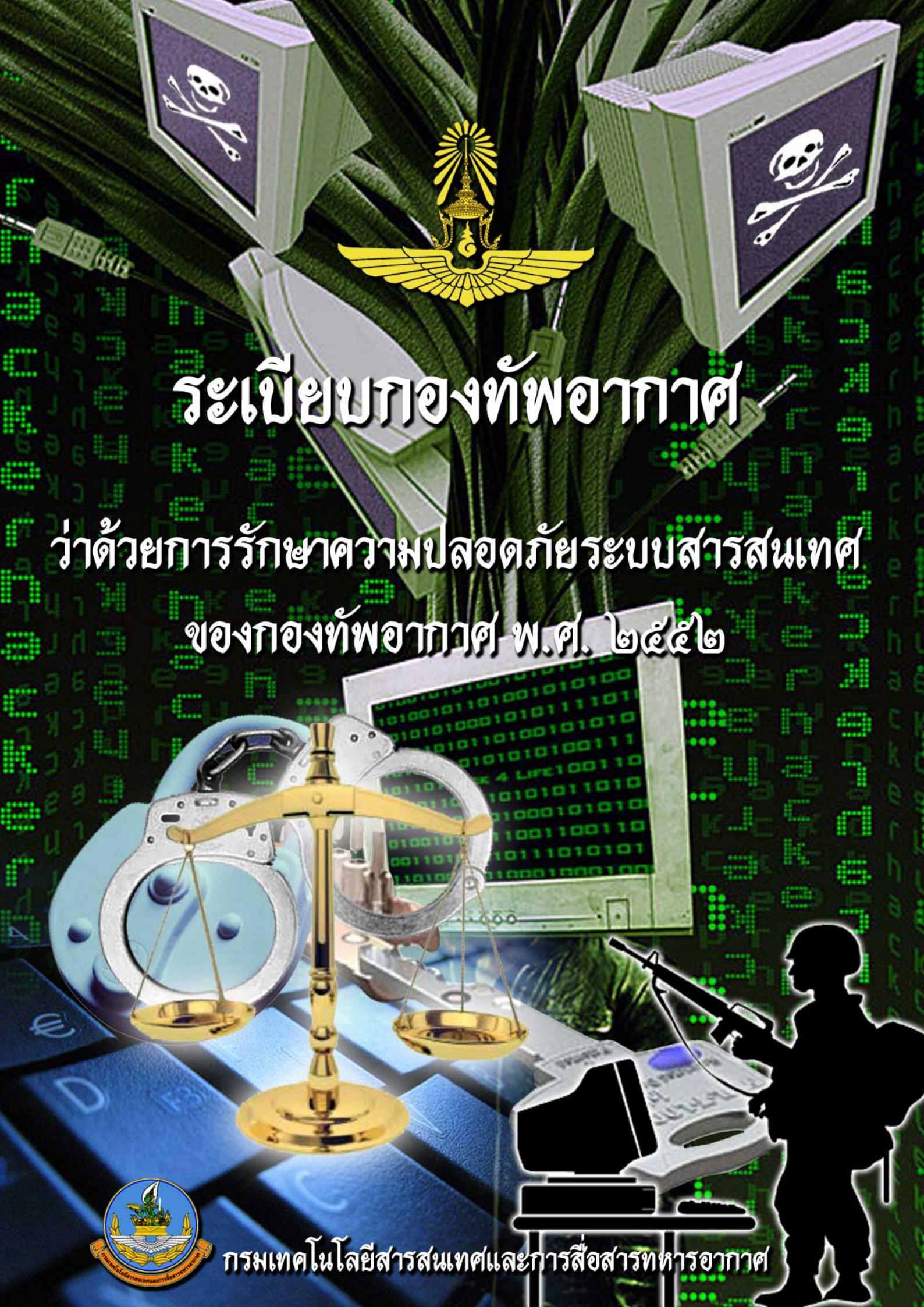

ระเบียบกองทัพอากาศ

ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. ๒๕๕๒

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ระเบียบกองทัพอากาศ
ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ
พ.ศ.๒๕๕๒

(สำเนา)

บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(กคส. โทร.๒-๑๔๔๑)

ที่ กห ๐๖๐๙.๗/๙๐๔ **วันที่** ๒๘ ก.ย.๕๒

เรื่อง ขออนุมัติใช้ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๕๒

เรียน ผบ.ทอ.

๑. ตามคำสั่ง ทอ.(เฉพาะ) ลับ ที่ ๔๐/๕๒ ลง ๑ เม.ย.๕๒ เรื่องแก้อัตรา ทอ.ให้ยกเลิกอัตรา ทอ.๓๙ และให้ใช้อัตรา ทอ.๕๒ อีกทั้งเทคโนโลยีสารสนเทศเปลี่ยนแปลงอย่างรวดเร็ว ส่งผลให้ระเบียบ ทอ. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๔๓ มีการเปลี่ยนแปลง จึงเห็นสมควรปรับปรุงแก้ไขระเบียบ ฯ ดังกล่าว เพื่อให้มีความสอดคล้องและเหมาะสมกับสภาวะการณ์ปัจจุบัน

๒. ทสส.ทอ.ได้ร่างระเบียบ ฯ เสนอให้ส่วนราชการ ทอ. ที่เกี่ยวข้อง ตรวจสอบความถูกต้องและความเหมาะสมแล้ว อีกทั้งเสนอให้ สบ.ทอ.ตรวจสอบความถูกต้องของหนังสือราชการ และให้ สธน.ทอ. ตรวจสอบการบังคับใช้ทางกฎหมาย พบว่ามีความถูกต้องไม่ขัดต่อกฎหมายและสามารถใช้บังคับได้

๓. ทสส.ทอ.พิจารณาแล้ว เพื่อให้การดำเนินการด้านการรักษาความปลอดภัยระบบสารสนเทศของ ทอ.เป็นไปด้วยความเรียบร้อย สมความมุ่งหมายของทางราชการ จึงเห็นสมควรยกเลิก ระเบียบ ทอ. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๔๓ และใช้ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ.พ.ศ.๒๕๕๒ ที่แนบแทน

จึงเรียนมาเพื่อพิจารณาอนุมัติตามข้อ ๓ และลงนามในระเบียบ ฯ ที่แนบให้ต่อไป

(ลงชื่อ) พล.อ.ต. โสภณ สรรพนุเคราะห์
จก.ทสส.ทอ.

(ลงชื่อ) พล.อ.ท. ทรงธรรม โชคคณาพิทักษ์
ผช.เสธ.ทอ.ฝยก.
๕ ต.ค.๕๒

(ลงชื่อ) พล.อ.ท. วินัย เปล่งวิทยา
รอง เสธ.ทอ.
๑๒ ต.ค.๕๒

เรียน ผบ.ทอ.

กระผมพิจารณาแล้ว เห็นสมควรอนุมัติ ตามข้อ ๓ และลงชื่อในระเบียบ ทอ. ที่แนบ

(ลงชื่อ) พล.อ.อ. ประจิน จั่นตอง
เสธ.ทอ.
๒๖ ต.ค.๕๒

อนุมัติตามข้อ ๓
ลงชื่อแล้ว

(ลงชื่อ) พล.อ.อ. อิทธพร ศุภวงศ์
ผบ.ทอ.
๒๐ พ.ย.๕๒

สำเนาถูกต้อง
น.อ.
(ธคุณ มุ่งเพียร)
รอง จก.ทสส.ทอ.
พ.ย.๕๒

นางเสมอดาว ฯ พิมพ์/ทาน
น.อ.ณัฐพล ฯ ตรวจ

ระเบียบกองทัพอากาศ

ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

พ.ศ. ๒๕๕๒

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศเป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. ๒๕๕๒”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ การดำเนินการรักษาความปลอดภัยตามระเบียบนี้ให้ยึดถือและปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ.๒๕๒๕ ระเบียบกระทรวงกลาโหมว่าด้วยการรักษาความปลอดภัยหน่วยกรรมวิธีข้อมูลอัตโนมัติ พ.ศ.๒๕๒๘ ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒ เป็นมูลฐาน

ข้อ ๔ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. ๒๕๔๓

บรรดาระเบียบ และคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัด หรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

สำหรับมาตรการรักษาความปลอดภัยอื่นใดที่มิได้กล่าวไว้ในระเบียบนี้ ให้ยึดถือตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒

ข้อ ๕ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานราชการ และลูกจ้างของกองทัพอากาศ ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพอากาศ

ข้อ ๖...

