปที่ ๓ การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)

๕.๒.๑ การควบคุมการเข้าถึง (Access Control)

๑) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงาน ถูกจำกัดไว้ที่

- บุคลากรและกิจกรรมที่ได้รับอนุญาต
- อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒) ในส่วนที่เกี่ยวกับภาระหน้าที่การตรวจสอบการเข้าถึงบริการที่สำคัญของหน่วยงาน ต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตมีการใช้เทคนิคการตรวจสอบสิทธิ์ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหนดการเข้าถึงบริการที่สำคัญ

๓) ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Log of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ความสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการ เข้าถึงดังกล่าว

๔) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, Serial Port) และการเข้าถึงทางโลจิคอล (Logical) มีการกำกับดูแลโดย

- ทำภายใต้กำกับดูแลของหน่วยงาน
- ดำเนินการในสถานที่ หากเป็นไปได้

๕.๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๑) ต้องสร้างมาตรฐานกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการ ที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงาน

๒) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

- สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- การแบ่งแยกหน้าที่ (Separation of Duties)
- การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- การลบบัญชีที่ไม่ได้ใช้งาน
- การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ ให้บริการภายนอก (Vendor Support Application)
- การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
- การป้องกันมัลแวร์ (Malware)
- การปรับปรุงซอฟต์แวร์และแพตซ์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๓) ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมี การเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

๔) ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐาน เหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๕) ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่อ อนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

๕.๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๑) ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงาน มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒) สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงาน ต้องปฏิบัติตามแนวทางปฏิบัติ ดังนี้

- ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยังไซต์ระยะไกล เมื่อจำเป็นเท่านั้น
- ในกรณีที่เป็นไปได้ ใช้ เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของ ข้อความ (Message Integrity) ที่แข็งแกร่ง
- ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น
- ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Command) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงาน เว้นแต่จะได้รับอนุญาต อย่างชัดเจนเนื่องจากความต้องการใช้งาน
- จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๕.๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๑) ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญหน่วยงาน โดยมาตรการ อย่างน้อย ดังนี้

- ในกรณีที่มีพังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น
- ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตจากหน่วยงานเท่านั้น
- ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

๒) ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงาน บนสื่อบันทึกข้อมูลแบบถอดได้

๕.๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๑) ต้องให้ความสำคัญกับแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอก บุคคลที่สามที่สามารถ เข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย

ดังต่อไปนี้

- กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่
    - พนักงานใหม่ (New employees)
    - ผู้ใช้และระดับบริหาร (User and Management)
    - เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS
    - ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendor, Contractor and Service Provider)
- การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการสำคัญของหน่วยงาน
- การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

๒) ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๕.๒.๖ การแบ่งปันข้อมูล (Information Sharing)

หน่วยงานต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์กระทรวงสาธารณสุข โดยต้องรายงานต่อคณะอนุกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีรูปแบบดังนี้

๑) การกำหนดมาตรฐานในการแบ่งปันข้อมูล
- จัดทำรูปแบบข้อมูลที่ใช้ร่วมกัน โดยข้อมูลควรถูกจัดรูปแบบในลักษณะที่ทุกฝ่ายเข้าใจตรงกัน เช่น การใช้ไฟล์ประเภท CSV, JSON, XML หรือมาตรฐานอื่นที่เป็นสากล
- ใช้ภาษามาตรฐาน โดยใช้ภาษาที่เหมาะสม เช่น ภาษาอังกฤษสำหรับการสื่อสารระหว่างประเทศ หรือภาษาไทยสำหรับในประเทศ
- กำหนด Metadata เพื่อระบุข้อมูลเกี่ยวกับข้อมูล เช่น วันที่สร้าง, ผู้สร้าง, และลักษณะการใช้งาน เพื่อช่วยในการติดตามและจัดการข้อมูล

