

สำเนา



ประกาศกองทัพอเรือ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอเรือ

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครรัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้นั้น กองทัพอเรือจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอเรือ เพื่อให้กำลังพลที่ใช้งานระบบสารสนเทศ รวมทั้งหน่วยที่มีระบบสารสนเทศในความรับผิดชอบรับทราบและใช้เป็นแนวทางในการปฏิบัติต่อไป โดยมีนโยบายสำคัญประกอบด้วย

๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอเรือ ประกอบด้วย

๑.๑ การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ เพื่อควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของกำลังพล มีเนื้อหาครอบคลุมใน ๔ เรื่อง ได้แก่

๑.๑.๑ การเข้าถึงระบบสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รวมทั้งควบคุมการเข้าถึงตามสิทธิและหน้าที่ตามความจำเป็นของภาระงานของแต่ละบุคคล

๑.๑.๒ การเข้าถึงระบบเครือข่าย เพื่อให้การใช้งานระบบเครือข่ายมีความปลอดภัย และสามารถเข้าใช้งานได้อย่างทั่วถึง

๑.๑.๓ การเข้าถึงระบบปฏิบัติการ เพื่อให้ระบบปฏิบัติการที่ติดตั้งในคอมพิวเตอร์ของกองทัพอเรือสามารถใช้งานได้อย่างต่อเนื่องและปลอดภัย

๑.๑.๔ การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ เพื่อควบคุมการติดตั้งและใช้งานโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๑.๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๑.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๒. การปฏิบัติตามนโยบายที่กำหนด ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอเรือที่ปรากฏตามเอกสารแนบท้ายประกาศ ทั้งนี้แนวปฏิบัติดังกล่าว เป็นการกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอเรือ ประกอบด้วยกระบวนการดังนี้

๒.๑ กรรการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ จัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอเรือ

๒.๒ ประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

๒.๓ เจ้ากรรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ ในฐานะผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพเรือ เป็นผู้รับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือในภาพรวม

๒.๔ ให้บทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือทุก ๒ ปี

ผู้บัญชาการทหารเรือในฐานะผู้บริหารสูงสุดของกองทัพเรือ (CEO) มีความรับผิดชอบต่อความเสี่ยง ความเสียหายและอันตรายที่เกิดขึ้นกับระบบสารสนเทศของกองทัพเรือ จึงให้กำลังพลทุกนาย รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพเรือ ซึ่งเป็นเอกสารแนบท้ายประกาศนี้อย่างเคร่งครัด ทั้งนี้หากเกิดกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัตินี้ ผู้บังคับบัญชาของหน่วยงานต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๒๐ มกราคม พ.ศ.๒๕๕๘

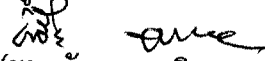
พลเรือเอก



(ไกรสร จันทรสูวนิชย์)

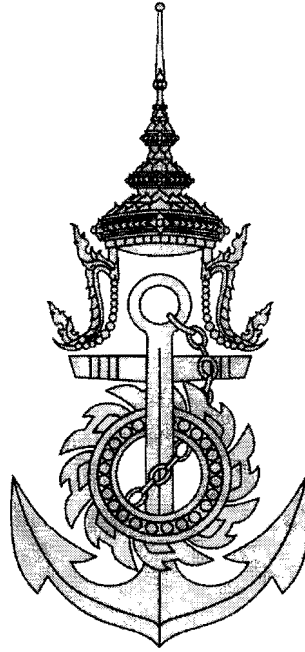
ผู้บัญชาการทหารเรือ

สำเนาถูกต้อง

น.อ. 
(ชาญชัย บุญเจริญผล)

ผอ.กสบ.สบ.ทร.

๒๕ ม.ค.๕๘



นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของกองทัพเรือ



คำนำ

ปัจจุบันระบบสารสนเทศเป็นสิ่งสำคัญที่เข้ามาอำนวยความสะดวก และสนับสนุนการปฏิบัติงานของกองทัพเรือ ส่งผลทำให้การเข้าถึงข้อมูล ข่าวสารมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพสูงขึ้น และยังช่วยลดค่าใช้จ่ายในการดำเนินงานของหน่วยที่มีการเชื่อมต่อในระบบอินเทอร์เน็ต อย่างไรก็ตามแม้ว่าระบบเครือข่ายดังกล่าวจะมีประโยชน์ และอำนวยความสะดวกในการปฏิบัติงาน แต่ในขณะเดียวกันก็มีความเสี่ยงสูงและก่อให้เกิดภัยอันตราย หรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบสารสนเทศเปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอก ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลากหลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการโจมตีทางระบบเครือข่าย เพื่อก่อวินาศภัยให้ระบบไม่สามารถใช้งานได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายเป็นอย่างมาก และยังทำให้สูญเสียชื่อเสียง และภาพลักษณ์ของกองทัพเรือ ดังนั้นผู้ใช้งาน และผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพเรือจำเป็นต้องตระหนักรู้ และให้ความสำคัญในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบสารสนเทศของกองทัพเรือ สามารถดำเนินการ หรือให้บริการต่าง ๆ ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัยและเชื่อถือได้

กองทัพเรือ ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือฉบับนี้ขึ้น เพื่อให้ผู้ใช้งาน และผู้ดูแลระบบสารสนเทศ ตลอดจนผู้บังคับบัญชาของหน่วยต่าง ๆ ในกองทัพเรือรับทราบ และยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดอย่างเคร่งครัด เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ของกองทัพเรือมีความมั่นคงปลอดภัยและเชื่อถือได้และเป็นไปตามกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้องต่อไป



สารบัญ

	หน้า
คำนำ	
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ	๑
- หลักการและเหตุผล	๑
- วัตถุประสงค์	๑
- องค์ประกอบ	๒
คำนิยาม	๓
นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ	๖
- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	๖
- ระบบสารสนเทศและระบบสำรองของสารสนเทศ	๗
- การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๗
กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ	๘
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ	๑๐
- ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access control)	๑๐
- ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)	๑๒
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)	๑๕
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	๑๗
- การควบคุมการเข้าถึงเครือข่าย (Network access control)	๒๐
- การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)	๒๓
- การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control)	๒๖
- การจัดทำระบบสำรองสำหรับระบบสารสนเทศ	๒๘
- การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๓๐
- การกำหนดความรับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ	๓๒
สรุป	๓๓



นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ โดยในส่วนของกองทัพเรือมีระเบียบกองทัพเรือ ว่าการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔ ซึ่งเป็นแนวทางและมาตรการในการป้องกันระบบสารสนเทศของทัพเรือในระดับหนึ่งแล้ว แต่เพื่อสร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกองทัพเรือเพิ่มขึ้น ตามแนวทางที่พระราชกฤษฎีกากำหนด กองทัพเรือจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกองทัพเรือขึ้น โดยมุ่งเน้นในรายละเอียดและข้อปฏิบัติต่าง ๆ เพื่อให้กำลังพลที่ใช้งานระบบสารสนเทศ รวมทั้งหน่วยที่มีระบบสารสนเทศในความรับผิดชอบรับทราบ และใช้เป็นแนวทางในการปฏิบัติต่อไป

๒. วัตถุประสงค์

การที่กองทัพเรือได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือฉบับนี้ขึ้น มีวัตถุประสงค์ดังนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกองทัพเรือ

๒.๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้กำลังพล และบุคคลที่ปฏิบัติงานด้านสารสนเทศ รวมทั้งการยืนยันตัวบุคคลการเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศของกองทัพเรือ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้ตามปกติต่อเนื่องเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๒.๔ เพื่อให้กองทัพเรือมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของที่สอดคล้องตามแนวทางของกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๕ เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๖ เพื่อให้มีการตรวจสอบ และประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

๒.๗ เพื่อสร้างความตระหนัก และส่งเสริมให้เกิดความรู้ความเข้าใจ และให้การอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่กำลังพลของกองทัพเรือ

๒.๘ เพื่อเป็นกรอบ และแนวทางการปรับปรุงพัฒนาระบบสารสนเทศของกองทัพเรือ ยกกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไปสู่สากล



๓. องค์ประกอบ

สาระสำคัญของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ ประกอบด้วย ๔ ส่วน ได้แก่

๓.๑ คำนียาม

๓.๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) ระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๓ กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

๓.๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

(๑) ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access control)

(๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

(๕) การควบคุมการเข้าถึงเครือข่าย (Network access control)

(๖) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

(๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control)

(๘) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ

(๙) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑๐) การกำหนดความรับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ



คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือประกอบด้วย

๑. “ระบบสารสนเทศ” หมายความว่า ระบบจัดการข้อมูลที่น่าเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสาร มาช่วยในการสร้างสารสนเทศ เพื่อนำมาใช้ในการวางแผน การบริหาร การพัฒนา และควบคุม ซึ่งประกอบด้วย

๑.๑ “ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑.๒ “ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ อันได้แก่

๑.๒.๑ ระบบ Intranet หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑.๒.๒ ระบบ Internet หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๑.๓ “สารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๒. “คอมพิวเตอร์” หมายความว่า เครื่องมือ หรืออุปกรณ์อิเล็กทรอนิกส์ ที่มีความสามารถในการรับข้อมูลเข้าประมวลผลตามโปรแกรมและแสดง บันทึก ส่งออกข้อมูล ซึ่งเป็นผลที่ได้จากการประมวลผลนั้น โดยมีลักษณะเป็นคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา ตลอดจนคอมพิวเตอร์อื่น ๆ

๓. “พื้นที่ใช้งานระบบสารสนเทศ” หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ หรือพื้นที่เตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งพื้นที่โต๊ะทำงานที่มีคอมพิวเตอร์ส่วนบุคคลติดตั้งประจำโต๊ะทำงาน

๔. “ผู้บังคับบัญชา” หมายความว่า ผู้ที่มีอำนาจและหน้าที่ในการปกครองบังคับบัญชาหน่วย

๕. “ผู้บริหารสูงสุด” หมายความว่า ผู้อำนวยการ และหน้าที่ในการปกครองบังคับบัญชาสูงสุดของกองทัพเรือ

๖. “ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงานราชการ และลูกจ้างของกองทัพเรือ รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพเรือที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศ

๗. “ผู้ดูแลระบบ” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลระบบงานสารสนเทศของหน่วยนั้น ๆ

๘. “ผู้ดูแลเครือข่าย” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบให้เป็นผู้ดูแลเครือข่ายสารสนเทศของหน่วยนั้น ๆ



๙. “ผู้ดูแลฐานข้อมูล” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบให้เป็นผู้ดูแลฐานข้อมูล

๑๐. “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ หรือเพื่อการเข้าถึงเข้าใช้สารสนเทศและสินทรัพย์สารสนเทศ

๑๑. “สินทรัพย์” หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศ และการสื่อสาร และหมายรวมถึงสิ่งใดก็ตามที่มีคุณค่าในระบบสารสนเทศ