ข้อ ๖ ในระเบียบนี้

๖.๑. “ระบบสารสนเทศ” (Information System) หมายความว่า ระบบที่ประกอบด้วย คน ระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร ข้อมูล และกระบวนการ (Process) โดยกระบวนการนั้นได้แก่ วิธีการในการเก็บข้อมูล ประมวลผลข้อมูลเพื่อที่จะเปลี่ยนข้อมูลให้เป็นสารสนเทศ และเผยแพร่ข้อมูลให้อยู่ในลักษณะของสารสนเทศของผู้ใช้ต้องการ

๖.๒ “คอมพิวเตอร์” (Computer) หมายความว่า เครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์ที่มีความสามารถในการคำนวณอัตโนมัติตามคำสั่ง ส่วนที่ใช้ประมวลผลเรียกว่าหน่วยประมวลผล ชุดของคำสั่งที่ระบุขั้นตอนการคำนวณเรียกว่าโปรแกรมคอมพิวเตอร์ ผลลัพธ์ที่ได้ออกมานั้นอาจเป็นได้ทั้ง ตัวเลข ข้อความ รูปภาพ เสียง หรืออยู่ในรูปอื่น ๆ โดยอาจมีลักษณะเป็น คอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์เคลื่อนที่ โทรศัพท์แบบฉลาด (Smart Phone) ตลอดจน ระบบคอมพิวเตอร์ฝังตัว (Embedded Computer) เป็นต้น

๖.๓ “ภัย” (Threat) หมายความว่า อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยคน (Person) สิ่งต่าง ๆ (Thing) หรือเหตุการณ์ (Event) ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูลข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่น ๆ ตามความต้องการของภัย นั้น

๖.๔ “ความอ่อนแอ” (Vulnerability) หมายความว่า จุดอ่อน หรือข้อบกพร่องใด ๆ ก็ตามของระบบสารสนเทศที่ภัยในรูปแบบที่เหมาะกัน สามารถนำไปใช้ประโยชน์ เพื่อก่อให้เกิดอันตรายต่อระบบสารสนเทศนั้น ๆ ได้

๖.๕ “ความเสี่ยง” (Risk) หมายความว่า โอกาสของการเกิดภัยในรูปแบบที่เหมาะกับความอ่อนแอ ที่มีอยู่ของระบบสารสนเทศ และความรุนแรงที่เกิดจากภัยนั้น ซึ่งภัยประเภทเดียวกันอาจมีระดับความเสี่ยงไม่เท่ากัน ในแต่ละพื้นที่ใช้งานระบบสารสนเทศ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่า ณ พื้นที่ใช้งานระบบสารสนเทศ แต่ละแห่งควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่นเพียงใด

๖.๖ “ประเมินความเสี่ยง” (Risk Assessment) หมายความว่า กระบวนการวิเคราะห์ภัยและความอ่อนแอของระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป

๖.๗ “ระบบสื่อสารข้อมูล” (Data Communication System) หมายความว่า ระบบที่ประกอบด้วยผู้รับ ผู้ส่ง และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล เช่น ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น ทั้งระบบวงจรมีสายและไร้สาย

๖.๘ “ระบบ...

๖.๘ “ระบบคอมพิวเตอร์” (Computer System) หมายความว่า ระบบที่ประกอบด้วยส่วนเครื่อง (Hardware) ส่วนชุดคำสั่ง (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware) ที่ใช้ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ

๖.๙ “สารสนเทศ” (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ เป็นต้น และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๖.๑๐ “พื้นที่ใช้งานระบบสารสนเทศ” (Information System Workspaces) หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ หรือเตรียมข้อมูลเก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้ง เครื่องคอมพิวเตอร์ส่วนบุคคลที่ติดตั้งประจำโต๊ะทำงาน

๖.๑๑ “เครือข่ายระบบสารสนเทศ” หมายความว่า การติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่างระบบสารสนเทศของกองทัพอากาศ ทั้งระบบสารสนเทศเพื่อการสนับสนุน (Support Information System: SIS) และระบบสารสนเทศเพื่อการยุทธ (Combat Information System: CIS) ตัวอย่างเช่น ระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link: TDL) ระบบป้องกันทางอากาศอัตโนมัติ (Royal Thai Air Defense System: RTADS) ระบบบัญชาการและควบคุมทางอากาศ (Air Command and Control System : ACCS) ระบบสารสนเทศเพื่อการบริหาร (Management Information System: MIS) ของส่วนราชการต่าง ๆ ระบบสารสนเทศสำหรับผู้บังคับบัญชาระดับสูง (Executive Information System: EIS) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๖.๑๒ “สารสนเทศที่กำหนดชั้นความลับ” หมายความว่า สารสนเทศในรูปข้อมูลหรือข่าวสารที่บันทึกไว้ในแบบใด ๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหาจำกัดการเข้าถึงหรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงจานบันทึก ประมวลลับ รหัส และรหัสผ่านที่กำลังใช้อยู่ หรือเตรียมจะใช้ ตลอดจนวัสดุ หรือเอกสารทุกอย่างที่บันทึกเรื่องดังกล่าว

๖.๑๓ “การรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า การดำเนินการเพื่อให้ระบบสารสนเทศมีคุณสมบัติดังนี้ มีการรักษาความลับของข้อมูล (Confidentiality) ให้เข้าถึงได้สำหรับผู้ที่มีสิทธิเท่านั้น มีการคงสภาพความถูกต้อง และความน่าเชื่อถือของข้อมูล (Integrity) โดยไม่มีการเปลี่ยนแปลงจากผู้ไม่มีสิทธิ และการเปลี่ยนแปลงที่ผิดพลาดจากผู้มีสิทธิ มีสภาพพร้อมใช้งาน (Availability) สามารถให้บริการต่อเนื่องอย่างมีเสถียรภาพ และเมื่อเกิดปัญหาสามารถกู้กลับคืนมาได้

๖.๑๔ “คณะ...

๖.๑๔ “คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า คณะกรรมการที่ได้รับการแต่งตั้งจากผู้บังคับบัญชา เพื่อช่วยในการบริหารและจัดดำเนินการงานด้านการรักษาความปลอดภัยระบบสารสนเทศของหน่วยงาน หรือของระบบตามสายงาน

๖.๑๕ “นายทหารรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า นายทหารสัญญาบัตรที่ได้รับการคัดเลือกและแต่งตั้ง ให้เป็นนายทหารรักษาความปลอดภัยระบบสารสนเทศ

๖.๑๖ “ผู้ปฏิบัติหน้าที่ด้านระบบสารสนเทศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า ผู้ที่เกี่ยวข้องกับการจัดการระบบสารสนเทศในด้านต่าง ๆ เช่น ผู้บริหารระบบ (System Administrator) ผู้บริหารฐานข้อมูล (Database Administrator) ผู้บริหารเครือข่าย (Network Administrator) ผู้เขียนโปรแกรม (Programmer)

ข้อ ๗ ให้เจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ รักษาการให้เป็นไปตามระเบียบนี้ และมีอำนาจกำหนดระเบียบปลีกย่อย คู่มือ คำแนะนำ หรือรายการปฏิบัติ โดยไม่ขัดหรือแย้งกับระเบียบนี้ได้ตามความจำเป็น

หมวด ๑
กล่าวทั่วไป
ส่วนที่ ๑
ความมุ่งหมาย

ข้อ ๘ ระเบียบนี้มีความมุ่งหมายเพื่อ

๘.๑ กำหนดหลักการ และมาตรการป้องกันภัยของระบบสารสนเทศของกองทัพอากาศ

๘.๒ พิทักษ์รักษา และป้องกันสารสนเทศที่กำหนดชั้นความลับ มิให้รั่วไหล หรือรู้ไปถึงหรือตกไปอยู่กับบุคคลผู้ไม่มีอำนาจหน้าที่ที่จะต้องทราบ

๘.๓ พิทักษ์รักษา และป้องกันการก่อวินาศกรรมแก่ระบบสารสนเทศของกองทัพอากาศในส่วนที่เป็นระบบคอมพิวเตอร์ และระบบสื่อสารข้อมูล

ส่วนที่ ๒
การแบ่งมอบความรับผิดชอบในการดำเนินงานด้านการรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๙ เพื่อให้การดำเนินงานในการรักษาความปลอดภัยระบบสารสนเทศที่มีประสิทธิภาพ จึงแบ่งมอบความรับผิดชอบดังนี้

๙.๑ ให้...

๙.๑ ให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ในฐานะส่วนราชการที่ทำหน้าที่ฝ่ายอำนวยการด้านเทคโนโลยีสารสนเทศและสงครามสารสนเทศ ซึ่งรวมถึง การรักษาความปลอดภัยระบบสารสนเทศ มีหน้าที่รับผิดชอบ กำหนดมาตรการ แนวทางปฏิบัติ ตรวจสอบ แจ้งเตือนภัยที่เกี่ยวข้องกับระบบสารสนเทศในกองทัพอากาศ

๙.๒ ให้ส่วนราชการที่รับผิดชอบระบบในสายงานต่าง ๆ กำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการ และแต่งตั้งนายทหารรักษาความปลอดภัยระบบสารสนเทศและคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ โดยแบ่งออกเป็น ๒ ประเภท ดังนี้

๙.๒.๑ นายทหารรักษาความปลอดภัยระบบสารสนเทศและคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงาน มีหน้าที่รับผิดชอบ ในการดูแลรักษาความปลอดภัยระบบสารสนเทศที่มีการติดตั้งใช้งานภายในกองทัพอากาศ ทั้งระบบสารสนเทศเพื่อการบริหาร และระบบสารสนเทศเพื่อการยุทธ

๙.๒.๒ นายทหารรักษาความปลอดภัยระบบสารสนเทศและคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของหน่วย มีหน้าที่รับผิดชอบ ในการดูแลรักษาความปลอดภัยระบบสารสนเทศเฉพาะภายในหน่วยงานตนเอง แต่หากระบบ นั้นมีการเชื่อมต่อกับระบบสารสนเทศของระบบงาน ก็จะทำหน้าที่ตามที่คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงานกำหนด

ข้อ ๑๐ การกำหนดชั้นความลับของสารสนเทศ ให้เป็นไปตามกฎหมาย หรือระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ หรือระเบียบอื่นใดที่กำหนดไว้เป็นอย่างอื่น

หมวด ๒
การรักษาความปลอดภัยสภาพแวดล้อมของระบบสารสนเทศ และการจัดการด้านการรักษาความปลอดภัยระบบสารสนเทศ
(Physical Security and Administrative Security)

ข้อ ๑๑ การรักษาความปลอดภัยสภาพแวดล้อมของระบบสารสนเทศและการจัดการด้านการรักษาความปลอดภัยระบบสารสนเทศ เป็นมาตรการรักษาความปลอดภัยทางด้านกายภาพ บุคคล และการจัดการของระบบสารสนเทศ ที่ช่วยสนับสนุนให้เกิดความปลอดภัยในสภาพแวดล้อมของระบบสารสนเทศที่กำลังดำเนินการป้องกันอยู่ในขณะนั้น

ส่วนที่ ๑

การรักษาความปลอดภัยเกี่ยวกับบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ

(Personnel Security)

ข้อ ๑๒ การรักษาความปลอดภัยเกี่ยวกับบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ มีความมุ่งหมาย เพื่อตรวจสอบบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ และเพื่อกำหนดระดับความไว้วางใจที่ให้ปฏิบัติหน้าที่เกี่ยวกับข้อมูล ซึ่งเป็นความลับของทางราชการ ตลอดจนควบคุมบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๓ ให้ส่วนราชการต้นสังกัดดำเนินการตรวจสอบความไว้วางใจโดยละเอียดผ่านกรมข่าวทหารอากาศ และให้หัวหน้าส่วนราชการนั้น ๆ รับรองความไว้วางใจบุคคล ก่อนที่จะมอบหมายให้บุคคลใดปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ โดยยึดถือผลการตรวจสอบประวัติ และพฤติการณ์ของบุคคลนั้น เป็นแนวทางการพิจารณาตามที่เห็นสมควร ในกรณีจำเป็นเร่งด่วนหัวหน้าส่วนราชการอาจรับรองความไว้วางใจบุคคลได้ โดยไม่ต้องรอผลการตรวจสอบประวัติ โดยมีเงื่อนไขว่าหากผลการตรวจสอบประวัติปรากฏว่าผู้นั้นมีประวัติ หรือพฤติการณ์ไม่เหมาะสม ให้ผู้ที่ได้รับการมอบหมายพ้นจากการปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศทันที

บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศโดยตรง เข้ามาทำงานเป็นประจำภายในพื้นที่ใช้งานระบบสารสนเทศ เช่น เจ้าหน้าที่รับ - ส่งหนังสือราชการ พนักงานทำความสะอาด หรือบุคคลอื่น ๆ ต้องทำการตรวจสอบประวัติ ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ข้อ ๒๕ ด้วย และให้กำหนดช่วงเวลาทำงานที่แน่นอนของบุคคลดังกล่าว ในระหว่างนั้น ต้องมีเจ้าหน้าที่ประจำพื้นที่ใช้งานระบบสารสนเทศควบคุมดูแลอยู่ด้วยอย่างน้อย ๑ คน

ข้อ ๑๔ ให้ส่วนราชการชี้แจงในเรื่องการรักษาความปลอดภัยตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ และเรื่องการรักษาความปลอดภัยเกี่ยวกับระบบสารสนเทศของกองทัพอากาศ ตามระเบียบนี้ แก่บุคคลที่จะปฏิบัติในหน้าที่เกี่ยวกับระบบสารสนเทศ

นายทหารรักษาความปลอดภัยระบบสารสนเทศ ตามข้อ ๙ ต้องมีความรู้เกี่ยวกับคอมพิวเตอร์ หรือระบบสารสนเทศ โดยจะต้องผ่านการอบรมเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศมาก่อน และจะต้องไม่ได้รับมอบหมายให้รับผิดชอบต่อภารกิจอื่นที่เป็นอุปสรรค หรือเป็นภัยต่อการรักษาความปลอดภัยระบบสารสนเทศ เมื่อได้รับมอบหมายให้ปฏิบัติหน้าที่การรักษาความปลอดภัยระบบสารสนเทศแล้วต้องปฏิบัติหน้าที่ด้วยความซื่อสัตย์ อดทน เสียสละ

ข้อ ๑๕...

ข้อ ๑๕ ให้ส่วนราชการที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศจัดทำทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศตามระดับความไว้วางใจที่แต่ละบุคคลได้รับอนุมัติ และสำเนาส่งให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ทราบด้วย

ข้อ ๑๖ เมื่อบุคคลใดพ้นจากหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ส่วนราชการนั้นตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ และสำเนาส่งให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ทราบด้วย

ข้อ ๑๗ ให้หัวหน้าส่วนราชการ หรือผู้ที่ได้รับมอบหมาย หรือนายทหารรักษาความปลอดภัยระบบสารสนเทศ ชี้แจงให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศได้ทราบถึงความเสียหายต่อความมั่นคงของชาติ ทัณฑ์ทางวินัยในการเปิดเผยความลับของทางราชการ รวมทั้งโทษตามกฎหมายในการเปิดเผยความลับของทางราชการแก่บุคคลผู้ไม่มีหน้าที่เกี่ยวข้องทราบ

ข้อ ๑๘ เมื่อบุคคลใดจะเข้าปฏิบัติหน้าที่ หรือพ้นหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ลงชื่อในใบบันทึกรับรองการรักษาความลับเมื่อเข้ารับตำแหน่งหรือหน้าที่ (รปภ.๑๗) หรือใบรับรองการรักษาความลับเมื่อพ้นตำแหน่งหรือหน้าที่ (รปภ.๑๘) แล้วแต่กรณี ตามที่กำหนดไว้ในระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ข้อ ๒๘, ๒๙, ๓๑ และข้อ ๕๕

ข้อ ๑๙ บุคคลอื่นใดไม่สามารถอ้างยศ ตำแหน่ง หรืออำนาจ เพื่อขอทราบ หรือให้ได้มาซึ่งข้อมูลที่ตนไม่ได้รับอนุญาต

ข้อ ๒๐ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ ควบคุม ดูแล และตรวจสอบสิทธิการเข้าถึงระบบสารสนเทศต่าง ๆ ในขอบเขตที่รับผิดชอบ

บุคคลที่จะเข้าใช้ระบบสารสนเทศจะต้องได้รับอนุญาตจากผู้มีอำนาจหน้าที่ก่อน และการเข้าถึงระบบสารสนเทศต้องคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

บุคคลที่ไม่มีอำนาจหน้าที่ จะอนุญาตให้บุคคลอื่นเข้าถึงระบบสารสนเทศไม่ได้

ข้อ ๒๑ หากเจ้าหน้าที่ หรือบุคคลผู้ใดมีพฤติการณ์ไม่น่าไว้วางใจหรืออาจเป็นภัยต่อระบบสารสนเทศ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ รีบรายงานตามลำดับชั้นถึง กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อดำเนินการตามมาตรการรักษาความปลอดภัยและข้อกฎหมายที่เกี่ยวข้องต่อไป

ส่วนที่ ๒...

ส่วนที่ ๒
การรักษาความปลอดภัยอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ
(Building and Workspace Security)

ข้อ ๒๒ การรักษาความปลอดภัยอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ มีความมุ่งหมาย เพื่อกำหนดมาตรการควบคุมและป้องกันภัยเกี่ยวกับสถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศ เพิ่มเติมจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ระเบียบกระทรวงกลาโหมว่าด้วยการรักษาความปลอดภัยหน่วยกรรมวิธีข้อมูลอัตโนมัติ พ.ศ.๒๕๒๘ และระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒

ข้อ ๒๓ ให้ส่วนราชการกำหนดให้ อาคาร สถานที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศอื่นใด เป็นพื้นที่หวงห้าม โดยพิจารณาตามความสำคัญว่าจะต้องพิทักษ์รักษาสิ่งที่เป็นความลับของระบบสารสนเทศในระดับใด โดยกำหนดเป็น “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ” แล้วแต่กรณี

พื้นที่ใช้งานระบบสารสนเทศในส่วนที่เป็นหน่วยแสดงผล ต้องปลอดภัยจากการได้ยินและการมองเห็นของผู้ไม่มีอำนาจหน้าที่ที่จะเข้าถึง ทั้งนี้รวมถึงการบันทึกภาพจากกล้องวงจรปิด และให้กำหนดมาตรการควบคุมบุคคลก่อนจะเข้าพื้นที่หวงห้ามอีกชั้นหนึ่งด้วย

ให้ส่วนราชการพิจารณากำหนดมาตรการป้องกันเพิ่มเติมให้เหมาะสม เช่น ห้ามนำอุปกรณ์สื่อสาร ถ่ายภาพ หรืออุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ได้ (Removable Storage Device) เข้าไปภายใน “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ”

ข้อ ๒๔ การปฏิบัติในเวลาฉุกเฉิน

๒๔.๑ อาคาร สถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศที่จัดให้มีเวร - ยามรักษาการณ์เพื่อพิทักษ์รักษาระบบสารสนเทศโดยเฉพาะแล้ว ให้ถือว่าเป็นการปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒ ข้อ ๖๔

๒๔.๒ ให้ส่วนราชการเจ้าของอาคาร สถานที่ จัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนป้องกันอัคคีภัยของระบบสารสนเทศ แผนเผชิญเหตุ (Contingency Plan) โดยเตรียมอุปกรณ์สนับสนุนในการเคลื่อนย้าย และทำลายไว้ให้พร้อมที่จะปฏิบัติได้ทันท่วงที และชี้แจงให้เจ้าหน้าที่ผู้เกี่ยวข้องเข้าใจวิธี และขั้นตอนปฏิบัติ โดยยึดแนวทางปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒ ข้อ ๗

๒๔.๓...

