



บันทึกข้อความ

ส่วนราชการ กบ.ท.สบส.กบ.ทหาร (ธุรการ โทร.๐ ๒๕๗๕ ๖๐๔๓ โทร.ทหาร ๕๗๒๒๒๐๗)

ที่ กท ๐๓๐๕.๔.๑/ ๕๕ วันที่ ๑๖ มี.ค.๖๑

เรื่อง ระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑

เรียน จก.กบ.ทหาร

อ้างถึง ระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๑

- สิ่งที่ส่งมาด้วย
๑. ร่างระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑
 ๒. ตารางเปรียบเทียบการปรับปรุงแก้ไขระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ
 ๓. สำเนาหนังสือ กกล.กบ.ทหาร ที่ ต่อ กกล.๗ เลขรับ ๑๙๖๓/๖๐ ลง ๑๒ ต.ค.๖๐
 ๔. สำเนาหนังสือ กบ.ท.สบส.กบ.ทหาร ที่ กท ๐๓๐๕.๔.๑/๑๙ ลง ๒๙ ม.ค.๖๑
 ๕. สำเนาหนังสือ กบ.ท.สบส.กบ.ทหาร ที่ กท ๐๓๐๕.๔.๑/๓๗ ลง ๒๐ ก.พ.๖๑
 ๖. สำเนาหนังสือ ศชบ.ทหาร ที่ กท ๐๓๐๑.๑๐/๑๐๒ ลง ๒ มี.ค.๖๑
 ๗. ตารางเปรียบเทียบความเห็นของ ศชบ.ทหาร ร่างระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑

๑. กบ.ท.สบส.กบ.ทหาร ขออนุมัติยกเลิกระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๑ ตามอ้างถึง และให้ใช้ร่างระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑ แทน รายละเอียดตามสิ่งที่ส่งมาด้วย ๑ โดยมีตารางเปรียบเทียบการปรับปรุงแก้ไขรายละเอียดตามสิ่งที่ส่งมาด้วย ๒

๒. ข้อเท็จจริง

๒.๑ สदन.ทหาร ได้ทำการตรวจสอบภายใน กบ.ทหาร ประจำปีงบประมาณ ๒๕๖๐ โดยได้ตรวจกิจกรรมงานสารสนเทศ พบว่า นโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยปฏิบัติตามระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๑ ไม่เป็นปัจจุบัน รายละเอียดตามสิ่งที่ส่งมาด้วย ๓

๒.๒ กบ.ท.สบส.กบ.ทหาร ได้ดำเนินการจัดทำร่างระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑ ใหม่ เพื่อใช้ทดแทนระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๑ ให้มีความเหมาะสมกับสถานการณ์ปัจจุบัน โดยให้ นชต.กบ.ทหาร ช่วยพิจารณาปรับแก้ไข ระเบียบฯ ให้มีความเหมาะสมทันสมัย สามารถใช้ปฏิบัติได้ รายละเอียดตามสิ่งที่ส่งมาด้วย ๔

๒.๓ กบท.สบส.กบ.ทหาร ได้ดำเนินการเสนอร่างระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑ ให้ ศชบ.ทหาร พิจารณาตรวจสอบความเหมาะสมถูกต้อง สอดคล้องกับแนวทางการบริหารจัดการด้านไซเบอร์ของ บก.ทท. รายละเอียดตามสิ่งที่ส่งมาด้วย ๕

๒.๔ ศชบ.ทหาร ได้พิจารณาร่างระเบียบฯ แล้ว เห็นว่าในภาพรวมมีความเหมาะสม ไม่ขัดหรือแย้งกับนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ.๒๕๕๙ และได้สรุปความเห็นเกี่ยวกับร่างระเบียบ กบ.ทหาร ฯ เพิ่มเติม ซึ่ง กบท.สบส.ฯ ได้ดำเนินการปรับแก้ไขเรียบร้อยแล้ว รายละเอียดตามสิ่งที่ส่งมาด้วย ๖ และ ๗

๓. ข้อพิจารณา เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของ กบ.ทหาร เป็นไปด้วยความเรียบร้อย เห็นสมควรยกเลิกระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๑ และให้ใช้ระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑ แทน

๔. ข้อเสนอ เห็นควรดำเนินการดังนี้

๔.๑ อนุมัติให้ยกเลิกระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๑ และให้ใช้ระเบียบ กบ.ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑ แทน

๔.๒ สำเนาให้ สน.จก.กบ.ทหาร สน.รอง จก.กบ.ทหาร (๑) (๒) สน.สสร.กบ.ทหาร สน.สบส.กบ.ทหาร และ นขต.กบ.ทหาร ทราบและยึดถือปฏิบัติโดยเคร่งครัด

๔.๓ สำเนาให้ ศชบ.ทหาร ทราบ

๔.๔ นำเรียน รอง จก.กบ.ทหาร (๒) และ ผอ.สสร.กบ.ทหาร เพื่อกำหนดทราบ

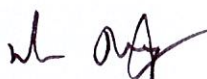
จึงเรียนมาเพื่อพิจารณา หากเห็นสมควรกรุณาอนุมัติตามข้อ ๔ และลงนามในร่างระเบียบฯ ที่แนบ

พ.อ.

(เลิศชาย สกุลสัตตบุษย์)

ผอ.กบท.สบส.กบ.ทหาร

- คนมีติดตามข้อ ๔
- ลงนามแล้ว

พล.ร.ท.  ฐน.

อ.ก.กบ.ทหาร

๖ เม.ย. ๖๖

พล.ท. 
ผอ.กบ.ทท.ทหาร
๖ เม.ย. ๖๖

พล.อ.ท. 
รอง จก.กบ.ทหาร
๖ เม.ย. ๖๖



ระเบียบกรมส่งเสริมการค้าระหว่างประเทศ
ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ
พ.ศ.๒๕๖๑

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของ กรมส่งเสริมการค้าระหว่างประเทศ เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบนี้ไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบ กรมส่งเสริมการค้าระหว่างประเทศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑”

ข้อ ๒ ระเบียบนี้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิกระเบียบกรมส่งเสริมการค้าระหว่างประเทศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๑ และให้ใช้ระเบียบนี้แทน

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ ลูกจ้างและพนักงานราชการ ที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวข้องกับระบบสารสนเทศของ กรมส่งเสริมการค้าระหว่างประเทศ

ข้อ ๕ ในระเบียบนี้

๕.๑ “ระบบสารสนเทศ” หมายความว่า ระบบการจัดการข้อมูลที่น่าเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสาร มาช่วยในการสร้างสารสนเทศ เพื่อนำมาใช้ในการวางแผนการบริหาร การพัฒนาและควบคุม ซึ่งประกอบด้วย

๕.๑.๑ “ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ ที่เชื่อมการทำงานเข้าด้วยกัน โดยต้องกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๕.๑.๒ “ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร ทั้งในระบบอินทราเน็ตและอินเทอร์เน็ตได้

๕.๑.๒.๑ ระบบอินทราเน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๕.๑.๒.๒ ระบบอินเทอร์เน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๕.๒ “สารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๕.๓ “คอมพิวเตอร์” หมายความว่า เครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์ที่มีความสามารถในการรับข้อมูลเข้าประมวลผลตามโปรแกรม และแสดง บันทึก ส่งออกข้อมูล ซึ่งเป็นผลที่ได้จากการประมวลผลนั้น โดยอาจเป็นคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา ตลอดจนคอมพิวเตอร์อื่น ๆ รวมถึงแท็บเล็ตและสมาร์ตโฟน

๕.๔ “ผู้บังคับบัญชา” หมายความว่า ผู้ที่มีอำนาจและหน้าที่ในการปกครองบังคับบัญชาหน่วย

๕.๕ “ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงานราชการ และลูกจ้างของกรมส่งกำลังบำรุงทหาร รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกรมส่งกำลังบำรุงทหารที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศ

๕.๖ “ผู้ดูแลระบบ” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศของหน่วยนั้น