๒) การกำหนดสิทธิ์การเข้าถึงข้อมูล
- การควบคุมการเข้าถึง (Access Control) โดยใช้ระบบ Role-Based Access Control (RBAC) หรือ Attribute-Based Access Control (ABAC) เพื่อให้แน่ใจว่าข้อมูลถูกเข้าถึงเฉพาะบุคคลที่ได้รับอนุญาต
- การระบุระดับความลับของข้อมูล เพื่อจัดระดับข้อมูลเป็น Confidential, Internal Use, หรือ Public เพื่อกำหนดวิธีการแบ่งปัน

๓) การใช้เครื่องมือและเทคโนโลยีที่เหมาะสม
- จัดหาระบบจัดเก็บและแบ่งปันข้อมูล (Data Repositories) โดยใช้ระบบคลาวด์ เช่น Google Drive, SharePoint หรือ AWS S๓ สำหรับการแบ่งปันข้อมูลในทีม

- พัฒนา API ที่ปลอดภัยสำหรับการเชื่อมต่อและแบ่งปันข้อมูลระหว่างระบบ
- ใช้เทคโนโลยี Blockchain ในการติดตามและรับรองความน่าเชื่อถือของข้อมูลที่แบ่งปัน

๔) มาตรการความปลอดภัยในการแบ่งปันข้อมูล

- การเข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลทั้งในระหว่างการส่งและการจัดเก็บ
- การใช้ VPN หรือ Secure Channels เป็นช่องทางที่ปลอดภัยสำหรับการส่งข้อมูล
- การทำ Auditing เพื่อบันทึกและตรวจสอบประวัติการเข้าถึงข้อมูลเพื่อป้องกันการละเมิด

๕) การสร้างกระบวนการและขั้นตอนที่เป็นมาตรฐาน

- การระบุขั้นตอนในการแบ่งปันข้อมูล: เช่น ขั้นตอนการขออนุญาต, การส่งข้อมูล, และการตรวจสอบหลังการส่ง
- การจัดทำ Service Level Agreement (SLA) โดยระบุขอบเขตและข้อกำหนดในการแบ่งปันข้อมูลกับคู่ค้าหรือพันธมิตร
- การทำ Data Sharing Policy โดยจัดทำเอกสารนโยบายที่กำหนดวิธีการแบ่งปันข้อมูลอย่างชัดเจน

๖) การส่งเสริมวัฒนธรรมการแบ่งปันข้อมูลในองค์กร

- การฝึกอบรมพนักงาน เพื่อให้พนักงานเข้าใจถึงความสำคัญและวิธีการแบ่งปันข้อมูลอย่างปลอดภัย
- การส่งเสริมการสื่อสารที่เปิดเผย โดยสนับสนุนให้ทีมงานแบ่งปันข้อมูลระหว่างกันอย่างเป็นระบบ
- การปรับเปลี่ยน Mindset เพื่อทำให้การแบ่งปันข้อมูลเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

๕.๓ <u>กิจกรรมกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)</u>

กิจกรรมการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) มีรายละเอียด ดังนี้

๑) ต้องสร้างกลไกและกระบวนการเพื่อ

- ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน
- การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ
- การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน

๒) ต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๕.๔ <u>กิจกรรมการกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)</u>

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ ๓ ขั้นตอน ดังต่อไปนี้

รูปที่ ๕ การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)

๕.๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องมีการจัดทำ การสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๕.๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๑) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์

๒) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

- จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต
- ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง
- ระบุกลุ่มเป้าหมาย และผู้ที่มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
- ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนของหน่วยงานเมื่อกล่าวแถลงกับสื่อมวลชน
- ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๓) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงที และมีประสิทธิภาพในช่วงวิกฤต

๕.๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๑) หน่วยงานต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษร ให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว อาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้อง ที่ระบุไว้ในแผนรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ดังกล่าว

๒) ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ ข้อมูลที่ คณะกรรมการอาจร้องขอภายใต้ข้อนี้ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะ วิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของหน่วยงาน

๕.๕ <u>กิจกรรมกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)</u>

กิจกรรมการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) มีรายละเอียด ดังนี้

๕.๕.๑ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจาก เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณา ความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกับขอบเขตคำนิยามและการกำหนดระยะเวลาที่ สำคัญ เช่น Maximum Tolerance Period of Disruption (MTPD) Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๕.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพ ของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์