๒๔.๓ หากสถานการณ์รุนแรงจนไม่สามารถพิทักษ์รักษาระบบสารสนเทศให้ปลอดภัยได้ ให้ใช้แผนการเคลื่อนย้าย และแผนการทำลายระบบสารสนเทศในเวลาฉุกเฉิน

๒๔.๔ เพื่อมิให้ส่วนใดส่วนหนึ่งของระบบสารสนเทศที่กำหนดชั้นความลับตกไปอยู่ในความครอบครองของฝ่ายตรงข้าม หรือผู้ไม่มีอำนาจหน้าที่ ให้ทำลายตามลำดับความสำคัญชั้นลับที่สุดก่อน

๒๔.๕ ให้ส่วนราชการเจ้าของอาคาร สถานที่ กำหนดมาตรการการป้องกันอัคคีภัย พร้อมจัดเตรียมอุปกรณ์ในการดับเพลิง สำหรับระบบคอมพิวเตอร์ มาตรการป้องกันภัยธรรมชาติพร้อมจัดเตรียมอุปกรณ์ป้องกันภัยธรรมชาติสำหรับระบบคอมพิวเตอร์ จัดเตรียมสถานที่ วัสดุ อุปกรณ์ที่จำเป็นสำหรับการฟื้นฟูระบบ รวมทั้งสถานที่เก็บรักษาสำรองข้อมูลที่ปลอดภัย

ส่วนที่ ๓
การจัดการการรักษาความปลอดภัยระบบสารสนเทศ
(Information System Security Management)

ข้อ ๒๕ การจัดการการรักษาความปลอดภัยระบบสารสนเทศ มีความมุ่งหมาย เพื่อกำหนดแนวทางการจัดการสำหรับผู้เกี่ยวข้องในระดับของส่วนราชการ และกองทัพอากาศ ในการพิจารณามาตรการควบคุม และป้องกันภัยระบบสารสนเทศที่เหมาะสมกับสภาพแวดล้อมของแต่ละระบบ

ข้อ ๒๖ การกำหนดมาตรการ หรือระบบการรักษาความปลอดภัย ต้องผ่านการประเมินความเสี่ยง (Risk Assessment) ความอ่อนแอ (Vulnerability) ภัย (Threat) ระบบสารสนเทศ เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับสภาพแวดล้อมของแต่ละระบบ โดยการทำแผนจัดการความเสี่ยง (Risk Management Plan)

ข้อ ๒๗ การรักษาความปลอดภัยระบบสารสนเทศ ต้องดำเนินการป้องกันให้ถึงระดับที่สมดุลกับความเสี่ยงของระบบสารสนเทศที่ประเมินได้

ข้อ ๒๘ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ในฐานะหน่วยงานที่รับผิดชอบงานด้านการรักษาความปลอดภัยระบบสารสนเทศ มีหน้าที่ดังนี้

๒๘.๑ กำหนดและรักษานโยบายการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

๒๘.๒ เสนอแนะการแต่งตั้งนายทหารรักษาความปลอดภัยระบบสารสนเทศตามข้อ ๙

๒๘.๓...

๒๘.๓ กำหนดหน้าที่รับผิดชอบเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

๒๘.๔ ประเมินความเสี่ยงของระบบสารสนเทศ เพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

๒๘.๕ พัฒนาหลักการ และกระบวนการด้านการรักษาความปลอดภัยระบบสารสนเทศและประสานงานด้านการรักษาความปลอดภัยระบบสารสนเทศกับกองบัญชาการกองทัพไทยและหน่วยงานอื่นที่เกี่ยวข้อง

๒๘.๖ สนับสนุนและส่งเสริมให้มีการศึกษาหลักสูตรการรักษาความปลอดภัยระบบสารสนเทศ

๒๘.๗ ให้มีการฝึกอบรม สัมมนาและดูงาน เกี่ยวกับงานด้านการรักษาความปลอดภัยระบบสารสนเทศ

๒๘.๘ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยที่เกี่ยวข้องกับระบบสารสนเทศ

๒๘.๙ ดำเนินการตรวจเยี่ยม เพื่อทำการตรวจสอบความปลอดภัยของระบบสารสนเทศ (IT Security Audit) เพื่อพิจารณาให้คำแนะนำ ติดตามและประเมินผลในการปฏิบัติตามนโยบายและแผนการรักษาความปลอดภัยระบบสารสนเทศ

๒๘.๑๐ รายงานอันตรายที่อาจเกิดขึ้น หรือที่เกิดขึ้นแล้วกับระบบสารสนเทศของกองทัพอากาศ ให้แก่ผู้บัญชาการทหารอากาศ หรือผู้ที่ได้รับมอบหมายจากผู้บัญชาการทหารอากาศ

๒๘.๑๑ ตรวจสอบหาหลักฐาน เมื่อมีการละเมิดเพื่อการดำเนินการทางกฎหมายต่อไป

ข้อ ๒๙ นายทหารรักษาความปลอดภัยระบบสารสนเทศ ซึ่งแต่งตั้งโดยหัวหน้าหน่วยขึ้นตรงกองทัพอากาศ มีหน้าที่ดังนี้

๒๙.๑ นายทหารรักษาความปลอดภัยระบบสารสนเทศของระบบงาน มีหน้าที่

๒๙.๑.๑ กำหนดมาตรการป้องกันสำหรับพื้นที่ที่กำหนดให้มีการรักษาความปลอดภัยตาม ข้อ ๒๓ ตามผลการประเมินความเสี่ยงของระบบสารสนเทศ และแจ้งให้ผู้เกี่ยวข้องทราบ

๒๙.๑.๒ ควบคุม ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ทั้งหมดของระบบงาน

๒๙.๑.๓ ควบคุมและตรวจสอบการติดตั้งโปรแกรมเข้าสู่ระบบสารสนเทศให้เป็นไปตามความมุ่งหมายของทางราชการ

๒๙.๑.๔...

๒๙.๑.๔ ควบคุม กำกับ ดูแลการเข้าใช้เครือข่ายระบบสารสนเทศในส่วนที่เกี่ยวข้องให้เป็นไปตามหน้าที่ความรับผิดชอบกำหนด และแจ้งให้นายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วยทราบ

๒๙.๑.๕ รับผิดชอบการตรวจสอบไวรัสคอมพิวเตอร์ รวมทั้งมาตรการป้องกันและการปรับแก้ไข

๒๙.๑.๖ ศึกษา ค้นคว้า และติดตามข้อมูลข่าวสารเกี่ยวกับการค้นพบจุดอ่อนของระบบต่าง ๆ หรือภัยรูปแบบใหม่ ๆ ของระบบสารสนเทศ เพื่อปรับปรุงมาตรการป้องกันให้ทันสมัยเสมอ

๒๙.๑.๗ พัฒนากระบวนการรักษาความปลอดภัยร่วมกับกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๒๙.๑.๘ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยที่เกี่ยวข้องภายในส่วนราชการ

๒๙.๑.๙ ให้คำแนะนำกับผู้เกี่ยวข้องให้มีความรู้และปฏิบัติตามกระบวนการรักษาความปลอดภัย

๒๙.๑.๑๐ ให้คำแนะนำกับคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงานในการจัดทำแผนต่าง ๆ ที่เกี่ยวข้อง

๒๙.๒ นายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วย มีหน้าที่

๒๙.๒.๑ กำหนดมาตรการป้องกันสำหรับพื้นที่ที่กำหนดให้มีการรักษาความปลอดภัยตาม ข้อ ๒๓ ตามผลการประเมินความเสี่ยงของระบบสารสนเทศ และแจ้งให้ผู้เกี่ยวข้องทราบ

๒๙.๒.๒ ควบคุม ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ทั้งหมดของส่วนราชการ และหากมีการเชื่อมต่อกับระบบสารสนเทศของระบบงาน ต้องปฏิบัติตามคำแนะนำของนายทหารรักษาความปลอดภัยระบบสารสนเทศของระบบงานโดยเคร่งครัด

๒๙.๒.๓ ควบคุมและตรวจสอบการติดตั้งโปรแกรมเข้าสู่ระบบสารสนเทศให้เป็นไปตามความมุ่งหมายของทางราชการ

๒๙.๒.๔ ควบคุม กำกับ ดูแลการเข้าใช้เครือข่ายระบบสารสนเทศให้เป็นไปตามที่ส่วนราชการเจ้าของระบบสารสนเทศนั้น ๆ กำหนด

๒๙.๒.๕ รับผิดชอบการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมประสงค์ร้ายอื่น ๆ รวมทั้งมาตรการป้องกันอื่น ๆ และการปรับแก้ไข

๒๙.๒.๖ ศึกษา ค้นคว้า และติดตามข้อมูลข่าวสารเกี่ยวกับการค้นพบจุดอ่อนของระบบต่าง ๆ หรือภัยรูปแบบใหม่ ๆ ของระบบสารสนเทศ เพื่อปรับปรุงมาตรการป้องกันให้ทันสมัยเสมอ

๒๙.๒.๗...

๒๙.๒.๗ ปฏิบัติตามกระบวนการรักษาความปลอดภัยตามคำแนะนำของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๒๙.๒.๘ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยที่เกี่ยวข้องภายในส่วนราชการ

๒๙.๒.๙ ให้คำแนะนำกับผู้เกี่ยวข้องให้มีความรู้และปฏิบัติตามกระบวนการรักษาความปลอดภัย

ข้อ ๓๐ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ มีองค์ประกอบและหน้าที่ ดังนี้

๓๐.๑ องค์ประกอบของคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ

๓๐.๑.๑ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงาน ซึ่งแต่งตั้งโดย หัวหน้าส่วนราชการ ผู้รับผิดชอบระบบ ประกอบด้วย

๓๐.๑.๑.๑ หัวหน้าส่วนราชการ หรือ รองหัวหน้าส่วนราชการ ผู้รับผิดชอบระบบ เป็นประธาน

๓๐.๑.๑.๒ หัวหน้าหน่วยขึ้นตรงของส่วนราชการผู้รับผิดชอบระบบ เป็นกรรมการ

๓๐.๑.๑.๓ นายทหารรักษาความปลอดภัยระบบสารสนเทศของระบบงาน เป็นกรรมการและเลขานุการ

๓๐.๑.๑.๔ ผู้เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศตามข้อ ๓๑ โดยพิจารณาตามความเหมาะสม เป็นกรรมการ

๓๐.๑.๒ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของหน่วย ซึ่งแต่งตั้งโดยหัวหน้าหน่วยขึ้นตรงกองทัพอากาศ ประกอบด้วย หัวหน้าส่วนราชการ หรือรองหัวหน้าส่วนราชการ เป็นประธาน และมีกรรมการ ตามจำนวนที่เหมาะสมโดยมีนายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วย เป็นกรรมการ และเลขานุการ

๓๐.๒ หน้าที่ของคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ

๓๐.๒.๑ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงาน มีหน้าที่

๓๐.๒.๑.๑ จัดทำแผนจัดการความเสี่ยงสำหรับระบบสารสนเทศของระบบงาน

๓๐.๒.๑.๒ กำหนดมาตรการรักษาความปลอดภัยเฉพาะสำหรับระบบสารสนเทศของระบบงานตามแผนใน ข้อ ๓๐.๒.๑.๑ หรือตามที่ได้รับการแนะนำ

๓๐.๒.๑.๓...