ข้อ ๖ ให้ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร เป็นผู้กำกับดูแลการดำเนินการให้เป็นไปตามระเบียบนี้

หมวด ๑

ความมุ่งหมาย

ข้อ ๗ เพื่อกำหนดแนวทางปฏิบัติในการดำเนินการด้านความมั่นคงปลอดภัยระบบสารสนเทศของกรมส่งกำลังบำรุงทหาร ให้เกิดความมั่นคงปลอดภัยมากที่สุด ครอบคลุมการรักษาความปลอดภัยด้วยมาตรการด้านการป้องกัน (Preventive) มาตรการด้านการตรวจสอบ (Detective) และมาตรการด้านการแก้ไข (Corrective) ในเรื่องดังต่อไปนี้

๗.๑ การรักษาความปลอดภัยเกี่ยวกับบุคคล

๗.๒ การรักษาความปลอดภัยอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ

๗.๓ การรักษาความปลอดภัยระบบสารสนเทศ

๗.๔ การรักษาความปลอดภัยระบบคอมพิวเตอร์และอุปกรณ์ประกอบ

๗.๕ การรักษาความปลอดภัยด้านโปรแกรม

๗.๖ การรักษาความปลอดภัยระบบสื่อสารข้อมูลและระบบเครือข่าย

๗.๗ การรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการปฏิบัติงานระบบสารสนเทศ

๗.๘ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

ข้อ ๘ นิยามศัพท์ต่าง ๆ หรือแนวปฏิบัติอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ที่ไม่ได้กำหนดไว้ในระเบียบนี้ หรือขัดแย้งกับประกาศกองบัญชาการกองทัพไทย เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙ ให้ยึดถือตามประกาศกองบัญชาการกองทัพไทย เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย ลงวันที่ ๑๙ กันยายน พ.ศ.๒๕๕๙

หมวด ๒

การรักษาความปลอดภัยเกี่ยวกับบุคคล

ข้อ ๙ ข้าราชการ ลูกจ้างและพนักงานราชการ กรมส่งเสริมการปกครองส่วนท้องถิ่น ที่ได้รับอนุญาตปฏิบัติงานด้านสารสนเทศ จะต้องศึกษาและทำความเข้าใจในเรื่องระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และที่แก้ไขเพิ่มเติม ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๕๔ และประกาศกองบัญชาการกองทัพไทย เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙ ที่เกี่ยวข้องและที่มีผลบังคับใช้ในปัจจุบัน หากตรวจพบว่าการละเมิดหรือบุคคลใดมีพฤติกรรมหรือสงสัยว่าจะเป็นภัยต่อระบบสารสนเทศที่ กรมส่งเสริมการปกครองส่วนท้องถิ่น รับผิดชอบอยู่ ไม่ว่าจะโดยเจตนาหรือไม่ก็ตาม ให้ผู้มีหน้าที่กำกับดูแลและจัดการอนุญาตชั่วคราว และสอบสวนให้得其ความจริงก่อนพิจารณาตัดสินหรือให้สิทธิ์การปฏิบัติงานต่อไป

ข้อ ๑๐ การจัดทำทะเบียนความไว้วางใจบุคลากร

๑๐.๑ จัดทำทะเบียนความไว้วางใจของเจ้าหน้าที่เทคนิคและเจ้าหน้าที่ที่ใช้ระบบงานตามกลุ่มงาน หน้าที่ความรับผิดชอบ โดยจัดระดับชั้นความลับที่ได้รับอนุมัติ

๑๐.๒ ลงทะเบียนเจ้าหน้าที่ใหม่ และยกเลิกการใช้งานทันทีที่พ้นหน้าที่

๑๐.๓ ต้องทบทวนสิทธิทุก ๖ เดือน และทุกครั้งที่มีการเปลี่ยนแปลง

ข้อ ๑๑ ผู้ที่พ้นจากหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ตัดชื่อออกจากทะเบียนความไว้วางใจ และนำเรียนเจ้ากรมส่งเสริมการปกครองส่วนท้องถิ่น ทราบภายใน ๒ วันทำการ

ข้อ ๑๒ การปฏิบัติด้านการรักษาความปลอดภัยของผู้ขอใช้บริการ จะต้องยึดถือและปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ และระเบียบอื่น ๆ ที่เกี่ยวข้อง และที่มีผลบังคับใช้ในปัจจุบัน รวมทั้งปฏิบัติตามนโยบาย และคำสั่งที่กำหนดย้อย่างเคร่งครัด

ข้อ ๑๓ การปฏิบัติด้านการรักษาความปลอดภัยของผู้ปฏิบัติงานชั่วคราว ให้จัดทำทะเบียนแยกกลุ่มต่างหาก โดยจะต้องผ่านการตรวจสอบความไว้วางใจเช่นเดียวกันก่อนจะได้รับอนุญาตให้ปฏิบัติงานชั่วคราว โดยเกี่ยวข้องกับเฉพาะเรื่องเป็นกรณีไป และให้ยกเลิกการอนุญาตทันทีเมื่อครบกำหนดสิ้นสุดการขอใช้งาน

ข้อ ๑๔ การปฏิบัติด้านการรักษาความปลอดภัยในการจัดจ้างองค์กรเอกชนภายนอกมาปฏิบัติงาน (Outsourcing) จะต้องกำหนดให้ผู้รับจ้างต้องไม่นำข้อมูลเอกสารผลงานต่าง ๆ เอกสารการฝึกอบรม ไปเผยแพร่หรือใช้ในกิจการที่ไม่เกี่ยวกับงานตามสัญญา และเจ้าหน้าที่ของผู้รับจ้างจะได้รับสิทธิในฐานะผู้ปฏิบัติงานชั่วคราว โดยรายละเอียดเหล่านี้จะต้องระบุไว้ในสัญญาอย่างชัดเจน

ข้อ ๑๕ ในกรณีที่เกิดเหตุการณ์ไม่ปกติ ข้าราชการ ลูกจ้างและพนักงานราชการ กรมส่งกำลังบำรุงทหาร ต้องปฏิบัติดังนี้

๑๕.๑ ฝ้าดูการปฏิบัติงานสารสนเทศของเจ้าหน้าที่เทคนิค และเจ้าหน้าที่ผู้ใช้ระบบงานไม่ให้ใช้งานนอกเหนือจากสิทธิที่ได้รับ

๑๕.๒ รายงานเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยซึ่งเกิดขึ้น (Security Incidents) รวมทั้งรายงานจุดอ่อนช่องโหว่หรือภัยคุกคามที่พบในระบบสารสนเทศ ให้ผู้รับผิดชอบทราบโดยด่วน

๑๕.๓ ผู้ดูแลระบบ ต้องบันทึกเหตุการณ์ในกรณีที่เกิดเหตุการณ์ไม่ปกติต่าง ๆ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

ข้อ ๑๖ จัดให้มีกระบวนการทางวินัยเพื่อลงโทษข้าราชการ ลูกจ้างและพนักงานราชการที่ฝ่าฝืนหรือละเมิดระเบียบ กรมส่งกำลังบำรุงทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑ โดยจะได้รับโทษทางวินัยแล้วแต่กรณี

หมวด ๓

การรักษาความปลอดภัยอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ

ข้อ ๑๗ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๑๘ กำหนดให้ที่ตั้งของระบบสารสนเทศและพื้นที่ที่ใช้งานระบบสารสนเทศภายใน กรมส่งกำลังบำรุงทหาร เป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะ โดยพิจารณาตามความสำคัญแล้วแต่กรณี ให้มีความเหมาะสม

/ข้อ ๑๘ ให้ติดตั้ง ...

