กรรมวิธีข้อมูล (ต้นเรื่อง)

บันทึกข้อความ

ส่วนราชการ ฐท.สส. (แผนกกรรมวิธีข้อมูล บก.ฐท.สส. โทร.๗๑๐๒๕)

ที่ ๒๕/๒๕๕๗ **วันที่** ๑๗ ก.พ.๕๗

เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ฐท.สส.

เสนอ กองและแผนกต่าง ๆ ใน บก.ฐท.สส. นขต.ฐท.สส. หน่วยสมทบ สวัสดิการ ฐท.สส. และ สวัสดิการสัตหีบ

ด้วย แผนกกรรมวิธีข้อมูล บก.ฐท.สส. ได้จัดทำนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ฐท.สส. ซึ่งสามารถดาวน์โหลดได้ที่ www.navy.mi.th/sattahipbase/ และเพื่อให้การใช้งานระบบสารสนเทศเป็นไปด้วยความเรียบร้อย จึงขอความกรุณาแจ้งกำลังพลในสังกัดทราบและถือเป็นแนวทางในการปฏิบัติโดยเคร่งครัด

รับคำสั่ง ผบ.ฐท.สส.

พล.ร.ต.

เสธ.ฐท.สส.

- ทราบ
[illegible]
[illegible]

บันทึกข้อความ

ส่วนราชการ แผนกกรรมวิธีข้อมูล บก.ฐท.สส. (โทร.๗๑๐๒๕)

ที่ ๑๑ /๒๕๕๗ **วันที่** ๒๑ ม.ค.๕๗

เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ฐท.สส.

เสนอ

ด้วย แผนกกรรมวิธีข้อมูล บก.ฐท.สส. ได้จัดทำนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ฐท.สส. โดยมุ่งเน้นในรายละเอียดและข้อปฏิบัติต่าง ๆ เพื่อให้กำลังพลที่ใช้งานระบบสารสนเทศรับทราบ และใช้เป็นแนวทางในการปฏิบัติต่อไป

จึงเสนอมาเพื่อโปรดพิจารณาอนุมัติ

น.ท.หญิง พักตร์พิสุทธิ์ แตงดี
หน.กรรมวิธีข้อมูล บก.ฐท.สส.

เสนอ

พิจารณาแล้ว เห็นสมควรอนุมัติตามที่ แผนก-กรรมวิธีข้อมูล ฯ เสนอ

น.อ.
ผู้ช่วยผู้บริหารเทคโนโลยีสารสนเทศฯ และ
ผอ.กพ.ฐท.สส.
๒๖ ม.ค.๕๗

-อนุมัติ
พล.ร.ท.
ผบ.ฐท.สส.
๒๗ ม.ค.๕๗

พล.ร.ต.
เสธ.ฐท.สส.
๒๖ ม.ค.๕๗

พล.ร.ต.
รอง ผบ.ฐท.สส.
๒๖ ม.ค.๕๗

นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของฐานทัพเรือสัตหีบ

คำนำ

ปัจจุบันระบบสารสนเทศเป็นสิ่งสำคัญที่เข้ามาอำนวยความสะดวก และสนับสนุนการปฏิบัติงานของฐานทัพเรือสัตหีบ ส่งผลทำให้การเข้าถึงข้อมูลข่าวสารมีความรวดเร็วการติดต่อสื่อสารมีประสิทธิภาพสูงขึ้น และยังช่วยลดค่าใช้จ่ายในการดำเนินงานของหน่วยที่มีการเชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์เป็นของหน่วยสำหรับเป็นช่องทางสำหรับการประชาสัมพันธ์ข่าวสารต่าง ๆ เป็นต้น อย่างไรก็ตามแม้ว่าระบบเครือข่ายดังกล่าวจะมีประโยชน์ และอำนวยความสะดวกในการปฏิบัติงาน แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตราย หรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบสารสนเทศเปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอก ทำให้มีโอกาสบุกรุกได้มากขึ้น อาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลากหลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการโจมตีทางระบบเครือข่าย เพื่อก่อกวนให้ระบบไม่สามารถใช้การได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายเป็นอย่างมาก และยังทำให้สูญเสียชื่อเสียงและภาพลักษณ์ของฐานทัพเรือสัตหีบ ดังนั้นผู้ใช้งานและผู้ดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของฐานทัพเรือสัตหีบ รวมถึงหน่วยขึ้นตรง และหน่วยสมทบ ของฐานทัพเรือสัตหีบจำเป็นต้องตระหนักรู้ และให้ความสำคัญในการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบสารสนเทศของฐานทัพเรือสัตหีบ สามารถดำเนินกิจกรรมหรือการให้บริการต่างๆได้อย่างต่อเนื่อง มีความมั่นคง ปลอดภัยและเชื่อถือได้

ฐานทัพเรือสัตหีบ ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ขึ้น เพื่อให้ผู้ใช้งานและผู้ดูแลระบบสารสนเทศ ตลอดจนผู้บังคับบัญชาทุกระดับชั้นของฐานทัพเรือสัตหีบ หน่วยขึ้นตรง และหน่วยสมทบ ทราบ และยึดถือปฏิบัติตามนโยบายและแนวทางปฏิบัติที่กำหนดอย่างเคร่งครัด เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ของฐานทัพเรือสัตหีบมีความมั่นคงปลอดภัยเชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่กำหนด

สารบัญ

นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของฐานทัพเรือสัตหีบ

๑.หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐ ต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัยและเชื่อถือได้ โดยในส่วนของฐานทัพเรือสัตหีบมีระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔ ซึ่งเป็นแนวทางและมาตราการในการป้องกันระบบสารสนเทศของฐานทัพเรือในระดับหนึ่งแล้ว แต่เพื่อสร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของฐานทัพเรือสัตหีบเพิ่มขึ้นตามแนวทางที่พระราชกฤษฎีกากำหนด ฐานทัพเรือสัตหีบได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฐานทัพเรือสัตหีบขึ้น โดยมุ่งเน้นในรายละเอียดและข้อปฏิบัติต่างๆ เพื่อให้กำลังพลที่ใช้งานระบบสารสนเทศ รวมทั้งหน่วยขึ้นตรงและหน่วยสมทบของฐานทัพเรือสัตหีบที่มีระบบสารสนเทศในความรับผิดชอบรับทราบ และใช้เป็นแนวทางในการปฏิบัติต่อไป

๒.วัตถุประสงค์

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายของฐานทัพเรือสัตหีบ

๒.๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้กำลังพล และบุคคลที่ปฏิบัติงานด้านสารสนเทศให้กับหน่วย รวมทั้งการยืนยันตัวบุคคลการเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศของฐานทัพเรือสัตหีบ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้ตามปกติต่อเนื่องเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๒.๔ เพื่อให้ฐานทัพเรือสัตหีบมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องตามแนวทางของกฎหมายและระเบียบที่เกี่ยวข้อง