๓๐.๒.๑.๓ จัดทำแผนที่เกี่ยวข้อง ดังนี้

๓๐.๒.๑.๓(๑) แผนการสำรองข้อมูลของระบบสารสนเทศ

๓๐.๒.๑.๓(๒) แผนฟื้นฟูระบบสารสนเทศ

๓๐.๒.๑.๓(๓) แผนป้องกันภัยธรรมชาติของระบบสารสนเทศ

๓๐.๒.๑.๓(๔) แผนป้องกันอัคคีภัยของระบบสารสนเทศ

๓๐.๒.๑.๓(๕) แผนเผชิญเหตุ (Contingency Plan)

๓๐.๒.๑.๓(๖) แผนป้องกันภัยที่ส่วนราชการนั้นพิจารณาว่าควรจัดทำตามสภาพแวดล้อม

๓๐.๒.๑.๔ จัดทำแผนผัง สถานที่ที่ติดตั้งอุปกรณ์คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของระบบงาน

๓๐.๒.๑.๕ จัดทำรายการอุปกรณ์ สถานภาพการใช้งานและผู้รับผิดชอบ

๓๐.๒.๑.๖ กำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์แต่ละหน่วยงาน โดยให้มีหน้าที่ ดูแล บำรุงรักษา ป้องกันภัย ตรวจสอบความพร้อมใช้งานตลอดจนควบคุมการใช้งานอุปกรณ์ให้เป็นไปตามที่กำหนดไว้

๓๐.๒.๒ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของหน่วยมีหน้าที่

๓๐.๒.๒.๑ จัดทำแผนจัดการความเสี่ยงสำหรับระบบสารสนเทศของหน่วย

๓๐.๒.๒.๒ กำหนดมาตรการรักษาความปลอดภัยเฉพาะสำหรับระบบสารสนเทศของระบบงานตามข้อมูลจากแผนใน ข้อ ๓๐.๒.๒.๑ หรือตามที่ได้รับการแนะนำ

๓๐.๒.๒.๓ จัดทำแผนที่เกี่ยวข้องตามความเหมาะสมดังนี้

๓๐.๒.๒.๓(๑) แผนการสำรองข้อมูลของระบบสารสนเทศ

๓๐.๒.๒.๓(๒) แผนฟื้นฟูระบบสารสนเทศ

๓๐.๒.๒.๓(๓)...

๓๐.๒.๒.๓(๓) แผนป้องกันภัยธรรมชาติของระบบสารสนเทศ

๓๐.๒.๒.๓(๔) แผนป้องกันอัคคีภัยของระบบสารสนเทศ

๓๐.๒.๒.๓(๕) แผนเผชิญเหตุ (Contingency Plan)

๓๐.๒.๒.๓(๖) แผนป้องกันภัยที่ส่วนราชการนั้นพิจารณาว่าควรจัดทำตามสภาพแวดล้อม

๓๐.๒.๒.๔ จัดทำแผนผัง สถานที่ที่ติดตั้งอุปกรณ์คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของหน่วย

๓๐.๒.๒.๕ จัดทำรายการอุปกรณ์ สถานภาพการใช้งานและผู้รับผิดชอบ

๓๐.๒.๒.๖ กำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์แต่ละหน่วยงาน โดยให้มีหน้าที่ ดูแล บำรุงรักษา ป้องกันภัย ตรวจสอบความพร้อมใช้งานตลอดจนควบคุมการใช้งานอุปกรณ์ให้เป็นไปตามที่กำหนดไว้

ข้อ ๓๑ ผู้ปฏิบัติหน้าที่ด้านระบบสารสนเทศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ นอกจากจะต้องมีความรู้และได้รับมอบหมายให้ปฏิบัติหน้าที่ ตามผนวก ก แล้วให้มีหน้าที่ดังนี้

๓๑.๑ ผู้บริหารระบบ (System Administrator) มีหน้าที่ดำเนินการให้ผู้ใช้ที่ได้รับอนุญาตเข้าถึงระบบคอมพิวเตอร์ได้ วางระบบป้องกันการเข้าถึงในระบบสารสนเทศให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับ คงสภาพและสร้างสภาพพร้อมใช้งานให้ระบบ ตามมาตรการป้องกันใน ข้อ ๒๘ โดยกำหนดให้มีกระบวนการพิสูจน์ทราบ (Authentication) กำหนดสิทธิ (Authorization) และบันทึกปูมใช้งานที่เหมาะสม (Audit Log) นอกจากนั้นต้องมีหน้าที่ในการปฏิบัติตามแผนสำรองและกู้ข้อมูล โดยหากเป็นเครือข่ายด้านยุทธการควรต้องกำหนดกระบวนการพิสูจน์ทราบที่ใช้มากกว่า password หรือเป็น Multi-Factor Authentication เช่น การใช้ Smart Card หรือ การอ่านลายนิ้วมือ

๓๑.๒ ผู้บริหารฐานข้อมูล (Database Administrator) มีหน้าที่ดำเนินการให้ผู้ใช้ที่ได้รับอนุญาตเข้าถึงฐานข้อมูลได้ วางระบบป้องกันการเข้าถึงฐานข้อมูลให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับ คงสภาพและสร้างสภาพพร้อมใช้งานให้ฐานข้อมูล ตามมาตรการป้องกันใน ข้อ ๒๘

๓๑.๓ ผู้บริหารเครือข่าย (Network Administrator) มีหน้าที่ดำเนินการเพื่อให้ผู้ได้รับอนุญาตสามารถเข้าถึงระบบเครือข่ายได้ วางระบบป้องกันการเข้าถึงเครือข่ายให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับโดยการเลือกใช้การเข้ารหัสที่เหมาะสม คงสภาพและสร้างสภาพพร้อมใช้งานให้ระบบเครือข่าย

รวมถึง...

รวมถึงดูแลการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ ทางกายภาพให้ตรงตามการใช้งานที่ได้กำหนดไว้ ตามมาตรการป้องกันใน ข้อ ๒๘

๓๑.๔ ผู้เขียนโปรแกรม (Programmer) มีหน้าที่ดำเนินการให้ผู้ใช้ที่ได้รับอนุญาตสามารถเข้าถึงโปรแกรมได้ ตรวจหาข้อบกพร่อง หรือสิ่งอื่นใดที่เป็นภัยต่อโปรแกรม เพื่อกำจัดก่อนนำเข้าสู่ระบบสารสนเทศ ตามมาตรการป้องกันใน ข้อ ๒๘

ข้อ ๓๒ ผู้ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ ต้องปฏิบัติและดำเนินการ ดังนี้

๓๒.๑ ปฏิบัติตามมาตรการใน ข้อ ๒๘

๓๒.๒ ดำเนินการใด ๆ กับข้อมูลเฉพาะที่ได้รับอนุญาตแล้วเท่านั้น และต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศอย่างเคร่งครัด

๓๒.๓ ใช้ระบบสารสนเทศอย่างระมัดระวัง ถูกต้องตามกระบวนการรักษาความปลอดภัย และใช้ในกิจการงานที่ได้รับอนุญาต หรือได้รับมอบหมายเท่านั้น

๓๒.๔ ตรวจสอบโปรแกรมประสงค์ร้ายก่อนนำมาใช้งานในระบบ

๓๒.๕ ไม่นำโปรแกรมที่ไม่ได้รับอนุญาต หรือไม่เกี่ยวข้องกับภารกิจหน้าที่ ที่ได้รับมอบหมายเข้าสู่ระบบสารสนเทศ

๓๒.๖ เก็บรักษาและใช้งานบัญชีผู้ใช้ (User Account) ซึ่งประกอบด้วยชื่อผู้ใช้ (user name) และรหัสผ่าน (Password) ให้เหมาะสม และเก็บรักษารหัสผ่าน (Password) ให้เป็นไปด้วยความปลอดภัย ไม่รั่วไหลถึงบุคคลอื่น

ข้อ ๓๓ ผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์ของหน่วยงานตามที่ได้รับการมอบหมายจากคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ ต้องปฏิบัติและดำเนินการ ดังนี้

๓๓.๑ ดำเนินการตามมาตรการป้องกัน ในข้อ ๒๙ และหน้าที่ตาม ข้อ ๓๐.๒.๑.๖

๓๓.๒ ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ในพื้นที่ที่รับผิดชอบ

๓๓.๓ ดูแลสภาพแวดล้อมการใช้งานให้เหมาะสม

ข้อ ๓๔ การกำหนดรหัสผ่าน (Password) ที่เหมาะสมสำหรับผู้ใช้ทุกระดับมีข้อกำหนดขั้นต่ำดังนี้

๓๔.๑ มีความยาวอย่างน้อย ๘ ตัวอักษร

๓๔.๒ ประกอบไปด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลขและอักขระพิเศษ

๓๔.๓ จะต้องไม่มีข้อมูลเกี่ยวกับผู้ใช้ เช่น วันเกิด ชื่อเล่น หมายเลขโทรศัพท์จดจำรหัสผ่านแทนการเขียนบันทึก หากเจ้าของรหัสผ่านลืมรหัสผ่าน หรือต้องการแก้ไขให้เจ้าของรหัสผ่านแจ้งผู้ดูแลระบบ ให้ดำเนินการ

๓๔.๔...

๓๔.๔ ต้องเปลี่ยนรหัสผ่านตามช่วงเวลาที่กำหนด หรือตามความเหมาะสม สำหรับระบบที่มีความสำคัญ

๓๔.๕ ความรับผิดชอบในการใช้งาน Username และ Password เป็นของเจ้าของผู้ใช้งาน ต้องไม่โอนสิทธิหรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตน ต้องไม่เปิดเผยรหัสผ่านให้แก่ผู้ใดทั้งสิ้น รวมถึงผู้ดูแลระบบสารสนเทศ

๓๔.๖ สำหรับระบบสารสนเทศที่มีความสำคัญ ต้องไม่ใช้รหัสผ่านเดียวกันสำหรับเข้าถึงระบบทั่วไป

๓๔.๗ ไม่ใช้รหัสผ่านร่วมกับผู้อื่นโดยเด็ดขาด แม้ว่าจะเป็นผู้ร่วมงานที่ต้องใช้แฟ้มข้อมูลเดียวกัน ทุกคนที่ได้รับอนุญาตจะต้องมีรหัสผ่านเป็นของตนเองในการเข้าใช้ข้อมูลดังกล่าว

หมวด ๓
การรักษาความปลอดภัยระบบคอมพิวเตอร์
(Computer System Security)

ข้อ ๓๕ การรักษาความปลอดภัยระบบคอมพิวเตอร์ เป็นมาตรการควบคุมและป้องกันเพื่อยืนยันถึงความถูกต้อง สิทธิการเข้าใช้ ความลับ และความพร้อมใช้งานของสารสนเทศที่ดำเนินการ หรือที่เก็บรักษาในระบบคอมพิวเตอร์

ส่วนที่ ๑
การรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์
(Computer Equipment Security)

ข้อ ๓๖ การรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์ มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ การรั่วไหล และความเสียหายของข้อมูลที่เกิดจากจุดอ่อน หรือข้อบกพร่องของอุปกรณ์คอมพิวเตอร์ หรือซอฟต์แวร์ที่เกี่ยวข้อง รวมทั้งสร้างสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์

ข้อ ๓๗ อุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศของทุกหน่วย หรือทุกชุด ต้องมีการกำหนดผู้รับผิดชอบ และจัดทำรายละเอียดที่จำเป็น เช่น ผู้ที่ได้รับอนุญาตให้เข้าใช้ การใช้งาน ตลอดจนระดับของการป้องกัน เป็นต้น

ข้อ ๓๘...

ข้อ ๓๘ การจัดเก็บสิ่งบันทึกที่สามารถแสดงผล หรือสื่อความเป็นสารสนเทศที่มีชั้นความลับได้ เช่น จานบันทึก ซีดีรอม และอื่น ๆ ที่นำมาแสดงผลโดยระบบคอมพิวเตอร์ได้ หากแสดงชั้นความลับไว้ในที่ดังกล่าวไม่ได้ ให้พิทักษ์รักษาตามชั้นความลับนั้น และให้เก็บในกล่อง หรือหีบห่อ ซึ่งมีเครื่องหมายแสดงชั้นความลับนั้น ๆ และห้ามมิให้ผู้ใดมีการใช้งานสื่อบันทึกข้อมูลที่เคลื่อนที่ได้ (Removable Storage Devices) ในสายงานที่เกี่ยวข้องกับงานด้านยุทธการที่มีชั้นความลับ เว้นแต่ผู้ที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เกี่ยวข้องเป็นลายลักษณ์อักษร และหากมีการกระทำความผิดเกี่ยวข้องกับสื่อบันทึกข้อมูลที่เคลื่อนที่ได้นั้น เจ้าของผู้ลงทะเบียนต้องรับผิดชอบ

ข้อ ๓๙ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ ตรวจสอบอุปกรณ์ที่นำมาติดตั้งใหม่ทุกครั้ง ว่าได้มาตรฐานในการรักษาความปลอดภัย สำหรับอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่แล้ว ให้ตรวจสอบทุกรอบ ๓ เดือน หรือเมื่อมีเหตุอันควรแก่การตรวจสอบ และรายงานให้หัวหน้าส่วนราชการทราบเมื่อสิ้นสุดระยะเวลาการตรวจสอบ

ข้อ ๔๐ การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เข้า - ออก นอกพื้นที่ใช้งานระบบสารสนเทศของส่วนราชการ หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะการทำงานของอุปกรณ์เปลี่ยนแปลงไป จะต้องแจ้งและขออนุญาตตามลำดับชั้นถึงนายทหารรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ และให้ผู้รับผิดชอบพื้นที่ใช้งานระบบสารสนเทศของส่วนราชการตรวจสอบความปลอดภัยก่อนการเคลื่อนย้ายทุกครั้ง

ข้อ ๔๑ ก่อนนำอุปกรณ์คอมพิวเตอร์ไปซ่อมบำรุง หรือจำหน่ายขายซากให้บุคคลภายนอกกองทัพอากาศ หรือนำอุปกรณ์คอมพิวเตอร์กลับไปใช้ในงานของภารกิจใหม่ภายหลังจากใช้ในงานของภารกิจอื่น ๆ มาแล้ว หรือต้องการทำลายข้อมูล เมื่อหมดความจำเป็นในการใช้งานแล้ว หรือเป็นการโอนสิทธิการถือครองอุปกรณ์คอมพิวเตอร์ในลักษณะอื่น ๆ ต้องทำลายข้อมูลทั้งหมดที่มีชั้นความลับตั้งแต่ “ลับ” ขึ้นไปที่อยู่ในอุปกรณ์ดังกล่าวไม่ให้สามารถกู้คืนมาใช้งานได้อีก

ในกรณีที่นำอุปกรณ์คอมพิวเตอร์ไปซ่อมภายนอกกองทัพอากาศ และมีการเปลี่ยนชิ้นส่วน เพื่อทดแทนชิ้นส่วนที่ชำรุดเสียหาย ให้นายทหารรักษาปลอดภัยระบบสารสนเทศของส่วนราชการที่ดำเนินการซ่อมบำรุงติดตามนำชิ้นส่วนดังกล่าวกลับมาดำเนินการให้ถูกต้องต่อไป

ส่วนที่ ๒
การรักษาความปลอดภัยการโปรแกรม
(Program Security)

ข้อ ๔๒ การรักษาความปลอดภัยการโปรแกรม มีความมุ่งหมาย เพื่อขจัดการใช้ประโยชน์จากจุดอ่อน หรือข้อบกพร่องของโปรแกรมในการทำอันตรายระบบสารสนเทศ

ข้อ ๔๓...

ข้อ ๔๓ ผู้พัฒนาโปรแกรมเพื่อนำไปใช้ในระบบสารสนเทศ ต้องพัฒนาโปรแกรมตามหลักวิชาการที่ยอมรับโดยทั่วไป และยินยอมให้ทำการตรวจสอบได้ตลอดเวลา รวมทั้งแสดงรายละเอียดที่จำเป็นต่อการรักษาความปลอดภัยไว้ที่รหัสต้นทาง (Source Code) เช่น ชื่อผู้เขียน วัน เดือน ปีที่เขียน หรือปรับปรุง วัตถุประสงค์ ระดับการป้องกัน สำหรับข้อมูลที่จำเป็นต้องใช้ในการพัฒนา เช่น ความสัมพันธ์ที่สามารถเชื่อมโยงไปถึงโปรแกรมหรือข้อมูลลับอื่น ๆ หรือผู้ที่ได้รับอนุญาตให้นำโปรแกรมไปใช้งานได้ให้เพิ่มเติมไว้ในเอกสารคู่มือ

ผู้พัฒนาโปรแกรมทั้งที่เป็นบุคลากรทางคอมพิวเตอร์ของกองทัพอากาศและบุคคลภายนอกที่รับจัดทำโปรแกรมให้กองทัพอากาศ ต้องคำนึงถึงความปลอดภัยในทุกขั้นตอนของการพัฒนาโปรแกรม รวมทั้งรับผิดชอบต่อการรักษาความลับของข้อมูลและความถูกต้องของโปรแกรม จัดทำเอกสารหรือคู่มือประกอบการใช้งานสำหรับผู้พัฒนาโปรแกรมและผู้ใช้ และพัฒนาโปรแกรมให้ตรงตามวัตถุประสงค์ของทางราชการเท่านั้น ให้ใช้เฉพาะซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น เพื่อป้องกันโปรแกรมประสงค์ร้าย หากเป็นโปรแกรมสำเร็จรูป เช่น โปรแกรมระบบปฏิบัติการ หรือ โปรแกรมสำนักงาน ต้องมีการปรับปรุงให้ทันสมัยตลอดเวลาเพื่ออุดช่องโหว่และเป็นการป้องกันโปรแกรมประสงค์ร้าย

ข้อ ๔๔ การพัฒนาโปรแกรมประยุกต์ให้ส่วนราชการ ผู้มีสิทธิและอำนาจในสารสนเทศนั้นเป็นผู้พิจารณาคุณสมบัติของผู้ที่สามารถใช้งานโปรแกรมดังกล่าวได้ตามสิทธิ

หมวด ๔
การรักษาความปลอดภัยระบบสื่อสาร
(Data Communication Security)

ข้อ ๔๕ การรักษาความปลอดภัยระบบสื่อสาร เป็นมาตรการควบคุมและป้องกันเพื่อยืนยันถึงความถูกต้องของการโอน การแลกเปลี่ยนสารสนเทศ หรือการติดต่อกันในลักษณะใดลักษณะหนึ่งผ่านทางระบบสื่อสารข้อมูลว่าได้กระทำโดยผู้มีอำนาจหน้าที่และป้องกันผู้ไม่เกี่ยวข้องเข้าถึงระบบสื่อสาร

ข้อ ๔๖ การรักษาความปลอดภัยเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ (Computer Network Security) เป็นการรักษาความปลอดภัยระบบสื่อสาร มีความมุ่งหมาย เพื่อกำหนดมาตรการควบคุมและป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต ความลับรั่วไหลการบิดเบือน และการทำลายสารสนเทศในระหว่างส่งผ่านทางระบบเครือข่ายคอมพิวเตอร์

ข้อ ๔๗ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิและอำนาจในสายงาน ที่มีการติดต่อแลกเปลี่ยนสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ เป็นผู้พิจารณาคุณสมบัติ

ของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึง และดำเนินการกับสารสนเทศดังกล่าว รวมทั้งพิจารณาระดับของการป้องกันที่ต้องการ โดยหากมีการแลกเปลี่ยนกับหน่วยงานนอกกองทัพอากาศ ต้องได้รับการตรวจสอบระดับความปลอดภัยที่เหมาะสมจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ข้อ ๔๘ การส่งสารสนเทศที่มีชั้นความลับผ่านระบบเครือข่ายคอมพิวเตอร์ จะต้องได้รับอนุมัติจากเจ้าของเรื่องสารสนเทศ ผู้มีสิทธิและอำนาจในสายงาน ที่กำหนดชั้นความลับนั้นก่อน เมื่อได้รับอนุมัติแล้ว สารสนเทศกำหนดชั้นความลับจะต้องส่งเข้ารหัส (Encryption) โดยมาตรฐานที่ได้รับการรับรองแล้วจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ผู้มีสิทธิและอำนาจในสายงานสามารถกำหนดระเบียบปฏิบัติของการเข้าใช้ที่สอดคล้องกับระเบียบนี้

ข้อ ๔๙ หากมีการใช้เครือข่ายไร้สายทั้งในด้านยุทธการ และธุรการต้องมีการป้องกันทั้งการพิสูจน์ทราบและการเข้ารหัส โดยต้องมีการขึ้นทะเบียนอุปกรณ์ (WiFi Access Point) เพื่อตรวจสอบและยืนยันความปลอดภัยจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ข้อ ๕๐ ห้ามมิให้เครือข่ายทางด้านยุทธการเชื่อมต่อกับระบบอินเทอร์เน็ตหรือระบบอื่น ๆ ของหน่วยงานภายนอกกองทัพอากาศ ยกเว้นแต่ที่ได้รับการตรวจสอบและเห็นชอบจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

หมวด ๕
การรักษาความปลอดภัยสารสนเทศ
(Information Security)

ข้อ ๕๑ การรักษาความปลอดภัยสารสนเทศ เป็นมาตรการป้องกันสารสนเทศที่อยู่ในระบบจากการเข้าถึง ด้วยการรักษาความลับไม่ให้รั่วไหล การคงสภาพข้อมูล และการสร้างสภาพพร้อมใช้งานให้แก่ผู้มีสิทธิ รวมถึงมาตรการป้องกันอื่น ๆ ที่จำเป็น

ส่วนที่ ๑
การรักษาความปลอดภัยฐานข้อมูล
(Database Security)

ข้อ ๕๒ การรักษาความปลอดภัยฐานข้อมูล มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึงการเปลี่ยนแปลง การโอนถ่ายข้อมูล หรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง ตลอดจนการเตรียมระบบสำรองและการฟื้นฟูระบบ

ข้อ ๕๓...

ข้อ ๕๓ ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิเข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย และหากเป็นข้อมูลที่มีชั้นความลับ ต้องมีการเข้ารหัสในการจัดเก็บที่เหมาะสม โดยใช้รูปแบบการเข้ารหัสตามมาตรฐานที่กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศกำหนด

ข้อ ๕๔ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ และจัดให้มีแฟ้มลงบันทึกเข้าออกและการใช้งาน (Audit Log) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕๕ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

ข้อ ๕๖ ต้องมีการจัดทำแผนสำรองและกู้ข้อมูลที่เหมาะสม และหากเป็นข้อมูลเกี่ยวกับงานด้านยุทธการต้องมีการสำรองข้อมูลอย่างน้อย ๒ ชุด โดยเก็บไว้ในพื้นที่ปฏิบัติงาน ๑ ชุดและเก็บไว้ห่างจากจุดที่มีการติดตั้งใช้อีก ๑ ชุด สำหรับระบบอื่น ๆ ให้กำหนดตามความเหมาะสม

ส่วนที่ ๒
การจัดการสารสนเทศ
(Information Management)

ข้อ ๕๗ การจัดการสารสนเทศ มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันและควบคุมการใช้สารสนเทศที่มีชั้นความลับในรูปแบบต่าง ๆ

ข้อ ๕๘ ให้ผู้มีส่วนเกี่ยวข้องกับการแสดงชั้นความลับของสารสนเทศ ปฏิบัติดังนี้

๕๘.๑ สารสนเทศที่จัดทำในรูปแบบเอกสารหรือรายงาน ให้แสดงหรือพิมพ์ตัวอักษรตามชั้นความลับกึ่งกลางหน้าทั้งด้านบน และด้านล่างของทุกหน้าเอกสารที่มีชั้นความลับนั้น โดยใช้ตัวอักษรที่มีขนาดใหญ่กว่าที่ใช้ในข้อความปกติ และใช้สีหรือความเข้มของตัวอักษรที่มีขนาดใหญ่

๕๘.๒ สารสนเทศที่จัดทำในรูปแบบ ภาพเขียน เรขา ภาพถ่าย แผนที่ แผนภูมิ แผนผัง ให้แสดงหรือพิมพ์ตัวอักษรตามชั้นความลับ เช่นเดียวกับ ข้อ ๕๘.๑ โดยให้แสดงชั้นความลับให้ปรากฏเห็นได้ชัดเจน หรือแสดงไว้ใกล้ชื่อภาพ หรือมาตราส่วน

๕๘.๓ ในการแสดง นำเสนอ หรือพูดถึงสารสนเทศที่มีชั้นความลับ ให้ผู้แสดงหรือผู้พูดแจ้งให้ผู้ดู หรือผู้ฟังทราบชั้นความลับที่กำหนดของสารสนเทศนั้น ๆ หากแสดงภาพฉายบนจอภาพให้แสดงชั้นความลับด้วยอักษร ทั้งก่อนและเมื่อเสร็จสิ้นการแสดง การนำเสนอหรือพูดแล้ว

๕๘.๔...

๕๘.๔ สารสนเทศที่กำหนดชั้นความลับ จะต้องวางระบบป้องกันมิให้ผู้ไม่มีหน้าที่เกี่ยวข้องเข้าถึงและแก้ไข ลบล้าง หรือทำลายโดยพลการ และหากมีข้อมูลที่เป็นชั้นความลับหลายชั้นความลับอยู่ในแฟ้มข้อมูลเดียวกัน ให้กำหนดชั้นความลับสูงสุดของสารสนเทศนั้นไว้ที่แฟ้มข้อมูลดังกล่าว

ข้อ ๕๙ การจัดทำซ้ำ หรือจัดทำสำเนาข้อมูลสารสนเทศที่กำหนดชั้นความลับ ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากเจ้าของเรื่องสารสนเทศ ที่กำหนดชั้นความลับนั้น และให้รวมหมายถึงการสั่งงานระบบคอมพิวเตอร์ให้จัดการพิมพ์ออกเป็นเอกสารลับนั้นด้วย

ข้อ ๖๐ การปรับ และยกเลิกชั้นความลับของสารสนเทศ ให้เจ้าของสารสนเทศตรวจสอบอยู่เสมอว่าชั้นความลับของสารสนเทศที่กำหนดไว้แต่เดิมยังจำเป็นต้องใช้อยู่หรือไม่ เพราะสารสนเทศอาจลดชั้น เพิ่มชั้นหรือยกเลิกชั้นความลับได้ตามความจำเป็น และควรลดชั้นลงทุกโอกาสเท่าที่กระทำได้เพื่อลดภาระในการรักษาความปลอดภัย

ข้อ ๖๑ สารสนเทศที่ได้รับจากรัฐบาลต่างประเทศ หรือองค์การระหว่างประเทศ หากรัฐบาลหรือองค์การนั้น ๆ ได้กำหนดชั้นความลับไว้ จะต้องปฏิบัติต่อสารสนเทศนั้นเท่าเทียมกับสารสนเทศที่กำหนดชั้นความลับ

ข้อ ๖๒ การเผยแพร่ข้อมูล ข่าวสาร หรือสารสนเทศใด ๆ ของทางราชการผ่านสื่อทางระบบสารสนเทศให้เป็นไปตามระเบียบ คำสั่งของส่วนราชการและกองทัพอากาศที่เกี่ยวข้อง โดยให้มีการเผยแพร่เท่าที่จำเป็นตามพระราชบัญญัติ ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ อีกทั้งให้บุคลากรของกองทัพอากาศระมัดระวังการให้ข้อมูลผ่านช่องทางที่ไม่เป็นทางการด้วย โดยให้ยึดถือตามแนวทางของกฎหมาย ดังกล่าวเช่นกัน

ข้อ ๖๓ สารสนเทศที่กำหนดชั้นความลับ “ลับที่สุด” และ “ลับมาก” ที่ใช้ร่วมกันระหว่างส่วนราชการต้องแบ่งระดับการเข้าถึงสารสนเทศตามหน้าที่ของผู้ใช้

ข้อ ๖๔ สารสนเทศที่อยู่ในระบบคอมพิวเตอร์ หากสารสนเทศเป็นร่าง หรือสำเนาของเอกสารที่มีชั้นความลับ จะต้องแสดงชั้นความลับเช่นเดียวกับเอกสารต้นฉบับ ในกรณีที่เอกสารต้นฉบับได้ดำเนินการทำลายแล้วให้ลบทิ้งสารสนเทศที่อยู่ในระบบคอมพิวเตอร์นั้นด้วย โดยการทำลายแบบไม่ให้สามารถกู้ข้อมูลกลับคืนได้ภายหลัง

ข้อ ๖๕ กุญแจเพื่อการเข้าและถอดรหัสลับ (Encryption and Decryption Key) ทุกชนิดที่ใช้ในการเข้ารหัสระบบสารสนเทศให้จัดเป็นสารสนเทศที่มีชั้นความลับ “ลับ” ขึ้นไป ต้องจำกัดการเข้าถึงเท่าที่จำเป็น โดยมีขนาดของกุญแจ (จำนวน bit) ที่เหมาะสมและควรเปลี่ยนตามวาระ ดังนี้

๖๕.๑...