ข้อ ๑๙ ให้ติดตั้งอุปกรณ์รักษาความปลอดภัย ณ สถานที่ตั้งระบบให้บริการ (Service System) ด้วยเทคโนโลยีที่เหมาะสมและทันสมัยเพื่อประโยชน์ในการรักษาความปลอดภัยทางด้านกายภาพของระบบ

ข้อ ๒๐ การเข้าถึงหรือเข้าออกพื้นที่ ให้เจ้าหน้าที่กรมส่งกำลังบำรุงทหาร ซึ่งได้รับมอบหมาย หรือได้รับอนุญาตเท่านั้น เป็นผู้มีสิทธิเข้าถึง หรือเข้าออกบริเวณพื้นที่ซึ่งติดตั้งอุปกรณ์

ข้อ ๒๑ การป้องกันรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบที่สามารถเคลื่อนย้ายได้และ/หรืออยู่นอกพื้นที่ควบคุม เมื่อถูกนำไปใช้งานนอกสถานที่ ต้องกำหนดการปฏิบัติในการใช้งาน การยืม/คืน และอื่น ๆ ให้สอดคล้องกับระเบียบว่าด้วยการรักษาความปลอดภัยอย่างรัดกุม

หมวด ๔

การรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๒๒ การกำหนดมาตรการหรือการรักษาความปลอดภัยระบบสารสนเทศ ต้องผ่านการประเมินความเสี่ยงระบบสารสนเทศ เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับสภาพแวดล้อมของแต่ละระบบ ทั้งนี้ ให้มีการทบทวนแผนการบริหารความเสี่ยงดังกล่าวอย่างน้อยปีละครั้ง หรือเมื่อมีเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อความปลอดภัยระบบสารสนเทศของ กรมส่งกำลังบำรุงทหาร

ข้อ ๒๓ การรักษาความปลอดภัยระบบสารสนเทศ ต้องดำเนินการรักษาความปลอดภัยระบบสารสนเทศให้ถึงระดับที่สอดคล้องกับความเสี่ยงระบบสารสนเทศที่ประเมินได้

ข้อ ๒๔ อำนาจและหน้าที่ของผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร และ นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งกำลังบำรุงทหาร

๒๔.๑ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร มีหน้าที่ดังนี้

๒๔.๑.๑ เป็นตัวแทนของกรมส่งกำลังบำรุงทหาร ในการประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับศูนย์ไซเบอร์ทหาร

๒๔.๑.๒ ให้ข้อเสนอแนะ กำกับดูแล ติดตามผล การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมส่งกำลังบำรุงทหาร ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ กองบัญชาการกองทัพบกไทย รวมถึงกฎหมายด้านไซเบอร์ที่เกี่ยวข้อง

๒๔.๑.๓ ประสานงานเพื่อจัดทำ งาน/แผนงาน/โครงการ ด้านไซเบอร์ของกรมส่งกำลังบำรุงทหาร

๒๔.๑.๔ กำกับดูแล การดำเนินการติดตามสถานการณ์และแก้ไขปัญหาจากเหตุการณ์ทางไซเบอร์ที่มีต่อข้อมูลหรือระบบสารสนเทศของกรมส่งกำลังบำรุงทหาร

๒๔.๑.๕ กำกับดูแล การสร้างความตระหนักรู้ทางไซเบอร์ของกรมส่งกำลังบำรุงทหาร

๒๔.๑.๖ อื่น ๆ ตามที่ รอง เสธ.ทหาร (๑)/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กองบัญชาการกองทัพไทย และคณะกรรมการความมั่นคงปลอดภัยไซเบอร์ กองบัญชาการกองทัพไทย กำหนด

๒๔.๒ นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งกำลังบำรุงทหาร มีหน้าที่ดังนี้

๒๔.๒.๑ ดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กรมส่งกำลังบำรุงทหาร ตามที่ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร กำหนด

๒๔.๒.๒ จัดทำ งาน/แผน/โครงการ ด้านไซเบอร์ของกรมส่งกำลังบำรุงทหาร

๒๔.๒.๓ ติดตามสถานการณ์และแก้ไขปัญหาจากเหตุการณ์ทางไซเบอร์ ที่มีต่อข้อมูลหรือระบบสารสนเทศของกรมส่งกำลังบำรุงทหาร

๒๔.๒.๔ ดำเนินการเกี่ยวกับการสร้างความตระหนักรู้ทางไซเบอร์ของ กรมส่งกำลังบำรุงทหาร

๒๔.๒.๕ รายงานเหตุการณ์ทางไซเบอร์ (Cyber Incidents) ของกรมส่งกำลังบำรุงทหาร ไปยัง ศูนย์ไซเบอร์ทหาร/ศูนย์ปฏิบัติการร่วมทางไซเบอร์ ศูนย์บัญชาการทางทหาร ทั้งนี้ ให้เป็นไปตามนโยบาย การรักษาความมั่นคงปลอดภัยไซเบอร์ กองบัญชาการกองทัพไทย หรือตามที่ ศูนย์ไซเบอร์ทหาร/ศูนย์ปฏิบัติการร่วมทางไซเบอร์ ศูนย์บัญชาการทางทหาร กำหนด

หมวด ๕

การรักษาความปลอดภัยระบบคอมพิวเตอร์และอุปกรณ์ประกอบ

ข้อ ๒๕ เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้แก่ เครื่องคอมพิวเตอร์ทุกชนิดและอุปกรณ์ทั้งปวง ที่มีการใช้งานร่วมกันระหว่างระบบงานต่าง ๆ อุปกรณ์ศูนย์กลางการประมวลผล อุปกรณ์ควบคุมการทำงานต่าง ๆ และอุปกรณ์อื่น ๆ ที่อยู่ในความดูแลของกรมส่งกำลังบำรุงทหาร

ข้อ ๒๖ การจัดหมวดหมู่และการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ให้ปฏิบัติดังนี้

๒๖.๑ จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบอย่างน้อย ๒ ชุด จัดเก็บไว้ในสถานที่ที่เหมาะสมกับชั้นความลับที่กำหนด ตามหมวดหมู่ กำหนดชั้นความลับ และระดับความสำคัญ

๒๖.๒ จัดทำป้ายชื่อผู้รับผิดชอบ ป้ายชั้นความลับ ลำดับการเคลื่อนย้ายกำกับไว้กับ อุปกรณ์ทุกชนิด รวมทั้งกำหนดวิธีป้องกันรักษาความปลอดภัยที่เหมาะสมประจำอุปกรณ์ด้วย

๒๖.๓ ให้ตรวจสอบบัญชีควบคุมทุก ๖ เดือน และจัดทำสรุปนำเสนอเรียน เจ้ากรมส่งกำลังบำรุงทหาร ภายใน ๑๕ วันทำการ

ข้อ ๒๗ การติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ จะต้องจัดให้มีสถานที่เฉพาะ มีระบบรักษาความปลอดภัยที่ดี มีสภาพแวดล้อมที่เหมาะสมต่ออุปกรณ์และภารกิจของอุปกรณ์นั้น ๆ โดยคำนึงถึงความสะดวกในการเข้าถึง การใช้งานและการรักษาความปลอดภัยเป็นสำคัญ

ข้อ ๒๘ จัดให้มีการควบคุมการเข้าถึงอุปกรณ์ต่าง ๆ ให้เหมาะสมกับชั้นความลับและความสำคัญดังนี้

๒๘.๑ กำหนดผู้รับผิดชอบกำกับดูแลทางกายภาพ (Physical) และทางตรรกะ (Logical) ในเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ตามห้วงระยะเวลาที่เหมาะสม

๒๘.๒ กำหนดรหัสป้องกัน และระบบกลั่นกรองการเข้าถึงอุปกรณ์เหล่านั้น

๒๘.๓ บันทึกการเข้าถึงอุปกรณ์ต่าง ๆ ตามรหัสป้องกันที่ได้กำหนดไว้ สามารถพิสูจน์ทราบผู้เป็นเจ้าของรหัสได้ โดยจัดเก็บเป็นบันทึกการเข้าถึงอุปกรณ์ต่าง ๆ ไว้อย่างเป็นระบบสามารถตรวจสอบได้ง่าย