๑๒. “การเข้าถึงการใช้งานสารสนเทศ” หมายความว่า ความสามารถในการเข้าไปใช้งานสารสนเทศ ด้วยวิธีการอ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใด ๆ สำหรับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ สารสนเทศ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์ และวิธีการทางกายภาพ

๑๓. “การควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตดังกล่าวสำหรับบุคคลภายนอก รวมทั้งการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมีขอบเอาไว้ด้วยก็ได้

๑๔. “จดหมายอิเล็กทรอนิกส์” หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์ และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียงที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้

๑๕. “บัญชีผู้ใช้บริการ” หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์หรือใช้บริการในระบบเครือข่ายของหน่วย

๑๖. “รหัสผ่าน” หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๗. “การพิสูจน์ยืนยันตัวตน” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๑๘. “โปรแกรมประสงค์ร้าย” หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่ง และหรือข้อมูล อิเล็กทรอนิกส์ ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อวินาศกรรมหรือสร้างความเสียหาย ไม่ว่าจะโดยตรง หรือโดยอ้อมแก่ระบบคอมพิวเตอร์ หรือระบบเครือข่าย

๑๙. “สื่อบันทึกพกพา” หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูลที่สามารถพกพาได้

๒๐. “ไฟร์วอลล์” หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยใช้ทั้งฮาร์ดแวร์ และหรือซอฟต์แวร์ในการรักษาความปลอดภัย

๒๑. “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การรักษาไว้ซึ่งความปลอดภัย ในบริบทของการรักษาความลับความเชื่อถือได้และความพร้อมใช้งานของข้อมูลสำหรับระบบสารสนเทศ



๒๒. “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า เหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศของหน่วย หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน ซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศโดยผลที่เกิดขึ้น อันส่งผลให้เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ การละเมิดต่อกฎหมายระเบียบข้อบังคับหรือข้อกำหนดต่าง ๆ การทำให้ภาพลักษณ์และชื่อเสียงเสื่อมเสีย

๒๓. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า เหตุบกพร่อง หรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งทำให้ระบบสารสนเทศสูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่าง ๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูกรบกวนหรือโจมตีทางช่องทาง และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่าง ๆ



นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

กองทัพเรือได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ สำหรับใช้เป็นแนวทางในการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งใช้เป็นกรอบสำหรับการกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ ซึ่งผู้ใช้งาน ผู้ดูแลระบบสารสนเทศ และผู้บังคับบัญชาของหน่วยต่าง ๆ ต้องรับทราบและยึดถือปฏิบัติต่อไป ทั้งนี้เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ของกองทัพเรือ มีความมั่นคงปลอดภัยและเชื่อถือได้ และเป็นไปตามที่กฎหมายกำหนด โดยนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือมีดังนี้

๑. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ เพื่อจัดการการเข้าถึง และการใช้งานสารสนเทศของกำลังพลของกองทัพเรือ ให้เป็นไปด้วยความปลอดภัย สอดคล้อง และเหมาะสมตามความจำเป็นของภารกิจ ขอบเขตหน้าที่ความรับผิดชอบ โดยมีรายละเอียดดังนี้

๑.๑ การเข้าถึงระบบสารสนเทศจะต้องปฏิบัติตามระเบียบกองทัพเรือ ว่าด้วยการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๔ และหรือที่มีการเปลี่ยนแปลง แก้ไขเพิ่มเติมภายหลัง โดยให้ความสำคัญในเรื่องการรักษาความปลอดภัยเกี่ยวกับตัวบุคคล อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศอย่างเคร่งครัด ทั้งนี้การเข้าถึงระบบสารสนเทศจะต้องได้รับอนุญาตจากผู้ที่มีอำนาจ โดยคำนึงถึงความจำเป็นตามหน้าที่ภาระงาน และต้องดำเนินการตรวจสอบ ทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ ทั้งนี้ระบบสารสนเทศที่มีชั้นความลับ ต้องมีปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ หรือระเบียบว่าด้วยการรักษาความลับของทางราชการหรือระเบียบอื่นใดที่กำหนดเป็นอย่างอื่น ๆ ตลอดจนต้องสร้างความรู้ความเข้าใจให้แก่กำลังพล ให้มีความตระหนักรู้ถึงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งต้องกำหนดบทลงโทษหากมีการฝ่าฝืนไม่ปฏิบัติตามที่กำหนด

๑.๒ การเข้าถึงระบบเครือข่าย ต้องจัดการการเข้าถึงระบบเครือข่ายให้สามารถเข้าใช้งานได้อย่างทั่วถึง สอดคล้อง และเหมาะสมกับความต้องการใช้งานตามภารกิจของผู้ใช้งาน รวมทั้งเป็นไปตามสิทธิที่ได้รับ รวมทั้งต้องบันทึกข้อมูลการเข้าใช้งานระบบเครือข่าย เพื่อใช้ในการยืนยันตัวผู้ใช้งาน และการตรวจสอบภายหลัง ตลอดจนต้องดำเนินการป้องกันการบุกรุก การเชื่อมต่อทางเครือข่ายโดยไม่ได้รับอนุญาต รวมทั้งควบคุมการเข้าถึงพอร์ต สำหรับการตรวจสอบเครือข่าย และการปรับแต่งค่าของระบบต่าง ๆ

๑.๓ การเข้าถึงระบบปฏิบัติการจะต้องได้รับอนุญาตจากผู้ที่มีอำนาจ โดยต้องควบคุมการเข้าถึง และใช้งานระบบปฏิบัติการให้เป็นไปตามสิทธิ และความจำเป็น รวมทั้งต้องบันทึกเข้าถึง และใช้งานระบบปฏิบัติการเพื่อการตรวจสอบภายหลัง ตลอดจนต้องควบคุมการใช้งานโปรแกรมมัลแวร์ที่มีผลกระทบต่อความปลอดภัยของระบบปฏิบัติการ

๑.๔ การใช้งานระบบสารสนเทศ จากโปรแกรมประยุกต์ หรือแอปพลิเคชันต่าง ๆ ที่ผ่านอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่จากภายนอก ต้องได้รับการอนุญาตจากผู้ที่มีอำนาจ และต้องมีการควบคุม เพื่อมิให้เกิดผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

ไม่สอดคล้อง
ระบบปฏิบัติการ



๒. ระบบสารสนเทศและระบบสำรองของสารสนเทศ

หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องดูแลระบบสารสนเทศให้มีความพร้อมใช้งานอยู่เสมอ รวมทั้งต้องจัดให้มีระบบสำรองของสารสนเทศ และต้องสำรองข้อมูลที่มีความสำคัญสำหรับปฏิบัติงานอย่างสม่ำเสมอ รวมทั้งให้จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน (Contingency Plan) ในกรณีที่เกิดเหตุการณ์ที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ รวมทั้งให้มีการทดสอบ และทบทวนแผนดังกล่าว

๓. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างสม่ำเสมอ ทั้งนี้การตรวจสอบและประเมินความเสี่ยง ต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วย หรือ ผู้ตรวจสอบอิสระจากภายนอกหน่วย



กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

เพื่อให้การนำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือไปสู่การปฏิบัติที่ชัดเจน จึงได้จัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือซึ่งได้กำหนดความรับผิดชอบของหน่วยและผู้ที่เกี่ยวข้องในการปฏิบัติดังนี้

๑. หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องให้ความสำคัญและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรืออย่างเคร่งครัด โดยผู้บังคับบัญชาต้องกำกับดูแล และควบคุมการใช้งานระบบสารสนเทศให้เป็นไปตามที่กำหนด

๒. ความรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือในส่วนของกำลังพล มีดังต่อไปนี้

๒.๑ ผู้ใช้งานต้องรับผิดชอบดังนี้

๒.๑.๑ ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรืออย่างเคร่งครัด และต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๒.๑.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของกองทัพเรือ

๒.๑.๓ ไม่รบกวน หรือแทรกแซงการสื่อสารในเครือข่ายสารสนเทศของกองทัพเรือ

๒.๑.๔ รายงานเหตุการณ์ความเสียหายฉุกเฉิน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังผู้บังคับบัญชา และผู้ดูแลระบบโดยเร็วที่สุด

๒.๒ กรณีที่ระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ อันเนื่องมาจากความบกพร่องละเอียดหรือฝ่าฝืนไม่ปฏิบัติตามตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บังคับบัญชาของหน่วยปฏิบัติดังนี้

๒.๒.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือ และหน่วยที่เกี่ยวข้องทราบ

๒.๒.๒ ส่งการสอบสวนหาตัวผู้กระทำผิด และผู้รับผิดชอบโดยเร็วที่สุด

๒.๒.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เกิดขึ้นซ้ำอีก

๒.๒.๔ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรง ให้อยู่ในดุลพินิจของผู้บังคับบัญชาสามารถแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติหากจำเป็น ให้รายงานหน่วยเหนือได้ตามความเหมาะสม

๒.๓ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัยให้ดำเนินการดังนี้

๒.๓.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสาร กรรมวิธีข้อมูลต่าง ๆ ประมวลลับ หรือรหัสผ่านที่จำเป็น ในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศได้รับผลกระทบกระเทือนหรือเกิดเสียหายหรือไม่อย่างไร

๒.๓.๒ ขจัดความเสียหายที่เกิดขึ้น หรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันที โดยต้องแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติพร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร



๓. เจ้ากรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ ในฐานะผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพเรือ ตามระเบียบกองทัพเรือ ว่าด้วยการรักษาความปลอดภัยด้านสารสนเทศ เป็นผู้รับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศในภาพรวมของกองทัพเรือ ทั้งนี้ให้ดำเนินการทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือทุก ๆ ๒ ปี เพื่อให้มีความทันสมัยอย่างต่อเนื่อง และสามารถนำไปสู่การปฏิบัติได้จริงอย่างเป็นรูปธรรม





แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ มีวัตถุประสงค์เพื่อกำหนดวิธีการปฏิบัติที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของกองทัพเรือ เพื่อให้ระบบสารสนเทศของกองทัพเรือมีความมั่นคงปลอดภัย โดยแนวปฏิบัติมีดังต่อไปนี้

๑. ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access control)

ข้อกำหนดการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศของหน่วย มีวัตถุประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศ ระบบเครือข่ายสารสนเทศ ระบบปฏิบัติการ โปรแกรมประยุกต์ และการใช้งานสารสนเทศ ให้เหมาะสมตามความจำเป็นต่อภารกิจหน้าที่ของผู้ใช้งาน รวมทั้งสามารถตรวจสอบการใช้งานได้ภายหลัง โดยมีข้อกำหนดดังนี้

๑.๑ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องจัดการการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศของหน่วย โดยกำหนดเป็นมาตรการ ๔ ด้านดังนี้