๒.๕ เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๖ เพื่อให้มีการตรวจสอบ และประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

๒.๗ เพื่อสร้างความตระหนัก และส่งเสริมให้เกิดความรู้ความเข้าใจ และให้การอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่กำลังพลของฐานทัพเรือสัตหีบ

๒.๘ เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบสารสนเทศของฐานทัพเรือสัตหีบ ยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไปสู่สากล

๓.องค์ประกอบ

สาระสำคัญของนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของฐานทัพเรือสัตหีบ ประกอบ ๓ ส่วน ได้แก่

๓.๑ คำนิยาม

๓.๒ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) ระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๓ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑) ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ

(๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน

(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๕) การควบคุมการเข้าถึงเครือข่าย

(๖) การควบคุมการเข้าถึงระบบปฏิบัติการ

(๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(๘) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ

(๙) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑๐) การกำหนดความรับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ

คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ประกอบด้วย

๑.**"ระบบสารสนเทศ"** หมายความว่า ระบบจัดการข้อมูลที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสาร มาช่วยในการสร้างสารสนเทศ เพื่อนำมาใช้ในการวางแผน การบริหาร การพัฒนาและควบคุม ซึ่งประกอดด้วย

๑.๑ **"ระบบคอมพิวเตอร์"** หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑.๒ **"ระบบเครือข่าย"** หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้ เช่น ระบบ Intranet , ระบบ Internet เป็นต้น

๑.๒.๑ ระบบ Intranet หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑.๒.๒ ระบบ Internet หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั้งโลก

๑.๓ **"สารสนเทศ"** หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๒. **"คอมพิวเตอร์"** หมายความว่า เครื่องมือ หรืออุปกรณ์อิเล็กทรอนิกส์ ที่มีความสามารถในการรับข้อมูลเข้าประมวลผลตามโปรแกรมและแสดง บันทึก ส่งออกข้อมูล ซึ่งเป็นผลที่ได้จากการประมวลผลนั้น โดยอาจมีลักษณะเป็นคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา ตลอดจนคอมพิวเตอร์อื่นๆ

๓. **"พื้นที่ใช้งานระบบสารสนเทศ"** หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่ายหรือระบบสารสนเทศอื่นๆ หรือพื้นที่เตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคคลากรทางคอมพิวเตอร์ รวมทั้งพื้นที่โต๊ะทำงานที่มีคอมพิวเตอร์ส่วนบุคคลติดตั้งประจำโต๊ะทำงาน

๔. **"ผู้บังคับบัญชา"** หมายความว่า ผู้ที่มีอำนาจและหน้าที่ในการปกครองบังคับบัญชาหน่วย

๕. **"ผู้ใช้งาน"** หมายความว่า ข้าราชการ พนักงานราชการ และลูกจ้างของฐานทัพเรือสัตหีบ รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของฐานทัพเรือสัตหีบที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศ

๖. **"ผู้ดูแลระบบ"** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลระบบงานสารสนเทศของหน่วย

๗. **"ผู้ดูแลเครือข่าย"** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบให้เป็นผู้ดูแลเครือข่ายสารสนเทศของหน่วย

๘.**"ผู้ดูแลฐานข้อมูล"** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบให้เป็นผู้ดูแลฐานข้อมูล

๙. **"สิทธิของผู้ใช้งาน"** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ หรือเพื่อการเข้าถึงเข้าใช้สารสนเทศและสินทรัพย์สารสนเทศ

๑๐. **"สินทรัพย์"** หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโลโลยีสารสนเทศและการสื่อสาร เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ และหมายรวมถึงสิ่งใดก็ตามที่มีคุณค่าในระบบสารสนเทศ

๑๑. **"การเข้าถึงการใช้งานสารสนเทศ"** หมายความว่า ความสามารถในการเข้าไป อันอาจทำให้สามารถจะอ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใดๆ หรือได้อ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใดๆ สำหรับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ สารสนเทศ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์ และวิธีการทางกายภาพ

๑๒. **"การควบคุมการใช้งานสารสนเทศ"** หมายความว่า การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๑๓. **"จดหมายอิเล็กทรอนิกส์"** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียงที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้

๑๔. **"บัญชีผู้ใช้บริการ"** หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์หรือใช้บริการในระบบเครือข่ายของหน่วย

๑๕. **"รหัสผ่าน"** หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่งคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๖. **"การพิสูจน์ยืนยันตัวตน"** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password)

๑๗. **"โปรแกรมประสงค์ร้าย"** หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่ง และหรือข้อมูลอิเล็กทรอนิกส์ ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยตรง หรือโดยอ้อมแก่ระบบคอมพิวเตอร์ หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือ สปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (torjan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

๑๘. **"สื่อบันทึกพกพา"** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูลที่สามารถพกพาได้ ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External HardDisk หรือ Floppy Disk เป็นต้น

๑๙. **“ไฟร์วอลล์”** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๒๐. **“ความมั่นคงปลอดภัยด้านสารสนเทศ”** หมายความว่า การรักษาไว้ซึ่งความปลอดภัยในบริบทของการรักษาความลับความเชื่อถือได้และความพร้อมใช้งานของข้อมูลสำหรับระบบสารสนเทศ

๒๑. **“เหตุการณ์ด้านความมั่นคงปลอดภัย”** หมายความว่า เหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศของหน่วยหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน ซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศโดยผลที่เกิดขึ้นอาจทำให้เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ การละเมิดต่อกฎหมาย ระเบียบข้อบังคับหรือข้อกำหนดต่างๆ การทำให้ภาพลักษณ์และชื่อเสียงเสื่อมเสีย ซึ่งตัวอย่างเหตุการณ์ด้านความมั่นคงปลอดภัย เช่น โปรแกรมประสงค์ร้ายการพบจุดอ่อนในซอฟต์แวร์ระบบงานหรือฮาร์ดแวร์ที่ใช้งานการแจ้งเตือนของระบบป้องกันการบุกรุก ระบบถูกบุกรุกทางเครือข่ายข้อมูล สำคัญถูกเปลี่ยนแปลงหรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต การใช้เครือข่ายของหน่วยเพื่อกระทำการที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ระบบสารสนเทศถูกโจมตีจนไม่สามารถให้บริการได้ ทรัพย์สินในระบบสารสนเทศถูกขโมย การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของกองทัพเรือ หรือการหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย

๒๒. **“สถานกรณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด”** หมายความว่า เหตุบกพร่อง หรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบสารสนเทศสูญเสียการปฏิบัติงานรวมถึงการให้บริการต่างๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูกบุกรุกหรือโจมตีทางช่องโหว่ และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่างๆ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของฐานทัพเรือสัตหีบ

๑. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๑ การเข้าถึงระบบสารสนเทศ

๑.๑.๑ การเข้าถึงระบบสารสนเทศจะต้องปฏิบัติตามระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๔ และหรือที่มีการเปลี่ยนแปลง แก้ไขเพิ่มเติมภายหลัง โดยให้ความสำคัญในเรื่องการรักษาความปลอดภัยเกี่ยวกับตัวบุคคล อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศอย่างเคร่งครัด

๑.๑.๒ การเข้าถึงระบบสารสนเทศจะต้องได้รับอนุญาตจากผู้ที่มีอำนาจรับผิดชอบระบบสารสนเทศ โดยคำนึงถึงความจำเป็นตามหน้าที่ภาระงาน

๑.๑.๓ ต้องสร้างความรู้ความเข้าใจให้แก่กำลังพลที่เกี่ยวข้องกับระบบสารสนเทศ ให้มีความตระหนักรู้ถึงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งต้องกำหนดบทลงโทษหากมีการฝ่าฝืนไม่ปฏิบัติตามที่กำหนด

๑.๑.๔ ต้องตรวจสอบ และทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ เพื่อให้สอดคล้องตามความจำเป็นในการใช้งานจริงตามภารกิจที่รับผิดชอบ

๑.๑.๕ ระบบสารสนเทศที่มีชั้นความลับ จะต้องมีปฏิบัติตามระเบียบสำนักนายกว่าด้วยการรักษาความปลอดภัยแห่งชาติ หรือระเบียบว่าด้วยการรักษาความลับของทางราชการหรือระเบียบอื่นใดที่กำหนดเป็นอย่างอื่นๆ

๑.๒ การเข้าถึงระบบเครือข่าย

๑.๒.๑ ต้องจัดการการเข้าถึงระบบเครือข่าย เพื่อให้ผู้ใช้งานสามารถเข้าใช้งานได้อย่างทั่วถึง สอดคล้องและเหมาะสม กับความต้องการใช้งานตามภารกิจ รวมทั้งเป็นไปตามสิทธิที่ได้รับ

๑.๒.๒ ผู้ดูแลเครือข่ายต้องบันทึกข้อมูลการเข้าใช้งานระบบเครือข่าย ช่วงเวลาเชื่อมต่อเครือข่ายหรืออุปกรณ์ที่เชื่อมต่อเข้าใช้งานเครือข่าย เพื่อใช้ในการตรวจสอบยืนยันตัวผู้ใช้ และการตรวจสอบภายหลัง

๑.๒.๓ ดำเนินการป้องกันการบุกรุก หรือการเชื่อมต่อทางเครือข่ายโดยไม่ได้รับอนุญาต รวมทั้งควบคุมการเข้าถึงพอร์ตสำหรับการตรวจสอบเครือข่าย และการปรับแต่งค่าของระบบต่างๆ

๑.๓ การเข้าถึงระบบปฏิบัติการ

๑.๓.๑ การเข้าถึงระบบปฏิบัติการจะต้องได้รับอนุญาตจากผู้มีอำนาจ

๑.๓.๒ ต้องควบคุมการเข้าถึง และใช้งานระบบปฏิบัติการให้เป็นไปตามสิทธิและความจำเป็น รวมทั้งต้องบันทึกเข้าถึง และใช้งานระบบปฏิบัติการ หรือแอพพิเคชั่นต่างๆ

๑.๔ การเข้าถึงระบบโปรแกรมประยุกต์ หรือแอพพิเคชั่นต่างๆ

การใช้งานระบบสารสนเทศ จากโปรแกรมประยุกต์ หรือแอพพิเคชั่นต่างๆ ที่ผ่านอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่จากภายนอก ต้องได้รับการอนุญาตจากผู้ที่มีอำนาจ และต้องมีการควบคุม เพื่อมิให้เกิดผลกระทบความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ความพร้อมของระบบสารสนเทศ

๒.๑ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องจัดให้มีระบบสำรองของสารสนเทศ เพื่อให้ระบบสารสนเทศพร้อมใช้งานอยู่เสมอ

๒.๒ ต้องสำรองข้อมูลที่มีความสำคัญสำหรับการปฏิบัติงาน

๒.๓ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน (Contingency Plan) ในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ รวมทั้งให้มีการทดสอบ และทบทวนแผนดังกล่าว

๓. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๑ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างสม่ำเสมอ

๓.๒ การตรวจสอบและประเมินความเสี่ยง ต้องดำเนินการโดยผู้ตรวจสอบภายในของกองทัพเรือ หรือผู้ตรวจสอบอิสระจากภายนอกกองทัพเรือ

การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องให้ความสำคัญและปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด โดยผู้บังคับบัญชาทุกลำดับชั้นต้องควบคุมกำกับดูแลการใช้งานระบบสารสนเทศ

๒. ความรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ ผู้ใช้งานต้องรับผิดชอบดังนี้

๒.๑.๑ ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ฐานทัพเรือสัตหีบนี้อย่างเคร่งครัด และต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๒.๑.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของฐานทัพเรือสัตหีบ

๒.๑.๓ ไม่รบกวน หรือแทรกแซงการสื่อสารในเครือข่ายสารสนเทศของฐานทัพเรือสัตหีบ

๒.๑.๔ รายงานเหตุการณ์ความเสี่ยงจุดอ่อนหรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังผู้บังคับบัญชา และผู้ดูแลระบบโดยเร็วที่สุด

๒.๒ ผู้บังคับบัญชาต้องรับผิดชอบในกรณีที่ระบบสารสนเทศหรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ อันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนไม่ปฏิบัติตามตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บังคับบัญชาสูงสุดของหน่วยเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้นโดยมีแนวทางปฏิบัติดังนี้

๒.๒.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือ และหน่วยที่เกี่ยวข้องทราบ

๒.๒.๒ สั่งการสอบสวนหาตัวผู้กระทำผิด และผู้รับผิดชอบโดยเร็วที่สุด

๒.๒.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๒.๒.๔ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของผู้บังคับบัญชาสามารถแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติหากจำเป็นให้รายงานหน่วยเหนือได้ตามความเหมาะสม

๒.๓ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ดำเนินการดังนี้

๒.๓.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสาร กรรมวิธีข้อมูลต่างๆ ประมวลลับ หรือรหัสผ่านที่จำเป็น ในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศได้รับผลกระทบกระเทือนหรือเกิดเสียหายหรือไม่อย่างไร

๒.๓.๒ ขจัดความเสียหายที่เกิดขึ้น หรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันที โดยอาจต้องการแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆที่เกี่ยวข้องตามที่เห็นสมควร

๓. แผนกกรรมวิธีข้อมูล กองบัญชาการฐานทัพเรือสัตหีบ ในฐานะผู้รับผิดชอบรักษาความปลอดภัยระบบสารสนเทศของฐานทัพเรือสัตหีบ ตามระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยด้านสารสนเทศเป็นผู้รับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศในภาพรวมของฐานทัพเรือสัตหีบ ทั้งนี้ ให้ดำเนินการทบทวน

นโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีความทันสมัยอย่างต่อเนื่อง และสามารถนำไปสู่การปฏิบัติได้จริงอย่างเป็นรูปธรรม โดยมีวงรอบการทบทวนปีงบประมาณละ ๑ ครั้ง

๔. หน่วยขึ้นตรงฐานทัพเรือสัตหีบและหน่วยสมทบ ให้รับผิดชอบรักษาความปลอดภัยระบบสารสนเทศของหน่วย ตามนโนบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของฐานทัพเรือสัตหีบอย่างเคร่งครัด

๒.๒ ผู้ดูแลระบบ ต้องทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยปฏิบัติตามแนวทางดังนี้

๒.๒.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบงานสารสนเทศแยกตามหน่วยงานภายในของฐานทัพเรือสัตหีบ

๒.๒.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยต่างๆ เพื่อดำเนินการทบทวนว่ามีรายชื่อที่หมดสิทธิการเข้าถึงระบบสารสนเทศไปแล้วหรือไม่ หรือมีการเปลี่ยนแปลงสิทธิแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๒.๒.๓ ผู้บังคับบัญชาของหน่วยแจ้งหรืออนุมัติรายชื่อของผู้มีสิทธิในระบบงานสารสนเทศที่ได้รับการแก้ไขให้ถูกต้องหรือไม่

๒.๒.๔ ผู้ดูแลระบบดำเนินการแก้ไขข้อมูลผู้มีสิทธิให้ถูกต้อง ตามที่ได้รับแจ้งหรือได้รับการอนุมัติ

๒.๓ ผู้ดูแลระบบต้องพิจารณาการเชื่อมโยงถึงกันของระบบงานสารสนเทศตามภารกิจของหน่วยต่างๆ โดยพิจารณาประเด็นทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในแต่ละระบบงานหรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างหน่วยภายในกองทัพเรือหรือหน่วยงานอื่นๆ ที่จะมาขอเชื่อมโยงกับกองทัพเรือเป็นต้นดังนี้

๒.๓.๑ กำหนดนโยบายและมาตรการเพื่อควบคุมป้องกันและบริหารจัดการการใช้ข้อมูลร่วมกัน

๒.๓.๒ พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๒.๓.๓ พิจารณาว่ามีกำลังพลใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

๒.๓.๔ พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

๒.๓.๕ ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญ หรือข้อมูลที่กำหนดชั้นความลับร่วมกัน ในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

๒.๔ ผู้ดูแลระบบต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging) ของระบบงานภายในฐานทัพเรือสัตหีบ โดยบันทึกเป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้งานเพื่อตรวจสอบว่า ใครเข้ามาใช้งานระบบ การตรวจสอบการบุกรุก รวมไปถึงการตรวจสอบข้อผิดพลาดที่เกิดขึ้น โดยจัดทำ รายงานเบื้องต้นสรุปข้อมูลว่า ใคร (Who) ทำอะไร (What) เมื่อไหร่ (When) ที่ไหน (Where) และอย่างไร (How) โดยข้อมูลที่ควรจัดเก็บมีดังนี้

๒.๔.๑ ข้อมูลชื่อบัญชีผู้ใช้ระบบงาน

๒.๔.๒ ข้อมูลวันเวลาที่เข้าถึงระบบงาน

๒.๔.๓ ข้อมูลวันเวลาที่ออกจากระบบงาน

๒.๔.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๒.๔.๕ ข้อมูลชื่อเครื่องคอมพิวเตอร์ที่ใช้งาน

๒.๔.๖ ข้อมูลการเข้าถึงระบบ (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

๒.๔.๗ ข้อมูลความพยายามในการเข้าถึงทรัพยากร เช่น ข้อมูลบัญชีผู้ใช้ฐานข้อมูลสำคัญของ ระบบงาน เป็นต้น ทั้งที่สำเร็จ และไม่สำเร็จ

๒.๔.๘ ข้อมูลการเปลี่ยนแปลงสิ่งแวดล้อมหรือการกำหนดค่า (Configuration) ของระบบงาน

๒.๔.๙ ข้อมูลแสดงการใช้สิทธิเช่นสิทธิของผู้ดูแลระบบเป็นต้น

๒.๗.๙ ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ อย่างเคร่งครัด

๒.๘ มาตรการป้องกันและรักษาความปลอดภัยจากการเชื่อมต่ออินเทอร์เน็ตความเร็วสูง

๒.๘.๑ การขอเปิดใช้บริการเชื่อมต่ออินเตอร์เน็ตความเร็วสูงผ่านโทรศัพท์เลขหมายเอกชนจะต้องเสนอขออนุมัติแผนกกรวิธีข้อมูล กองบัญชาการฐานทัพเรือสัตหีบ เพื่อพิจารณาความเหมาะสมและความจำเป็น

๒.๘.๒ การเชื่อมต่ออินเตอร์เน็ตความเร็วสูงจะต้องไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ของทางราชการที่เชื่อมต่อกับเครือข่ายภายในกองทัพเรือ (Intranet) หรือเครื่องคอมพิวเตอร์ส่วนตัวที่มีข้อมูลข่าวสารของกองทัพเรือที่เป็นชั้นความลับ และ/หรือข้อมูลที่อาจส่งผลกระทบด้านความมั่นคงของประเทศโดยเด็ดขาด

๒.๙ แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๒.๙.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกองทัพเรือให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การเปลี่ยนตำแหน่งเปลี่ยนต้นสังกัดการลาออกจากราชการการเกษียณอายุ

๒.๙.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานใหม่ และรหัสผ่านสำหรับการใช้งาน ครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกองทัพเรือ

๒.๙.๓ ผู้ใช้งานจะต้องกำหนดรหัสผ่านที่ดี (Good Password) โดยมีแนวทางปฏิบัติตามที่ระบุในข้อ ๔.๑.๒

๒.๙.๔ รหัสผ่านของจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านแต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น " * " หรือ " ● " ในการพิมพ์แต่ละตัวอักษร

๒.๙.๕ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของกองทัพเรือหรือจดหมายอิเล็กทรอนิกส์ของภาครัฐเพื่อใช้ในการติดต่องานราชการ

๒.๙.๖ ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๙.๗ ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เช่น ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

๒.๙.๘ ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกองทัพเรือ หรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกองทัพเรือ

๒.๙.๙ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นผู้ใช้งานควรทำการออกจากระบบ (Logout) ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒.๙.๑๐ ผู้ใช้งานควรทำการตรวจสอบเอกสารที่แนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบแฟ้มข้อมูล โดยใช้โปรแกรมป้องกันไวรัส เพื่อป้องกันการเปิดแฟ้มข้อมูลที่เป็น Executable File เช่น .exe, .com เป็นต้น

๒.๙.๑๑ ผู้ใช้งานต้องไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๑๐ แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

- ให้ตรวจสอบ หรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๔.๓.๕ การควบคุมการเดินสายไฟสายสื่อสารและสายเคเบิ้ลอื่นๆ (Cabling Security)

- เครือข่ายที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณ และป้องกันสัตว์ต่างๆกัดสาย

- การเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน

- จัดทำแผนผังสายสัญญาณสื่อสารต่างๆให้ครบถ้วนและถูกต้อง

๔.๓.๖ การควบคุมการนำสินทรัพย์ออกนอกหน่วยงาน (Removal of Property)

- ให้กำหนดมาตรการรักษาความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ของหน่วยออกไปใช้งานนอก

- บันทึกข้อมูลการนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วยไว้เป็นหลักฐาน เพื่อป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อมีการนำส่งคืนเรียบร้อยเพื่อการตรวจสอบย้อนหลัง

๔.๔ ให้นำวิธีการเข้ารหัสมาใช้กับข้อมูลชั้นความลับ โดยปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางทางราชการพ.ศ.๒๕๔๔

๕. การควบคุมการเข้าถึงเครือข่าย (Network access control)

การควบคุมการเข้าถึงเครือข่าย (Network access control) มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยหน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องดำเนินการดังนี้

๕.๑ การใช้งานบริการเครือข่ายต้องกำหนดมาตรการทางเครือข่ายสื่อสารข้อมูล เพื่อป้องกันข้อมูลในเครือข่ายระบบงานหรือบริการต่าง ๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต

๕.๑.๑ ผู้ใช้งานจะสามารถเข้าถึงเครือข่ายได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ทั้งนี้ให้พิจารณาตามความจำเป็นตามภาระงาน

๕.๑.๒ กำหนดมาตรการป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๕.๑.๓ บันทึกข้อมูลพฤติกรรมการใช้งาน และเก็บข้อมูลของอุปกรณ์เครือข่าย เพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๕.๑.๔ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆเพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๕.๑.๕ ใช้ฮาร์ดแวร์หรือซอฟต์แวร์สำหรับการบริหารจัดการเครือข่ายเพื่อระบุเฝ้าตรวจและติดตามสถานะอุปกรณ์ในระบบสารสนเทศของฐานทัพเรือสัตหีบ

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User authentication for external connections)

๕.๒.๑ จัดทำบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของผู้ใช้งานที่อยู่ภายนอกหน่วย

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

๕.๒.๓ ผู้ดูแลระบบจะต้องจัดการพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอกเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของฐานทัพเรือสัตหีบโดยมีแนวทางปฏิบัติ ดังนี้

- การแสดงตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงตัวตนด้วยชื่อของผู้ใช้ (Username)
- การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่า เป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือ การใช้สมาร์ทการ์ด หรือ การใช้ USB token ที่มีความสามารถ PKI เป็นต้น
- การเข้าสู่ระบบสารสนเทศของฐานทัพเรือสัตหีบจากอินเทอร์เน็ต จะมีการตรวจสอบผู้ใช้งานด้วย
- การเข้าสู่ระบบจากระยะไกล (Remote access) จะต้องมีการตรวจสอบเพื่อพิสูจนตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือ วิธีการเข้ารหัส เพื่อเพิ่มความปลอดภัย
- การเข้าสู่ระบบสารสนเทศของหน่วยนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี

๕.๓ การแบ่งแยกเครือข่าย และการควบคุมการเชื่อมต่อทางเครือข่าย

๕.๓.๑ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ ต้องแยกและติดตั้งเครื่องคอมพิวเตอร์ที่ให้บริการในวงเครือข่าย ออกจากวงเครือข่ายของผู้ใช้งาน และใช้ Firewall หรืออุปกรณ์เครือข่ายอื่นๆเพื่อจำกัดให้เฉพาะกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้น จึงจะสามารถเชื่อมต่อเข้าไปยังเครื่องคอมพิวเตอร์ให้บริการนั้นได้ สำหรับแนวทางปฏิบัติการใช้งานของไฟร์วอลล์ (Firewall) มีดังนี้

- ผู้ดูแลเครือข่าย มีหน้าที่ในการบริหารจัดการการติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด
- การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
- เส้นทางเชื่อมต่ออินเทอร์เน็ต และบริการอินเทอร์เน็ตที่ไม่ได้รับอนุญาตจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์
- ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง
- ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
- การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
- ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน
- การกำหนดระเบียบในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปเฉพาะที่ได้ อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากฐานทัพเรือสัตหีบก่อน

- การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

- จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

- เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

- ผู้ดูแลเครือข่าย มีสิทธิ์ที่จะระงับ หรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

- การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

๕.๓.๒ ผู้ใช้งานที่ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์จะถูกระงับการใช้งานอินเทอร์เน็ตหรือเชื่อมต่อเครือข่ายภายในโดยทันที

๕.๓.๓ การเข้าสู่ระบบเครือข่ายภายในของฐานทัพเรือสัตหีบ โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๕.๓.๔ ผู้ดูแลเครือข่ายต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๓.๕ ผู้ดูแลเครือข่ายต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕.๓.๖ ผู้ดูแลเครือข่าย ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ เช่น การเชื่อมต่อเข้าสู่เครื่องคอมพิวเตอร์ ให้บริการเพื่อบริหารจัดการระบบ ให้กำหนดเฉพาะชุดไอพีแอดเดรสของผู้ดูแลเครือข่ายเท่านั้นที่สามารถเข้าถึงเครื่องคอมพิวเตอร์ให้บริการนั้นได้

๕.๓.๗ ผู้ดูแลเครือข่าย ตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๕.๓.๘ กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๓.๙ ระบบเครือข่ายทั้งหมดของหน่วยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วย ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ เป็นต้น

๕.๓.๑๐ ให้ติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่าน

ระบบเครือข่ายการใช้งาน ในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง และสำหรับแนวทางปฏิบัติการใช้งานของอุปกรณ์ป้องกันการบุกรุก (IDS/IPS) ดังนี้

- ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของฐานทัพเรือสัตหีบและเครือข่ายข้อมูลทั้งหมดรวมถึงเส้นทางที่ข้อมูลอาจเดินทางทั้งที่เชื่อมต่อสู่เครือข่ายภายนอกและเครือข่ายภายในทุกเส้นทาง

- ระบบทั้งหมดที่สามารถเข้าถึงได้จากเครือข่ายภายนอกหรือเครือข่ายสาธารณะต่าง ๆ จะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

- ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

- โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

- ตรวจสอบ และ Update Patch/Signature ของ IDS/IPS เป็นประจำ

- ตรวจสอบเหตุการณ์ข้อมูลจราจรพฤติกรรมการใช้งานกิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวัน

- IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

- เครื่องคอมพิวเตอร์ที่ให้บริการที่มีการติดตั้ง Host - based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

- พฤติกรรมการใช้งานกิจกรรมหรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุกการโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

- พฤติกรรมกิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบภายใน๑ชั่วโมงที่ตรวจพบ

- การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

- มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผนเผชิญเหตุที่เกิดขึ้น

๕.๓.๑๑ ผู้ดูแลเครือข่าย มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบโดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๕.๓.๑๒ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิด การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันทีหากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและสินทรัพย์ของฐานทัพเรือสัตหีบ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมายต่อไป

๕.๓.๑๓ การเข้าสู่ระบบงานเครือข่ายภายในหน่วยผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๕.๔ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control)

๕.๔.๑ ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ (IP Address) ของระบบงานเครือข่ายภายในต้องมีการป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศของหน่วยได้โดยง่าย

๕.๔.๒ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอก และอุปกรณ์ต่างๆ และต้องปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๔.๓ การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชา หรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๔.๔ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ และต้องจัดทำเป็นบัญชีไว้สำหรับระบุอุปกรณ์บนเครือข่ายได้

๕.๔.๕ ให้บันทึกการทำงานของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการตรวจสอบย้อนหลัง และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อยกว่า ๓ เดือน

๕.๔.๖ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำาเสมอ

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยจะต้องปฏิบัติดังนี้

๖.๑ การควบคุมการติดตั้งระบบปฏิบัติการในเครื่องคอมพิวเตอร์(Control of operational software)

๖.๑.๑ ให้ควบคุมการเปลี่ยนแปลงระบบปฏิบัติการที่อาจมีผลต่อระบบงานของหน่วย เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

๖.๑.๒ การเปลี่ยนแปลงระบบปฏิบัติการ จะต้องดำเนินการโดยผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น

๖.๑.๓ กำหนดให้มีการจัดเก็บซอร์สโค้ด และไลบรารี่สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๖.๑.๔ ผู้ดูแลระบบต้องทดสอบระบบปฏิบัติการตามจุดประสงค์ที่กำหนด อย่างครบถ้วนเพียงพอก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงานเป็นต้น

๖.๑.๕ ผู้ดูแลระบบต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบปฏิบัติการอย่างครบถ้วนก่อนดำเนินการติดตั้ง

๖.๑.๖ ทำการปรับปรุงไลบรารี่สำหรับซอฟต์แวร์ของระบบปฏิบัติการให้มีความทันสมัย

๖.๑.๗ ในกรณีที่เป็นการติดตั้งระบบปฏิบัติการ เพื่อทดแทนระบบปฏิบัติการเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูลซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่น ๆ ที่เกี่ยวข้องกับระบบปฏิบัติการนั้น

๖.๑.๘ กรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบปฏิบัติการเดิม เพื่อไปสู่ข้อมูลในระบบปฏิบัติการใหม่ ให้จัดทำแผนการถ่ายโอนหรือแปลงข้อมูล เพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้อง และครบถ้วนหรือไม่

๖.๑.๙ ให้กำหนดแผนการติดตั้งสำหรับระบบปฏิบัติการใหม่ ซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า สำหรับซอฟต์แวร์ที่จะทำการติดตั้งให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

๖.๑.๑๐ ให้อ่านและปฏิบัติตามเงื่อนไข หรือ ข้อตกลงการใช้งานซอฟต์แวร์ที่ จะทำการติดตั้งอย่างเคร่งครัด

๖.๑.๑๑ การติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility Software) ต้องตรวจสอบก่อนว่า เป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้

๖.๑.๑๒ ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ (Patch) ที่เกี่ยวข้องกับระบบปฏิบัติการตามความจำเป็น เช่น โปรแกรมแก้ไข ช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๖.๒ กำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes) ดังนี้

๖.๒.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบ เกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๖.๒.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๖.๓ การปฏิบัติเพื่อการเข้าถึงระบบปฏิบัติการ

๖.๒.๑ ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๖.๒.๒ ต้องจำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่านเมื่อต้องเข้าถึงระบบปฏิบัติการ

๖.๒.๓ ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาหน้าจอแสดงผล (Screen Saver) โดยตั้งเวลาในกรณีไม่ได้ใช้งานในห้วงระยะเวลาขณะหนึ่ง เพื่อให้ทำการปิดกั้นการใช้งาน (Lock) สำหรับหน้าจอแสดงผล

๖.๒.๔ ระบบต้องยุติการเชื่อมต่อเมื่อพบว่ามีการพยายามคาดเดารหัสผ่าน หากทำการล็อกอินไม่สำเร็จเกินกว่า ๓ ครั้ง

๖.๒.๕ ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอแสดงผลเป็นเวลานาน

๖.๒.๖ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบปฏิบัติการได้

๖.๓ การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) การเข้าถึงระบบปฏิบัติการ จะระบุตัวตนของผู้ใช้งาน และการยืนยันตัวตนที่เหมาะสมโดยมีแนวทางปฏิบัติดังนี้

๖.๓.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๖.๓.๒ ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสารนี้

๖.๔ การบริหารจัดการรหัสผ่าน (Password management system) ในการเข้าถึงระบบปฏิบัติการต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๖.๕ ควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานสามารถหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัย

๖.๕.๑ จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุม ในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๖.๕.๒ ให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๖.๕.๓ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

๖.๕.๕ ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้เพื่อการตรวจสอบภายหลัง

๖.๖ การว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งาน (Session time-out)

๖.๖.๑ ให้มีการตัดการติดต่อ และหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๖.๖.๒ ระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานที่มีข้อมูลสำคัญ ระบบงานที่กำหนดชั้นความลับ ต้องมีการตัดการติดต่อและหมดเวลาการใช้งานที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- เมื่อผู้ใช้งานไม่ได้ใช้งานหรือว่างเว้นจากการใช้งานในระยะเวลา ๑ ชั่วโมง หรือตามที่ผู้ดูแลระบบกำหนดให้มีการตัดการเชื่อมต่อการใช้งานออกจากระบบสารสนเทศโดยอัตโนมัติ
- ถ้ามีความพยายามเข้าสู่ระบบใหม่ให้ยืนยันการใช้งานโดยใส่ชื่อผู้ใช้(Username) และรหัสผ่าน (password) หรือวิธีการที่ปลอดภัยในการยืนยันตัวบุคคลในทุกๆครั้ง

๖.๗ การจำกัดระยะเวลาการเชื่อมต่อ (Limitation of connection time)

๖.๗.๑ ให้มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ สำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถเข้าถึงภายในระยะเวลาที่กำหนดเท่านั้น

๖.๗.๒ การจำกัดช่วงระยะเวลาการเชื่อมต่อ เพื่อป้องกันบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึงข้อมูลได้โดยง่าย