๒๘.๔ สรุปนำเรียนเจ้ากรมส่งกำลังบำรุงทหาร ทุก ๖ เดือน

ข้อ ๒๙ การซ่อมบำรุงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ กรณีที่เป็นเครื่องคอมพิวเตอร์ที่มีหน่วยความจำถาวร ให้ดำเนินการดังนี้

๒๙.๑ ห้ามผู้ใช้งานดำเนินการถอดเปลี่ยนหรือซ่อมแก้ไขเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบโดยพลการ

๒๙.๒ ทำการสำรองข้อมูลที่จำเป็นไว้ทั้งหมด และจัดบันทึกข้อมูลที่เกี่ยวข้องกับการใช้งานระบบต่าง ๆ และระบบเครือข่าย

๒๙.๓ เมื่อได้รับเครื่องคอมพิวเตอร์คืนแล้วให้ดำเนินการดังนี้

๒๙.๓.๑ ตรวจสอบความครบถ้วนของระบบโปรแกรมในเครื่องคอมพิวเตอร์

๒๙.๓.๒ ตรวจสอบโปรแกรมเพิ่มเติมหรือแปลกปลอม

๒๙.๓.๓ เปลี่ยนรหัสผ่านที่ใช้สำหรับปฏิบัติงานใหม่ทั้งหมด

๒๙.๓.๔ จัดให้มีการปรนนิบัติบำรุง (Maintenance) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบตามระยะเวลาและวิธีการที่ถูกต้องตามหลักวิชาและคู่มือประจำเครื่อง (User Manual)

๒๙.๔ จัดทำประวัติการซ่อมบำรุงพร้อมรายชื่อผู้ทำการซ่อมบำรุง สามารถตรวจสอบได้เมื่อเกิดเหตุละเมิดการรักษาความปลอดภัย หรือการรั่วไหลของข้อมูล

๒๙.๕ จัดทำบัญชีของอุปกรณ์ที่สามารถทดแทนกันได้พร้อมที่ตั้งของอุปกรณ์เหล่านั้น

๒๙.๖ ให้ดำเนินการซ่อมบำรุงตามแนวทางการซ่อมบำรุงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบที่กรมการสื่อสารทหารกำหนด

ข้อ ๓๐ การทำสำรองและคืนสภาพ (Backup and Recovery)

๓๐.๑ จัดทำแผนการทำสำรองและคืนสภาพที่มีประสิทธิภาพ สามารถดำเนินการให้คืนสภาพได้ในทันทีและดำเนินการทดสอบการคืนสภาพอย่างน้อยปีละครั้ง หรือเมื่อมีเหตุการณ์สำคัญที่อาจส่งผลกระทบอย่างร้ายแรงต่อความปลอดภัยระบบสารสนเทศของกรมส่งกำลังบำรุงทหาร

๓๐.๒ จัดเก็บสื่อบันทึกข้อมูลสำรองตามวิธีปฏิบัติในข้อ ๓๕ โดยนำสื่อดังกล่าวเก็บในสถานที่อื่นนอกเหนือจากพื้นที่เดียวกับต้นฉบับ

๓๐.๓ จัดทำบันทึกทะเบียนประวัติการทำสำรองและคืนสภาพ โดยให้มีข้อมูลครบถ้วนและทันสมัยตลอดเวลา โดยจัดเก็บไว้ในที่เหมาะสมและปลอดภัย สามารถนำมาตรวจสอบได้

ข้อ ๓๑ เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบที่จะติดตั้งเข้าสู่ระบบสารสนเทศ ของกรมส่งเสริมการเกษตร จะต้องมีความปลอดภัยขั้นต่ำตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกรมการสื่อสารทหารกำหนด หากเป็นอุปกรณ์ที่ยังมิได้กำหนดคุณลักษณะไว้ ให้ทำเรื่องขอกำหนดคุณลักษณะเฉพาะของอุปกรณ์ดังกล่าวต่อกรมการสื่อสารทหาร

ข้อ ๓๒ อุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศของ กรมส่งเสริมการเกษตร ทุกรายการ ต้องได้รับการกำหนดผู้รับผิดชอบ ผู้มีสิทธิ์ใช้งานและวิธีการด้านรักษาความปลอดภัยประจำเครื่องคอมพิวเตอร์ และอุปกรณ์

ข้อ ๓๓ อุปกรณ์ที่นำมาติดตั้งใหม่ทุกครั้ง ต้องตรวจสอบและรายงานให้ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งเสริมการเกษตร ทราบและให้ความเห็นชอบ สำหรับอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่แล้ว ให้ตรวจสอบทุกรอบ ๖ เดือน หรือกรณีมีเหตุอันควรให้ตรวจสอบ แล้วจึงรายงานให้เจ้ากรมส่งเสริมการเกษตร ทราบ

ข้อ ๓๔ การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เข้า – ออก พื้นที่ทำงานระบบสารสนเทศ ของ กรมส่งเสริมการเกษตร หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะการทำงานของอุปกรณ์เปลี่ยนแปลงไป จะต้องได้รับอนุญาตจาก ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งเสริมการเกษตร ตรวจสอบความปลอดภัยก่อนการเคลื่อนย้ายทุกครั้ง

ข้อ ๓๕ การรักษาความปลอดภัยสื่อที่ใช้ในการบันทึกข้อมูล ให้กำหนดวิธีปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูล เพื่อป้องกันข้อมูลมิให้รั่วไหลหรือถูกทำลายดังนี้

๓๕.๑ ติดป้ายชื่อไว้ที่สื่ออย่างชัดเจน แสดงชั้นความลับของข้อมูลที่เก็บ หากเป็นกรณี ที่รวบรวมเก็บในกล่องหรือหีบห่อ ให้แสดงไว้ที่กล่องหรือหีบห่อนั้น ๆ ด้วย

๓๕.๒ กำหนดบุคคลที่มีสิทธิ์ใช้งานและระดับการเข้าถึงสื่อบันทึกข้อมูลนั้น ๆ

๓๕.๓ จัดเก็บสื่อบันทึกข้อมูลไว้ในสถานที่และสภาวะแวดล้อมที่เหมาะสมปลอดภัย

๓๕.๔ จัดทำทะเบียนสื่อบันทึกข้อมูลไว้อย่างเป็นระเบียบและครบถ้วนสามารถตรวจสอบได้

๓๕.๕ สื่อบันทึกที่สามารถถอดแยกได้ (Removable Computer Media) เช่น สื่อข้อมูลแบบพกพา เทปบันทึกข้อมูล ให้ลบข้อมูลที่มีได้ใช้งานทิ้งทันทีที่หมดความต้องการใช้ หรือกำหนดสิทธิของบุคคลที่ถอดแยกได้

/ข้อ ๓๖ ให้ติดตั้ง...

ข้อ ๓๖ ให้ติดตั้งซอฟต์แวร์ป้องกันภัยคุกคามในเครื่องคอมพิวเตอร์ทุกเครื่อง และห้ามถอนการติดตั้ง (Uninstall) ทั้งนี้หากเครื่องคอมพิวเตอร์ใดมีการลบซอฟต์แวร์ป้องกันภัยคุกคามโดยเจตนาหรือโดยประมาท ผู้ใช้ประจำเครื่องนั้นและผู้ดำเนินการ จะต้องเป็นผู้รับผิดชอบในความเสียหายที่เกิดขึ้น

ข้อ ๓๗ ให้บันทึกการเข้าติดตั้งใหม่ หรือปรับแต่งระบบ หรือเปลี่ยนแปลงองค์ประกอบของอุปกรณ์คอมพิวเตอร์ทั้งทางตรรกะและทางกายภาพทุกครั้ง

หมวด ๖

การรักษาความปลอดภัยด้านโปรแกรม

ข้อ ๓๘ โปรแกรมประยุกต์ (Application Program) คือกลุ่มของโปรแกรม หรือโปรแกรมคำสั่งต่าง ๆ ที่ใช้เพื่อการปฏิบัติงานของหน่วย

ข้อ ๓๙ โปรแกรมประยุกต์ที่ใช้ในราชการ จะต้องเป็นไปตามมาตรฐานเทคโนโลยีสารสนเทศของกระทรวงกลาโหม และจัดทำเอกสารรายละเอียดโปรแกรม (Program Specification) ตามมาตรฐานเป็นที่ยอมรับตามหลักวิชาการทั่วไป

ข้อ ๔๐ กำหนดผู้รับผิดชอบหรือผู้บริหารจัดการระบบงาน ผู้ใช้ สิทธิในการเข้าถึง/แก้ไขข้อมูล และปรับปรุงให้ทันสมัย โดยทำเป็นลายลักษณ์อักษร นำเรียนเจ้ากรมส่งกำลังบำรุงทหาร ลงนาม และแจ้งให้ผู้มีรายชื่อทราบ

ข้อ ๔๑ จัดให้มีผู้บริหารจัดการฐานข้อมูล (Database Administrator : DBA) เป็นผู้รับผิดชอบฐานข้อมูลที่อยู่ในความรับผิดชอบของ กรมส่งกำลังบำรุงทหาร เพื่อควบคุมกำกับดูแลทางเทคนิค การกำหนดสิทธิทางเทคนิคในการแก้ไขทางกายภาพของฐานข้อมูล สิทธิการเข้าถึงเนื้อหาข้อมูลที่มีชั้นความลับ รวมถึงความสัมพันธ์ของฐานข้อมูลที่ใช้งานทั้งสิ้น และแต่งตั้งผู้ประสานงานด้านข้อมูลกรณีที่ใช้ข้อมูลร่วมกับส่วนราชการอื่น

ข้อ ๔๒ การแก้ไขฐานข้อมูลในระบบทำได้โดยเจ้าหน้าที่ที่ได้รับอนุมัติในข้อ ๔๑ เท่านั้น โดยจัดทำเป็นบันทึกพร้อมรายละเอียดและเหตุผลการแก้ไข เพื่อให้สามารถตรวจสอบได้

ข้อ ๔๓ จัดทำระบบสำรองต้นฉบับของโปรแกรมประยุกต์ (Source Code) ทุกโปรแกรมตามวงรอบทุก ๖ เดือน และทุกครั้งที่มีการแก้ไขโปรแกรม และจัดเก็บไว้ในที่ปลอดภัยและเหมาะสม

ข้อ ๔๔ ผู้พัฒนาโปรแกรม ต้องพัฒนาตามหลักวิชาการที่ยอมรับโดยทั่วไป รวมทั้งแสดงรายละเอียดที่จำเป็นต่อการรักษาความปลอดภัยไว้ที่ต้นฉบับโปรแกรม (Source Code) ได้แก่ ชื่อผู้เขียน วัน เดือน ปี ที่เขียนหรือปรับปรุง วัตถุประสงค์ ระดับการป้องกัน

ข้อ ๔๕ ผู้พัฒนาโปรแกรม เป็นผู้รับผิดชอบต่อการรักษาความลับของโครงสร้างข้อมูล ความลับของตรรกะที่ใช้ในโปรแกรม ความถูกต้องของโปรแกรม และทำการพัฒนาโปรแกรมให้ตรงตามวัตถุประสงค์ของทางราชการ

ข้อ ๔๖ การวิเคราะห์พัฒนาและบำรุงรักษาระบบสารสนเทศ เจ้าของระบบงานผู้มีสิทธิ์และอำนาจในสารสนเทศจะต้องทราบว่า ผู้ใดเป็นผู้มีหน้าที่ในการวิเคราะห์พัฒนาและบำรุงรักษาโปรแกรมประยุกต์ของระบบสารสนเทศนั้น

ข้อ ๔๗ การรักษาความปลอดภัยระบบงานให้ปฏิบัติดังนี้

๔๗.๑ การพัฒนาโปรแกรมประยุกต์

๔๗.๑.๑ มีการจัดทำและเสนอความต้องการเป็นลายลักษณ์อักษร ลงนามโดยผู้อำนวยการกอง โดยผ่านความเห็นชอบจาก ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร ก่อนนำเรียนเจ้ากรมส่งกำลังบำรุงทหาร เพื่อขออนุมัติการจัดทำโปรแกรมระบบงาน

๔๗.๑.๒ ผู้พัฒนาระบบ จัดทำระบบตามที่วางแผนและออกแบบไว้ ร่วมกับนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งกำลังบำรุงทหาร เพื่อให้เกิดความมั่นใจว่าระบบดังกล่าวมีความปลอดภัยระบบสารสนเทศในระดับที่เหมาะสม และสาธิตโปรแกรมต้นแบบ (Prototype) ให้เจ้าของระบบพิจารณาความถูกต้องตรงความต้องการและอนุมัติให้ดำเนินการในรายละเอียด

๔๗.๒ จัดให้มีรหัสผ่านในการเข้าสู่ระบบงานอย่างน้อย ๑ ระดับ

๔๗.๓ ระบบงานหรือโปรแกรมประยุกต์จะต้องถูกออกแบบให้ผู้ใช้งานสามารถเรียกดู หรือเปลี่ยนแปลงข้อมูลได้เฉพาะในส่วนที่ได้รับสิทธิ์เท่านั้น

๔๗.๔ จัดทำเอกสารประกอบระบบงาน หรือโปรแกรมประยุกต์ตามมาตรฐานที่กำหนด โดยให้ครอบคลุมถึงการเสนอความต้องการ การกำหนดข้อมูลต่าง ๆ การเคลื่อนไหวของข้อมูล คุณสมบัติของโปรแกรมต่าง ๆ รายละเอียดการทำงานของโปรแกรมข้อมูลเข้า และข้อมูลออก

๔๗.๕ จัดทำเอกสารข้อปฏิบัติด้านการรักษาความปลอดภัยของระบบงานที่พัฒนาแล้ว ส่งมอบให้ผู้ใช้งานและผู้มีสิทธิ์ในสารสนเทศนั้น ๆ เพื่อรับทราบ การปฏิบัติพร้อมกันเอกสารประกอบระบบงาน

ข้อ ๔๘ การพัฒนาโปรแกรมประยุกต์ ให้ปฏิบัติดังนี้

๔๘.๑ ผู้พัฒนาระบบต้องไม่เข้าสู่ระบบที่ใช้งานเป็นประจำ แต่ให้จัดทำข้อมูลสมมุติที่ครอบคลุมทุกเงื่อนไขของข้อมูลจริง เพื่อใช้ในการทดสอบโปรแกรมโดยเฉพาะ และต้องทดสอบโปรแกรมการใช้ร่วมกับเจ้าของระบบอย่างน้อย ๓ ครั้ง

๔๘.๒ ต้องทดสอบความปลอดภัย (Security Acceptance Test) ก่อนติดตั้งใช้งานจริง (Production)

๔๘.๓ โปรแกรมประยุกต์ที่บันทึกหรือแก้ไขข้อมูลต้องมีตรรกะตรวจสอบข้อมูลให้ถูกต้อง (Data Validation) ครบถ้วนสมบูรณ์ และจะต้องให้ผู้มีสิทธิ์บันทึกหรือแก้ไขข้อมูล สามารถดำเนินการได้เฉพาะส่วนของข้อมูลที่ตนเองมีสิทธิ์เกี่ยวข้องเท่านั้น

/๔๘.๔ ผู้บริหาร...

๔๘.๔ ผู้บริหารจัดการระบบงาน (Administrator) ต้องจัดทำบัญชีรายชื่อของผู้มีสิทธิเข้าถึงระบบงาน มีการตรวจสอบความทันสมัยและถูกต้องของบัญชีตามวงรอบ ๖ เดือน โดยต้องยกเลิกรายชื่อผู้ที่หมดสิทธิออกด้วย

๔๘.๕ การแก้ไขโปรแกรมต่าง ๆ จะต้องมีการร้องขอจากผู้มีสิทธิในการปรับแก้ระบบงานนั้น ๆ ก่อนเสมอ

๔๘.๖ เมื่อมีการแก้ไขคำสั่งในโปรแกรมประยุกต์ใช้งานจริง (Production) ต้องแยกดำเนินขั้นตอนการทดสอบให้เรียบร้อย ก่อนนำไปใช้งานจริง และบันทึกรายละเอียดคำขอแก้ไขไว้

๔๘.๗ การปรับปรุงเอกสารประกอบระบบงาน ต้องบันทึกการปรับปรุงตามระยะเวลาต่าง ๆ เพื่อให้เอกสารประกอบระบบงานมีความถูกต้อง และทันสมัยอยู่ตลอดเวลา

๔๘.๘ ต้องไม่เก็บต้นฉบับโปรแกรมประยุกต์ (Source Code) ที่อยู่ในระหว่างทดสอบ (Testing) ไว้ในพื้นที่เดียวกับโปรแกรมประยุกต์ที่ใช้งานจริง (Production) กรณีซอฟต์แวร์ที่จัดหา ต้องตรวจสอบก่อนติดตั้งใช้งานจริง เพื่อป้องกันคำสั่งที่ไม่ประสงค์ดี (Malicious Code) แฝงมา

ข้อ ๔๙ การรักษาความปลอดภัยฐานข้อมูล

๔๙.๑ ต้องไม่ใช่ชื่อผู้ใช้และรหัสผ่านโดยใช้ค่าปริยาย (Default Username/Password)

๔๙.๒ ต้องจัดทำบัญชีรายชื่อของผู้มีสิทธิทางเทคนิค ในการเข้าถึงฐานข้อมูลแต่ละระดับ และกำหนดรหัสผ่านให้เป็นรายบุคคล ดำเนินการตรวจสอบแก้ไขบัญชีให้ทันสมัยถูกต้อง ทุกวงรอบ ๓ เดือน

๔๙.๓ ต้องเก็บรักษาความลับชื่อผู้ใช้และรหัสผ่านของตนเองโดยเคร่งครัดและรับผิดชอบหากมีการรั่วไหลด้วยรหัสของตน

๔๙.๔ ให้มีการจัดทำสำเนาฐานข้อมูลทุกระบบ ๓ วงรอบ (Generation) วงรอบละ ๑ เดือน และจัดเก็บไว้ในที่เหมาะสมปลอดภัย

๔๙.๕ ห้ามใช้ฐานข้อมูลจริงและ/หรือฐานข้อมูลสำรองที่ได้จัดทำสำเนาไว้ในการทดลองการพัฒนาโปรแกรม การฝึก หรือการศึกษาโดยเด็ดขาด

๔๙.๖ ห้ามทำการพิมพ์หรือสำเนาข้อมูลไว้เพื่อการอื่นซึ่งไม่ใช่เพื่อใช้พื้นที่ระบบหรือตามความต้องการของผู้เป็นเจ้าของระบบงาน

๔๙.๗ การแลกเปลี่ยนสารสนเทศและซอฟต์แวร์

๔๙.๗.๑ จัดทำข้อตกลงระหว่างส่วนราชการหรือองค์กรที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร ในการแลกเปลี่ยนข้อมูลสารสนเทศและซอฟต์แวร์ (Information and Software Exchange Agreement)

๔๙.๗.๒ กำหนดการจัดส่งสื่อบันทึกข้อมูล (Media Transit) โดยเลือกใช้การนำสารทางทหาร มีการหีบห่อสื่อที่ปลอดภัย

ข้อ ๕๐ โปรแกรมอื่น ๆ ซึ่งจัดให้มีขึ้นเพื่อใช้ในการปฏิบัติราชการ รวมทั้งแฟ้มข้อมูลต่าง ๆ ที่เกี่ยวข้องจะต้องมีระบบรักษาความปลอดภัยที่เหมาะสม มีการปรับปรุงแฟ้มข้อมูลต่าง ๆ ที่ใช้ในการทำงานให้ทันสมัยตลอดเวลา และดำเนินการต่อแฟ้มข้อมูลเหล่านั้นให้สอดคล้องกับชั้นความลับที่กำหนดไว้

ข้อ ๕๑ รายละเอียดของโปรแกรมใด ๆ และแฟ้มข้อมูลต่าง ๆ ที่อยู่ในเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ เป็นข้อมูลที่จัดเป็นความลับ จะต้องให้รู้เฉพาะผู้ที่มีความจำเป็นต้องรู้เท่านั้น การให้ข้อมูลเหล่านี้กับบุคคลภายนอกใด ๆ จะต้องอยู่ภายใต้ความควบคุมอย่างใกล้ชิด

ข้อ ๕๒ การเผยแพร่โปรแกรมระบบงานที่หน่วยพัฒนาขึ้น หากเห็นว่าเป็นประโยชน์ต่อส่วนรวม และสามารถนำไปเผยแพร่ประชาสัมพันธ์หรือนำไปใช้ได้ จะต้องได้รับความเห็นชอบจาก ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร และผู้บังคับบัญชาตามลำดับชั้นก่อนจึงจะดำเนินการได้

หมวด ๗

การรักษาความปลอดภัยระบบสื่อสารข้อมูลและระบบเครือข่าย

ข้อ ๕๓ ระบบสื่อสารข้อมูล (Data Communication) คือ ระบบที่ใช้เพื่อการนำข้อมูลจากจุดต้นทางไปยังจุดปลายทาง ตามที่ได้กำหนดไว้ โดยประกอบด้วยอุปกรณ์ต่าง ๆ และโปรแกรมคำสั่งที่ใช้ควบคุมการทำงานของอุปกรณ์เหล่านั้น

ข้อ ๕๔ ระบบเครือข่าย (Network) คือ การเชื่อมโยงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบที่แยกกันอยู่อย่างอิสระเข้าเป็นเครือข่ายเดียวกัน โดยระบบสื่อสารข้อมูล เพื่อใช้ในการสารสนเทศ ทำการแบ่งปันการใช้ทรัพยากร เช่น ข้อมูลและอุปกรณ์ต่อพ่วงอื่น ๆ แบ่งตามลักษณะการใช้งานเป็น ๒ ระบบดังนี้

๕๔.๑ ระบบเครือข่ายกองบัญชาการกองทัพไทย เป็นเครือข่ายที่ทุกหน่วยในส่วนราชการในกองบัญชาการกองทัพไทยใช้ในการปฏิบัติงานร่วมกัน โดยมีกรมการสื่อสารทหารเป็นหน่วยรับผิดชอบดำเนินการ

๕๔.๒ ระบบเครือข่ายภายในของกรมส่งกำลังบำรุงทหาร ซึ่งกรมส่งกำลังบำรุงทหารรับผิดชอบดำเนินการและบริหารดูแล ใช้เพื่อการปฏิบัติงานภายในหน่วย

ข้อ ๕๕ การเชื่อมโยงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบเข้ากับระบบเครือข่ายของกรมส่งกำลังบำรุงทหาร จะต้องได้รับการพิจารณาอนุมัติจาก เจ้ากรมส่งกำลังบำรุงทหาร โดยผ่านความเห็นชอบจากผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร ก่อนดำเนินการทุกครั้ง และให้กองบริหารสิ่งอุปกรณ์ทางทหาร สำนักบริหารสิ่งอุปกรณ์ กรมส่งกำลังบำรุงทหาร เป็นผู้กำหนดขั้นตอนและรับผิดชอบในการปฏิบัติ

๕๕.๑ ต้องมีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่นอกพื้นที่ สามารถเข้าใช้งานเครือข่ายได้

๕๕.๒ กำหนดสิทธิการใช้งานของเจ้าหน้าที่ให้สามารถใช้เฉพาะเครือข่ายที่อนุญาตเท่านั้น และจำกัดการใช้เส้นทางบนเครือข่ายเพื่อมิให้เจ้าหน้าที่สามารถใช้ออกเส้นทางอื่นได้

๕๕.๓ กำหนดข้อปฏิบัติในการใช้งานเครือข่ายคอมพิวเตอร์

ข้อ ๕๖ การใช้ระบบสื่อสารข้อมูลในเครือข่ายสารสนเทศ

๕๖.๑ ให้ใช้เครือข่ายระบบโทรคมนาคมทหารเป็นหลัก ในกรณีที่มีระบบโทรคมนาคมทหารไม่สามารถให้การสนับสนุนได้ ให้เลือกใช้ระบบที่มีประสิทธิภาพเหมาะสม และมีความปลอดภัยมากที่สุด ในสถานการณ์นั้น

๕๖.๒ ต้องแยกระบบเครือข่ายสารสนเทศภายใน (ระบบอินทราเน็ต) ที่สำคัญและมีชั้นความลับสูงออกจากระบบเครือข่ายสารสนเทศที่เปิดเผยเป็นสาธารณะเชื่อมต่อออกสู่ภายนอก (ระบบอินเทอร์เน็ต) หรือระบบเครือข่ายสารสนเทศที่มีชั้นความลับต่ำ

๕๖.๓ เมื่อเกิดปัญหาที่เกี่ยวกับการใช้ระบบสื่อสารข้อมูล ในกรณีที่มีผลกระทบต่อการทำงานเชื่อมโยงเป็นส่วนรวมทำให้ไม่สามารถใช้งานเครือข่ายสารสนเทศได้ ให้รีบประสานผู้รับผิดชอบทำการแก้ไข โดยด่วน พร้อมทั้งรายงานข้อขัดข้องและการดำเนินการแก้ไขให้ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร ทราบทันที และต้องกำหนดรหัสผ่านในการเข้าปรับปรุงเปลี่ยนแปลงหรือจัดการการทำงานของอุปกรณ์สื่อสารข้อมูล และให้ใช้ได้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น โดยปฏิบัติตามแนวทางเดียวกับหัวข้อรหัสผ่าน (หมวด ๘)

๕๖.๔ ในกรณีที่ต้องให้บุคคลอื่นภายนอกดำเนินการเกี่ยวกับระบบสื่อสารข้อมูล ต้องจัดเจ้าหน้าที่ร่วมดำเนินการและรับทราบทุกขั้นตอน และต้องได้รับการอนุญาตจากคณะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร ก่อนดำเนินการ

ข้อ ๕๗ การดำเนินการเกี่ยวกับโปรแกรมคำสั่งต่าง ๆ และอุปกรณ์ในระบบสื่อสารข้อมูล

๕๗.๑ การย้าย เปลี่ยนแปลงที่ตั้ง การตั้งโปรแกรมคำสั่ง หรือมีการกระทำใด ๆ ต่ออุปกรณ์สื่อสารข้อมูล จะต้องได้รับการอนุมัติและกำกับดูแลจาก ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กรมส่งกำลังบำรุงทหาร หรือผู้ที่ได้รับมอบหมายให้กำกับดูแลรับผิดชอบ

๕๗.๒ จัดให้มีเครื่องมืออุปกรณ์หรือระบบรักษาความปลอดภัยเครือข่ายที่ทันสมัย และมีมาตรฐานได้รับการรับรอง สามารถป้องกันการบุกรุกเครือข่ายและภัยคุกคามได้และสามารถพัฒนาให้ทันต่อวิวัฒนาการของภัยคุกคามอยู่ตลอดเวลา พร้อมทั้งบันทึกและรายงานการบุกรุกหรือภัยคุกคามจากภายนอกทุกครั้ง

๕๗.๓ จัดให้มีเครื่องมืออุปกรณ์หรือระบบเข้า - ถอดรหัสข้อมูลที่มีมาตรฐาน ได้รับการรองรับแล้วเมื่อมีการรับส่งผ่านเครือข่าย เพื่อรักษาความลับของข้อมูลหากมีการรั่วไหลระหว่างช่องทางการรับส่ง

๕๗.๔ จัดให้มีเครื่องมืออุปกรณ์หรือระบบตรวจสอบเส้นทางการเชื่อมโยงเครือข่าย และทำงานตลอดเวลา และมีการบันทึกข้อผิดพลาดที่เกิดขึ้นทุกครั้ง

๕๗.๕ จะต้องมีการทดสอบเครื่องมืออุปกรณ์ต่าง ๆ ทุก ๓ เดือน และรายงานผลให้ เจ้ากรมส่งกำลังบำรุงทหาร ทราบ

หมวด ๘

การรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการปฏิบัติงานระบบสารสนเทศ

ข้อ ๕๘ จัดให้มีคำแนะนำการใช้ระบบงาน พร้อมเอกสารประกอบระบบงานให้เจ้าหน้าที่ผู้เกี่ยวข้อง เพื่อปฏิบัติตามอย่างเคร่งครัด

ข้อ ๕๙ กระบวนการตรวจสอบบันทึกเหตุการณ์ในระบบ (Audit Logging Procedures)

๕๙.๑ นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งกำลังบำรุงทหาร ทำการตรวจสอบระบบเป็นประจำ เพื่อช่วยในการควบคุมและแก้ไขความเสียหายที่อาจเกิดขึ้น โดยจะตรวจสอบจากข้อมูลบันทึกเหตุการณ์ต่าง ๆ (Log Event) และทำการบันทึกข้อมูลที่จำเป็นเพิ่มเติม เพื่อเป็นรายงานในการอ้างอิงต่อไป

๕๙.๒ เจ้าหน้าที่ผู้ดูแลระบบ แจ้งให้นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งกำลังบำรุงทหาร ในกรณีเกิดเหตุการณ์ไม่ปกติเกี่ยวกับความปลอดภัยระบบสารสนเทศ เพื่อให้สามารถแก้ไขสถานการณ์ได้ทันที่

ข้อ ๖๐ การเริ่มใช้ระบบงานใหม่

๖๐.๑ จะต้องมีการจัดทำข้อมูลให้สมบูรณ์ถูกต้องก่อนเริ่มใช้ระบบงาน

๖๐.๒ จะต้องมีการทำงานคู่มืออย่างน้อย ๒ วงรอบ ก่อนการใช้งานระบบงานจริง

๖๐.๓ ในการเริ่มใช้ระบบงานใหม่ จะต้องมีการอบรมการใช้และบำรุงรักษาระบบงานแก่เจ้าหน้าที่ผู้เกี่ยวข้องก่อน

๖๐.๔ จะต้องจัดทำเอกสารรับและส่งมอบระบบงาน โดยมีการลงนามในเอกสาร และส่งมอบให้กันก่อนที่จะเริ่มใช้ระบบงานใหม่ และสำเนาเอกสารอีก ๑ ชุด แนบไว้ที่เอกสารประกอบการพัฒนาระบบงานต่างหากจากการดำเนินการทางธุรการปกติ

ข้อ ๖๑ การดูแลระบบงานที่ใช้งานจริง

๖๑.๑ จะต้องมีเจ้าหน้าที่ผู้รับผิดชอบโดยตรงในระบบงานนั้น ๆ และจะต้องมีผู้รับผิดชอบรองลงไปไม่น้อยกว่า ๒ คน

๖๑.๒ จะต้องมีการประเมินการทำงานของระบบงานทุก ๖ เดือน และจัดทำสรุปเพื่อนำเรียน เจ้ากรมส่งกำลังบำรุงทหาร

ข้อ ๖๒ การจัดเก็บเอกสารเกี่ยวกับระบบงาน

๖๒.๑ จะต้องจัดเก็บเอกสารประกอบระบบงานทั้งหมดของแต่ละระบบไว้ด้วยกัน โดยจัดทำไว้อย่างน้อย ๒ ชุด จัดเก็บที่ส่วนกรรมวิธีข้อมูล ๑ ชุด และผู้รับผิดชอบระบบ ๑ ชุด

๖๒.๒ เอกสารย่อย อาจจะทำสำเนาเก็บไว้สำหรับเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อใช้ในการทำงานได้ตามความเหมาะสม

๖๒.๓ มีการกำหนดชั้นความลับของเอกสารดังกล่าวให้เหมาะสมตามชั้นความลับของระบบงาน

๖๒.๔ ดำเนินการจัดเก็บระบบงานเอกสารตามระเบียบกองบัญชาการทหารสูงสุดว่าด้วยการเก็บเอกสาร พ.ศ.๒๕๒๒ และที่แก้ไขเพิ่มเติม

ข้อ ๖๓ การดำเนินการด้านรหัสผ่าน (Password)

๖๓.๑ กำหนดระดับบุคคล/หน่วยงาน ที่สามารถเข้าถึงและ/หรือแก้ไขข้อมูลตามสิทธิและอำนาจหน้าที่

๖๓.๒ กำหนดชื่อและรหัสผ่านให้แก่บุคคล/หน่วยงานใน ข้อ ๖๓.๑ เป็นรายบุคคล (Single Password) ห้ามใช้ร่วมกัน

๖๓.๓ กำหนดรอบระยะเวลาการเปลี่ยนรหัสผ่าน โดยกำหนดวันหมดอายุทุก ๙๐ วัน ยกเว้นอุปกรณ์หรือระบบงานที่ไม่สามารถกระทำได้ทางเทคนิค

๖๓.๔ ห้ามเก็บ (Save) รหัสผ่านไว้ในหน่วยความจำเพื่อใช้โดยปริยาย (default)

๖๓.๕ หากสงสัยว่ามีผู้อื่นรู้รหัสผ่านของตน ให้ดำเนินการเปลี่ยนรหัสผ่านทันที

๖๓.๖ การเปิดใช้รหัสผ่าน (Log in) ต้องมีการปิด (Log out) เมื่อเลิกใช้ ทุกครั้ง

๖๓.๗ การส่งมอบรหัสผ่าน ต้องดำเนินการในลักษณะชั้นความลับ “ลับที่สุด” ไม่จดหรือบันทึกรหัสผ่านไว้ในที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๖๓.๘ กรณีผู้ใช้ลืมรหัสผ่าน จะต้องดำเนินการตามมาตรการตรวจสอบและได้รับการยืนยันจากผู้ดูแลระบบ (admin) ก่อนจะออกรหัสผ่านให้ใหม่

๖๓.๙ ในกรณีการฝึกหัดศึกษา เจ้าหน้าที่เทคนิคภายนอกองค์กรจะได้รับชื่อและรหัสผ่านชั่วคราว และยกเลิกทันทีที่สิ้นสุดกำหนดการใช้งาน

ข้อ ๖๔ ห้ามติดตั้งซอฟต์แวร์หรือถ่ายเข้าข้อมูลจากภายนอกที่ไม่ได้ผ่านการตรวจสอบมัลแวร์หรือภัยคุกคามอื่น ๆ ที่ติดตาม รวมทั้งห้ามนำอุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมมาติดตั้งหรือใช้งานโดยพลการ หากเกิดการละเมิด ผู้เป็นเจ้าหน้าที่ประจำเครื่องนั้น ๆ เป็นผู้รับผิดชอบ

ข้อ ๖๕ ผู้ใช้เครื่องคอมพิวเตอร์ส่วนบุคคล ต้องทำการสำเนาข้อมูลเครื่องนั้น ๆ ด้วยตนเอง เพื่อสามารถกู้คืนสภาพได้ โดยไม่ต้องทำเป็นส่วนรวม และต้องปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ครอบครองใช้งานประจำเมื่อเสร็จสิ้นภารกิจหรือหยุดการใช้งานเกินกว่า ๑ ชั่วโมง ยกเว้นเครื่องให้บริการส่วนรวม (Server) ที่ต้องเปิดตลอด ๒๔ ชั่วโมง

ข้อ ๖๖ ห้ามปรับแต่งหรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันมัลแวร์ที่กำหนดติดตั้งใช้งานบนเครื่องคอมพิวเตอร์โดยพลการ

หมวด ๙

การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

ข้อ ๖๗ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

๖๗.๑ เมื่อตรวจพบหรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ หรือพบสิ่งผิดปกติเกิดขึ้นในระบบสารสนเทศ หรือมีการเข้าถึงระบบสารสนเทศโดยผู้ไม่มีอำนาจหน้าที่ ให้ผู้ตรวจพบ รวบรวมข้อมูลผู้บังคับบัญชา และแจ้งให้นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งกำลังบำรุงทหาร ทราบโดยทันที

๖๗.๒ นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งกำลังบำรุงทหาร ดำเนินการ ดังต่อไปนี้

๖๗.๒.๑ ลดความเสียหายเบื้องต้น โดยการระงับใช้ แก๊ซ หรือยกเลิกระบบ สารสนเทศนั้น หากเป็นสารสนเทศที่มีการกำหนดชั้นความลับ จะต้องแจ้งให้เจ้าของเรื่องสารสนเทศที่มีชั้นความลับนั้น ทราบเพื่อพิจารณายกเลิกชั้นความลับโดยทันที

๖๗.๒.๒ รายงานขั้นต้นต่อเจ้ากรมส่งกำลังบำรุงทหาร โดยทันที และรายงาน ตามลำดับชั้นถึงผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง กองบัญชาการกองทัพไทย หากพบว่า เป็นการละเมิดต่อสารสนเทศที่กำหนดชั้นความลับ หรืออาจกระทบกับส่วนราชการอื่น หรือเกินขีดความสามารถ ในการจัดการของหน่วย

๖๗.๒.๓ สืบหาความเสียหายที่เกิดจากการละเมิด ตรวจสอบสาเหตุและจุดอ่อน หรือข้อบกพร่องที่ก่อให้เกิดการละเมิดในเบื้องต้น

๖๗.๒.๔ รายงานสรุปเหตุการณ์ที่เกิดขึ้นให้ผู้บริหารความมั่นคงปลอดภัย สารสนเทศระดับสูง กองบัญชาการกองทัพไทยทราบ พร้อมทั้งแนวทางป้องกันมิให้เกิดการละเมิดซ้ำ

ข้อ ๖๘ ความรับผิดชอบของกรมส่งกำลังบำรุงทหาร ที่มีต่อผู้ละเมิดการรักษาความปลอดภัย

๖๘.๑ ลงโทษทางวินัยผู้ละเมิดและผู้รับผิดชอบต่อการละเมิดตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำ ในกรณีที่ผู้ละเมิดเป็นบุคคลภายนอกให้หน่วยเกี่ยวข้องดำเนินการตามกฎหมาย ต่อไป

๖๘.๒ หากก่อให้เกิดความเสียหายต่อทางราชการอย่างร้ายแรงหรือเข้าข่ายความผิด ตามกฎหมาย ให้ส่งตัวไปดำเนินคดีตามกฎหมายต่อไป

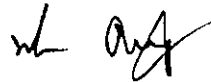
๖๘.๓ พิจารณาข้อมูลสารสนเทศที่มีการกำหนดชั้นความลับที่อยู่ในความรับผิดชอบ หากได้รับความเสียหายหรือได้รับผลกระทบ ต้องดำเนินการแก้ไขโดยเร็วที่สุด

/๖๘.๔ กำหนด...

๖๘.๔ กำหนดมาตรการป้องกันเพิ่มเติม เพื่อขจัดความเสียหายที่เกิดจากการละเมิดซ้ำ หรือเปลี่ยนแปลงวิธีการปฏิบัติ ยกเลิกโปรแกรม และอื่น ๆ

ข้อ ๖๙ สำหรับมาตรการรักษาความปลอดภัยอื่นใดที่มีได้กล่าวไว้ในระเบียบนี้ ให้ยึดถือตาม ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และที่แก้ไขเพิ่มเติม รวมทั้งระเบียบคำสั่งของทางราชการที่เกี่ยวข้องโดยเคร่งครัด

ประกาศ ณ วันที่ ๖ เมษายน พ.ศ.๒๕๖๑

พลเรือโท 

(ทิวา ดาราเมือง)

เจ้ากรมส่งกำลังบำรุงทหาร

กองบริหารสิ่งอุปกรณ์ทางทหาร