๑.๑.๑ ด้านการเข้าถึงระบบสารสนเทศทั่วไป ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบ ในเข้าถึงระบบสารสนเทศตามความจำเป็นต่อภารกิจหน้าที่ของผู้ใช้งานนั้น ๆ ทั้งนี้ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบของผู้ใช้งาน โดยการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่กำหนด เพื่อขอสิทธิ์ในการเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และให้มีการลงนามอนุมัติเอกสารดังกล่าวจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน โดยผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบ เฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๑.๑.๒ ด้านการเข้าถึงระบบเครือข่ายสารสนเทศ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลเครือข่ายตามสิทธิ์ และความจำเป็นในการเข้าถึงเครือข่ายก่อนที่จะเข้าใช้งาน โดยผู้ดูแลเครือข่ายมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดการอนุญาตในการผ่านเข้าสู่เครือข่ายตามสิทธิ์และความจำเป็นในการปฏิบัติงานเท่านั้น ทั้งนี้ผู้ดูแลเครือข่ายจะต้องจัดให้มีการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน ล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่น ๆ อีกด้วย

๑.๑.๓ ด้านการเข้าถึงระบบปฏิบัติการ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบระบบปฏิบัติการ ซึ่งเป็นทรัพย์สินของกองทัพเรือ จึงจะสามารถเข้าถึงการใช้งานได้ โดยผู้รับผิดชอบระบบปฏิบัติการ มีหน้าที่ตรวจสอบสิทธิ์อนุญาตให้เข้าใช้งานระบบปฏิบัติการของผู้ใช้งาน และควบคุมการใช้งานให้เป็นไปตามสิทธิ์และความจำเป็นในการใช้งาน รวมถึงบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งานไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน รวมถึงล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่น ๆ อีกด้วย

๑.๑.๔ ด้านการเข้าถึงโปรแกรมประยุกต์ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบโปรแกรมประยุกต์ ซึ่งเป็นทรัพย์สินของกองทัพเรือ จึงจะสามารถเข้าถึงการใช้งานได้ โดยผู้รับผิดชอบโปรแกรมประยุกต์ มีหน้าที่ตรวจสอบสิทธิ์อนุญาตให้เข้าใช้งานโปรแกรมประยุกต์ของผู้ใช้งาน และควบคุมการใช้งานให้เป็นไปตามสิทธิ์ และความจำเป็นในการใช้งาน รวมถึงบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งาน



ใช้งานไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน รวมถึงล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่น ๆ อีกด้วย

๑.๒ ผู้ดูแลฐานข้อมูล ต้องกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงข้อมูลของผู้ใช้งาน โดยต้องจำแนกสิทธิการเข้าถึงข้อมูลในแต่ละประเภทของผู้ใช้งาน อันได้แก่ การอ่านอย่างเดียว การสร้างข้อมูล การป้อนข้อมูล การแก้ไขข้อมูล การอนุมัติ ข้อมูลไม่มีสิทธิ์เข้าถึง โดยพิจารณาตามความจำเป็นต่อการใช้งานตามภารกิจหน้าที่ของผู้ใช้งานนั้น ๆ รวมทั้งต้องดำเนินการทบทวน สิทธิอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับความจำเป็นหรือระดับสิทธิ์ที่ได้รับ หากหมดความจำเป็นในการใช้งาน

๑.๓ ผู้ดูแลฐานข้อมูลต้องกำหนดการจัดการเกี่ยวกับข้อมูลดังนี้

๑.๓.๑ กำหนดประเภทของข้อมูล ซึ่งประกอบด้วย ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายใน และข้อมูลชั้นความลับ

๑.๓.๒ กำหนดแนวทางในการจัดหมวดหมู่ข้อมูลชั้นความลับ โดยพิจารณาจาก

- แหล่งที่มาของข้อมูล โดยหากข้อมูลนั้นมาจากภายนอก และเป็นข้อมูลลับชั้นความลับ ก็จะต้องคงไว้ดังเดิมเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับก็จะเป็นประเภทเปิดเผยได้เป็นต้น

- วิธีการนำไปใช้ประโยชน์ หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หรือ หากถูกเปิดเผยจะส่งผลกระทบต่อด้านระบบงบประมาณของหน่วย ข้อมูลนี้จะอยู่ในประเภทลับ

- จำนวนบุคคลที่รับทราบ โดยข้อมูลใดสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้

- ผลกระทบหากมีการเปิดเผย ข้อมูลใดหากถูกเปิดเผยจะมีผลกระทบต่อด้านชื่อเสียง ด้านภาพลักษณ์ ด้านการงบประมาณ ด้านการไม่ปฏิบัติตามกฎระเบียบข้อบังคับที่หน่วยกำหนดต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ซึ่งข้อมูลดังกล่าวจะสามารถจัดอยู่ในประเภทใช้ภายในเท่านั้น หรือประเภทชั้นความลับ

๑.๓.๓ ขั้นตอนการปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับให้ปฏิบัติดังนี้

- ผู้ดูแลฐานข้อมูลต้องกำหนดวิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับของผู้ใช้งานของแต่ละบุคคล ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

- ผู้ดูแลฐานข้อมูลหรือเจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

- การเข้าถึงข้อมูลประเภทชั้นความลับ จะต้องมีการพิสูจน์ตัวตนผู้ใช้งานทุกครั้ง

- การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ผู้ใช้งานต้องได้รับการเข้ารหัส (Encryption)

ที่เป็นมาตรฐานสากล

- ให้เปลี่ยนรหัสผ่านสำหรับการเข้าถึงข้อมูลชั้นความลับตามระยะเวลาที่กำหนด

- ให้กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ การส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรอง หรือลบข้อมูลที่มีสำคัญที่เก็บอยู่ในสื่อบันทึกก่อน

๑.๓.๔ การกำหนดช่วงเวลาและช่องทางการเข้าถึงสารสนเทศของมีดังนี้

- ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงได้ตลอด

๒๔ ชั่วโมง โดยผ่านระบบ Internet



- ระบบงานภายในกองทัพเรือ (Back Office) สำหรับใช้งานได้เฉพาะข้าราชการของกองทัพเรือ ตามสิทธิที่ได้รับอนุญาต โดยสามารถเข้าใช้งานได้ตลอด ๒๔ ชม. โดยผ่านระบบ Intranet

๑.๓.๕ มาตรการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลสำคัญที่ยังคงค้างอยู่ โดยปฏิบัติตามแนวทางดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การตัดด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้การตัดด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการฟอร์แมตเป็นจำนวนหลายรอบ)

๑.๓.๖ ให้กำหนดมาตรการป้องกันข้อมูลสำคัญที่มีการส่งพิมพ์ออกมาทางเครื่องพิมพ์ เพื่อป้องกันการเข้าถึงโดยผู้อื่น

๑.๓.๗ จัดทำบัญชีรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูล และสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๒. ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

ผู้ดูแลระบบ ต้องควบคุมและจำกัดสิทธิของผู้ใช้งาน เพื่อสามารถเข้าถึงและใช้งานสารสนเทศตามความเหมาะสมของภารกิจ และขอบเขตรับผิดชอบงานของผู้ใช้งานแต่ละบุคคล โดยเฉพาะอย่างยิ่งการกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ จะต้องได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของผู้ใช้งาน รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการเข้าถึงที่เกินอำนาจหน้าที่

๒.๑ การควบคุมการเข้าถึงสารสนเทศ

๒.๑.๑ การกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ อันได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์จัดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต ต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่เท่านั้น และต้องได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๑.๒ ผู้ดูแลระบบ ต้องทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยให้ปฏิบัติดังนี้

- พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบงานสารสนเทศแยกตามหน่วยงานภายในของกองทัพเรือ
- จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยต่าง ๆ เพื่อดำเนินการทบทวนว่ามีรายชื่อทั้งหมดสิทธิการเข้าถึงระบบสารสนเทศไปแล้วหรือไม่ หรือมีการเปลี่ยนแปลงสิทธิ์ แต่ยังไม่ได้มีการแก้ไขสิทธิ์การเข้าถึงให้ถูกต้องหรือไม่



- ผู้บังคับบัญชาของหน่วยแจ้งหรืออนุมัติรายชื่อของผู้มีสิทธิในระบบงานสารสนเทศที่ได้รับการแก้ไขให้ถูกต้องแล้ว

- ผู้ดูแลระบบดำเนินการแก้ไขข้อมูลผู้มีสิทธิให้ถูกต้อง ตามที่ได้รับแจ้งหรือได้รับการอนุมัติ

๒.๒ ข้อกำหนดในการใช้งานระบบสารสนเทศ

๒.๒.๑ แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์ ให้ปฏิบัติดังนี้

- ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกองทัพเรือให้เหมาะสมกับการเข้าใช้บริการและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งให้ทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เมื่อมีการเปลี่ยนตำแหน่ง เปลี่ยนต้นสังกัด การลาออกจากราชการ การเกษียณอายุ

- ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกองทัพเรือ

- ผู้ใช้งานจะต้องกำหนดรหัสผ่านที่ดี (Good Password) โดยมีแนวทางปฏิบัติตามที่ระบุในข้อ ๔.๑.๒

- รหัสผ่านของจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏ หรือแสดงรหัสผ่าน แต่ต้องแสดงออกมาในรูปของสัญลักษณ์ “ * ” หรือ “ ● ” แทนตัวอักษรของรหัสนั้น ๆ ในการพิมพ์แต่ละตัวอักษร

- ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของกองทัพเรือ หรือจดหมายอิเล็กทรอนิกส์ของภาครัฐ เพื่อใช้ในการติดต่องานราชการ

- ห้ามผู้ใช้งานตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

- ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อกองทัพเรือ หรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกองทัพเรือ

- หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องทำการออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

- ผู้ใช้งานต้องตรวจสอบเอกสารที่แนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบแฟ้มข้อมูล โดยใช้โปรแกรมป้องกันไวรัส เพื่อป้องกันการเปิดแฟ้มข้อมูลที่เป็น Executable File

- ผู้ใช้งานต้องไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๒.๒ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต มีดังนี้

- ผู้ดูแลเครือข่ายต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ต ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย

- เครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต เพื่อใช้งานโปรแกรมเข้าชมเว็บไซต์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่โปรแกรมเข้าชมเว็บไซต์ติดตั้งอยู่ก่อนการใช้งาน

- ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกองทัพเรือ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม



- ผู้ดูแลระบบต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่าย และความปลอดภัยทางข้อมูล
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับทางราชการ โดยไม่ได้รับอนุญาตผ่านเครือข่ายอินเทอร์เน็ต
- ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
- การใช้งานกระดานสนทนา (Web Board) ของหน่วยผู้ใช้ต้องไม่เปิดเผยข้อมูล ที่สำคัญ ข้อมูลส่วนบุคคล และเป็นความลับของทางราชการโดยไม่ได้รับอนุญาต รวมทั้งต้องไม่บันทึกข้อมูลที่เป็นการใส่ร้ายให้ร้ายบุคคลอื่น และการบันทึกข้อมูลที่ผิดกฎหมายต่าง ๆ
- หลังจากใช้งานอินเทอร์เน็ตเสร็จเรียบร้อยแล้ว ให้ทำการออกจากระบบ (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ
- ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ อย่างเคร่งครัด

๒.๒.๓ การเชื่อมต่ออินเทอร์เน็ตความเร็วสูง ให้ปฏิบัติตามนี้

- การขอเปิดใช้บริการเชื่อมต่ออินเทอร์เน็ตความเร็วสูงผ่านโทรศัพท์เลขหมายเอกชน จะต้องเสนอขออนุมัติกองทัพเรือ เพื่อพิจารณาความเหมาะสมและความจำเป็นในการใช้งาน
- การเชื่อมต่ออินเทอร์เน็ตความเร็วสูง จะต้องไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ของทางราชการ ที่เชื่อมต่อกับเครือข่ายภายในกองทัพเรือ (Intranet) หรือเครื่องคอมพิวเตอร์ส่วนตัวที่มีข้อมูลข่าวสารของกองทัพเรือที่เป็นชั้นความลับ และ/หรือข้อมูลที่ส่งผลกระทบต่อความมั่นคงของประเทศโดยเด็ดขาด

๒.๒.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ให้ปฏิบัติตามนี้

- ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในกองทัพเรือจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน
- ผู้ดูแลระบบเครือข่ายต้องทำการลงทะเบียน กำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
- ผู้ดูแลระบบเครือข่าย ต้องใช้ซอฟต์แวร์และหรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ
- การระบุอุปกรณ์ที่จะเข้าใช้งานในเครือข่ายไร้สายของกองทัพเรือ นอกจากการลงทะเบียนการใช้งานแล้ว จะต้องแจ้งค่า MAC address ของเครื่องหรืออุปกรณ์ที่จะเข้ามาใช้งานเพื่อให้ผู้รับผิดชอบเครือข่ายไร้สายของกองทัพเรือบันทึกเป็นหลักฐานการเข้าใช้งานต่อไป

๒.๒.๕ ผู้ดูแลระบบต้องพิจารณาการเชื่อมโยงถึงกันของระบบงานสารสนเทศตามภารกิจของหน่วยต่าง ๆ โดยพิจารณาประเด็นทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในแต่ละระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกันระหว่างหน่วยภายในกองทัพเรือ หรือหน่วยงานอื่น ๆ ที่จะมาขอเชื่อมโยงกับกองทัพเรือเป็นต้น โดยมีแนวทางพิจารณาดังนี้

- กำหนดนโยบายและมาตรการเพื่อควบคุมป้องกันและบริหารจัดการการใช้ข้อมูลร่วมกัน
- พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
- พิจารณาว่ามีกำลังพลใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน



- พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
 - ใ้ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญ หรือข้อมูลที่กำหนดชั้นความลับร่วมกัน ในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

๒.๒.๖ ผู้ดูแลระบบต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging) ของระบบงานภายในกองทัพเรือ โดยบันทึกเป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้งาน เพื่อตรวจสอบว่าใครเข้ามาใช้งานระบบ การตรวจสอบการบุกรุก รวมไปถึงการตรวจสอบข้อผิดพลาดที่เกิดขึ้นโดยจัดทำรายงานเบื้องต้นสรุปข้อมูลว่า ใคร (Who) ทำอะไร (What) เมื่อไหร่ (When) ที่ไหน (Where) และอย่างไร (How) โดยข้อมูลที่จัดเก็บมีดังนี้

- ข้อมูลชื่อบัญชีผู้ใช้ระบบงาน
- ข้อมูลวันเวลาที่เข้าถึงระบบงาน
- ข้อมูลวันเวลาที่ออกจากระบบงาน
- ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
- ข้อมูลชื่อเครื่องคอมพิวเตอร์ที่ใช้งาน
- ข้อมูลการเข้าถึงระบบ (Log in) ทั้งที่สำเร็จ และไม่สำเร็จ
- ข้อมูลความพยายามในการเข้าถึงทรัพยากร ทั้งการเข้าถึงที่สำเร็จ และไม่สำเร็จ
- ข้อมูลการเปลี่ยนแปลงสิ่งแวดล้อมหรือการกำหนดค่า (Configuration) ของระบบงาน
- ข้อมูลแสดงการใช้สิทธิต่าง ๆ
- ข้อมูลแสดงการใช้งานโปรแกรมประยุกต์ (Application Program)
- ข้อมูลแสดงการเข้าถึงแฟ้มข้อมูล (File) และการกระทำกับแฟ้มข้อมูล (File)
- ข้อมูลไอพีแอดเดรสที่เข้าถึง
- ข้อมูลโปรโตคอลของเครือข่ายที่ใช้งาน
- ข้อมูลการแจ้งเตือนเกี่ยวกับการเข้าถึงระบบจากการบุกรุก
- ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันการบุกรุก
- ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญ ๆ
- ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) มีวัตถุประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และสร้างความตระหนักรู้ของผู้ใช้งานในเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness) โดยการบริหารจัดการการเข้าถึงของผู้ใช้งาน มีดังนี้

๓.๑ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ จะต้องสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนัก และความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ทั้งนี้ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ เป็นหน่วยรับผิดชอบในการเปิดอบรมหลักสูตรที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security) ให้แก่กำลังพลของกองทัพเรือ



๓.๒ ผู้ดูแลระบบต้องดำเนินการเกี่ยวกับการลงทะเบียนผู้ใช้งาน (User registration) ดังนี้

๓.๒.๑ การลงทะเบียน มีขั้นตอนดังนี้

- หน่วยต้นสังกัดของผู้ใช้งานใหม่ แจ้งข้อมูลการลงทะเบียนผู้ใช้งานใหม่เป็นลายลักษณ์อักษร ตามสายการบังคับบัญชาให้ผู้ดูแลระบบ
- ผู้ดูแลระบบพิจารณาข้อมูลการลงทะเบียนของผู้ใช้งานใหม่ โดยตรวจสอบความถูกต้องว่าเป็นผู้ใช้งานจริง และได้รับสิทธิ์ในการใช้งานตามคำร้องขอลงทะเบียนอย่างถูกต้อง
- เมื่อผู้ดูแลระบบพิจารณาอนุมัติให้ลงทะเบียนผู้ใช้งานใหม่แล้ว ให้แจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชา และผู้ใช้งานใหม่ทราบต่อไป

๓.๒.๒ การยกเลิกสิทธิ์การใช้งาน มีขั้นตอนดังนี้

- หน่วยต้นสังกัดของผู้ใช้งานแจ้งข้อมูลการขอยกเลิกสิทธิ์การใช้งานเป็นลายลักษณ์อักษร ตามสายการบังคับบัญชาให้ผู้ดูแลระบบ
- ผู้ดูแลระบบพิจารณาข้อมูลการขอยกเลิกสิทธิ์การใช้งาน โดยตรวจสอบให้ถูกต้องว่าเป็นได้รับการยกเลิกสิทธิ์ในการใช้งานตามคำร้องอย่างถูกต้อง
- เมื่อผู้ดูแลระบบพิจารณาอนุมัติให้ยกเลิกสิทธิ์การใช้งานแล้ว ให้แจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชาและผู้ใช้งานนั้นทราบต่อไป

๓.๒.๓ ไม่อนุญาตให้ผู้ใช้งานเข้าใช้ระบบงานสารสนเทศเข้าใช้ระบบ จนกว่าจะได้รับอนุมัติแล้ว

๓.๒.๔ กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน และถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของผู้ใช้งานต่อไป

๓.๒.๕ จำกัดการใช้งานบัญชีชื่อผู้ใช้งานแบบกลุ่ม ซึ่งมีการใช้งานร่วมกันจะอนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้น และผู้ใช้งานบัญชีแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน

๓.๒.๖ จัดเก็บข้อมูลการลงทะเบียนของใช้งาน สำหรับใช้อ้างอิงหรือตรวจสอบในภายหลัง

๓.๓ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User management) ให้ปฏิบัติดังนี้

๓.๓.๑ ผู้ดูแลระบบต้องควบคุมและจำกัดสิทธิ์ของผู้ใช้งาน เพื่อสามารถเข้าถึงและใช้งานระบบสารสนเทศตามความเหมาะสมของภารกิจและขอบเขตงานรับผิดชอบของผู้ใช้งานแต่ละบุคคล โดยเฉพาะอย่างยิ่งการกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาผู้ใช้งานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๓.๒ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุม เพียงพอ และต้องได้รับความเห็นชอบและอนุมัติจากผู้ที่มีอำนาจ โดยมีแนวทางดำเนินการดังนี้

- ควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- กำหนดช่วงระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ให้มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยให้เปลี่ยนรหัสผ่านทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานให้กำหนดวงจรรอบในการเปลี่ยนรหัสผ่านทุกเดือน



๓.๔ ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านของผู้ใช้งาน (User password management) ให้มีความมั่นคงปลอดภัยดังนี้

๓.๔.๑ ต้องเก็บรักษารหัสผ่านของผู้ใช้งานให้เป็นความลับ

๓.๔.๒ รูปแบบการกำหนดรหัสผ่าน ต้องมีมากกว่าหรือเท่ากับ ๖ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๓.๔.๓ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และกำหนดข้อบัญญัติผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกันอีกด้วย

๓.๔.๔ เมื่อผู้ใช้งานของหน่วยงานลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้หน่วยแจ้งผู้ดูแลระบบทันทีเพื่อเปลี่ยนสิทธิ์ หรือถอดถอนสิทธิ์

๓.๔.๕ การเปลี่ยนรหัสผ่าน ต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๓.๔.๖ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยเพียงพอ

๓.๕ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights) ให้ปฏิบัติดังนี้

๓.๕.๑ ผู้ดูแลระบบเป็นผู้รับผิดชอบในการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

๓.๕.๒ วงรอบการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานให้ทบทวนทุก ๆ ๖ เดือน หรือ เมื่อเกิดการเปลี่ยนแปลงสิทธิ์ของผู้ใช้ ได้แก่ การลาออก การย้ายหน่วย เป็นต้น อีกทั้งการทบทวนสิทธิ์ต้องพิจารณาถึงพฤติกรรมการทำงานของผู้ใช้งาน รวมทั้งถ้ามีการเปลี่ยนแปลงของระบบงานใหม่จะต้องมีการทบทวนสิทธิ์การใช้งานทุกครั้งอีกด้วย

๓.๕.๓ การทบทวนสิทธิ์ผู้ดูแลระบบจะต้องแจ้งรายงานการทบทวนสิทธิ์เป็นลายลักษณ์อักษรให้ผู้บังคับบัญชาของหน่วยอนุมัติให้ดำเนินการต่อไป

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) มีวัตถุประสงค์เพื่อให้ผู้ใช้งานมีความเข้าใจถึงหน้าที่ และความรับผิดชอบ ตลอดจนการมีส่วนร่วมในการป้องกันการเข้าถึงระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผยการล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยผู้ใช้งานมีหน้าที่ความรับผิดชอบดังนี้

๔.๑ การใช้งานรหัสผ่าน มีข้อปฏิบัติดังนี้

๔.๑.๑ ผู้ใช้งานต้องใช้งานรหัสผ่านของตนเอง หรือตามที่ได้รับอนุมัติเท่านั้น และต้องเก็บรักษา รหัสผ่านให้เป็นความลับ และต้องปฏิบัติให้เป็นไปตามวิธีการบริหารจัดการรหัสผ่านอย่างเคร่งครัด

๔.๑.๒ ห้ามผู้ใช้งานกำหนดรหัสผ่านส่วนบุคคล จากชื่อหรือนามสกุลของผู้ใช้งาน หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม หรือตัวเลขที่ง่ายต่อการคาดเดา เช่น PASSWORD , 123456 ไม่จดหรือบันทึกที่รหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) และต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๖๐ วัน หรือทุกครั้งที่ได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่านใหม่จากผู้ดูแลระบบ



๔.๑.๓ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น หลังจากดำเนินการเรียบร้อยแล้วให้ทำการเปลี่ยนรหัสผ่านใหม่โดยทันที

๔.๑.๔ เมื่อได้รับรหัสผ่านชั่วคราวสำหรับการใช้ใช้งานครั้งแรก ผู้ใช้งานต้องเปลี่ยนรหัสใหม่ทันทีที่ล็อกอินเข้าใช้งานครั้งแรก

๔.๑.๕ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกองทัพเรือ และหากการพิสูจน์ตัวตนนั้น มีปัญหาไม่ว่าจะเกิดจากรหัสผ่านการโดนลื้อคดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที ทั้งนี้การพิสูจน์ตัวตนมีดังนี้

- คอมพิวเตอร์โน้ตบุ๊ก (Notebook) ต้องทำการพิสูจน์ตัวตนในระดับไบออส (BIOS) ก่อนการใช้งาน

- คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

- การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

- การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูล

ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์ หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง และต้องป้องกันไม่ให้ผู้ที่ไม่มีความรู้หรือสิทธิการใช้งานสินทรัพย์ที่อยู่ในความรับผิดชอบ เพื่อป้องกันการสูญหาย หรือเข้าใช้งานโดยไม่ได้รับอนุญาต ดังนี้

๔.๒.๑ กำหนดพื้นที่ใช้งานระบบสารสนเทศในบริเวณที่เหมาะสม

๔.๒.๒ เมื่อไม่มีผู้ใช้งาน ต้องการปิดล็อก ประตู และหน้าต่าง และจัดเก็บอุปกรณ์ในสถานที่ปลอดภัย เพื่อการป้องกันการโจรกรรมหรือลักลอบขโมยข้อมูล

๔.๒.๓ เมื่อผู้ใช้งานเสร็จสิ้นการใช้งานจะต้องออกจากระบบสารสนเทศ หรือผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๔.๒.๔ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ โดยตั้งเวลาในการพักหน้าจอเมื่อไม่มีผู้ใช้งาน ๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๔.๒.๕ ป้องกันให้ไม่ให้ผู้อื่นแอบใช้กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร ในการลักลอบทำสำเนาเอกสารต่าง ๆ โดยไม่ได้รับอนุญาต รวมทั้งต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๔.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องมีการควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญ ให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยมีแนวปฏิบัติดังนี้

๔.๓.๑ การรักษาความปลอดภัยทางกายภาพ (Physical security management) ให้ปฏิบัติดังนี้

- กำหนดระดับความสำคัญของพื้นที่ หรือการจำแนกพื้นที่ใช้งาน และมีการพิสูจน์ตัวตนด้วยวิธีการแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่

- พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน โดยเฉพาะศูนย์ข้อมูลกลาง (Data Center) ให้ติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น



- ๔.๓.๒ การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบสิ่งอุปกรณ์โดยบุคคลภายนอก ให้ปฏิบัติดังนี้
- จำกัดการเข้าถึงพื้นที่ หรือบริเวณที่มีการส่งมอบหรือขนถ่ายสิ่งอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
 - จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น
 - ตรวจสอบและลงทะเบียนหรือขึ้นบัญชีคุมสิ่งอุปกรณ์ที่ส่งมอบโดยผู้ถูกจ้างผู้ขายหรือผู้ให้บริการภายนอก
- ๔.๓.๓ การจัดวางและการป้องกันอุปกรณ์ (Equipment Siting and Protection) ให้ปฏิบัติดังนี้
- จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้องศูนย์ข้อมูลกลาง (Data Center) ให้น้อยที่สุด
 - อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย
 - ดำเนินการตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติ และดูแลสภาพแวดล้อมบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว
- ๔.๓.๔ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ให้ปฏิบัติดังนี้
- จัดให้มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังนี้ ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) ระบบระบายอากาศ ระบบปรับอากาศ และควบคุมความชื้น และระบบป้องกันอัคคีภัย
 - ตรวจสอบ หรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- ๔.๓.๕ การควบคุมการเดินสายไฟสายสื่อสารและสายเคเบิลอื่น ๆ (Cabling Security) ให้ปฏิบัติดังนี้
- เครือข่ายที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณ และป้องกันสัตว์ต่าง ๆ กัดสาย
 - การเดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน
 - จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง
- ๔.๓.๖ การควบคุมการนำสินทรัพย์ออกนอกหน่วยงาน (Removal of Property) ให้ปฏิบัติดังนี้
- กำหนดมาตรการรักษาความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ของหน่วยออกไปใช้งานนอก
 - บันทึกข้อมูลการนำส่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วยไว้เป็นหลักฐาน เพื่อป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อมีการนำส่งคืนเรียบร้อยเพื่อการตรวจสอบย้อนหลัง
- ๔.๓.๗ การทำลายข้อมูลสำคัญ ซึ่งหมดความจำเป็นในการใช้งาน และยังคงค้างในสื่อบันทึกให้ทำการ Delete หรือ Format ข้อมูลออกจากสื่อบันทึกนั้น
- ๔.๓.๘ การทำลายสื่อบันทึกข้อมูล ให้ปฏิบัติตามมาตรการทำลายสื่อบันทึกข้อมูล ตามข้อ ๑.๓.๕
- ๔.๔ ให้นำวิธีการเข้ารหัสมาใช้กับข้อมูลชั้นความลับ โดยปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการพ.ศ.๒๕๕๔



๕. การควบคุมการเข้าถึงเครือข่าย (Network access control)

การควบคุมการเข้าถึงเครือข่าย (Network access control) มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติดังนี้

๕.๑ กำหนดมาตรการทางเครือข่ายสื่อสารข้อมูล เพื่อป้องกันข้อมูลในเครือข่ายระบบงาน หรือบริการต่าง ๆ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือถูกทำลาย โดยให้ปฏิบัติดังนี้

๕.๑.๑ ผู้ใช้งานจะสามารถเข้าถึงเครือข่ายได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ทั้งนี้ให้พิจารณาตามความจำเป็นตามภาระงาน

๕.๑.๒ กำหนดมาตรการการป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๕.๑.๓ บันทึกข้อมูลพฤติกรรมการใช้งาน และเก็บข้อมูลของอุปกรณ์เครือข่าย เพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๕.๑.๔ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๕.๑.๕ ใช้ฮาร์ดแวร์หรือซอฟต์แวร์สำหรับการบริหารจัดการเครือข่าย เพื่อระบุ ฝ้าตรวจ และติดตามสถานะอุปกรณ์ในระบบสารสนเทศของกองทัพเรือ

๕.๒ การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวตน ก่อนที่จะอนุญาตให้เข้าใช้งานเครือข่าย โดยมีแนวทางดังนี้

๕.๒.๑ จัดทำบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของผู้ใช้งานที่อยู่ภายนอกหน่วย

๕.๒.๒ การเข้าใช้งานเครือข่าย และระบบสารสนเทศของหน่วยของผู้ใช้งานที่อยู่ภายนอก ต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง และต้องมีการบันทึกข้อมูล ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๕.๒.๓ ผู้ดูแลระบบจะต้องจัดการพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก เมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบของกองทัพเรือ โดยมีแนวทางปฏิบัติดังนี้

- การแสดงตัวตน (Identification) คือ ขั้นตอนที่ใช้แสดงตัวตนด้วยชื่อของผู้ใช้ (Username)

- การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง ด้วยวิธีการใช้รหัสผ่าน (Password) หรือ การใช้สมาร์ทการ์ด หรือ การใช้ USB token ที่มีความสามารถ PKI

- การเข้าสู่ระบบสารสนเทศของกองทัพเรือจากอินเทอร์เน็ต จะมีการตรวจสอบผู้ใช้งานด้วย

- การเข้าสู่ระบบจากระยะไกล (Remote access) จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานด้วยรหัสผ่าน หรือ วิธีการเข้ารหัส เพื่อเพิ่มความปลอดภัย

- การเข้าสู่ระบบสารสนเทศของหน่วยนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี



๕.๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่บริหารเครือข่ายและสัญญาณ กองโทรคมนาคม สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (กทค.สปก.สสท.ทร.) และต้องจัดทำเป็นบัญชีไว้สำหรับการระบุอุปกรณ์บนเครือข่าย โดยบัญชีดังกล่าวต้องประกอบด้วย วันเดือนปี ที่ติดตั้งและเชื่อมต่ออุปกรณ์ ข้อมูลทะเบียนหมายเลข IP รายละเอียดของอุปกรณ์ที่ติดตั้ง รวมถึงสถานที่ติดตั้งเพื่อให้สามารถระบุอุปกรณ์บนเครือข่ายได้

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ระบบเครือข่ายและอุปกรณ์ที่เกี่ยวข้องกับเครือข่าย ต้องมีการป้องกันการเข้าถึงตัวอุปกรณ์ทางกายภาพ โดยต้องติดตั้งอยู่ในห้องที่สามารถจำกัดการเข้าถึงได้ และต้องกำหนดบุคคลที่รับผิดชอบพร้อมกำหนดสิทธิ์การเข้าถึงอุปกรณ์ดังกล่าวอย่างชัดเจนในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) และมีการทบทวนสิทธิ์การเข้าถึงและการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๕ การแบ่งแยกเครือข่าย และการควบคุมการเชื่อมต่อทางเครือข่าย ให้ปฏิบัติดังนี้

๕.๕.๑ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ จะต้องทำการแยกเครือข่ายตามกลุ่มด้วยอุปกรณ์ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่น ๆ ดังนี้

- กลุ่มบริการสารสนเทศ เป็นระบบสารสนเทศที่เข้าถึงและใช้งานโดยผู้ใช้งาน
- กลุ่มระบบสารสนเทศ เป็นระบบสารสนเทศพื้นฐาน ได้แก่ ระบบฐานข้อมูล ระบบ Directory Service ซึ่งถูกใช้งานโดยระบบสารสนเทศในกลุ่มบริการสารสนเทศ แต่ต้องไม่ถูกเข้าถึงโดยตรงจากผู้ใช้งาน
- กลุ่มผู้ใช้งาน เป็นเครือข่ายคอมพิวเตอร์ของผู้ใช้งาน

๕.๕.๒ แนวทางการควบคุมการเชื่อมต่อเครือข่ายที่แบ่งแยกชนิดตามข้อ ๕.๕.๑ ด้วยอุปกรณ์ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่น ๆ มีดังนี้

- ผู้ดูแลเครือข่าย มีหน้าที่ในการบริหารจัดการการติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด
- การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
- เส้นทางเชื่อมต่ออินเทอร์เน็ต และบริการอินเทอร์เน็ตที่ไม่ได้รับอนุญาตจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

- ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง
- มีการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
- การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

- ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

- การกำหนดระเบียบในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปเฉพาะที่ได้อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากกองทัพเรือก่อน

- การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายชื่อเครื่องที่ให้บริการจริง



- จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า
 - เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป
 - ผู้ดูแลเครือข่าย มีสิทธิ์ที่จะระงับ หรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข
 - การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน
- ๕.๕.๓ ผู้ใช้งานที่ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์จะถูกระงับการใช้งานอินเทอร์เน็ต หรือเชื่อมต่อเครือข่ายภายในโดยทันที
- ๕.๕.๔ การเข้าสู่ระบบเครือข่ายภายในของกองทัพเรือ โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี
- ๕.๕.๕ ผู้ดูแลเครือข่ายต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
- ๕.๕.๖ ผู้ดูแลเครือข่ายต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน
- ๕.๕.๗ ผู้ดูแลเครือข่าย ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ
- ๕.๕.๘ ผู้ดูแลเครือข่าย ตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน
- ๕.๕.๙ ระบบเครือข่ายทั้งหมดของหน่วยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering
- ๕.๕.๑๐ ผู้ดูแลเครือข่าย มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบโดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า
- ๕.๕.๑๑ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิด การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและสินทรัพย์ของกองทัพเรือจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมายต่อไป
- ๕.๕.๑๒ การเข้าสู่ระบบงานเครือข่ายภายในหน่วยผ่านทางอินเทอร์เน็ต ต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
- ๕.๖ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านข้อมูลหรือสารสนเทศ สอดคล้องรองรับกับการควบคุมการเข้าถึงการใช้งาน โดยมีแนวปฏิบัติดังนี้
- ๕.๖.๑ ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ (IP Address) ของระบบงานเครือข่ายภายใน ต้องมีการป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้



บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศของหน่วยได้โดยง่าย

๕.๖.๒ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ และต้องปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๖.๓ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชา หรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๖.๔ ให้บันทึกการทำงานของระบบป้องกันการบุกรุก อันได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการตรวจสอบย้อนหลัง และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อยกว่า ๓ เดือน

๕.๖.๕ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติดังนี้

๖.๑ การควบคุมการติดตั้งระบบปฏิบัติการในเครื่องคอมพิวเตอร์ (Control of operational software) ให้ปฏิบัติดังนี้

๖.๑.๑ ควบคุมการเปลี่ยนแปลงระบบปฏิบัติการที่มีผลกระทบต่อระบบงานของหน่วย เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

๖.๑.๒ การเปลี่ยนแปลงระบบปฏิบัติการ จะต้องดำเนินการโดยผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น

๖.๑.๓ กำหนดให้มีการจัดเก็บซอร์สโค้ด และไลบรารีสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๖.๑.๔ ผู้ดูแลระบบต้องทดสอบระบบปฏิบัติการตามจุดประสงค์ที่กำหนด อย่างครบถ้วนเพียงพอ ก่อนที่จะดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๖.๑.๕ ผู้ดูแลระบบต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบปฏิบัติการอย่างครบถ้วน ก่อนดำเนินการติดตั้ง

๖.๑.๖ ให้ปรับปรุงไลบรารีสำหรับซอฟต์แวร์ของระบบปฏิบัติการให้มีความทันสมัย

๖.๑.๗ ในกรณีที่เป็นการติดตั้งระบบปฏิบัติการ เพื่อทดแทนระบบปฏิบัติการเดิม ให้ทำการสำรองข้อมูลที่จำเป็นอันได้แก่ ฐานข้อมูลซอฟต์แวร์ ค่าคอนฟิกูเรชัน หรืออื่น ๆ ที่เกี่ยวข้องกับระบบปฏิบัติการนั้น

๖.๑.๘ กรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบปฏิบัติการเดิม เพื่อไปสู่ข้อมูลในระบบปฏิบัติการใหม่ ให้จัดทำแผนการถ่ายโอนหรือแปลงข้อมูล เพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้อง และครบถ้วนหรือไม่

๖.๑.๙ ให้กำหนดแผนการติดตั้งสำหรับระบบปฏิบัติการใหม่ ซึ่งรวมถึงระยะเวลาที่จะดำเนินการรวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า สำหรับซอฟต์แวร์ที่จะทำการติดตั้งให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

๖.๑.๑๐ ให้อ่าน และปฏิบัติตามเงื่อนไข หรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด



๖.๑.๑๑ การติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้อง และเชื่อถือได้

๖.๑.๑๒ ต้องติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ (Patch) ที่เกี่ยวข้องกับระบบปฏิบัติการตามความจำเป็นอันได้แก่ โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๖.๒ การทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes) โดยให้ปฏิบัติดังนี้

๖.๒.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบ เกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๖.๒.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๖.๓ การปฏิบัติเพื่อการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยมิได้รับอนุญาตให้ปฏิบัติดังนี้

๖.๓.๑ ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๖.๓.๒ ต้องจำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่านเมื่อต้องเข้าถึงระบบปฏิบัติการ

๖.๓.๓ ผู้ใช้ต้องตั้งการใช้งานโปรแกรมรักษาหน้าจอแสดงผล (Screen Saver) โดยตั้งเวลาในกรณีไม่ได้ใช้งานในห้วงระยะเวลาขณะหนึ่ง เพื่อให้ทำการปิดกั้นการใช้งาน (Lock) สำหรับหน้าจอแสดงผล

๖.๓.๔ ระบบต้องยุติการเชื่อมต่อเมื่อพบว่ามีการพยายามคาดเดารหัสผ่าน หากทำการล็อกอินไม่สำเร็จเกินกว่า ๓ ครั้ง

๖.๓.๕ ผู้ใช้ต้องทำการ Logout ออกจากระบบทันที เมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอแสดงผลเป็นเวลานาน

๖.๓.๖ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากจะสร้างความเสียหายให้กับระบบปฏิบัติการได้

๖.๔ การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) การเข้าถึงระบบปฏิบัติการ ต้องระบุตัวตนของผู้ใช้งาน และการยืนยันตัวตนที่เหมาะสม โดยให้ปฏิบัติดังนี้

๖.๔.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๖.๔.๒ ผู้ใช้ต้องกำหนดรหัสผ่านให้มีคุณภาพตามที่ระบุไว้ในเอกสารนี้

๖.๕ การบริหารจัดการรหัสผ่าน (Password management system) ในการเข้าถึงระบบปฏิบัติการ ผู้ใช้งานจะต้องกำหนดรหัสผ่านที่มีคุณภาพตามข้อ ๓.๔.๒ ข้อ ๓.๔.๓ และข้อ ๔.๑.๒ ทั้งนี้ผู้ดูแลระบบต้องจัดทำระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) เพื่อให้คำแนะนำเกี่ยวกับวิธีการกำหนดรหัสผ่านที่มีคุณภาพ รวมทั้งในกรณีที่ผู้ใช้งานกำหนดรหัสผ่านไม่เป็นไปตามข้อกำหนดดังกล่าว ระบบต้องไม่อนุญาตการใช้รหัสผ่านนั้น พร้อมแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ จนกว่าการกำหนดรหัสผ่านจะเป็นไปตามข้อกำหนด



๖.๖ ควบคุมการใช้งานโปรแกรมมัลแวร์ประโชชน์ เนื่องจากการใช้งานโปรแกรมมัลแวร์ประโชชน์บางชนิดสามารถทำให้ผู้ใช้งานสามารถหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัย ให้ปฏิบัติดังนี้

- ๖.๖.๑ จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุม ในการอนุญาตให้ใช้โปรแกรมมัลแวร์ประโชชน์
- ๖.๖.๒ ห้ามผู้ใช้งานติดตั้งและใช้งานโปรแกรมมัลแวร์ประโชชน์ที่เข้าช่วยการละเมิดสิทธิการใช้งาน
- ๖.๖.๓ ให้อนุญาตใช้งานโปรแกรมมัลแวร์ประโชชน์เป็นรายครั้งไป
- ๖.๖.๔ จัดเก็บโปรแกรมมัลแวร์ประโชชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ
- ๖.๖.๕ ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้เพื่อการตรวจสอบภายหลัง

๖.๗ การวางเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งาน (Session time-out) เพื่อควบคุม และจำกัดการเข้าถึง หรือการใช้งาน ให้สอดคล้องตามความจำเป็นตามภารกิจ และสิทธิที่ได้รับของผู้ใช้งาน ให้ปฏิบัติดังนี้

๖.๗.๑ ให้มีการตัดการติดต่อ และหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๖.๗.๒ ระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง อันได้แก่ ระบบงานที่มีข้อมูลสำคัญ ระบบงานที่กำหนดชั้นความลับ ต้องมีการตัดการติดต่อและหมดเวลาการใช้งานที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- เมื่อผู้ใช้งานไม่ได้ใช้งานหรือวางเว้นจากการใช้งานในระยะเวลา ๑ ชั่วโมง หรือตามที่ผู้ดูแลระบบกำหนดให้มีการตัดการเชื่อมต่อการใช้งานออกจากระบบสารสนเทศโดยอัตโนมัติ

- ถ้ามีความพยายามเข้าสู่ระบบใหม่ให้ยืนยันการใช้งานโดยใส่ชื่อผู้ใช้ (Username) และรหัสผ่าน (password) หรือวิธีการที่ปลอดภัยในการยืนยันตัวบุคคลในทุก ๆ ครั้ง

๖.๘ การจำกัดระยะเวลาการเชื่อมต่อ (Limitation of connection time) เพื่อให้มีความมั่นคงปลอดภัยมากขึ้น สำหรับระบบสารสนเทศที่มีความสำคัญ หรือมีความเสี่ยงสูง ให้ปฏิบัติดังนี้

๖.๘.๑ จำกัดช่วงระยะเวลาการเชื่อมต่อ สำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานภายในระยะเวลาที่กำหนดเท่านั้น

๖.๘.๒ การจำกัดช่วงระยะเวลาการเชื่อมต่อ เพื่อป้องกันบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึงข้อมูลได้โดยง่าย โดยมีแนวทางดังนี้

- การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพเรือ กำหนดให้ใช้งานได้ ๔ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หรือตามที่ผู้บังคับบัญชาเห็นสมควร

- การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพเรือ กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น

- การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพเรือ ถ้ากระทำในช่วงนอกเวลาทำงานตามปกติต้องได้รับอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร



๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control)

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control) เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชัน และสารสนเทศ โดยไม่ได้รับอนุญาต และให้การเข้าถึงมีความเหมาะสมตามภารกิจ และขอบเขตงานของผู้ใช้งาน โดยมีแนวปฏิบัติดังนี้

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) เพื่อจำกัดการเข้าถึงสารสนเทศของผู้ใช้งานเฉพาะส่วนที่มีความจำเป็นตามภารกิจ โดยหน่วยที่มีระบบสารสนเทศในความรับผิดชอบจะต้องดำเนินการดังนี้

๗.๑.๑ ผู้ดูแลฐานข้อมูล จะต้องดำเนินการจำแนกสารสนเทศที่มีอยู่ว่ามีสารสนเทศใดบ้าง และจะต้องวิเคราะห์ความสำคัญของสารสนเทศในแต่ละกลุ่มนั้นว่ามีความสำคัญต่อปฏิบัติงานมากน้อยเพียงใด โดยสารสนเทศใดหากถูกเปลี่ยนแปลง แก้ไข สูญหาย ถูกทำลาย หรือลักลอบนำไปใช้โดยไม่ได้รับอนุญาต จะทำให้หน่วยเสียหาย ให้ถือว่าสารสนเทศนั้นมีความสำคัญ และความอ่อนไหวสูง จำเป็นต้องมีการจำกัดการเข้าถึงสารสนเทศนั้น

๗.๑.๒ การกำหนดให้ผู้ใช้งานใดที่จะสามารถเข้าถึงสารสนเทศใดบ้าง ให้พิจารณาจากบทบาทและหน้าที่(Roles) ของผู้ใช้งานนั้น ๆ สารสนเทศบางประเภทสามารถกำหนดให้ผู้ใช้งานทุกคนสามารถเข้าถึงได้ สารสนเทศบางประเภทต้องกำหนดให้เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้นที่จะสามารถเข้าถึงได้

๗.๑.๓ กำหนดสิทธิ์ในการเข้าถึง (Access Permissions) ให้สอดคล้องกับผู้ใช้งาน และสารสนเทศที่ได้จำแนกไว้ โดยสิทธิ์ที่ได้รับสามารถกำหนดอยู่ในรูปแบบของการใช้งานประเภทต่าง ๆ อันได้แก่ การประมวลผลการแก้ไข การอ่านเพียงอย่างเดียว

๗.๑.๔ กรณีมีการจ้างบุคคลภายนอก (Outsource) ในการพัฒนา ดูแล และบำรุงรักษาระบบสารสนเทศนั้น ให้ปฏิบัติดังนี้

- ตรวจสอบประวัติบุคคลภายนอกที่เข้ามาปฏิบัติงาน ตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ และต้องควบคุมการปฏิบัติงานของบุคคลภายนอกให้อยู่ภายในขอบเขตที่กำหนด

- ให้มีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของซอฟต์แวร์ หรือระบบงานที่จะทำการพัฒนาขึ้นมาอย่างเป็นลายลักษณ์อักษร

- บุคคลภายนอกต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ รวมทั้งต้องจำกัดการเข้าถึงสารสนเทศเฉพาะที่ความจำเป็นเท่านั้น

- ต้องตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์ในซอฟต์แวร์ต่าง ๆ ที่ถูกพัฒนาขึ้นก่อนดำเนินการติดตั้ง หรือทดสอบการใช้งานจริง

๗.๒ สารสนเทศที่อ่อนไหว (Sensitive) มีผลกระทบ และมีความสำคัญสูงต่อองค์กร ต้องกำหนดให้สามารถใช้งานเฉพาะกลุ่มเท่านั้น และต้องกำหนดช่องทางและวิธีการในการเข้าถึง โดยจัดให้มีเครื่องแม่ข่ายควบคุมแยกต่างหาก การติดต่อกับเครื่องแม่ข่ายต้องผ่านระบบ firewalls การจำกัดการเข้าถึงเฉพาะการใช้เครื่องข่ายภายในเท่านั้น และต้องกำหนดมาตรการควบคุมการเข้าถึงเป็นกรณีพิเศษจากอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่ หรือการใช้งานระบบจากภายนอก (Mobile computing and Teleworking)



- ๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ที่ใช้งานผ่านเครือข่ายไร้สายของ ทร. ปฏิบัติดังนี้
- ๗.๓.๑ ให้สิทธิการใช้งานสำหรับผู้ใช้งานที่มีชั้นยศตั้งแต่ น.อ. ขึ้นไป โดยผู้ใช้งานต้องแจ้งความประสงค์ขอใช้งานบริการระบบเครือข่ายไร้สายที่ แผนกบริการสารสนเทศ ศูนย์ข้อมูลกลาง สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (ศชก.สปก.สสท.ทร.) พร้อมแจ้งรายละเอียดของอุปกรณ์ หมายเลข MAC Address ของอุปกรณ์ พร้อมชื่อผู้ใช้งาน
- ๗.๓.๒ แผนกบริการสารสนเทศ ศูนย์ข้อมูลกลาง สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (ศชก.สปก.สสท.ทร.) บันทึกข้อมูลลงในระบบ เพื่อลงทะเบียน MAC Address ของอุปกรณ์ พร้อมทดสอบการใช้งานเบื้องต้น และแจ้งคำชี้แนะ การให้บริการ ขั้นตอนการใช้งาน จุดบริการ รวมทั้งวิธีแก้ปัญหาต่าง ๆ ให้ผู้ใช้งานทราบ
- ๗.๔ ผู้ดูแลระบบต้องจัดการควบคุมการเข้าใช้งานระบบจากภายนอก (Teleworking) ดังนี้
- ๗.๔.๑ การเข้าสู่ระบบเครือข่ายจากระยะไกล (Remote access) ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของระบบสารสนเทศ จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้น จากมาตรการการเข้าสู่ระบบภายใน
- ๗.๔.๒ วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจาก ผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และต้องควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้อง ปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
- ๗.๔.๓ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้บังคับบัญชา
- ๗.๔.๔ มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการ โทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้อง และเหมาะสมแล้วเท่านั้น
- ๗.๔.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น โดยช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้งานได้ต่อเมื่อมีการร้องขอเท่านั้น
- ๗.๕ มาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อป้องกันชุดคำสั่งไม่พึงประสงค์มีดังนี้
- ๗.๕.๑ ห้ามการติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ แฟ้มข้อมูล (File) อื่นที่ไม่อนุญาตให้ใช้งาน
- ๗.๕.๒ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการ ติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต
- ๗.๕.๓ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ให้กับระบบเทคโนโลยีสารสนเทศ
- ๗.๕.๔ ให้ผู้ดูแลระบบดำเนินการตรวจสอบชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ ที่ให้บริการ และอุปกรณ์เทคโนโลยีสารสนเทศอื่น ๆ ในบริเวณจุดทางเข้า - ออกเครือข่ายอย่างสม่ำเสมอ เพื่อดักจับชุดคำสั่งไม่พึงประสงค์ที่จะเข้าสู่ระบบ
- ๗.๕.๕ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการจัดการชุดคำสั่งไม่พึงประสงค์ ได้แก่ การรายงานการเกิดขึ้นของชุดคำสั่งไม่พึงประสงค์ การวิเคราะห์การจัดการการกู้คืนระบบจากความเสียหายที่ตรวจพบ เป็นต้น
- ๗.๕.๖ มีการติดตามข้อมูลข่าวสารเกี่ยวกับชุดคำสั่งไม่พึงประสงค์อย่างสม่ำเสมอ



๗.๕.๗ ให้มีการสร้างความตระหนักเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ เพื่อให้ผู้ใช้งานมีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติ เมื่อพบเหตุชุดคำสั่งไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร รวมทั้งให้จัดการฝึกอบรมสร้างความตระหนักอย่างน้อยปีละ ๑ ครั้ง

๘. การจัดทำระบบสำรองสำหรับระบบสารสนเทศ

หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ จะต้องดำเนินการจัดทำระบบสำรองสำหรับระบบสารสนเทศ เพื่อให้มั่นใจว่าระบบสารสนเทศ และข้อมูลสำคัญจะยังคงมีอยู่ สามารถเข้าถึงและใช้งานได้ แม้เกิดเหตุการณ์ในกรณีฉุกเฉิน โดยมีแนวปฏิบัติดังนี้

๘.๑ การคัดเลือกและจัดทำระบบสำรองและกู้คืนระบบ ให้ดำเนินการดังนี้

๘.๑.๑ กำหนดระบบงานที่มีความสำคัญ และจัดทำเป็นบัญชีรายชื่อของระบบงานดังกล่าว รวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

๘.๑.๒ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๘.๑.๓ กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบข้อมูลสำหรับตัวระบบ อันได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และ ซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้องเป็นต้น

๘.๑.๔ กำหนดความถี่ในการสำรองข้อมูลของระบบงาน โดยระบบงานที่มีความถี่ของการเปลี่ยนแปลงข้อมูลบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๘.๑.๕ ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และต้องนำข้อมูลที่สำรองเก็บไว้นอกสถานที่ อย่างน้อย ๑ ชุด

๘.๑.๖ ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้นสำเร็จครบถ้วนหรือไม่

๘.๑.๗ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้งรวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

๘.๒ แนวทางปฏิบัติสำหรับการสำรองข้อมูลมีดังนี้

๘.๒.๑ ผู้ดูแลฐานข้อมูลต้องจัดให้มีการสำรอง และทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ โดยให้เป็นไปตามแนวทางการสำรองข้อมูล

๘.๒.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลฐานข้อมูลต้องทำบันทึก รายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๘.๒.๓ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลฐานข้อมูลต้องทำรายงานข้อผิดพลาด จากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๘.๒.๔ ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหา และสรุปผลการแก้ไขปัญหา พร้อมทั้งรายงานต่อผู้รับผิดชอบระบบสารสนเทศของหน่วยทราบ

๘.๒.๕ ให้ผู้ดูแลฐานข้อมูล กำหนดชนิด และช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

๘.๒.๖ แนวทางที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลฐานข้อมูล ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด



๘.๒.๗ ความถี่ในการสำรองข้อมูลมีดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรอง
ระบบ E-mail	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลในส่วน Mailbox	๑ ครั้งต่อเดือน
Web Server	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลต่าง ๆ ที่เผยแพร่บนเว็บไซต์	๑ ครั้งต่อเดือน
Database Server	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ฐานข้อมูลที่มีความสำคัญ	๑ ครั้งต่อเดือน
อุปกรณ์ Firewall	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูล Rule ของอุปกรณ์นั้น	๑ ครั้งต่อเดือน
อุปกรณ์ IDS/IPS	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูล Rule ของอุปกรณ์นั้น	๑ ครั้งต่อเดือน
อุปกรณ์ Server อื่น ๆ	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลที่มีความสำคัญของระบบงานที่ถูกเก็บในอุปกรณ์ต่าง ๆ เหล่านี้	๑ ครั้งต่อเดือน

๘.๓ แนวทางปฏิบัติสำหรับการกู้คืนระบบมีดังนี้

๘.๓.๑ ในกรณีพบปัญหาที่สร้างความเสียหายต่อระบบคอมพิวเตอร์ ระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบหรือผู้ดูแลเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไข พร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้รับผิดชอบระบบ สารสนเทศของหน่วยหรือผู้ที่ได้รับมอบหมายทราบ

๘.๓.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๘.๓.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งาน ให้ผู้ดูแลระบบแจ้งผู้ใช้งานทราบ พร้อมทั้งรายงานความคืบหน้าการกู้คืนเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๘.๔ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ จะต้องดำเนินการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินดังนี้

๘.๔.๑ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน (Contingency Plan) เพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้น ทั้งวิธีการทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งให้กำหนดการทดสอบแผนดังกล่าวทุกปี โดยแผนต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

- การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
- การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญ และกำหนดมาตรการเพื่อลด

ความเสี่ยง อันได้แก่ ไฟฟ้าดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

- การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน



- การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
- การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก อันได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ
- การสร้างความตระหนัก หรือให้ความรู้แก่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุ
- ให้ปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยมุ่งเน้นที่ระบบที่มีความสำคัญสูง

๘.๔.๒ ให้ทำการสำรองข้อมูลตามชนิดความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลสำรองมีความครบถ้วนหรือไม่

๘.๔.๓ ให้ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไขและบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

๘.๔.๔ ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน รวมทั้งเมื่อมีการปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินใหม่จะต้องจัดประชุมใหม่ และแจ้งให้ผู้ที่เกี่ยวข้องทราบ

๘.๔.๕ กรณีที่เกิดเหตุการณ์กรณีฉุกเฉินต่อระบบสารสนเทศของกองทัพเรือ สามารถติดต่อประสานงานกับผู้รับผิดชอบ ดังนี้

- ผู้อำนวยการศูนย์ข้อมูลกลาง สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ โทร. ๕๗๘๐๑

- หัวหน้าแผนกควบคุม ศูนย์ข้อมูลกลาง สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ โทร. ๕๗๘๑๒

๙. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ เพื่อให้ทราบถึงระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ และระดับความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะนำไปสู่การปรับปรุงแก้ไขต่อไป โดยมีแนวปฏิบัติดังนี้

๙.๑ ผู้ดูแลระบบต้องกำหนดการประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่ใช้งาน เพื่อกำหนดแนวทางในการเฝ้าระวังและดูแลระบบเหล่านั้น และกำหนดให้มีการเฝ้าระวัง และดูแลระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่ต้องปฏิบัติตามอย่างสม่ำเสมอโดยการตรวจสอบดังต่อไปนี้

๙.๑.๑ ชื่อบัญชีผู้ใช้งาน

๙.๑.๒ กิจกรรมการใช้งานและประเภทของกิจกรรม

๙.๑.๓ วัน/เวลาที่เข้าถึง

๙.๑.๔ แพ้มข้อมูลหรือข้อมูลที่ถูกเข้าถึง

๙.๑.๕ โปรแกรมทั่วไปและอรรถประโยชน์ต่าง ๆ (Utilities) ที่ถูกเรียกใช้งาน

๙.๑.๖ การใช้บัญชีผู้ใช้งานในระดับสูง อันได้แก่ Supervisor, Root, Administrator เป็นต้น

๙.๑.๗ การเปิด-ปิดการทำงานของระบบ



- ๙.๑.๘ การถอดถอนหรือติดตั้งอุปกรณ์สำหรับนำเข้าและส่งออกข้อมูล (I/O)
- ๙.๑.๙ การใช้คำสั่งของผู้ใช้งานที่ได้รับการปฏิเสธโดยระบบ
- ๙.๑.๑๐ ความพยายามในการเข้าถึงข้อมูลหรือทรัพยากรของระบบที่ได้รับการปฏิเสธโดยระบบ
- ๙.๑.๑๑ การแจ้งเตือนจากไฟร์วอลล์หรือระบบป้องกันการบุกรุก
- ๙.๑.๑๒ การแจ้งเตือนจากอุปกรณ์แจ้งเตือน (Console) ของผู้ดูแลระบบ
- ๙.๑.๑๓ การแจ้งเตือนเมื่อระบบทำงานผิดปกติ
- ๙.๑.๑๔ การแจ้งเตือนจากโปรแกรมบริหารจัดการเครือข่าย
- ๙.๑.๑๕ การแจ้งเตือนการทำงานของระบบล้มเหลวหรือหยุดชะงัก
- ๙.๑.๑๖ ความพยายามในการเปลี่ยนแปลงค่าการติดตั้งระบบ (Configuration) ด้านความมั่นคง

ปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๙.๒ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องจัดให้มีการประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง ซึ่งประกอบด้วยทรัพย์สิน ๕ หมวด ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลและระบบงาน โดยปฏิบัติตามแนวทางการประเมินดังนี้

- ๙.๒.๑ กำหนดให้มีการจัดทำบัญชีทรัพย์สินสารสนเทศ
- ๙.๒.๒ ระบุและประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ
- ๙.๒.๓ จัดลำดับความเสี่ยงจากสูงมาต่ำ
- ๙.๒.๔ จัดทำแผนการลดความเสี่ยงโดยคำนึงถึงการจัดการกับความเสี่ยงสูงก่อน
- ๙.๒.๕ กำหนดให้มีการปฏิบัติตามแผนการลดความเสี่ยงที่กำหนดไว้และติดตามจนกระทั่งแล้วเสร็จ

๙.๓ ความรับผิดชอบในการตรวจสอบและประเมินความเสี่ยง มีดังนี้

- ๙.๓.๑ กรณีการตรวจสอบจากผู้ตรวจสอบภายในหน่วยงาน (Internal auditor) ให้ดำเนินการดังนี้
 - ให้แต่งตั้งคณะทำงาน หรือคณะกรรมการรับผิดชอบการตรวจสอบและประเมินความ

เสี่ยงระบบสารสนเทศภายในหน่วย

- ภายหลังจากตรวจสอบให้รายงานผลการตรวจสอบ ให้หน่วยที่ได้รับการตรวจสอบและผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

- ๙.๓.๒ กรณีผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) ให้ดำเนินการดังนี้

- ให้หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ พิจารณาจัดทำแผนงานการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศจากผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอกหน่วย

- ภายหลังจากตรวจสอบให้รายงานผลการตรวจสอบให้หน่วยที่ได้รับการตรวจสอบและผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป



๑๐. การกำหนดความรับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ

ตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กำหนดให้ ผบ.ทร. ในฐานะผู้บริหารสูงสุดของกองทัพเรือ (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบความเสี่ยงความเสียหาย และอันตรายที่เกิดขึ้นกับระบบสารสนเทศ อันเนื่องมาจากความบกพร่อง ละเลย ฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ จึงให้ผู้บังคับบัญชาของทุกหน่วยรับทราบ และปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนด รวมทั้งให้กำกับ ดูแล และกวดขันกำลังพลในการใช้งานระบบสารสนเทศของกองทัพเรือ ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้อย่างเคร่งครัด ทั้งนี้หากเกิดกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัตินี้ ให้ผู้บังคับบัญชาของหน่วยปฏิบัติดังนี้

๑๐.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือ และหน่วยที่เกี่ยวข้องทราบ

๑๐.๒ สั่งการสอบสวนหาตัวผู้กระทำผิด และผู้รับผิดชอบโดยเร็วที่สุด

๑๐.๓ พิจารณาแก้ไขข้อบกพร่อง และป้องกันมิให้เหตุการณ์ดังกล่าวเกิดขึ้นซ้ำ

๑๐.๔ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบต่อกระเทือนเสียหายอย่างร้ายแรง ให้อยู่ในดุลพินิจของผู้บังคับบัญชาสามารถแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติหากจำเป็นให้รายงานหน่วยเหนือได้ตามความเหมาะสม

ให้หน่วยที่มีศูนย์สารสนเทศ หรือศูนย์กรรมวิธีข้อมูลที่อยู่ในสังกัด สามารถออกระเบียบปลีกย่อยได้ โดยไม่ขัดต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกองทัพเรือนี้



สรุป

รถไฟได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรถไฟฉบับนี้ขึ้น โดยมีสาระสำคัญ ๔ ส่วน ได้แก่ คำนิยาม เพื่อจำกัดความ และสร้างความเข้าใจความหมายที่ตรงกัน ส่วนนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้หน่วยต่าง ๆ เข้าใจถึงเจตนารมณ์ของรถไฟเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และใช้เป็นแนวทางสำหรับการกำหนดแนวปฏิบัติต่อไป ดังนั้น ผู้บังคับบัญชาของหน่วยจึงต้องทำความเข้าใจในนโยบายแต่ละข้อให้ชัดเจน เพื่อใช้เป็นกรอบแนวความคิด สำหรับกำกับการ และตัดสินใจในการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่รับผิดชอบ ในส่วนกระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นการกำหนดขอบเขตความรับผิดชอบของผู้ที่เกี่ยวข้อง เพื่อให้เข้าใจถึงบทบาท หน้าที่ และการมีส่วนร่วมในการสร้างความมั่นคงปลอดภัยด้านสารสนเทศ และส่วนท้ายสุด ซึ่งได้แก่ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นรายละเอียดแนวทาง วิธีปฏิบัติ วิธีการควบคุม และการใช้งานระบบสารสนเทศ เพื่อให้การใช้งานระบบสารสนเทศมีความมั่นคงปลอดภัย เชื่อถือได้ จึงเป็นหน้าที่ของผู้เกี่ยวข้องต่าง ๆ ทั้งผู้บังคับบัญชาของหน่วย ผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้ดูแลฐานข้อมูล และผู้ใช้งาน จะต้องปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัดเพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ของรถไฟมีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนด