นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของกองทัพเรือ

พ.ศ. ๒๕๖๘

สำเนา

ประกาศกองทัพเรือ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ
พ.ศ.๒๕๖๘

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย และเชื่อถือได้นั้น ทร.จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ทร. และได้ดำเนินการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ทร. (ฉบับเดิม) เพื่อให้มีความทันสมัยและสอดคล้องกับสถานการณ์ภัยคุกคามทางไซเบอร์ในปัจจุบัน รวมทั้งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ โดยมีความมุ่งหมาย เพื่อให้กำลังพลที่ใช้งานระบบสารสนเทศ รวมทั้งส่วนราชการที่มีระบบสารสนเทศในความรับผิดชอบรับทราบ และใช้เป็นแนวทางในการปฏิบัติต่อไป โดยมีนโยบายสำคัญดังนี้

๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ทร. ประกอบด้วย

๑.๑ การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ เพื่อควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของกำลังพล มีเนื้อหาครอบคลุมใน ๖ เรื่อง ได้แก่

๑.๑.๑ การเข้าถึงระบบสารสนเทศจะต้องปฏิบัติตามระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๔ และต้องได้รับอนุญาตจากผู้ที่มีอำนาจ โดยคำนึงถึงความจำเป็นตามหน้าที่และภาระงาน และต้องดำเนินการทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ

๑.๑.๒ การกำกับดูแลระบบสารสนเทศชั้นความลับต้องปฏิบัติตามกฎหมายหรือระเบียบที่เกี่ยวข้องอย่างครบถ้วนและเคร่งครัด

๑.๑.๓ การพิสูจน์ตัวตนผู้ใช้งานของระบบสารสนเทศชั้นความลับต้องมีความน่าเชื่อถือและปลอดภัย

๑.๑.๔ การสร้างความตระหนักรู้การรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่กำลังพลของ ทร.

๑.๑.๕ การควบคุมการเข้าถึงระบบสารสนเทศของ ทร. ทั้งจากหน่วยงานหรือบุคคลภายนอก

๑.๑.๖ การควบคุมการใช้งานเทคโนโลยีสารสนเทศสมัยใหม่ที่มีผลต่อความปลอดภัยของระบบสารสนเทศ

๑.๒ การรักษาความมั่นคงปลอดภัยไซเบอร์ มุ่งเน้นการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐและมาตรฐานสากล เพื่อให้ระบบสารสนเทศของ ทร. มีความปลอดภัย พร้อมใช้งานอยู่เสมอ และมีแนวปฏิบัติในทิศทางเดียวกัน โดยครอบคลุมการตรวจสอบ การประเมินความเสี่ยง และการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์

๑.๓ การกำหนดความรับผิดชอบตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ที่กำหนดให้ผู้บริหารสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบความเสี่ยงความเสียหายและอันตรายที่เกิดขึ้นกับระบบสารสนเทศ

๒. การปฏิบัติตามนโยบาย ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ทร. ที่ปรากฏตามเอกสารแนบท้ายประกาศ ทั้งนี้ แนวปฏิบัติดังกล่าวเป็นการกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ทร. ประกอบด้วยกระบวนการดังนี้

๒.๑ สสท.ทร.จัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

๒.๒ ประกาศนโยบายและข้อปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

๒.๓ ให้ทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ทร. ทุก ๓ ปี หรือหากมีการเปลี่ยนแปลงของกฎหมายที่เกี่ยวข้อง

๓. ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) ของ ทร. มีหน้าที่ต้องรายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และคณะกรรมการที่เกี่ยวข้องโดยตรง

ผบ.ทร. ในฐานะผู้บริหารสูงสุดของ ทร. (CEO) มีความรับผิดชอบต่อความเสี่ยง ความเสียหายและอันตรายที่เกิดขึ้นกับระบบสารสนเทศของ ทร. จึงให้กำลังพลทุกนายรับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทร. พ.ศ.๒๕๖๘ ซึ่งเป็นเอกสารแนบท้ายประกาศนี้อย่างเคร่งครัด ทั้งนี้ หากระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัตินี้ ผู้บังคับบัญชาของส่วนราชการที่เกี่ยวข้อง ต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๓๐ ธันวาคม พ.ศ.๒๕๖๘

พล.ร.อ.

(ไพโรจน์ เฟื่องจันทร์)

ผบ.ทร

สำเนาถูกต้อง

น.อ.หญิง

(ปิยวดี เสนาลักษณ์)

ผอ.กสบ.สบ.ทร.

๓๐ ธ.ค.๖๘

คำนำ

ปัจจุบันระบบสารสนเทศเป็นสิ่งสำคัญที่เข้ามาอำนวยความสะดวก และสนับสนุนการปฏิบัติงานของกองทัพเรือ ส่งผลทำให้การเข้าถึงข้อมูลข่าวสารมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพสูงขึ้น อย่างไรก็ตาม แม้ว่าระบบสารสนเทศจะมีประโยชน์ และอำนวยความสะดวกในการปฏิบัติงาน ในขณะเดียวกันก็มีความเสี่ยงและอาจสร้างความเสียหายต่อกองทัพเรือได้เช่นกัน เพราะการใช้งานระบบสารสนเทศเปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอก ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลากหลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการโจมตีทางไซเบอร์ เพื่อก่อกวนให้ระบบไม่สามารถใช้การได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายต่องาน ภาพลักษณ์ของกองทัพเรือ ดังนั้นกำลังพลของกองทัพเรือ ตระหนักรู้ และให้ความสำคัญในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบสารสนเทศของกองทัพเรือ สามารถดำเนินการหรือให้บริการต่าง ๆ ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัย และเชื่อถือได้

กองทัพเรือจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือฉบับนี้ขึ้น เพื่อให้กำลังพลของกองทัพเรือรับทราบ และยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดอย่างเคร่งครัด เพื่อให้การดำเนินงาน ด้วยวิธีการทางอิเล็กทรอนิกส์ของกองทัพเรือมีความมั่นคงปลอดภัยและเชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

สารบัญ

หน้า

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

๑. หลักการและเหตุผล

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ โดยในส่วนของกองทัพเรือมีระเบียบกองทัพเรือ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ. ๒๕๕๔ ซึ่งเป็นแนวทางและมาตรการในการป้องกันระบบสารสนเทศของกองทัพเรือในระดับหนึ่งแล้ว แต่เพื่อสร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกองทัพเรือให้สอดคล้องตามที่พระราชกฤษฎีกากำหนด พร้อมทั้งได้ผนวกรวมแนวทางปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงกฎหมายลำดับรองที่ออกตามมา กองทัพเรือจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ พ.ศ. ๒๕๖๘ ขึ้น โดยมุ่งเน้นในรายละเอียดและข้อปฏิบัติต่าง ๆ เพื่อให้กำลังพลและส่วนราชการของกองทัพเรือที่มีระบบสารสนเทศในความรับผิดชอบนำไปใช้เป็นแนวทางในการปฏิบัติเดียวกันต่อไป

๒. วัตถุประสงค์

การที่กองทัพเรือได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือฉบับนี้ขึ้น มีวัตถุประสงค์ดังนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกองทัพเรือ

๒.๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้กับกำลังพลในการใช้งานระบบสารสนเทศของกองทัพเรือ

๒.๓ เพื่อให้ระบบสารสนเทศสามารถใช้งานได้ตามปกติอย่างต่อเนื่อง เหมาะสม และปลอดภัย

๒.๔ เพื่อให้กองทัพเรือมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องตามแนวทางของกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๕ เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอและมีแผนกู้คืนระบบ

๓. องค์ประกอบ

สาระสำคัญของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ พ.ศ. ๒๕๖๘ มีองค์ประกอบ ๓ ส่วนดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

- ๓.๑.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
- ๓.๑.๒ การรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

- ๓.๒.๑ ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)
- ๓.๒.๒ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)
- ๓.๒.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
- ๓.๒.๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
- ๓.๒.๕ การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
- ๓.๒.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓.๒.๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control)

๓.๒.๘ การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

๓.๒.๙ การกำหนดความรับผิดชอบ

๓.๓ ภาคผนวก

๓.๓.๑ ผนวก ก การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๓.๒ ผนวก ข การรักษาความมั่นคงปลอดภัยไซเบอร์

๔. คำนิยาม

๔.๑ **"ส่วนราชการ"** หมายความว่า หน่วยระดับหน่วยขึ้นตรงกองทัพเรือหรือเทียบเท่า และหน่วยเฉพาะกิจของกองทัพเรือ รวมทั้งคณะกรรมการที่กองทัพเรือแต่งตั้งเป็นการถาวร

๔.๒ **"ผู้บังคับบัญชา"** หมายความว่า ผู้ที่มีอำนาจและหน้าที่ในการปกครองบังคับบัญชาหน่วยระดับหน่วยขึ้นตรงของกองทัพเรือหรือเทียบเท่า และหน่วยเฉพาะกิจกองทัพเรือ รวมทั้งคณะกรรมการ ที่กองทัพเรือแต่งตั้งเป็นการถาวรที่มีพื้นที่ใช้งานระบบสารสนเทศ

๔.๓ **"ระบบสารสนเทศ"** หมายความว่า ระบบจัดการข้อมูลที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบสื่อสารมาช่วยในการสร้างสารสนเทศ ประกอบด้วย ระบบคอมพิวเตอร์ ระบบเครือข่าย และสารสนเทศ

๔.๔ **"ระบบคอมพิวเตอร์"** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ แบ่งเป็น ๒ ส่วน คือ เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๔.๕ **"ระบบเครือข่าย"** หมายความว่า ระบบที่ประกอบด้วยชุดอุปกรณ์ เครื่องมือ หรือช่องทางที่สามารถใช้ในการติดต่อสื่อสารหรือการรับ - ส่งข้อมูลของกองทัพเรือ ซึ่งแบ่งเป็น ๒ ระดับ ได้แก่

๔.๕.๑ "Backbone" เป็นเครือข่ายที่เชื่อมต่อระดับพื้นที่หลักและพื้นที่รอง

๔.๕.๒ "Distribute" เป็นเครือข่ายที่เชื่อมต่อระหว่าง Backbone กับที่ตั้งของส่วนราชการ

๔.๖ **"สารสนเทศ"** หมายความว่า ข้อมูลที่ถูกประมวลผลให้มีความหมาย โดยผ่านกรรมวิธีการจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือรูปภาพ ให้เป็นระบบที่สามารถเข้าใจได้ และสามารถนำไปใช้ประโยชน์ต่อไปในการบริหาร การวางแผนการตัดสินใจ และอื่น ๆ ได้

๔.๗ **"พื้นที่ใช้งานระบบสารสนเทศ"** หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ หรือพื้นที่เตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งพื้นที่โต๊ะทำงานที่มีคอมพิวเตอร์ส่วนบุคคลติดตั้งประจำโต๊ะทำงาน

๔.๘ **"ผู้ใช้งาน"** หมายความว่า ข้าราชการ พนักงานราชการ และลูกจ้างของกองทัพเรือ ที่มีสิทธิเข้าถึงและใช้งานระบบสารสนเทศของกองทัพเรือ

๔.๙ **"สิทธิของผู้ใช้งาน"** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ

๔.๑๐ **"ทรัพย์สินสารสนเทศ"** หมายความว่า ข้อมูล ฐานข้อมูล โปรแกรมประยุกต์ และระบบสื่อสาร หมายรวมถึงสิ่งใดก็ตามที่มีคุณค่าในระบบสารสนเทศที่กองทัพเรือ หรือส่วนราชการของกองทัพเรือเป็นเจ้าของ

๔.๑๑ **"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ"** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๔.๑๒ **"บัญชีผู้ใช้งาน"** หมายความว่า รายชื่อผู้ที่มีสิทธิใช้งานระบบสารสนเทศ

๔.๑๓ **"รหัสผ่าน"** หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน เพื่อควบคุมการเข้าถึงข้อมูล และฐานข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๔.๑๔ **"การยืนยันตัวตน"** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบซึ่งเป็นขั้นตอนในการยืนยันตัวตนของผู้ใช้งาน

๔.๑๕ **"โปรแกรมประสงค์ร้าย"** หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่งหรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยตรงหรือโดยอ้อมแก่เครื่องคอมพิวเตอร์และระบบสารสนเทศ

๔.๑๖ **"สื่อบันทึกข้อมูล"** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล

๔.๑๗ **"ไฟร์วอลล์"** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย

๔.๑๘ **"ความมั่นคงปลอดภัยด้านสารสนเทศ"** หมายความว่า การรักษาไว้ซึ่งความปลอดภัยในบริบทของการรักษาความลับ (Confidentiality) ความเชื่อถือได้ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสำหรับระบบสารสนเทศ

๔.๑๙ **"เหตุการณ์ด้านความมั่นคงปลอดภัย"** หมายความว่า เหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศโดยผลที่เกิดขึ้นอันส่งผลทำให้เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญการละเมิดต่อกฎหมาย ระเบียบข้อบังคับ หรือข้อกำหนดต่าง ๆ การทำให้ภาพลักษณ์และชื่อเสียงเสื่อมเสีย

๔.๒๐ **"ระบบปฏิบัติการ"** หมายความว่า ชุดโปรแกรมที่ทำหน้าที่ในการควบคุม ดูแล และการดำเนินการต่าง ๆ ของระบบคอมพิวเตอร์ เพื่อประสานการทำงานระหว่างทรัพยากรต่าง ๆ ในระบบทั้งในส่วนที่เป็นซอฟต์แวร์ และส่วนที่เป็นฮาร์ดแวร์ให้สามารถดำเนินการทำงานร่วมกันได้อย่างเหมาะสม

๔.๒๑ **"เฟิร์มแวร์ (Firmware)"** หมายความว่า โปรแกรมคำสั่งรูปแบบหนึ่งที่ติดตั้งบนอุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่มีความเกี่ยวข้องกับระบบสารสนเทศโดยถาวร ทำหน้าที่ควบคุมการทำงานพื้นฐานของอุปกรณ์

๔.๒๒ **"ผู้ตรวจสอบ"** หมายความว่า เจ้าหน้าที่ที่ได้รับการแต่งตั้งจากผู้บังคับบัญชาให้มีหน้าที่ตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ

๔.๒๓ **"ไซเบอร์"** หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่มีลักษณะคล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

๔.๒๔ **"โครงสร้างพื้นฐานสำคัญทางสารสนเทศ"** หมายความว่า ระบบสารสนเทศของส่วนราชการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

๔.๒๕ **"ลายมือชื่ออิเล็กทรอนิกส์"** หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

กองทัพเรือได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ สำหรับใช้เป็นแนวทางในการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งใช้เป็นกรอบสำหรับการกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ ซึ่งกำลังพลของกองทัพเรือ ต้องรับทราบและยึดถือปฏิบัติต่อไป ทั้งนี้เพื่อให้การใช้งานระบบสารสนเทศของกองทัพเรือมีความมั่นคงปลอดภัยและเชื่อถือได้ และเป็นไปตามที่กฎหมายกำหนด โดยนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือมีดังนี้

๑. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ เพื่อจัดการการเข้าถึงและการใช้งานสารสนเทศของกำลังพลของกองทัพเรือ ให้เป็นไปด้วยความปลอดภัย สอดคล้อง และเหมาะสมตามความจำเป็นของภารกิจ ขอบเขตหน้าที่ความรับผิดชอบ โดยมีรายละเอียดดังนี้

๑.๑ การเข้าถึงระบบสารสนเทศจะต้องปฏิบัติตามระเบียบกองทัพเรือ ว่าด้วยการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๔ โดยให้ความสำคัญในเรื่องการรักษาความปลอดภัยเกี่ยวกับตัวบุคคล อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศอย่างเคร่งครัด

๑.๒ การเข้าถึงระบบสารสนเทศจะต้องได้รับอนุญาตจากผู้ที่มีอำนาจ โดยคำนึงถึงความจำเป็นตามหน้าที่และภาระงาน และต้องดำเนินการทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ รวมทั้งต้องบันทึกการเข้าถึง เพื่อให้ง่ายต่อการตรวจสอบในภายหลัง

๑.๓ ระบบสารสนเทศที่มีชั้นความลับ ต้องปฏิบัติตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม ระเบียบกองทัพเรือ ว่าด้วยการรักษาความปลอดภัย พ.ศ. ๒๕๖๓ หรือระเบียบอื่นใดที่เกี่ยวข้อง

๑.๔ ให้นำวิธีการรหัสมาใช้กับข้อมูลชั้นความลับ โดยอ้างอิงตามประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ม ๑/๒๕๖๕ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและแบ่งปันข้อมูลภาครัฐ และที่ ม ๒/๒๕๖๖ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

๑.๕ ระบบสารสนเทศที่มีชั้นความลับตั้งแต่ “ลับ” ขึ้นไป ต้องกำหนดให้ผู้ใช้งานพิสูจน์ตัวตนด้วย Multi-Factor Authentication (MFA)

๑.๖ สร้างความตระหนักรู้การรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามผนวก ก รวมทั้งต้องกำหนดบทลงโทษหากมีการฝ่าฝืนไม่ปฏิบัติตามที่กำหนด

๑.๗ การใช้งานหรือจัดเก็บสารสนเทศที่มีชั้นความลับด้วยเทคโนโลยีคลาวด์ (Cloud) หรือปัญญาประดิษฐ์ (Artificial Intelligence) ต้องได้รับการพิจารณาจาก สสท.ทร.

๑.๘ การเข้าถึงระบบสารสนเทศของกองทัพเรือ โดยบุคคลภายนอก เพื่อพัฒนา ดูแล หรือบำรุงรักษาต้องได้รับการควบคุมและกำกับดูแล

๑.๙ การเชื่อมต่อระบบสารสนเทศของกองทัพเรือ กับหน่วยงานภายนอก ต้องได้รับการพิจารณาความปลอดภัยทางเทคนิคจาก สสท.ทร.

๑.๑๐ การเชื่อมต่อหรือใช้งานอุปกรณ์ Internet of Things ที่เกี่ยวข้องกับสารสนเทศที่มีชั้นความลับต้องได้รับการพิจารณาจาก สสท.ทร.

๒. การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนราชการเจ้าของระบบสารสนเทศต้องกำกับดูแลระบบสารสนเทศที่ตนรับผิดชอบ ให้สอดคล้องกับแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐ และมาตรฐานสากล เพื่อให้ระบบสารสนเทศของกองทัพเรือมีความปลอดภัย พร้อมใช้งานอยู่เสมอ และมีแนวปฏิบัติในทิศทางเดียวกัน โดยมีนโยบายดังนี้

๒.๑ จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์จากผู้ตรวจสอบภายใน อย่างน้อยปีละ ๑ ครั้ง

๒.๒ จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยง มีการติดตาม ทบทวน รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยง เพื่อให้การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ และต่อเนื่อง

๒.๓ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ เตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน (Contingency Plan) ในกรณีที่เกิดเหตุการณ์ที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ มีการสำรองข้อมูลของระบบสารสนเทศที่มีความสำคัญสำหรับกระบวนการกู้คืน รวมทั้งให้มีการทดสอบ และทบทวนแผนดังกล่าว เพื่อให้ระบบสารสนเทศสามารถปฏิบัติงานได้อย่างต่อเนื่อง

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ มีวัตถุประสงค์เพื่อกำหนดวิธีการปฏิบัติที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของกองทัพเรือ เพื่อให้ระบบสารสนเทศของกองทัพเรือมีความมั่นคงปลอดภัย โดยแนวปฏิบัติมีดังต่อไปนี้

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศ มีวัตถุประสงค์เพื่อควบคุมให้เฉพาะผู้ใช้งานที่มีสิทธิตามหน้าที่หรือภารกิจเท่านั้น ที่สามารถเข้าถึงและใช้งานสารสนเทศ มีแนวปฏิบัติดังนี้

๑.๑ ระบบสารสนเทศที่ใช้ในราชการของกองทัพเรือ หรือที่เกี่ยวข้องทั้งหมดต้องพิจารณากำหนดชั้นความลับ ตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ได้แก่ ลับที่สุด (Top Secret) ลับมาก (Secret) และลับ (Confidential)

๑.๒ สารสนเทศชั้นความลับทั้งหมดต้องถูกกำหนดระดับชั้นการเข้าถึง โดยพิจารณาจากหน้าที่และภารกิจ และต้องสอดคล้องตามบัญชี รปภ.๕ ของส่วนราชการที่ได้รับการอนุมัติไว้แล้ว

๑.๓ ส่วนราชการที่มีระบบสารสนเทศในความรับผิดชอบต้องจัดทำรายการสารสนเทศของตน โดยต้องกำหนดกลุ่มผู้ใช้งาน และสิทธิของกลุ่มผู้ใช้งาน รวมถึงกำหนดผู้รับผิดชอบ จำแนกตามรายการสารสนเทศ

๑.๔ ควบคุมสินทรัพย์ระบบสารสนเทศให้อยู่ในสถานที่ที่มีความปลอดภัย โดยมีแนวทางปฏิบัติดังนี้

๑.๔.๑ กำหนดพื้นที่ใช้งานระบบสารสนเทศให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒

๑.๔.๒ จัดวางอุปกรณ์ระบบสารสนเทศในพื้นที่ที่เหมาะสม และปลอดภัย ตามลำดับความสำคัญของอุปกรณ์ พร้อมทั้งกำหนดระดับความสำคัญของพื้นที่ และสิทธิการเข้าถึง โดยให้สิทธิเฉพาะผู้มีหน้าที่เท่านั้น

๑.๔.๓ ดูแลความชื้น อุณหภูมิ และสภาพแวดล้อมของพื้นที่ให้เหมาะสมกับอุปกรณ์ และจัดให้มีระบบสนับสนุนที่เพียงพอต่อความต้องการใช้งานของส่วนราชการ เช่น ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องไฟฟ้าสำรอง (Generator) ระบบระบายอากาศ ระบบปรับอากาศและควบคุมความชื้น เป็นต้น

๑.๔.๔ บันทึกข้อมูลการเข้าถึง และการนำอุปกรณ์สารสนเทศเข้าหรือออกจากพื้นที่

๑.๕ ต้องกำหนดช่วงเวลาและช่องทางในการใช้งานระบบสารสนเทศดังนี้

๑.๕.๑ ระบบสารสนเทศสำหรับงานบริการ e-Service (Front Office) สำหรับบุคคลภายนอกและผู้ใช้งาน ต้องกำหนดให้สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง ผ่านระบบเครือข่ายสาธารณะ (Internet)

๑.๕.๒ ระบบสารสนเทศภายในกองทัพเรือ (Back Office) สำหรับกำลังพลของกองทัพเรือต้องกำหนดให้สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง ผ่านระบบเครือข่ายภายใน (Intranet) และระบบเครือข่ายสาธารณะ (Internet) ด้วยระบบเครือข่ายส่วนบุคคลเสมือน (Virtual Private Network: VPN) ของกองทัพเรือ

๑.๕.๓ ระบบสารสนเทศที่จัดทำขึ้นเพื่อให้กำลังพลของกองทัพเรือใช้งานในช่วงเวลาที่กำหนด เช่น ระบบประเมิน และระบบทดสอบ ต้องกำหนดให้สามารถเข้าถึงได้เฉพาะในช่วงระยะเวลาที่ต้องการใช้งานผ่านระบบเครือข่ายภายใน (Intranet) และระบบเครือข่ายสาธารณะ (Internet) ด้วย VPN ของกองทัพเรือ

๑.๖ ระบบสารสนเทศที่กำลังปรับปรุงหรือเกิดข้อขัดข้อง ต้องยุติการเข้าถึงจากผู้ใช้งานที่ไม่เกี่ยวข้องกับการแก้ไขปรับปรุง จนกว่าระบบสารสนเทศนั้นจะอยู่ในสถานภาพใช้งานได้ปกติ

๑.๗ การเข้าสู่ระบบเครือข่ายจากระยะไกล (Remote Access) ต้องกำหนดมาตรการรักษาความปลอดภัยและจัดการควบคุมการเข้าใช้งานระบบจากภายนอก (Teleworking) ดังนี้

๑.๗.๑ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้บังคับบัญชาของส่วนราชการเจ้าของระบบ

๑.๗.๒ วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกล เช่น ระบบเครือข่ายส่วนบุคคลเสมือน (VPN) ต้องได้รับการอนุมัติจาก สสท.ทร. และต้องควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๑.๗.๓ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น โดยช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้งานได้ต่อเมื่อมีการร้องขอเท่านั้น

๑.๘ ต้องกำหนดให้มีการยืนยันตัวตนของผู้ใช้งานที่อยู่ภายนอก เพื่อเข้าใช้งานระบบเครือข่ายภายในดังนี้

๑.๘.๑ ต้องจัดทำบัญชีผู้ใช้งานภายนอกที่มีสิทธิเข้าใช้งานระบบเครือข่ายภายใน

๑.๘.๒ ผู้ใช้งานที่อยู่ภายนอกส่วนราชการต้องยืนยันตัวตน (Authentication) ผ่านการยืนยันตัวตนจากระบบของกองทัพเรือ เพื่อตรวจสอบความถูกต้อง ทุกครั้งก่อนการเข้าใช้งานระบบเครือข่ายภายในและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนของผู้ใช้งานได้

๑.๘.๓ การเข้าสู่ระบบเครือข่ายภายในของกองทัพเรือของบุคคลภายนอก ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจาก จก.สสท.ทร. ก่อนการใช้งาน และต้องมีเจ้าหน้าที่คอยกำกับการใช้งานอย่างใกล้ชิด ทั้งนี้เมื่อเสร็จสิ้นภารกิจแล้วให้ปลดสายสื่อสารออกจากระบบเครือข่ายภายในทันที

๑.๙ การจ้างบุคคลภายนอก (Outsource) ในการพัฒนา ดูแล และบำรุงรักษาระบบสารสนเทศให้ปฏิบัติดังนี้

๑.๙.๑ การเข้าสู่ระบบสารสนเทศของกองทัพเรือ ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของส่วนราชการเจ้าของระบบก่อนการใช้งาน

๑.๙.๒ ต้องจัดให้มีการควบคุมการใช้งาน กำหนดสิทธิในการใช้งานเฉพาะที่จำเป็น

๑.๙.๓ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๑.๙.๔ ต้องกำหนดวิธีการยืนยันตัวตนสำหรับผู้ใช้งานภายนอก

๑.๙.๕ ต้องจัดเก็บบันทึกข้อมูลการเข้า-ออกพื้นที่ และการเข้าใช้งานของผู้ปฏิบัติงานจากภายนอก

๑.๙.๖ ระบบที่สำคัญจะต้องทดสอบบนระบบทดสอบให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริงและต้องได้รับอนุญาตจากผู้บังคับบัญชาก่อนทุกครั้ง

๑.๙.๗ ต้องตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์ในซอฟต์แวร์ต่างๆ ที่ถูกพัฒนาขึ้นก่อนดำเนินการติดตั้ง หรือทดสอบการใช้งานจริง

๑.๑๐ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิด พยายามเข้าถึงโดยมิชอบ โจมตี หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้ระบบเครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพย์สินของกองทัพเรือจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมายต่อไป

๒. ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศแบ่งเป็น การควบคุมการเข้าถึงสารสนเทศ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และการใช้ลายมือชื่ออิเล็กทรอนิกส์ มีแนวปฏิบัติดังนี้

๒.๑ การควบคุมการเข้าถึงสารสนเทศ มีแนวปฏิบัติดังนี้

๒.๑.๑ กำหนดแนวทางการควบคุมการเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศ ตามสิทธิหน้าที่ และภารกิจของผู้ใช้งาน

๒.๑.๒ ต้องจัดให้มีการบันทึกและติดตามการใช้งานระบบสารสนเทศ

๒.๑.๓ ต้องจัดให้มีการตรวจสอบการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๒.๑.๔ ต้องจัดให้มีการบันทึกการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ มีแนวปฏิบัติดังนี้

๒.๒.๑ ต้องปรับปรุงสิทธิของผู้ใช้งาน ได้แก่ แก้ไข เพิ่ม และยกเลิกบัญชีผู้ใช้งาน เมื่อมีการปรับเปลี่ยนตำแหน่ง บรรจุใหม่ หรือออกจากราชการ โดยประสานงานกับ กพ.ทร. หรือต้นสังกัดของผู้ใช้งาน

๒.๒.๒ การปรับปรุงข้อกำหนดในการใช้งาน ให้มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๒.๓ การเข้าถึงสารสนเทศเกินสิทธิที่ได้รับเพื่อบรรลุงานตามภารกิจ ต้องได้รับอนุญาตจากส่วนราชการเจ้าของสารสนเทศ และต้องกำหนดระยะเวลาในการใช้งานสิทธิที่ได้รับเพิ่มเติม

๒.๓ การใช้ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature Requirements) ลงนามในระบบสารสนเทศต้องมีความน่าเชื่อถือ ตรวจสอบได้ และปลอดภัย โดยต้องปฏิบัติให้สอดคล้องกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ดังนี้

๒.๓.๑ การลงลายมือชื่ออิเล็กทรอนิกส์ต้องสามารถยืนยันได้ว่าผู้ลงลายมือชื่อเพื่อรับรองข้อมูลอิเล็กทรอนิกส์นั้น คือบุคคลที่มีอำนาจหรือได้รับสิทธิในการกระทำการนั้น และสามารถตรวจสอบย้อนหลังได้ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ มาตรา ๙

๒.๓.๒ การลงลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับการอนุมัติหรือการสั่งการ ต้องมีมาตรการการรักษาความปลอดภัยของลายมือชื่ออิเล็กทรอนิกส์ เพื่อป้องกันการปลอมแปลงหรือการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) การเข้ารหัส (Encryption) และการพิสูจน์ตัวตน (Authentication) ตามที่ระบุใน พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ มาตรา ๒๖ ด้วย

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดมาตรการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องเข้าถึงระบบสารสนเทศและเครือข่ายภายในของกองทัพเรือหรือส่วนราชการโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิการใช้งาน และต้องมีการตรวจสอบติดตามผู้ใช้งานที่เข้าใช้งานระบบสารสนเทศของกองทัพเรือ โดยกำหนดแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยสารสนเทศดังนี้

๓.๑ ต้องดำเนินการเกี่ยวกับการลงทะเบียนผู้ใช้งานดังนี้

๓.๑.๑ การลงทะเบียน มีขั้นตอนดังนี้

๓.๑.๑.๑ ต้นสังกัดของผู้ต้องการใช้งานส่งคำขอลงทะเบียนใช้งานต่อส่วนราชการเจ้าของระบบ

๓.๑.๑.๒ ส่วนราชการเจ้าของระบบสารสนเทศต้องพิจารณากำหนดสิทธิของผู้ใช้งานระบบให้เป็นไปตามสิทธิที่ควรได้รับเท่านั้น

๓.๑.๑.๓ แจ้งผลการพิจารณาและการดำเนินการให้ส่วนราชการและผู้ต้องการใช้งานนั้นทราบ

๓.๑.๑.๔ ไม่อนุญาตให้ผู้ใช้งานเข้าใช้ระบบสารสนเทศจนกว่าจะได้รับอนุมัติแล้ว

๓.๑.๒ การยกเลิกสิทธิการใช้งาน มีขั้นตอนดังนี้

๓.๑.๒.๑ ต้นสังกัดของผู้ใช้งานแจ้งขอยกเลิกสิทธิการใช้งานต่อส่วนราชการเจ้าของระบบ

๓.๑.๒.๒ ส่วนราชการเจ้าของระบบต้องพิจารณาและดำเนินการยกเลิกสิทธิการใช้งานให้ถูกต้อง