- การเชื่อมต่อเข้าสู่ระบบสารสนเทศของฐานทัพเรือสัตหีบ กำหนดให้ใช้งานได้ ๔ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หรือตามที่ผู้บังคับบัญชาเห็นสมควร
- การเชื่อมต่อเข้าสู่ระบบสารสนเทศของฐานทัพเรือสัตหีบ กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น
- การเชื่อมต่อเข้าสู่ระบบสารสนเทศของฐานทัพเรือสัตหีบ ถ้ากระทำในช่วงนอกเวลาทำงานตามปกติต้องได้รับอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and information access control)

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) เพื่อที่จำกัดการเข้าถึงสารสนเทศของผู้ใช้งานเฉพาะส่วนที่มีความจำเป็นตามภารกิจ โดยหน่วยที่มีระบบสารสนเทศในความรับผิดชอบ จะต้องดำเนินการดังนี้

๗.๑.๑ ผู้ดูแลฐานข้อมูลจะต้องดำเนินการจำแนกสารสนเทศที่มีอยู่ ว่ามีสารสนเทศใดบ้าง เช่น ฐานข้อมูลด้านบุคคล ฐานข้อมูลด้านงบประมาณ ฐานข้อมูลที่เป็นความลับของหน่วย และจะต้องวิเคราะห์ความสำคัญของสารสนเทศในแต่ละกลุ่มว่า มีความสำคัญต่อปฏิบัติงานมากน้อยเพียงใด เช่น หากถูกทำลายไปอาจทำให้หน่วยเสียหาย ก็จะถือว่าสารสนเทศนั้นมีความสำคัญ และมีความอ่อนไหวสูง

๗.๑.๒ กำหนดผู้ใช้งานใดที่ควรเข้าถึงสารสนเทศใด โดยพิจารณาตามบทบาทและหน้าที่ (Roles) เช่น บางสารสนเทศอาจกำหนดให้ผู้ใช้งานทุกคนสามารถเข้าถึงได้และในบางสารสนเทศอาจกำหนดให้เพียงผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้นที่จะสามารถเข้าถึงได้

๗.๑.๓ กำหนดสิทธิ์ในการเข้าถึง (Access Permissions) ให้สอดคล้องกับผู้ใช้งาน และสารสนเทศที่ได้จำแนกไว้ โดยสิทธิที่ได้รับอาจอยู่ในรูปแบบของการประมวลผล การแก้ไข การอ่านอย่างเดียว

๗.๒ สารสนเทศที่อ่อนไหว (Sensitive) มีผลกระทบ และมีความสำคัญสูงต่อองค์กร อาจกำหนดให้สามารถใช้งานเฉพาะกลุ่มเท่านั้น และอาจกำหนดช่องทางในการเข้าถึง เช่น จัดให้มีเครื่องแม่ข่ายควบคุมแยกต่างหาก หากการติดต่อกับเครื่องแม่ข่ายต้องผ่านระบบ firewalls การจำกัดการเข้าถึงเฉพาะการใช้เครือข่ายภายในเท่านั้น หรือกำหนดมาตรการควบคุมการเข้าถึงเป็นกรณีพิเศษจากอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ หรือการใช้งานระบบจากภายนอก (Mobile computing and Teleworking)

๗.๓ ผู้ดูแลระบบต้องจัดการควบคุมการเข้าใช้งานระบบจากภายนอก (Teleworking)

๗.๓.๑ การเข้าสู่ระบบเครือข่ายจากระยะไกล (Remote access) ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของระบบสารสนเทศ จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรการการเข้าสู่ระบบภายใน

๗.๓.๒ วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และต้องควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๗.๔ มาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อป้องกันชุดคำสั่งไม่พึงประสงค์

๗.๔.๑ ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มากจากแหล่งภายนอก รวมทั้งการใช้แฟ้มข้อมูล (File) อื่นที่ไม่ได้รับอนุญาตให้ใช้งาน

๗.๔.๒ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๗.๔.๓ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ให้กับระบบเทคโนโลยีสารสนเทศ

๗.๔.๔ ให้ผู้ดูแลระบบดำเนินการตรวจสอบชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ที่ให้บริการ และอุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ในบริเวณจุดทางเข้า – ออกเครือข่ายอย่างสม่ำเสมอ เพื่อดักจับชุดคำสั่งไม่พึงประสงค์ที่จะเข้าสู่ระบบ

๗.๔.๕ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ สำหรับการจัดการชุดคำสั่งไม่พึงประสงค์ ได้แก่ การรายงานการเกิดขึ้นของชุดคำสั่งไม่พึงประสงค์ การวิเคราะห์การจัดการ การกู้คืนระบบจากความเสียหายที่ตรวจพบ เป็นต้น

๗.๔.๖ มีการติดตามข้อมูลข่าวสารเกี่ยวกับชุดคำสั่งไม่พึงประสงค์อย่างสม่ำเสมอ

๗.๔.๗ ให้มีการสร้างความตระหนักเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ เพื่อให้ผู้ใช้งานมีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติ เมื่อพบเหตุชุดคำสั่งไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร รวมทั้งให้จัดการฝึกอบรม สร้างความตระหนักอย่างน้อยปีละ ๑ ครั้ง

๘. การจัดทำระบบสารสนเทศสำรอง

หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ จะต้องดำเนินการจัดทำระบบสารสนเทศสำรอง เพื่อให้มั่นใจว่าระบบสารสนเทศ และข้อมูลสำคัญ จะยังคงมีอยู่ สามารถเข้าถึงและใช้งานได้ แม้เกิดเหตุการณ์ในกรณีฉุกเฉิน

๘.๑ การคัดเลือกและจัดทำระบบสำรองและกู้คืนระบบ

๘.๑.๑ กำหนดระบบงานที่มีความสำคัญ และจัดทำเป็นบัญชีรายชื่อของระบบงานดังกล่าว รวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

๘.๑.๒ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๘.๑.๓ กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วยข้อมูลในฐานข้อมูลของระบบข้อมูลสำหรับตัวระบบเช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้องเป็นต้น

๘.๑.๔ กำหนดความถี่ในการสำรองข้อมูลของระบบงาน เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อยควรมีความถี่ในการสำรองข้อมูลมากขึ้นเป็นต้น

๘.๑.๕ ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๘.๑.๖ ทำการตรวจสอบกู้คืนข้อมูลที่เกิดขึ้นนั้นสำเร็จครบถ้วนหรือไม่

๘.๑.๗ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

๘.๒ แนวทางปฏิบัติสำหรับการสำรองข้อมูลดังนี้

๘.๒.๑ ผู้ดูแลฐานข้อมูลต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามแนวทางการสำรองข้อมูล

๘.๒.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลฐานข้อมูลต้องทำบันทึกรายละเอียดการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๘.๒.๓ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลฐานข้อมูลต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๘.๒.๔ ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้รับผิดชอบระบบสารสนเทศของหน่วยทราบ

๘.๒.๕ ให้ผู้ดูแลฐานข้อมูล กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

๘.๒.๖ แนวทางที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลฐานข้อมูลต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

๘.๒.๗ สำหรับความถี่ในการสำรองข้อมูลมีดังนี้

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 อื่นๆ	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลที่มีความสำคัญของระบบงานที่ถูกเก็บในอุปกรณ์ต่าง ๆ เหล่านั้น	๑ ครั้งต่อเดือน

๘.๓ แนวทางปฏิบัติสำหรับการกู้คืนระบบดังนี้

๘.๓.๑ ในกรณีพบปัญหาที่อาจสร้างความเสียหารต่อระบบคอมพิวเตอร์ ระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบ หรือผู้ดูแลเครือข่ายดำเนินการแก้ไขรายการผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้รับผิดชอบระบบ สารสนเทศของหน่วยหรือผู้ที่ได้รับมอบหมายทราบ

๘.๓.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความ เหมาะสมเพื่อกู้คืนระบบ

๘.๓.๓ หากความเสียหายที่เกินขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งาน ให้ผู้ดูแลระบบแจ้งให้ผู้ใช้งานทราบพร้อมทั้งรายงานความคืบหน้าการกู้คืนเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๘.๔ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบ จะต้องดำเนินการจัดทำระบบแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินดังนี้

๘.๔.๑ จัดทำแผนเตรียมความพร้อมกรณีเหตุฉุกเฉิน (Contingency Plan) เพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้น ทั้งวิธีการทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งให้กำหนดการทดสอบแผนดังกล่าวทุกปี โดยแผนต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

- การกำหนดหน้าที่และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
- การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญและกำหนดมาตรการเพื่อลดความเสี่ยง เช่น ไฟฟ้าดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
- การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
- การกำหนดขั้นตอนปฏิบัติงานในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้
- การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ
- การสร้างความตระหนัก หรือให้ความรู้แก่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุ
- ให้ปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยมุ่งเน้นที่ระบบที่มีความสำคัญสูง

๘.๔.๒ ให้ทำการสำรองข้อมูลตามชนิดความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองมีความครบถ้วนหรือไม่

๘.๔.๓ ให้ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่

๘.๔.๔ ให้แจ้งผู้ที่เกี่ยวข้องทั้งหมดรับทราบรายละเอียดของแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน รวมทั้งเมื่อมีการปรับปรุงแผนเตรียมความพร้อม

๙. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๙.๑ ผู้ดูแลระบบเทคโนโลยีสนเทศของหน่วยต้องกำหนดการประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่ใช้งานเพื่อกำหนดแนวทางในการเฝ้าระวังและดูแลระบบเหล่านั้น และกำหนดให้มีการเฝ้าระวัง และดูแลระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆที่ต้องปฏิบัติตามอย่างสม่ำเสมอโดยการตรวจสอบดังต่อไปนี้

๙.๑.๑ ชื่อบัญชีผู้ใช้งาน
๙.๑.๒ กิจกรรมการใช้งานและประเภทของกิจกรรม
๙.๑.๓ วัน/เวลาที่เข้าถึง
๙.๑.๔ แฟ้มข้อมูลหรือข้อมูลที่ถูกเข้าถึง
๙.๑.๕ โปรแกรมทั่วไปและอรรถประโยชน์ต่างๆ (Utilities) ที่ถูกเรียกใช้งาน
๙.๑.๖ การใช้บัญชีผู้ใช้งานในระดับสูงเช่น Supervisor, Root, Administrator เป็นต้น
๙.๑.๗ การเปิด-ปิดการทำงานของระบบ
๙.๑.๘ การถอดถอนหรือติดตั้งอุปกรณ์สำหรับขาเข้าและส่งออกข้อมูล (I/O) เช่น ฮาร์ดดิสก์ เป็นต้น

๙.๑.๙ การใช้คำสั่งของผู้ใช้งานที่ได้รับการปฏิเสธโดยระบบเช่นพยายามใช้คำสั่งทั้งที่ไม่มีสิทธิการพยายามเข้าถึงระบบอย่างไม่ถูกต้องเป็นต้น

๙.๑.๑๐ ความพยายามในการเข้าถึงข้อมูลหรือทรัพยากรของระบบที่ได้รับการปฏิเสธโดยระบบ

๙.๑.๑๑ การแจ้งเตือนจากไฟร์วอลล์หรือระบบป้องกันการบุกรุก

๙.๑.๑๒ การแจ้งเตือนจากอุปกรณ์แจ้งเตือน (Console) ของผู้ดูแลระบบ

๙.๑.๑๓ การแจ้งเตือนเมื่อระบบทำงานผิดปกติเช่นฮาร์ดดิสก์เต็ม เป็นต้น

๙.๑.๑๔ การแจ้งเตือนจากโปรแกรมบริหารจัดการเครือข่าย

๙.๑.๑๕ การแจ้งเตือนการทำงานของระบบล้มเหลวหรือหยุดชะงัก

๙.๑.๑๖ ความพยายามในการเปลี่ยนแปลงค่าการติดตั้งระบบ (Configuration) ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๙.๒ หน่วยที่มีระบบสารสนเทศในความรับผิดชอบต้องจัดให้มีการประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ซึ่งประกอบด้วยทรัพย์สิน ๕ หมวด ได้แก่ บุคคลากร ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลและระบบงาน โดยปฏิบัติตามแนวทางการประเมินดังนี้

๙.๒.๑ กำหนดให้มีการจัดทำบัญชีทรัพย์สินสารสนเทศ

๙.๒.๒ ระบุและประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ

๙.๒.๓ จัดลำดับความเสี่ยงจากสูงมาต่ำ

๙.๒.๔ จัดทำแผนลดความเสี่ยงโดยคำนึงถึงการจัดการกับความเสี่ยงสูงก่อน

๙.๒.๕ กำหนดให้มีการปฏิบัติตามแผนการลดความเสี่ยงที่กำหนดไว้และติดตามจนกระทั่งแล้วเสร็จ

๑๐. การกำหนดความรับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ

ความรับผิดชอบของผู้บังคับบัญชา กรณีที่มีการละเมิดการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศฐานทัพเรือสัตหีบนี้ โดยเฉพาะกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยสารสนเทศของกองทัพเรือ พ.ศ.๒๕๕๔ ให้ผู้บังคับบัญชาสูงสุดรับผิดชอบระบบสารสนเทศของหน่วย และเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น โดยมีแนวทางปฏิบัติดังนี้

๑๐.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือทราบ

๑๐.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๑๐.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้เกิดขึ้นซ้ำอีก

๑๐.๔ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรง ให้อยู่ในดุลพินิจของผู้บังคับบัญชา สามารถแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติ หากจำเป็นให้รายงานหน่วยเหนือได้ตามความเหมาะสม

ให้หน่วยขึ้นตรงฐานทัพเรือสัตหีบ และหน่วยสมทบ สามารถออกแบบระเบียบปลีกย่อยได้ โดยไม่ขัดต่อนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของฐานทัพเรือสัตหีบนี้