ประกาศกรมทรัพยากรน้ำ
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘

สืบเนื่องจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว และเพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ฉะนั้นอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม และตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรมทรัพยากรน้ำจึงออกประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า “ประกาศกรมทรัพยากรน้ำ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘”

๒. การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมทรัพยากรน้ำ มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์

๒.๒ เพื่อความมั่นคงปลอดภัยทางไซเบอร์ สำหรับการใช้งานระบบเครือข่ายและข้อมูลสารสนเทศของกรมทรัพยากรน้ำ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล ตลอด ๒๔x๗

๒.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานของกรมทรัพยากรน้ำ ได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

๒.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมทรัพยากรน้ำตระหนักถึงความสำคัญการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจะต้องมีการทบทวน ให้สอดคล้องกับสภาพแวดล้อมและกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๓. กรณี...

๓. กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยคณะกรรมการการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมทรัพยากรน้ำถือปฏิบัติตามที่ได้มีการแก้ไข หรือเพิ่มเติม นั้น

๔. ให้ใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมทรัพยากรน้ำ ตามแนบท้ายประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑๔ พฤษภาคม พ.ศ. ๒๕๖๘

(นายธีระชุณ บุญสิทธิ์)
อธิบดีกรมทรัพยากรน้ำ

เอกสารแนบท้ายประกาศ

กรมทรัพยากรน้ำ

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษา
ความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘

วันที่ ๑๔ พฤษภาคม ๒๕๖๘

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘

วันที่ ๑๔ พฤษภาคม ๒๕๖๘

คำนำ

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มุ่งเน้นให้หน่วยงานทั้งภาครัฐและเอกชนดำเนินการป้องกันภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ และความปลอดภัยของประชาชน และอ้างอิงตามมาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ดังนั้น เพื่อให้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของกรมทรัพยากรน้ำเกิดความชัดเจนและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล กรมทรัพยากรน้ำจึงได้จัดทำ “ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘” ขึ้นเพื่อให้ภารกิจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมทรัพยากรน้ำเป็นไปได้อย่างมีประสิทธิภาพ ส่งผลให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินงานได้อย่างต่อเนื่อง เกิดความปลอดภัยจากการถูกโจมตีหรือบุกรุก ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ ได้กำหนดแนวทางปฏิบัติที่ครอบคลุมทั้งด้านการป้องกัน การเฝ้าระวัง และการตอบสนองต่อเหตุการณ์ด้านไซเบอร์ ตลอดจนช่วยให้มีแนวทางในการรับมือและฟื้นฟูระบบอย่างรวดเร็วหลังจากภัยคุกคามสิ้นสุดลง เพื่อให้สอดคล้องกับกรอบกฎหมาย มาตรฐานสากล แนวปฏิบัติที่เหมาะสม และพระราชบัญญัติดังกล่าว เพื่อให้เจ้าหน้าที่และผู้เกี่ยวข้องรับทราบและนำไปปฏิบัติต่อไป

กรมทรัพยากรน้ำ
พฤษภาคม ๒๕๖๘

สารบัญ

	หน้า
วัตถุประสงค์	๑
องค์ประกอบ	๒
คำนิยาม	๓
ส่วนที่ ๑ ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๕
๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๕
๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๕
๓. แผนการรับมือภัยคุกคามทางไซเบอร์	๖
ส่วนที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๘
หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)	
๑.๑ การจัดการทรัพย์สิน (Asset Management)	๘
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	๙
๑.๓ การประเมินช่องโหว่และการทดสอบการเจาะระบบ (Vulnerability Assessment and Penetration Testing)	๙
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)	๑๑
หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)	๑๑
๒.๑ การควบคุมการเข้าถึง (Access Control)	๑๑
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	๑๒
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)	๑๓
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)	๑๓
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	๑๔
๒.๖ การแบ่งปันข้อมูล (Information Sharing)	๑๔
หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	๑๕
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	๑๕
หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	๑๕
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	๑๕
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	๑๕
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity exercise)	๑๖
หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	๑๖
๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	๑๖