๓.๑.๒.๓ แจ้งผลการพิจารณาและการดำเนินการให้ส่วนราชการและผู้ใช้งานนั้นทราบ

๓.๑.๓ ต้องควบคุมมิให้มีบัญชีผู้ใช้งานที่ซ้ำซ้อนกัน

๓.๑.๔ จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มตามเหตุผลความจำเป็นเท่านั้น และผู้ใช้งานบัญชีแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน

๓.๑.๕ ต้องจัดเก็บข้อมูลการใช้งานของผู้ใช้งานสำหรับการตรวจสอบ

๓.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องควบคุมและจำกัดสิทธิของผู้ใช้งานเพื่อสามารถเข้าถึงและใช้งานระบบ สารสนเทศตามความเหมาะสมของภารกิจและขอบเขตงานรับผิดชอบของผู้ใช้งานแต่ละบุคคล โดยเฉพาะ อย่างยิ่งการกำหนดสิทธิการใช้ระบบสารสนเทศที่สำคัญ จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาผู้ใช้งาน เป็นลายลักษณ์อักษร ทั้งนี้การกำหนดสิทธิของผู้ใช้งาน พิจารณาให้สิทธิน้อยที่สุดที่เพียงพอต่อการใช้งานตามหน้าที่และภาระงาน โดยสิทธิเรียงลำดับจากน้อยไปมากได้ดังนี้

๓.๒.๑ อ่าน (Read)

๓.๒.๒ สร้าง (Create)

๓.๒.๓ แก้ไข (Edit)

๓.๒.๔ ลบ (Delete)

๓.๓ ต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยดังนี้

๓.๓.๑ ต้องเก็บรักษารหัสผ่านของผู้ใช้งานให้เป็นความลับ

๓.๓.๒ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสผ่านใหม่

๓.๓.๓ ต้องกำหนดขั้นตอนสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยเพียงพอที่จะสามารถยืนยันตัวบุคคลได้จริง

๓.๓.๔ ต้องยุติการเชื่อมต่อเมื่อพบว่ามีการพยายามคาดเดารหัสผ่าน ไม่สำเร็จเกินกว่า ๓ ครั้ง

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) มีวัตถุประสงค์เพื่อให้ผู้ใช้งานมีความเข้าใจถึงหน้าที่และความรับผิดชอบ ตลอดจนการมีส่วนร่วมในการป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยการล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ระบบสารสนเทศ โดยผู้ใช้งานมีหน้าที่ความรับผิดชอบดังนี้

๔.๑ การควบคุมทรัพย์สินด้านสารสนเทศและการใช้งานระบบคอมพิวเตอร์ มีแนวปฏิบัติดังนี้

๔.๑.๑ จัดเก็บเอกสารและสื่อบันทึกข้อมูลที่มีความสำคัญหรือเป็นความลับ ไว้ในสถานที่ที่มีการป้องกันและมีความปลอดภัย

๔.๑.๒ การเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือทรัพย์สินด้านสารสนเทศ ต้องผู้ได้รับอนุญาตจากเจ้าของหรือผู้ได้รับมอบหมายเท่านั้น

๔.๑.๓ ต้องมีมาตรการหรือเทคนิคในการป้องกันข้อมูลที่มีความสำคัญ

๔.๑.๔ สำรองหรือลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์หรือเครื่องถ่ายเอกสารไปตรวจซ่อม เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔.๑.๕ โปรแกรมประยุกต์ที่เป็นทรัพย์สินของกองทัพเรือ ห้ามผู้ใช้งานคัดลอกโปรแกรม แก้ไข นำไปให้ผู้อื่น เผยแพร่สู่สาธารณะ หรือนำไปใช้เพื่อประโยชน์ส่วนตัว ซึ่งไม่เป็นไปตามวัตถุประสงค์ของกองทัพเรือ

๔.๑.๖ ต้องมีการควบคุมและป้องกันจากผู้ไม่ได้รับอนุญาตในการใช้งานอุปกรณ์ถ่ายภาพหรืออุปกรณ์ทำสำเนา ได้แก่ กล้องถ่ายภาพ เครื่องสแกนเอกสาร และเครื่องสำเนาเอกสาร เป็นต้น เพื่อป้องกันไม่ให้ทำสำเนาข้อมูลสารสนเทศที่สำคัญ

๔.๒ เอกสารสำคัญหรือเป็นความลับซึ่งได้รับการพิมพ์ออกจากเครื่องพิมพ์ จะต้องถูกเก็บออกจากเครื่องพิมพ์ทันทีเมื่อมีการพิมพ์แล้วเสร็จ

๔.๓ เมื่อมีความจำเป็นต้องทำลายข้อมูลบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามข้อปฏิบัติการทำลายข้อมูลหรือสื่อบันทึกข้อมูลตามผนวก ก

๔.๔ การยืนยันตัวตนทุกครั้ง ก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกองทัพเรือ และหากการยืนยันตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านการโดนล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้รับผิดชอบระบบสารสนเทศทราบทันที

๔.๕ ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์ หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง และต้องป้องกันไม่ให้ผู้ที่ไม่มีสิทธิเข้าใช้งานทรัพย์สินที่อยู่ในความรับผิดชอบ เพื่อป้องกันการสูญหายดังนี้

๔.๕.๑ ต้องมีการกำหนดรหัสผ่าน (Password) รายละเอียดตามผนวก ก สำหรับเข้าใช้งานอุปกรณ์

๔.๕.๒ ต้องตั้งค่าให้ใส่รหัสผ่านใหม่หากไม่มีการใช้งานเครื่องคอมพิวเตอร์เป็นระยะเวลา ๑๕ นาที

๔.๕.๓ ต้องปิดเครื่องหรือออกจากระบบทันทีเมื่อเสร็จสิ้นการใช้งานอุปกรณ์

๔.๕.๔ เมื่อไม่มีผู้ใช้งาน ต้องปิดล็อคประตูและหน้าต่าง และจัดเก็บอุปกรณ์ในสถานที่ปลอดภัยเพื่อการป้องกันการโจรกรรมหรือลักลอบขโมยข้อมูล

๔.๕.๕ ห้ามติดตั้งซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการทำงานหรือที่ไม่อนุญาตให้ใช้งาน

๕. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติดังนี้

๕.๑ ระบบเครือข่ายในระดับ Backbone กำหนดให้ สสท.ทร. มีหน้าที่รับผิดชอบดำเนินการดังนี้

๕.๑.๑ พื้นที่ที่เกี่ยวข้องกับอุปกรณ์สำคัญของระบบเครือข่ายในระดับ Backbone กำหนดให้เป็นเขตหวงห้ามเด็ดขาด

๕.๑.๒ กำหนดและจัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน และควบคุมการจัดเส้นทางบนระบบเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของเครื่องคอมพิวเตอร์ และการส่งผ่านข้อมูลในระบบสารสนเทศสอดคล้องรองรับกับการควบคุมการเข้าถึงการใช้งาน โดยมีแนวปฏิบัติดังนี้

๕.๑.๒.๑ ข้อมูลหมายเลข IP Address ของระบบเครือข่ายภายในต้องมีการป้องกันไม่ให้การเชื่อมต่อจากภายนอกสามารถมองเห็นได้

๕.๑.๒.๒ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและภายนอก และต้องปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ

๕.๑.๒.๓ ให้บันทึกการทำงานของระบบป้องกันการบุกรุก เพื่อประโยชน์ในการตรวจสอบย้อนหลัง และต้องเก็บบันทึกข้อมูลดังกล่าวไว้ไม่น้อยกว่า ๙๐ วัน

๕.๑.๒.๔ กำหนดมาตรการป้องกัน และจำกัดการใช้เส้นทางบนระบบเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย ให้กับระบบสารสนเทศที่สำคัญ

๕.๑.๒.๕ ระบบเครือข่ายทั้งหมดของส่วนราชการที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering

๕.๑.๒.๖ การใช้งานเครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชา และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๑.๒.๗ กำหนดสิทธิผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาต

๕.๑.๒.๘ มีการบันทึกและตรวจสอบการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๕.๑.๓ ใช้ฮาร์ดแวร์หรือซอฟต์แวร์สำหรับการบริหารจัดการระบบเครือข่ายเพื่อระบุเฝ้าตรวจและติดตามสถานภาพอุปกรณ์ในระบบสารสนเทศของกองทัพเรือ รวมทั้งกำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบสารสนเทศที่สำคัญ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๕.๑.๔ การติดตั้ง และเชื่อมต่ออุปกรณ์เครือข่ายต้องดำเนินการโดย สสท.ทร. และจัดทำเป็นบัญชีไว้สำหรับการระบุอุปกรณ์บนระบบเครือข่าย โดยบัญชีดังกล่าวต้องมีข้อมูลดังนี้ วัน/เดือน/ปี ที่ติดตั้งและเชื่อมต่ออุปกรณ์ ข้อมูลทะเบียนหมายเลข IP Address รายละเอียดของอุปกรณ์ที่ติดตั้ง และสถานที่ติดตั้ง

๕.๑.๕ การควบคุมการเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ให้ปฏิบัติดังนี้

๕.๑.๕.๑ ระบบเครือข่ายที่ต้องวางผ่านบริเวณที่มีบุคคลภายนอกเข้าถึงได้ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณ และป้องกันสัตว์ต่าง ๆ กัดสาย

๕.๑.๕.๒ ต้องเดินสายสื่อสารและสายไฟแยกออกจากกัน เพื่อป้องกันสัญญาณรบกวนกัน

๕.๑.๕.๓ จัดทำแผนผังสายสื่อสารต่าง ๆ และต้องปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ

๕.๑.๕.๔ จำแนกสีอุปกรณ์ปลายทางที่เชื่อมต่อระบบเครือข่ายตามชั้นความลับตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๕.๒ ระบบเครือข่ายในระดับ Distribute ให้เป็นความรับผิดชอบของผู้บังคับบัญชาของส่วนราชการในการแต่งตั้งผู้รับผิดชอบระบบเครือข่ายเพื่อทำหน้าที่กำกับ ดูแลระบบเครือข่ายทางกายภาพให้เป็นไปตามระเบียบการรักษาความปลอดภัยสารสนเทศ พ.ศ. ๒๕๕๔

๕.๓ กำหนดมาตรการป้องกันระบบสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ โดยมีแนวปฏิบัติดังนี้

๕.๓.๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศจะต้องไม่มีการเชื่อมต่อเพื่อใช้งานระบบเครือข่ายสาธารณะ เว้นแต่มีความจำเป็นโดยจะต้องได้รับอนุญาตจาก สสท.ทร.

๕.๓.๒ การเชื่อมต่อไปยังระบบเครือข่ายสาธารณะที่ไม่ได้รับอนุญาตจะต้องถูกตัดการเชื่อมต่อ

๕.๓.๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ต้องทำบันทึกขออนุญาตดำเนินการเสนอ สสท.ทร.

๕.๔ กำหนดมาตรการเพื่อป้องกันข้อมูลในระบบเครือข่ายจากการถูกเข้าถึงโดยไม่ได้รับอนุญาตดังนี้

๕.๔.๑ ผู้ใช้งานจะสามารถเข้าถึงระบบเครือข่ายเมื่อได้รับอนุญาตให้เข้าถึงตามภาระงานเท่านั้น

๕.๔.๒ บันทึกข้อมูลพฤติกรรมการใช้งาน และเก็บข้อมูลของอุปกรณ์เครือข่าย อย่างสม่ำเสมอ

๕.๔.๓ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ ของระบบสารสนเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๕.๕ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ระบบเครือข่ายและอุปกรณ์เครือข่าย ต้องมีการป้องกันการเข้าถึงอุปกรณ์ทางกายภาพโดยต้องติดตั้งอยู่ภายในห้องที่สามารถจำกัดการเข้าถึงได้ และต้องกำหนดผู้รับผิดชอบ พร้อมกำหนดสิทธิการเข้าถึงอุปกรณ์เครือข่ายอย่างชัดเจนในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) มีการทบทวนสิทธิ อย่างน้อยปีละ ๑ ครั้ง และต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๖ แนวทางการควบคุมการเชื่อมต่อระบบเครือข่ายด้วยอุปกรณ์ไฟร์วอลล์ (Firewall) หรืออุปกรณ์เครือข่ายอื่น ๆ มีดังนี้

๕.๖.๑ กำหนดผู้รับผิดชอบ ให้มีหน้าที่ในการบริหารจัดการ และกำหนดค่าของไฟร์วอลล์ทั้งหมด รวมถึงสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยง

๕.๖.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกระบบเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๕.๖.๓ เมื่อมีการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๕.๖.๔ การเข้าถึงอุปกรณ์ไฟร์วอลล์ จะต้องเป็นผู้ที่ได้รับมอบหมายเท่านั้น

๕.๖.๕ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๕.๖.๖ การกำหนดระเบียบในการให้บริการระบบเครือข่ายสาธารณะ กับเครื่องคอมพิวเตอร์ลูกข่ายจะต้องเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมเท่าที่ได้อนุญาตให้ใช้งานเท่านั้น ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือจากที่กำหนด จะต้องได้รับการอนุมัติจาก สสท.ทร.

๕.๖.๗ การกำหนดค่าพอร์ตการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของระบบเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดย Policy จะต้องถูกระบุให้เฉพาะเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการจริง

๕.๖.๘ ต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๕.๖.๙ ต้องตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่าย ที่ไม่มีความจำเป็นในการใช้งาน

๕.๗ ต้องจัดทำบัญชีอุปกรณ์ในระบบเครือข่ายของส่วนราชการตาม สสท.ทร. กำหนด โดยปรับปรุงข้อมูลอย่างน้อยปีละ ๑ ครั้ง

๕.๘ การควบคุมอุปกรณ์ต่าง ๆ ที่ใช้งานผ่านระบบเครือข่ายไร้สายของกองทัพเรือ ให้ปฏิบัติดังนี้

๕.๘.๑ ให้สิทธิการใช้งานเฉพาะกำลังพลของกองทัพเรือ โดยผู้ใช้งานต้องแจ้งความประสงค์ขอใช้งานบริการระบบเครือข่ายไร้สายของกองทัพเรือที่ สสท.ทร.

๕.๘.๒ สสท.ทร. จัดเก็บและลงทะเบียนข้อมูลของผู้แจ้งความประสงค์ขอใช้งานบริการระบบเครือข่ายไร้สายของกองทัพเรือ พร้อมแจ้งคำแนะนำการใช้งาน รวมทั้งให้คำปรึกษากรณีเกิดปัญหาในการใช้งาน

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติดังนี้

๖.๑ การควบคุมการติดตั้งระบบปฏิบัติการ (Control of Operational Software) ให้ปฏิบัติดังนี้

๖.๑.๑ ให้กำหนดแผนการติดตั้งสำหรับระบบปฏิบัติการใหม่ และ การปรับปรุงระบบปฏิบัติการเดิม ซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า สำหรับระบบปฏิบัติการที่จะทำการติดตั้งให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

๖.๑.๒ ต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบปฏิบัติการอย่างครบถ้วนก่อนติดตั้ง

๖.๑.๓ แจ้งผู้ที่เกี่ยวข้องให้รับทราบ เกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๖.๑.๔ ให้อ่านและปฏิบัติตามเงื่อนไข หรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

๖.๑.๕ การติดตั้งโปรแกรมอรรถประโยชน์ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่ถูกต้องและเชื่อถือได้

๖.๑.๖ การเปลี่ยนแปลงระบบปฏิบัติการจะต้องดำเนินการโดยผู้รับผิดชอบเท่านั้น

๖.๑.๗ ในกรณีที่เป็นการติดตั้งระบบปฏิบัติการเพื่อทดแทนระบบปฏิบัติการเดิม ให้ทำการสำรองข้อมูลที่จำเป็นอันได้แก่ ฐานข้อมูลซอฟต์แวร์ ค่าคอนฟิกกูเรชัน (Configuration) หรืออื่น ๆ ที่เกี่ยวข้องกับระบบปฏิบัติการนั้น

๖.๑.๘ กรณีที่จำเป็นต้องถ่ายโอนข้อมูลในระบบปฏิบัติการเดิมไปสู่ระบบปฏิบัติการใหม่ ให้จัดทำแผนการถ่ายโอนข้อมูล เพื่อตรวจสอบความถูกต้องและครบถ้วนของข้อมูลที่ถ่ายโอน

๖.๑.๙ ต้องอัพเดทแพตช์ (Patch) ที่เกี่ยวข้องกับความปลอดภัยของระบบปฏิบัติการ

๖.๒ การปฏิบัติเพื่อการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ให้ปฏิบัติดังนี้

๖.๒.๑ ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดใด ๆ (Misconfiguration) ก่อนเข้าสู่ระบบ

๖.๒.๒ ผู้ใช้ต้อง Log Out จากระบบทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอแสดงผล เป็นเวลานาน

๖.๒.๓ การเชื่อมต่อระบบปฏิบัติการผ่าน Command Line เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control)

การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control) เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์และสารสนเทศโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติดังนี้

๗.๑ สารสนเทศที่มีชั้นความลับ “ลับมาก” ขึ้นไป ต้องกำหนดให้สามารถใช้งานเฉพาะกลุ่ม และต้องจำกัดการเข้าถึงเฉพาะการใช้ระบบเครือข่ายที่ สสท.ทร. ให้การรับรองเท่านั้น

๗.๒ มาตรการควบคุมการเข้าถึงระบบสารสนเทศเพื่อป้องกันชุดคำสั่งไม่พึงประสงค์มีดังนี้

๗.๒.๑ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๗.๒.๒ ให้ดำเนินการตรวจสอบชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ ที่ให้บริการอย่างสม่ำเสมอ เพื่อดักจับชุดคำสั่งไม่พึงประสงค์ที่จะเข้าสู่ระบบ

๗.๒.๓ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับจัดการชุดคำสั่งไม่พึงประสงค์ ได้แก่ การรายงานการเกิดขึ้นของชุดคำสั่งไม่พึงประสงค์ การวิเคราะห์ การจัดการการกู้คืนระบบ เป็นต้น

๗.๒.๔ ให้ติดตามข้อมูลข่าวสารเกี่ยวกับชุดคำสั่งไม่พึงประสงค์อย่างสม่ำเสมอ มีการสร้างความตระหนักเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ เพื่อให้ผู้ใช้งานมีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุชุดคำสั่งไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร

๗.๒.๕ การพัฒนาโปรแกรมประยุกต์ ให้ส่วนราชการเจ้าของสารสนเทศที่เชื่อมต่อกับระบบเครือข่ายของกองทัพเรือต้องขออนุญาต สสท.ทร. ก่อน ส่วนการใช้งานโปรแกรมที่พัฒนาให้ผู้มีสิทธิและอำนาจในสารสนเทศด้านนั้น ๆ เป็นผู้พิจารณาคุณสมบัติของผู้ที่สามารถใช้งานโปรแกรมดังกล่าวได้ตามสิทธิ

๗.๒.๖ ต้องควบคุมมิให้มีการเปลี่ยนเส้นทางจาก HTTP ไปยัง HTTPS (Redirecting HTTP to HTTPS) โดยให้ปฏิเสธการเปลี่ยนเส้นทางทุกกรณี

๘. การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อ้างอิงตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) เพื่อให้เกิดความสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ส่งผลให้การใช้งานระบบสารสนเทศของกองทัพเรือมีความมั่นคงปลอดภัยมากขึ้น มีการรักษาความลับ (Confidentiality) ความเชื่อถือได้ (Integrity) และสามารถใช้งานได้อย่างต่อเนื่อง (Availability) โดยใช้แนวทาง

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ดังนี้

๘.๑ ระบุความเสี่ยง (Identify)

๘.๑.๑ การจัดการทรัพย์สิน (Asset Management) จัดทำทะเบียนทรัพย์สินที่ระบุทรัพย์สินของบริการ โดยระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ และดำเนินการตรวจสอบและปรับปรุงทะเบียนทรัพย์สินให้เป็นปัจจุบัน อย่างน้อย ปีละ ๑ ครั้ง

๘.๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๘.๑.๒.๑ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศตามผนวก ข ตารางที่ ๒ การกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำโดยผู้ตรวจสอบภายในของกองทัพเรือ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และรายงานผลการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศเสนอ สสท.ทร ภายในเดือนกันยายนของทุกปี

๘.๑.๒.๒ กำหนดให้มีคณะผู้ตรวจสอบภายในของกองทัพเรือ ทำหน้าที่ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศที่สำคัญ

๘.๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ศซบ.สสท.ทร. ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งอื่นที่น่าเชื่อถือ และประเมินช่องโหว่ของบริการที่สำคัญอย่างน้อยปีละ ๑ ครั้ง โดยอ้างอิงตามหลักการบริหารความเสี่ยงของ สสท.ทร. ติดตาม ปรับปรุง และแก้ไขตามข้อเสนอแนะจากผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหวในระดับวิกฤติ และระดับสูง

๘.๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) ให้ดำเนินการตามข้อ ๑.๘ - ๑.๙

๘.๒ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect) ทั้งนี้ให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๘ ฉบับนี้

๘.๓ มาตรการตรวจสอบและฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๘.๓.๑ ให้ ศซบ.สสท.ทร. ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ จัดประเภทและวิเคราะห์เหตุการณ์ที่ตรวจพบ และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับระบบสารสนเทศของกองทัพเรือ ทำการทบทวนกลไกและกระบวนการต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง

๘.๓.๒ ระบบสารสนเทศของส่วนราชการใด ๆ ที่ไม่ได้อยู่ในระบบสารสนเทศของกองทัพเรือ ให้ดำเนินการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์โดยประสานการปฏิบัติกับ ศซบ.สสท.ทร. กรณีตรวจพบภัยคุกคามทางไซเบอร์ให้ส่วนราชการเสนอรายงานไปยังส่วนที่เกี่ยวข้องตามคำแนะนำของ ศซบ.สสท.ทร.

๘.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๘.๔.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม และทบทวนปรับปรุง แผนการรับมือภัยคุกคาม ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๔.๒ จัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๘.๔.๓ ฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนการสื่อสารฯ เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด อย่างน้อย ปีละ ๑ ครั้ง

๘.๔.๔ ศซบ.สสท.ทร. จัดตั้งทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Protection Team: CPT) และรายงานเมื่อตรวจพบภัยคุกคามทางไซเบอร์ระดับวิกฤตให้ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (CISO) ของกองทัพเรือทราบ

๘.๕ มาตรการรักษาและฟื้นฟูความเสียหาย (Recover)

๘.๕.๑ จัดทำแผนการกู้คืนระบบทั้งระหว่างเกิดเหตุและหลังเกิดเหตุภัยคุกคาม (Disaster Recovery Plan: DRP) ของระบบสารสนเทศที่สำคัญ

๘.๕.๒ ดำเนินการสำรอง (Backup) ข้อมูลสำหรับระบบสารสนเทศ เพื่อให้มั่นใจว่าระบบสารสนเทศยังคงสามารถให้บริการได้อย่างต่อเนื่อง แม้เกิดกรณีฉุกเฉิน โดยมีแนวปฏิบัติดังนี้

๘.๕.๒.๑ พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและทำการสำรองข้อมูล

๘.๕.๒.๒ จัดทำแผนการสำรองข้อมูล โดยมีรายละเอียดผู้รับผิดชอบในการสำรองข้อมูลของระบบสารสนเทศ ความถี่ในการสำรองข้อมูล หากระบบมีการเปลี่ยนแปลงมาก ให้มีความถี่การสำรองข้อมูลมากขึ้น และระยะเวลาในการจัดเก็บข้อมูลสำรอง ให้พิจารณาตามประเภทของข้อมูล

๘.๕.๒.๓ วิธีการสำรองข้อมูล ได้แก่ การสำรองข้อมูลเฉพาะส่วนต่าง (Differential Backup) การสำรองข้อมูลเฉพาะส่วนเพิ่ม (Incremental Backup) และการสำรองข้อมูลเต็มรูปแบบ (Full Backup)

๘.๕.๒.๔ จำนวนชุดของข้อมูลสำรอง อย่างน้อย ๒ ชุด โดยแยกจัดเก็บคนละที่

๘.๕.๒.๕ จัดให้มีการบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูลอย่างน้อยได้แก่ ชื่อข้อมูลที่สำรอง ผู้ดำเนินการสำรองข้อมูล วัน เวลา และความสำเร็จของการสำรองข้อมูล

๘.๕.๒.๖ ข้อมูลที่สำรองต้องมีการเข้ารหัสข้อมูลด้วย Algorithm ไม่ต่ำกว่า AES-256

๘.๕.๓ การทดสอบและการกู้คืนให้ปฏิบัติดังนี้

๘.๕.๓.๑ ต้องจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลจากข้อมูลที่ได้สำรองไว้

๘.๕.๓.๒ หากความเสียหายที่เกิดขึ้นมีผลกระทบต่อการให้บริการหรือการใช้งาน ให้แจ้งผู้ใช้งานทราบตามช่องทางการสื่อสารต่าง ๆ ทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๘.๕.๓.๓ ต้องตรวจสอบและทดสอบสภาพพร้อมใช้งานและขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

ภายหลังจากส่วนราชการได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศ ซึ่งพิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในเรื่องการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน และได้ระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์แต่ละเรื่องเป็นระดับต่ำ ระดับกลาง หรือระดับสูง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศแล้ว ให้ส่วนราชการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศนั้นในแต่ละระดับตามหัวข้อ ตามผนวก ข ตารางที่ ๑ แบบประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๙. การกำหนดความรับผิดชอบ

ตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กำหนดให้ ผบ.ทร. ในฐานะผู้บริหารสูงสุดของกองทัพเรือ (CEO) เป็นผู้รับผิดชอบความเสี่ยงความเสียหาย และอันตรายที่เกิดขึ้นระบบสารสนเทศ อันเนื่องมาจากความบกพร่อง ละเลย ฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ จึงให้ผู้บังคับบัญชาของทุกส่วนราชการรับทราบ และปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนด รวมทั้งให้กำกับ ดูแล และกวดขันกำลังพลในการใช้งาน ระบบสารสนเทศของกองทัพเรือ ให้เป็นไปตามนโยบาย

และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ อย่างเคร่งครัด ทั้งนี้หากเกิดกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัตินี้

๙.๑ ให้ผู้บังคับบัญชาของส่วนราชการปฏิบัติดังนี้

๙.๑.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชา และส่วนราชการที่เกี่ยวข้องทราบ

๙.๑.๒ เมื่อมีการละเมิดต้องจัดให้มีการสอบสวนหาตัวผู้กระทำผิด และผู้รับผิดชอบโดยเร็วที่สุด

๙.๑.๓ ให้พิจารณาแก้ไขข้อบกพร่อง และป้องกันมิให้เหตุการณ์ดังกล่าวเกิดขึ้นซ้ำ

๙.๑.๔ ให้พิจารณาบทลงโทษต่อผู้กระทำผิดตาม พรบ.ว่าด้วยวินัยทหาร พ.ศ. ๒๔๗๖

๙.๑.๕ ต้องให้ความร่วมมือทั้งด้านการปฏิบัติและข้อมูลแก่ สสท.ทร. เมื่อได้รับการร้องขอในกรณีที่เกิดหรือคาดว่าจะเกิดการละเมิด

๙.๑.๖ สามารถออกมาตรการควบคุมภายในส่วนราชการเพิ่มเติมได้ โดยต้องไม่ขัดต่อนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือนี้

๙.๒ ให้ สสท.ทร. ปฏิบัติดังนี้

๙.๒.๑ ต้องดำเนินการหรือร่วมดำเนินการตรวจสอบ กรณีที่การละเมิดส่งผลอย่างร้ายแรงต่อกองทัพเรือ

๙.๒.๒ สามารถออกมาตรการควบคุมด้านสารสนเทศภายในกองทัพเรือเพิ่มเติมได้ โดยต้องไม่ขัดต่อนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือนี้

ภาคผนวก

ผนวก ก
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. ข้อปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับกำลังพลของกองทัพเรือและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๑.๑ จัดให้มีการเสริมเนื้อหาเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ ในทุกครั้งที่มีการจัดฝึกอบรมภายในกองทัพเรือที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ

๑.๒ จัดให้มีการประชาสัมพันธ์ผ่านช่องทางต่าง ๆ เช่น inavy ข่าวราชนาวี เว็บไซต์ หรือสื่อสังคมออนไลน์ เพื่อให้ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรืออย่างสม่ำเสมอในลักษณะของเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๑.๓ จัดให้มีการติดตามและประเมินผล ความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกำลังพลในกองทัพเรือ

๒. ข้อปฏิบัติการใช้งานรหัสผ่าน

๒.๑ ผู้ใช้งานต้องใช้งานรหัสผ่านของตนเอง หรือตามที่ได้รับอนุมัติเท่านั้น และเก็บรักษารหัสผ่านไว้เป็นความลับอยู่ตลอดเวลา

๒.๒ เลือกรหัสผ่านที่ปลอดภัยตามคำแนะนำการกำหนดรหัสผ่านดังนี้

๒.๒.๑ ตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น ห้ามผู้ใช้งานกำหนดรหัสผ่านส่วนบุคคลจากชื่อนามสกุลของผู้ใช้งาน หรือบุคคล ในครอบครัว บุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม หรือตัวเลขที่ง่ายต่อการ คาดเดา เช่น PASSWORD, 0123456789, 6aaaaaa

๒.๒.๒ การกำหนดรหัสผ่านต้องมีไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษเข้าด้วยกัน

๒.๓ ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดสิทธิ หรือ การเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ

๒.๔ ไม่ลักลอบใช้รหัสผ่าน หรือถอดรหัสผ่านของผู้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

๒.๕ รายงานการละเมิดความปลอดภัยในระบบให้ผู้รับผิดชอบทราบในทันที

๒.๖ เมื่อได้รับรหัสผ่านชั่วคราวสำหรับการเข้าใช้งานครั้งแรก ผู้ใช้งานต้องเปลี่ยนรหัสใหม่ทันทีที่ล็อกอินเข้าใช้งานครั้งแรก

๒.๗ ไม่ใช้รหัสผ่านเดียวกัน และเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานอื่น ๆ ยกเว้นระบบที่มีการใช้ Single Sign-on (SSO) หรือมีการยืนยันตัวบุคคลผ่านระบบบริหารจัดการบัญชีผู้ใช้งาน

๒.๘ ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

๒.๙ ไม่การกำหนดให้เครื่องคอมพิวเตอร์จดจำรหัสผ่านของตนเองไว้

๒.๑๐ ควรเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือ มีผู้อื่นล่วงรู้หรือทุกครั้งที่ได้รับการแจ้งเตือน

๒.๑๑ ควรเปลี่ยนรหัสผ่านหลังจากที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากการทำงาน

๒.๑๒ ควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๓. ข้อปฏิบัติการทำลายข้อมูลหรือสื่อบันทึกข้อมูล

๓.๑ ในสถานการณ์ปกติเมื่อต้องทำลายข้อมูลหรือสื่อบันทึกข้อมูล ผู้รับผิดชอบข้อมูลต้องเป็นผู้ทำลายหรือควบคุมการทำลายข้อมูลหรือสื่อบันทึกข้อมูล

๓.๒ ในสถานการณ์ที่คาดว่าข้อมูลหรือสื่อบันทึกข้อมูลจะตกไปอยู่กับศัตรูหรือผู้ไม่หวังดี ให้กำลังพลของกองทัพเรือทุกนายสามารถทำลายข้อมูลหรือสื่อบันทึกข้อมูลได้

๓.๓ กำหนดวิธีการทำลายสื่อบันทึกข้อมูลดังนี้

ประเภท สื่อบันทึกข้อมูล	**วิธีการทำลาย แบบนำกลับมา ใช้ใหม่ได้**	**วิธีการทำลาย แบบนำสื่อบันทึกกลับมาใช้ใหม่ไม่ได้**
กระดาษ	ไม่มี	ใช้การย่อยทำลายหรือเผาทำลาย
Flash Drive	ใช้วิธีการ Format	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย หมายเหตุ การเผาทำลายสื่อบันทึกที่มีโลหะและแก้วเป็นส่วนประกอบต้องใช้ความร้อนสูง อาจก่อให้เกิดอันตราย
แผ่น Optical Disc เช่น CD/DVD	ไม่มี	
เทปบันทึกข้อมูล	ไม่มี	
ฮาร์ดดิสก์	ลบข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการ Format และเขียนทับเป็นจำนวนหลายรอบ หมายเหตุ โปรแกรม เช่น CCleaner, Mac Disk Utility และ Eraser สามารถใช้ลบข้อมูลตามวิธีการดังกล่าวได้	
Solid State Disk (SSD)	ใช้วิธีการลบข้อมูลด้วยวิธีการ Secure Erase หมายเหตุ โปรแกรม เช่น Parted Magic สามารถใช้ลบข้อมูลตามวิธีการดังกล่าวได้	

ผนวก ข
การรักษาความมั่นคงปลอดภัยไซเบอร์

๑. การประเมินความเสี่ยง (Risk Assessment)

๑.๑ ส่วนราชการต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าว อาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก โดยระบุรายละเอียดอย่างน้อยดังนี้

๑.๑.๑ ผู้กระทำให้เกิดความเสี่ยงและเหตุการณ์ความเสี่ยง เช่น ผู้ไม่ประสงค์ดี หรือช่องโหว่

๑.๑.๒ ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านโปรแกรม ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ และความเสี่ยงด้านการบริหารโครงการ เป็นต้น

๑.๑.๓ สาเหตุของการเกิดเหตุการณ์ เช่น กระบวนการปฏิบัติงาน และปัจจัยภายนอกอื่น ๆ

๑.๑.๔ ผลกระทบต่อทรัพย์สิน ทรัพยากร การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมถึงการดำเนินธุรกิจของส่วนราชการ

๑.๒ การวิเคราะห์ความเสี่ยง (Risk Analysis) ส่วนราชการต้องวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสมดังนี้

๑.๒.๑ กำหนดเจ้าของความเสี่ยง (Risk Owner)

๑.๒.๒ ระบุการควบคุมที่มีอยู่ในปัจจุบัน (Existing Control)

๑.๒.๓ พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้

๑.๒.๔ วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๑.๓ การประเมินค่าความเสี่ยง (Risk Evaluation) ส่วนราชการต้องประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และผลกระทบต่อการปฏิบัติงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)ดังนี้

๑.๓.๑ กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ เช่น ด้านการเงิน เป็นต้น

๑.๓.๒ กำหนดระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

๑.๓.๓ ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๑.๓.๔ จัดลำดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒. การจัดการความเสี่ยง (Risk Treatment)

ต้องกำหนดแนวทางจัดการและป้องกันความเสี่ยงที่สอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับที่ยอมรับได้ดังนี้

๒.๑ กำหนดแนวทางจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การหยุดหรือเลี่ยงความเสี่ยง การลดโอกาสเกิดความเสี่ยง การลดผลกระทบที่เกิดขึ้น การโอนความเสี่ยง และการยอมรับความเสี่ยง เป็นต้น

๒.๒ ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ

๒.๓ ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (Residual Risk)

๒.๔ จัดทำแผนการบริหารจัดการความเสี่ยง โดยจัดลำดับความสำคัญในการดำเนินการ

๒.๕ ขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒.๖ ให้ความรู้เรื่องแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อกำลังพล

๓. การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ที่กำหนดไว้ และมีการจัดเก็บข้อมูลอย่างเป็นระบบ เพื่อให้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ โดยมีรายละเอียดดังนี้

๓.๑ การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

๓.๒ ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น

๓.๓ ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์

๓.๔ ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและองค์กรอื่น

๓.๕ รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามรอบที่กำหนด

๔. การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (CISO) ของกองทัพเรือ และ สสท.ทร. เป็นประจำ โดยการรายงานมีรายละเอียดดังนี้

๔.๑ สถานะและผลลัพธ์ของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ประจำปี

๔.๒ ผลการประเมินและการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร

๔.๓ รายงานดัชนีชี้วัดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และรายงานสรุปเหตุการณ์ผิดปกติ

๔.๔ แนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับหน่วยงาน

๔.๕ ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

ตารางที่ ๑ การกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	**ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ**		
	ต่ำ	**กลาง**	**สูง**
ประมวลแนวทางปฏิบัติ			
องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)		✓	✓
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)	✓	✓	✓
องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	✓	✓	✓

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)			
๑.๑ การจัดการทรัพย์สิน (Asset Management)	✓	✓	✓
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	✓	✓	✓
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			✓
๑.๔ การจัดการผู้ใช้บริการภายนอก (Third Party Management)			✓
๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)			
๒.๑ การควบคุมการเข้าถึง (Access Control)	✓	✓	✓
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	✓	✓	✓
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)		✓	✓
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		✓	✓
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	✓	✓	✓
๒.๖ การแบ่งปันข้อมูล (Information Sharing)			✓
๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)			
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	✓	✓	✓
๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)			
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	✓	✓	✓
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	✓	✓	✓
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	✓	✓	✓

๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)			
๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)			✓

ตารางที่ ๒ แบบประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

แบบสอบถามส่วนที่ ๑ ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม				
ชื่อ ..... ตำแหน่ง ..... สถานที่ทำงาน				
แบบสอบถามส่วนที่ ๒ ข้อมูลการประเมินความพร้อมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์				
ตอนที่ ๑ Identify การระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง				
ลำดับ	**กระบวนการ**	**ความพร้อม (Readiness)**		
		Informal	Developing	Established	N/A
๑.	มีการจัดทำรายการทรัพย์สินของอุปกรณ์และระบบทางกายภาพ เช่น คอมพิวเตอร์ โทรศัพท์มือถือฯลฯ หรือไม่				
๒.	มีรายการซอฟต์แวร์และแอปพลิเคชัน (เช่น Microsoft, MacOS, Linux) หรือไม่				
๓.	มีการจัดทำเอกสารเกี่ยวกับการติดต่อสื่อสารและแผนภาพแสดงการไหลของข้อมูลขององค์กร หรือไม่				
๔.	มีการจัดลำดับความสำคัญของทรัพยากร (เช่น อุปกรณ์ฮาร์ดแวร์ ข้อมูล และซอฟต์แวร์) ตามผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ หรือไม่				
๕.	มีการจัดทำรายงานภัยคุกคามภายในและภายนอกองค์กร หรือไม่				
๖.	มีการระบุผลกระทบต่อการดำเนินภารกิจขององค์กรที่อาจเกิดขึ้นในแต่ละกรณี (เช่น ความน่าจะเป็น และผลกระทบที่อาจเกิดขึ้นกับองค์กรอันเป็นผลที่เกิดจากการเข้าถึงโดยไม่ได้รับอนุญาต) หรือไม่				

๗.	มีการประเมินความเสี่ยงของภัยคุกคามช่องโหว่ และผลกระทบต่อการดำเนินภารกิจขององค์กร หรือไม่				
๘.	มีกระบวนการกำกับดูแลและการบริหารความเสี่ยง หรือไม่				
๙.	มีการจัดลำดับความสำคัญและตอบสนองต่อความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่กำหนด หรือไม่				
๑๐.	มีการระบุและบันทึกช่องโหว่ของสินทรัพย์ หรือไม่				
๑๑.	มีกระบวนการจัดการยอมรับความเสี่ยงขององค์กร หรือไม่				
๑๒.	มีกระบวนการแจ้งความเสี่ยงเพื่อกำหนดระดับความเสี่ยงที่ยอมรับได้สำหรับภัยคุกคามความปลอดภัยทางไซเบอร์ขององค์กร หรือไม่				
๑๓.	จำนวนจุดการเชื่อมต่ออินเทอร์เน็ต (Internet Link) ทั้งหมด ที่เชื่อมต่อเข้ามาหรือออกไปยังเครือข่ายของหน่วยงาน				
๑๔.	จำนวนจุดการเชื่อมต่ออินทราเน็ตทั้งหมดที่เชื่อมต่อมาหรือออกไปยังเครือข่ายของ นขต.ทร.อื่น ๆ				
๑๕.	จำนวนครั้งความพยายามในการบุกรุกโจมตีระบบสารสนเทศปีล่าสุด เช่น SQL-injection, DoS, DDoS เป็นต้น				
๑๖.	จำนวนครั้งความพยายามในการบุกรุกโจมตีระบบสารสนเทศปีล่าสุด แต่สามารถควบคุมและจำกัดความเสียหายได้ ไม่ส่งผลกระทบและมีความเสียหาย				
๑๗.	จำนวนครั้งความพยายามในการบุกรุกโจมตีระบบสารสนเทศปีล่าสุด และมีผลกระทบความเสียหาย				
๑๘.	ประวัติการตรวจพบการบุกรุกโจมตีของ Computer Virus และ Malware ในปีล่าสุด				
๑๙.	ประวัติการตรวจพบการโจมตีในลักษณะ Phishing ในปีล่าสุด				
๒๐.	มีประวัติการร้องเรียนหรือแจ้งเหตุการณ์ที่เกี่ยวกับภัยไซเบอร์ เช่น โดนขโมยบัญชีผู้ใช้งาน หรือแจ้งทรัพย์สินหาย เป็นต้น				

ตอนที่ ๒ Protect การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร					
๑.	มีการระบุแสดงตัวตนผู้ใช้งานสำหรับเข้าสู่ระบบของอุปกรณ์ที่ต้องได้รับอนุญาตหรือไม่				
๒.	มีการจัดการและป้องกันการเข้าถึงสินทรัพย์จากทางกายภาพ หรือไม่				
๓.	มีการควบคุมหรือจัดการ การเข้าถึงจากระยะไกล (Remote Access) หรือไม่				
๔.	มีการจัดการสิทธิการเข้าถึงระบบ (รวมถึงสิทธิขั้นต่ำและการแบ่งแยกหน้าที่) หรือไม่				
๕.	มีการปกป้องความถูกต้องของระบบเครือข่ายและการใช้งานระบบเครือข่ายส่วนย่อยอื่น ๆ ที่เหมาะสม หรือไม่				
๖.	ผู้ใช้ทุกคนได้รับการฝึกอบรม ให้เข้าใจถึงบทบาทและความรับผิดชอบของตน หรือไม่				
๗.	ผู้บริหารระดับสูง มีความเข้าใจบทบาทและความรับผิดชอบ มากเพียงใด				
๘.	มีการปกป้องข้อมูลที่จัดเก็บอยู่ใน Storage หรือไม่				
๙.	มีการปกป้องข้อมูลที่มีการโอนย้ายระหว่างอุปกรณ์ หรือไม่				
๑๐.	มีการจัดการสินทรัพย์อย่างเป็นทางการระหว่างลบ โอนถ่าย และจำหน่าย หรือไม่				
๑๑.	มีการตรวจสอบว่ามีพื้นที่ความจุเพียงพอสำหรับความพร้อมใช้ข้อมูล หรือไม่				
๑๒.	มีการตรวจสอบซอฟต์แวร์ เฟิร์มแวร์ และความถูกต้องข้อมูลเป็นประจำ หรือไม่				
๑๓.	มีแนวทางหรือมาตรการอื่น ๆ เพื่อป้องกันการรั่วไหลของข้อมูล หรือไม่				
๑๔.	มีการทำลายข้อมูลตามนโยบายที่กำหนดไว้หรือไม่				
๑๕.	มีการป้องกันและจำกัดการใช้งานของแฟลชไดรฟ์ หรือไม่				
๑๖.	ก่อนการติดตั้งระบบ มีการประเมินความเสี่ยงฮาร์ดแวร์และซอฟต์แวร์ใหม่ หรือไม่				
๑๗.	ผู้ดูแลระบบ ได้รับการฝึกอบรมอย่างเหมาะสมในเรื่องความปลอดภัยทางไซเบอร์ และเข้าใจวิธีการตรวจจับและแก้ไขความผิดปกติ หรือไม่				

๑๘.	ในกรณีที่มีการใช้อีเมลเพื่อส่งข้อมูลที่ละเอียดอ่อน มีการตรวจสอบให้แน่ใจว่าไฟล์แนบได้รับการป้องกันด้วยการเข้ารหัสหรือรหัสผ่านที่รัดกุม และรหัสผ่านสำหรับการถอดรหัสจะถูกแชร์กับผู้รับผ่านกลไกอื่นที่ไม่ใช่อีเมล เช่น SMS หรือการโทร หรือไม่				
๑๙.	จัดทำผังเครือข่ายให้เป็นปัจจุบันอยู่เสมอหรือไม่				
๒๐.	จัดทำทะเบียนหมายเลข IP Address ของเครือข่ายภายในและภายนอกไว้ทั้งหมด หรือไม่				
ตอนที่ ๓ Detect การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ					
๑.	มีการสร้างและจัดการเครือข่ายพื้นฐานและการไหลของข้อมูล หรือไม่				
๒.	มีการวิเคราะห์เหตุการณ์ที่ตรวจพบเพื่อทำความเข้าใจเป้าหมายและวิธีการโจมตีหรือไม่				
๓.	มีการรวบรวมข้อมูลจากเหตุการณ์และเชื่อมโยงไปยังหลายแหล่งข้อมูล หรือไม่				
๔.	มีการกำหนดผลกระทบของเหตุการณ์ หรือไม่				
๕.	มีการกำหนดระดับการแจ้งเตือนเหตุการณ์หรือไม่				
๖.	ภายในเครือข่าย มีการตรวจจับเหตุการณ์ความปลอดภัยทางไซเบอร์ หรือไม่				
๗.	มีการสแกนช่องโหว่ของระบบ หรือไม่				
๘.	มีการกำหนดความรับผิดชอบในการตรวจจับโดยมีบทบาทและความรับผิดชอบของบุคลากรที่ชัดเจน หรือไม่				
๙.	มีการติดต่อสื่อสารที่เกี่ยวข้องกับเหตุการณ์ทางไซเบอร์ไปยังฝ่ายที่เกี่ยวข้อง หรือไม่				
๑๐.	มีการปรับปรุงกระบวนการตรวจจับอย่างต่อเนื่อง หรือไม่				

ตอนที่ ๔ Respond การรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น					
๑.	มีการจัดทำแผนการรับมือ/ตอบสนองต่อเหตุการณ์ทางไซเบอร์ หรือไม่ หมายเหตุ "แผนการตอบสนองต่อเหตุการณ์ทางไซเบอร์" คือแนวทางที่เป็นระบบในการจัดการ (ตอบสนอง) เหตุการณ์ด้านความปลอดภัยทางไซเบอร์ การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (CIRP) ควรดำเนินการในลักษณะที่จะบรรเทาความเสียหาย ลดเวลาการกู้คืน และลดค่าใช้จ่ายให้เหลือน้อยที่สุด ชุดคำสั่งที่องค์กรใช้เพื่อชี้แนะทีมตอบสนองต่อเหตุการณ์เมื่อมีเหตุการณ์ด้านความปลอดภัย (เช่น การละเมิดความปลอดภัย) เกิดขึ้น				
๒.	มีการใช้แผนเผชิญเหตุระหว่างหรือหลังเหตุการณ์ทางไซเบอร์ที่ตรวจพบ หรือไม่				
๓.	มีแผนการสื่อสารที่เชื่อมโยงกับแผนการตอบสนองและการจัดการเหตุการณ์ไซเบอร์ในกรณีที่เกิดเหตุการณ์ หรือไม่				
๔.	มีการทบทวนแผนการรับมือ/ตอบสนองต่อเหตุการณ์ทางไซเบอร์ หรือไม่ หมายเหตุ แผนตอบสนองต่อเหตุการณ์ทางไซเบอร์จะต้องได้รับการตรวจสอบและทดสอบเป็นระยะเพื่อให้แน่ใจว่าทุกฝ่ายเข้าใจบทบาทและความรับผิดชอบของตนซึ่งเป็นส่วนหนึ่งของแผน ซึ่งผลการทดสอบหลังการทดสอบควรแจ้งถึงการปกป้องทางเทคนิคของระบบหรือบริการในอนาคตอันใกล้นี้ เพื่อให้แน่ใจว่าปัญหาที่ระบุจะไม่เกิดขึ้นในลักษณะเดียวกันอีก ช่องโหว่ของระบบที่ระบุจะต้องได้รับการแก้ไขและทดสอบ				
๕.	มีมาตรการบรรเทาผลกระทบจากการตรวจจับเหตุการณ์ที่เกิดขึ้น หรือไม่ หมายเหตุ เมื่อค้นพบเหตุการณ์ มาตรการบรรเทาจะต้องรายงาน ประเมิน และนำไปใช้โดยเร็วที่สุด โดยใช้คำแนะนำจากผู้เชี่ยวชาญตามความจำเป็น				

๖.	มีการแบ่งปันข้อมูลหลังเหตุการณ์เกิดขึ้นแล้วหรือไม่ หมายเหตุ หลังเหตุการณ์เกิดขึ้น มาตรการบรรเทา ผลกระทบอาจถูกแบ่งปันเป็นความลับ และการรวบรวมหลักฐานจะต้องได้รับการเก็บรักษาตามความเหมาะสม สอดคล้องกับข้อผูกพันทางกฎหมาย				
๗.	มีการบทเรียนหลังเหตุการณ์ที่ได้รับ เพื่อให้เกิดการเรียนรู้ หรือไม่ หมายเหตุ เหตุการณ์หลังไซเบอร์ จะต้องมีการทบทวนอย่างเป็นทางการ และบทเรียนที่ได้รับจะถูกเพิ่มเข้าไปในแผนการตอบสนองต่อเหตุการณ์ไซเบอร์				
๘.	มีการฝึกอบรมบุคลากรเกี่ยวกับบทบาทและลำดับการปฏิบัติงาน หรือไม่				
๙.	มีการประสานงานกับผู้มีส่วนได้ส่วนเสีย เพื่อให้แน่ใจว่ามีการดำเนินการเป็นไปตามแผนเผชิญเหตุ หรือไม่				
๑๐.	มีการจัดทำเอกสารสำหรับการยอมรับความเสี่ยงสำหรับช่องโหว่ที่พบใหม่ หรือไม่				
ตอนที่ ๕ Recover การทำให้ระบบสามารถใช้งานได้อย่างต่อเนื่อง และฟื้นฟูระบบ					
๑.	มีการศึกษา ทำความเข้าใจและกำหนดวัตถุประสงค์จุดกู้คืน (RPOs) สำหรับทุกระบบที่จำเป็นต้องได้รับการกู้คืน หรือไม่ หมายเหตุ RPO คือช่วงเวลาที่ข้อมูลได้รับการสำรองข้อมูลในรูปแบบที่ใช้งานมากที่สุด และจำเป็นสำหรับกระบวนการกู้คืน				
๒.	มีการจัดทำแผนกู้คืน/ฟื้นฟูภัยพิบัติ (DRP) สำหรับเหตุการณ์ความปลอดภัยทางไซเบอร์ใด ๆ หรือไม่ หมายเหตุ DRP จะกำหนดวิธีที่หน่วยงานจะกู้คืนการเข้าถึงระบบในช่วงเวลาที่กำหนด				
๓.	ได้ดำเนินการหรือปฏิบัติตามแผนการกู้คืนในระหว่างหรือหลังเหตุการณ์ หรือไม่				

๔.	มีหรือได้กำหนดข้อตกลงระดับการให้บริการ (SLA) หรือบันทึกความเข้าใจ (MOU) พร้อมรายละเอียดเวลาในการตอบสนองและการกู้คืนระบบ หรือไม่				
๕.	มีแผนการติดต่อสื่อสารที่ประกอบด้วยรายละเอียดเกี่ยวกับวิธีการสื่อสารกับผู้มีส่วนได้เสียภายในและภายนอกในระหว่างกระบวนการฟื้นฟู หรือไม่				
๖.	มีการระบุตำแหน่งการจัดเก็บ ซึ่งประกอบด้วยรายละเอียดแสดงตำแหน่งของสถานที่สำหรับการสำรองข้อมูลที่สามารถเข้าถึงได้ในกรณีที่ข้อมูลถูกบุกรุก หรือไม่				
๗.	มีการทดสอบและการทบทวนแผนกู้คืน/ฟื้นฟูภัยพิบัติ (DRP) หรือไม่ <u>หมายเหตุ</u> มาตรการทั้งหมดที่ระบุไว้ควรได้รับการทบทวนเป็นระยะเพื่อพิจารณาการเปลี่ยนแปลงเทคโนโลยี แนวปฏิบัติ และบุคลากร				
๘.	มีกิจกรรมการกู้คืนหลังเหตุการณ์ หรือไม่ <u>หมายเหตุ</u> จะต้องแจ้งถึงการป้องกันทางเทคนิคในทันทีของเครือข่าย ระบบ หรือบริการ เพื่อให้แน่ใจว่าปัญหาจะไม่เกิดขึ้นในลักษณะเดียวกันอีก ซึ่งช่องโหว่ของระบบที่ระบุจะต้องได้รับการแก้ไข				
๙.	มีการรวบรวมบทเรียนที่ได้รับ หรือไม่				
๑๐.	มีกิจกรรมการสื่อสารภายในองค์กรในเรื่องของการกู้คืนระบบ หรือไม่				