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์

๑.๒ เพื่อความมั่นคงปลอดภัยทางไซเบอร์ สำหรับการใช้งานระบบเครือข่ายและข้อมูลสารสนเทศของกรมทรัพยากรน้ำ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล ตลอด ๒๔x๗

๑.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานของกรมทรัพยากรน้ำ ได้รับทราบ และถือปฏิบัติตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมทรัพยากรน้ำตระหนักถึงความสำคัญการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจะต้องมีการทบทวน ให้สอดคล้องกับสภาพแวดล้อมและกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๒. องค์ประกอบ

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘ ฉบับนี้ ประกอบด้วย ๒ ส่วน ดังนี้

ส่วนที่ ๑ ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. **คำนิยาม**

คำนิยามที่ใช้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๘ ประกอบด้วย

๓.๑ **กรมทรัพยากรน้ำ** หมายถึง กรมทรัพยากรน้ำ กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

๓.๒ **ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าสายงานให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ สามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อดูแลและจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๓.๓ **ผู้บริหารระดับสูงสุดของกรมทรัพยากรน้ำ (CEO)** หมายถึง อธิบดีกรมทรัพยากรน้ำ

๓.๔ **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมของกรมทรัพยากรน้ำ (DCIO)** หมายถึง ผู้ที่ได้รับการแต่งตั้งให้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมประจำกรมทรัพยากรน้ำ

๓.๕ **หน่วยงานภายนอก** หมายถึง หน่วยงานภายนอกที่กรมทรัพยากรน้ำอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของกรมทรัพยากรน้ำ โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๓.๖ **สินทรัพย์** หมายถึง ข้อมูลระบบ ข้อมูลทรัพย์สินด้านระบบสารสนเทศ หรือสิ่งใดก็ตามที่มีคุณค่าของกรมทรัพยากรน้ำ

๓.๗ **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่ให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓.๘ **ระบบปฏิบัติการ (Operating system)** หมายถึง โปรแกรมที่ทำหน้าที่เป็นตัวกลางเชื่อมต่อระหว่างฮาร์ดแวร์กับซอฟต์แวร์ โดยจะทำหน้าที่ควบคุมการแสดงผลการทำงานของฮาร์ดแวร์ในการรับ-ส่ง และจัดเก็บข้อมูลกับฮาร์ดแวร์ และจัดสรรการใช้ทรัพยากรระบบ (Resources)

๓.๙ **ซอฟต์แวร์ (Software)** หมายถึง ซอฟต์แวร์แอปพลิเคชัน (Application Software) ซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์ (Operating System Software) เครื่องมือในการพัฒนาระบบงาน (Development Tool) และโปรแกรมอรรถประโยชน์ (Utility)

๓.๑๐ **ฮาร์ดแวร์ (Hardware)** หมายถึง เครื่องคอมพิวเตอร์และอุปกรณ์รอบข้างที่สามารถสัมผัสได้ ประกอบด้วย อุปกรณ์ทางด้านอิเล็กทรอนิกส์ที่ควบคุมการประมวลผลข้อมูล การรับข้อมูล การแสดงผลข้อมูลของเครื่องคอมพิวเตอร์ มีทั้งที่ติดตั้งภายในเครื่องคอมพิวเตอร์และเชื่อมต่อภายนอกกับเครื่องคอมพิวเตอร์

๓.๑๑ **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๓.๑๒ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๓.๑๓ **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓.๑๔ **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของกรมทรัพยากรน้ำได้

๓.๑๕ **การเข้าถึง** หมายถึง การอนุญาต การกำหนดสิทธิ ให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

๓.๑๖ **แผนการรับมือภัยคุกคามทางไซเบอร์** (Cybersecurity Incident Response Plan) หมายถึง แผนการรับมือภัยคุกคามทางไซเบอร์ ที่กำหนดโครงสร้างทีม และแผนรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การตอบสนองและรับมือต่อภัยคุกคามทางไซเบอร์ของผู้ที่มีส่วนเกี่ยวข้อง เป็นไปในทิศทางเดียวกัน

ส่วนที่ ๑
ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ อย่างน้อยประกอบด้วย:

(ก) การวิเคราะห์ผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่กรมทรัพยากรน้ำเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานการปฏิบัติงาน และทิศทางที่คณะกรรมการอาจออกให้

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้กรมทรัพยากรน้ำ สามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง กรมทรัพยากรน้ำ ต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้ โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk assessment)

(ก) การระบุความเสี่ยง (Risk identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) การประเมินค่าความเสี่ยง (Risk evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk appetite)

๒.๒ การจัดการความเสี่ยง (Risk treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ (Key risk indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๒.๓ การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

ต้องกำหนดกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการขององค์กรที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการบริหารความเสี่ยง เป็นต้น

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

๓.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องระบุรายละเอียดอย่างน้อย ดังนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

(ข) โครงสร้างการรายงานเหตุการณ์ซึ่งกำหนดว่า กรมทรัพยากรน้ำจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึง แต่ไม่จำกัดเพียงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement protocols) กับบุคคลภายนอกรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์ / การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

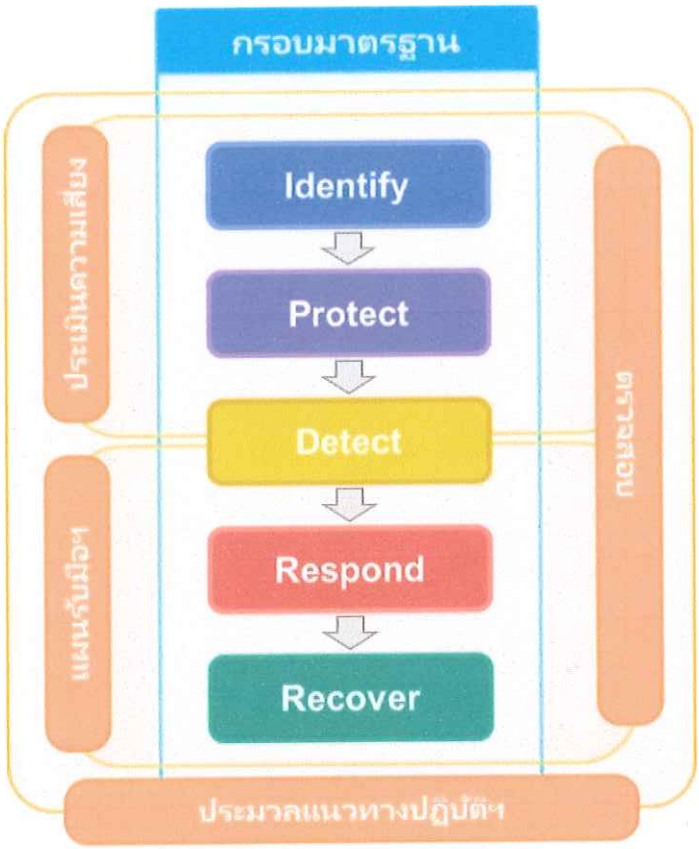
(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-action review process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๓.๒ ต้องมีการสื่อสารแผนการรับมือภัยคุกคามไซเบอร์ และมีการตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของกรมทรัพยากรน้ำ

๓.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละหนึ่ง (๑) ครั้ง โดยเริ่มตั้งแต่การจัดทำแผน

๓.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของกรมทรัพยากรน้ำ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย ๕ หัวข้อหลักดังนี้

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

นิยาม กระบวนการระบุและทำความเข้าใจถึงสินทรัพย์ (Assets) ความเสี่ยง (Risks) และช่องโหว่ (Vulnerabilities) ที่อาจส่งผลกระทบต่อองค์กร ประกอบไปด้วย ๔ ส่วน ดังนี้

๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑.๑.๑ ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของกรมทรัพยากรน้ำ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(ก) ชื่อ / คำอธิบายของทรัพย์สินของบริการที่สำคัญกรมทรัพยากรน้ำ

(ข) ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญกรมทรัพยากรน้ำ

(ค) เจ้าของและ / หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญกรมทรัพยากรน้ำ

(ง) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญกรมทรัพยากรน้ำแต่ละรายการ และ

(จ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญของกรมทรัพยากรน้ำบนระบบ / เครือข่ายภายในและ / หรือภายนอก

๑.๑.๒ ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของกรมทรัพยากรน้ำ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and significant interface)

๑.๑.๓ ต้องปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และเมื่อมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญใด ๆ ของกรมทรัพยากรน้ำ

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑.๒.๑ หน่วยงานจะต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๒.๒ หน่วยงานจะต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

(ก) วันที่ระบุความเสี่ยง
(ข) คำอธิบายของความเสี่ยง
(ค) โอกาสที่จะเกิดขึ้น
(ง) ความรุนแรงของเหตุการณ์ (Severity of the occurrence)
(จ) การจัดการความเสี่ยง (Risk treatment)
(ฉ) เจ้าของความเสี่ยง (Risk owner)
(ช) สถานะของการจัดการความเสี่ยง (Status of risk treatment) และ
(ซ) ความเสี่ยงที่เหลือ (Residual risk)

๑.๓ การประเมินช่องโหว่และการทดสอบการเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๑.๓.๑ ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญของกรมทรัพยากรน้ำอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุม

(ก) สำหรับบริการที่สำคัญของกรมทรัพยากรน้ำซึ่งเป็นระบบเทคโนโลยีสารสนเทศหรือ IT (Information Technology system)
(ข) สำหรับบริการที่สำคัญของกรมทรัพยากรน้ำซึ่งเป็นระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรมหรือ ICS (Industrial Control System)

๑.๓.๒ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย:

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) และ

(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๓ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของกรมทรัพยากรน้ำ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของกรมทรัพยากรน้ำ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน การอัปเกรดระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๔ ควรพิจารณาดำเนินการทดสอบการเจาะระบบ (Penetration testing) บริการที่สำคัญของกรมทรัพยากรน้ำ โดยเฉพาะที่เชื่อมต่อกับอินเทอร์เน็ต (Internet facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการเจาะระบบด้วย

๑.๓.๕ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบการเจาะระบบ (Scope of a penetration test) รวมถึงการทดสอบการเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของกรมทรัพยากรน้ำ

๑.๓.๖ ควรพิจารณาดำเนินการทดสอบการเจาะระบบอย่างน้อย ๑ (หนึ่ง) ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของกรมทรัพยากรน้ำ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การอัปเกรดระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๗ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration testers) ที่กำลังทำการทดสอบการเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศมีการรับรองและได้รับประกาศนียบัตร (Accreditations and certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะ

๑.๓.๘ ต้องตรวจสอบให้แน่ใจว่าการทดสอบการเจาะระบบทั้งหมด โดยผู้ให้บริการทดสอบการเจาะระบบได้ดำเนินการภายใต้การดูแลของหน่วยงาน

๑.๓.๙ ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในการประเมินช่องโหว่และในการทดสอบการเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

๑.๓.๑๐ หากได้รับการร้องขอจาก กกม. หรือสำนักงาน กรมทรัพยากรน้ำต้องส่งสำเนารายงานสรุปผลการทดสอบการเจาะระบบข้อมูล ซึ่งถูกพิจารณาให้เป็นไปตามมาตรา ๕๔

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยังสำนักงานภายในสามสิบ (๓๐) วันนับตั้งแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งสำเนาส่งให้หน่วยงานควบคุมหรือกำกับดูแล เพื่อดำเนินการตามมาตรา ๕๕ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๑.๔.๑ หน่วยงานต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษา/ความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตาม ในส่วนของบริการที่สำคัญกรมทรัพยากรน้ำ

๑.๔.๒ หน่วยงานต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอก ในข้อตกลงระดับการให้บริการ (Service level agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดควรคำนึงถึงสิ่งต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญกรมทรัพยากรน้ำ ตามความต้องการทางธุรกิจขององค์กรและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของกรมทรัพยากรน้ำจากภัยคุกคามทางไซเบอร์

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ และ

(ง) สิทธิ์ของกรมทรัพยากรน้ำในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ ควรพิจารณาดำเนินเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ๆ

หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

๒.๑.๑ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของกรมทรัพยากรน้ำถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต และ

(ข) อุปกรณ์ และอินเทอร์เฟซที่ได้รับอนุญาต

๒.๑.๒ ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ ๒.๑.๑ กรมทรัพยากรน้ำต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity risk profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญของกรมทรัพยากรน้ำ

๒.๑.๓ ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of all access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของกรมทรัพยากรน้ำ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๑.๔ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซของบริการที่สำคัญของกรมทรัพยากรน้ำ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอลมีการกำกับดูแลโดย

(ก) ทำภายใต้การดูแลของกรมทรัพยากรน้ำเท่านั้น และ

(ข) ดำเนินการในสถานที่ หากเป็นไปได้

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ หน่วยงานต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการ ที่สำคัญของกรมทรัพยากรน้ำ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity risk profile) ของบริการที่สำคัญของกรมทรัพยากรน้ำ

๒.๒.๒ หน่วยงานต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) จะกล่าวถึงหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least access privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ และ

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๒.๒.๓ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) ตามที่ระบุไว้ ก่อนที่

จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของกรมทรัพยากรน้ำ

๒.๒.๔ หน่วยงานต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standard) ของบริการที่สำคัญของกรมทรัพยากรน้ำอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ หน่วยงานต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change management process) เพื่ออนุญาต และตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของกรมทรัพยากรน้ำ

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒.๓.๑ ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของกรมทรัพยากรน้ำมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของกรมทรัพยากรน้ำ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) ในกรณีที่เป็นไปได้ ให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกลเมื่อจำเป็นเท่านั้น

(ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission security) และความสมบูรณ์ของข้อความ (Message integrity) ที่แข็งแกร่ง

(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด ผ่านโปรโตคอลที่มีความปลอดภัย มีการเข้ารหัสลับ และมีการพิสูจน์ตัวตน เช่น Hypertext Transfer Protocol Secure (HTTPS) , Secure Shell (SSH) , Secure Copy Protocol (SCP) เป็นต้น

(ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing system commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของกรมทรัพยากรน้ำ เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ และจำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของกรมทรัพยากรน้ำ โดยใช้มาตรการอย่างน้อย ดังนี้

(ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งาน เมื่อจำเป็นเท่านั้น

(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ ๒.๑.๑ (ข) เท่านั้น และ

(ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญกรมทรัพยากรน้ำ

๒.๔.๒ ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของกรมทรัพยากรน้ำบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๕.๑ ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ อย่างน้อยจะรวมถึงสิ่งต่อไปนี้

(ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

๑. พนักงานใหม่ (New employees)

๒. ผู้ใช้และระดับบริหาร (Users and management)

๓. เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS

๔. ผู้ขาย ผู้รับเหมา และผู้ให้บริการ (Vendors, contractors and service providers)

(ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญกรมทรัพยากรน้ำ

(ค) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎระเบียบนโยบาย แนวปฏิบัติมาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ

(ง) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

๒.๕.๒ ต้องทบทวนแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญกรมทรัพยากรน้ำ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญของกรมทรัพยากรน้ำ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

๓.๑.๑ ต้องสร้างกลไกและกระบวนการเพื่อ

(ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของกรมทรัพยากรน้ำ

(ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของกรมทรัพยากรน้ำหรือไม่

(ง) ต้องดำเนินการทบทวนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๔.๑.๑ ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๑.๒ เมื่อมีกรณีตรวจพบเหตุคุกคามทางไซเบอร์ (Cyber Security Incident) หน่วยงานต้องจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าการดำเนินการให้คณะกรรมการทราบ

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีรายละเอียดดังนี้

(ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

(ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

(ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ

(จ) ระบุแพลตฟอร์ม / ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๔.๒.๓ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผล ในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity exercise)

๔.๓.๑ ตามมาตรา ๒๒ (๑๓) ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ ต้องมีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน กรมทรัพยากรน้ำ ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๕.๑.๑ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (“Business Continuity Plan: BCP”) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมทรัพยากรน้ำ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของกรมทรัพยากรน้ำ เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๑.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อประเมินประสิทธิภาพของ แผนความต่อเนื่องทางธุรกิจ (“Business Continuity Plan: BCP”) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์