๖๕.๑ ตามห้วงระยะเวลาอย่างน้อย ๓ เดือนต่อหนึ่งครั้ง หรือ ตามความจำเป็นหากเกี่ยวข้องกับงานด้านยุทธการ แต่ต้องไม่กำหนดระยะเวลาที่แน่นอนได้

๖๕.๒ เมื่อมีการเปลี่ยนเจ้าหน้าที่ที่เกี่ยวข้องกับการเข้ารหัส พร้อมทั้งสั่งยกเลิกกุญแจเพื่อเข้าและถอดรหัสลับ (Encryption and Decryption Key) เดิม

๖๕.๓ เมื่อความลับรั่วไหลหรือสงสัยว่าความลับรั่วไหล

ข้อ ๖๖ รหัสผ่าน (Password) ของผู้ใช้ ที่ใช้ในระบบสารสนเทศให้จัดเป็นสารสนเทศที่มีชั้นความลับ “ลับ” ขึ้นไป และให้ผู้ใช้ทุกคนปฏิบัติตามวิธีการรักษาความปลอดภัยเกี่ยวกับรหัสผ่านประจำตัว

หมวด ๖
การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๖๗ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ มีความมุ่งหมาย เพื่อให้เป็นแนวทางปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยต่อระบบสารสนเทศของกองทัพอากาศ และลดความเสียหายที่เกิดขึ้นจากการกระทำที่ฝ่าฝืน หรือละเลยให้เหลือน้อยที่สุด พร้อมทั้งตรวจสอบ ค้นหาสาเหตุ ผลเสียหายเพื่อปรับปรุงมาตรการป้องกันการละเมิดที่จะเกิดขึ้นซ้ำอีกกับกำหนดวิธีดำเนินการต่อผู้ละเมิดการรักษาความปลอดภัย

ข้อ ๖๘ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ มีดังนี้

๖๘.๑ เมื่อตรวจพบ หรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ หรือมีสิ่งผิดปกติเกิดขึ้นในระบบสารสนเทศ ให้รีบรายงานผู้บังคับบัญชา และนายทหารรักษาความปลอดภัยระบบสารสนเทศทราบโดยเร็วที่สุด

๖๘.๒ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ ดำเนินการดังนี้

๖๘.๒.๑ รายงานขั้นต้นต่อ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อการค้นหาและพิสูจน์หลักฐานทางดิจิตอลที่อยู่ในอุปกรณ์คอมพิวเตอร์ (Computer Forensic) หากพบว่าเป็นการละเมิดต่อสารสนเทศที่มีชั้นความลับให้แจ้ง กรมข่าวทหารอากาศ ในฐานะสายวิทยาการรักษาความปลอดภัยทราบด้วย

๖๘.๒.๒ ลดความเสียหายเบื้องต้น โดยการระงับใช้ แก้ไข หรือยกเลิกระบบสารสนเทศที่สงสัยว่าถูกละเมิดนั้น หากเป็นสารสนเทศที่มีชั้นความลับจะต้องแจ้งให้เจ้าของเรื่องสารสนเทศที่มีชั้นความลับนั้นทราบ เพื่อพิจารณายกเลิกชั้นความลับ

๖๘.๒.๓...

๖๘.๒.๓ สำรวจความเสียหายที่เกิดจากการละเมิด ตรวจสอบสาเหตุและจุดอ่อน หรือข้อบกพร่องที่ก่อให้เกิดการละเมิดโดยให้มีผู้แทนจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ และกรมข่าวทหารอากาศร่วมในการตรวจสอบสาเหตุด้วย

๖๘.๒.๔ รายงานเหตุการณ์ที่เกิดขึ้นให้ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ พร้อมทั้งแนวทางป้องกันมิให้เกิดการละเมิดซ้ำ

๖๘.๒.๕ หากปรากฏหลักฐาน หรือสงสัยว่าระบบสารสนเทศถูกจารกรรม ให้รายงานให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ เพื่อแก้ไขโดยเร็วที่สุด

ข้อ ๖๙ หน้าที่และความรับผิดชอบของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ มีดังนี้

๖๙.๑ แจ้งให้ส่วนราชการเจ้าของสารสนเทศร่วม ทราบโดยเร็วที่สุด

๖๙.๒ แต่งตั้งคณะกรรมการร่วมกับส่วนราชการที่มีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ เพื่อดำเนินการสืบสวนสอบสวนหาตัวผู้รับผิดชอบและผู้กระทำผิดโดยเร็วที่สุด

๖๙.๓ แจ้งให้ส่วนราชการต้นสังกัด ลงโทษผู้รับผิดชอบและผู้กระทำผิดต่อการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ ตามกรณีที่ก่อให้เกิดความเสียหายต่อระบบ หรือส่งตัวผู้กระทำผิดไปดำเนินการตามกฎหมายแล้วแต่กรณี

๖๙.๔ สั่งให้แก้ไขข้อบกพร่อง และป้องกันมิให้เกิดเหตุการณ์ซ้ำขึ้นอีก

ข้อ ๗๐ หน้าที่และความรับผิดชอบของส่วนราชการที่มีผู้ละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

๗๐.๑ ลงโทษหรือลงทัณฑ์ทางวินัยกับผู้ละเมิด และผู้รับผิดชอบต่อการละเมิดดังกล่าวตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำขึ้นอีก ในกรณีผู้ละเมิดเป็นบุคคลภายนอกกองทัพอากาศ ให้หน่วยเกี่ยวข้องดำเนินการตามกฎหมายต่อไป

๗๐.๒ หากก่อให้เกิดความเสียหายต่อทางราชการอย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ส่งตัวไปดำเนินการตามกฎหมายต่อไป

๗๐.๓ พิจารณาข้อมูลสารสนเทศที่มีชั้นความลับ รหัสประมวลลับ (Code) กุญแจเข้าและถอดรหัสที่อยู่ในความรับผิดชอบ หากได้รับความเสียหาย รั่วไหล หรือได้รับความกระทบกระเทือน ต้องดำเนินการแก้ไขโดยเร็วที่สุด

๗๐.๔ กำหนดมาตรการป้องกันเพิ่มเติม เพื่อขจัดความเสียหายที่จะเกิดการละเมิดซ้ำหรือเปลี่ยนแปลงวิธีการปฏิบัติ ยกเลิกโปรแกรม และอื่น ๆ

๗๐.๕...

๗๐.๕ หากก่อให้เกิดความเสียหายต่อระบบสารสนเทศ และต้องเสียค่าใช้จ่ายในการกู้คืนมา ให้ส่วนราชการเรียกร้องค่าเสียหายส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้ระบบด้วย

ข้อ ๗๑ ในกรณีที่มีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ อันก่อให้เกิดความเสียหายต่อระบบสารสนเทศของกองทัพอากาศอย่างร้ายแรง ให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ สั่งการแก้ไข เปลี่ยนแปลงระบบ แผนงาน และวิธีปฏิบัติได้ตามความจำเป็นและความเหมาะสม

ข้อ ๗๒ เพื่อให้การดำเนินมาตรการรักษาความปลอดภัยเกี่ยวกับระบบสารสนเทศตามระเบียบนี้เป็นไปด้วยความเรียบร้อยและรวดเร็ว ให้คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง มีความหมายตามผนวก ข

ประกาศ ณ วันที่ ๒๐ พฤศจิกายน พ.ศ.๒๕๕๒

(ลงชื่อ) พลอากาศเอก อิทธพร ศุภวงศ์

(อิทธพร ศุภวงศ์)

ผู้บัญชาการทหารอากาศ

การแจกจ่าย ผบ.ทอ., รอง ผบ.ทอ., ปธ.คปษ.ทอ., ผช.ผบ.ทอ., เสธ.ทอ., ปษ.พิเศษ ทอ., หน.คณะนายทหารฝ่ายเสนาธิการประจำผู้บังคับบัญชา, รอง เสธ.ทอ., ผช.เสธ.ทอ., สน.ผบ.ทอ., สน.รอง ผบ.ทอ., สน.ปธ.คปษ.ทอ., สน.ผช.ผบ.ทอ., สน.เสธ.ทอ., สน.รอง เสธ.ทอ., สน.ผช.เสธ.ทอ., สน.ปษ.ทอ., สน.ผทค.ทอ., ผนน.บก.ทอ., นขต.ทอ. และ นขต.ทสส.ทอ.

สำเนาถูกต้อง

น.อ.

(ธคุณ มุ่งเพียร)

รอง จก.ทสส.ทอ.

๒๔ พ.ย.๕๒

นางเสมอดาว ฯ พิมพ์/ทาน

น.อ.ณัฐพล ฯ ตรวจ

ผนวก ก

หน้าที่การรักษาความปลอดภัยระบบสารสนเทศแบ่งตามบทบาท

๑. ผู้บริหารระบบ (System Administrator) มีความรู้ด้านฮาร์ดแวร์ ซอฟต์แวร์ระบบเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๑.๑ บริหารและดูแลอุปกรณ์คอมพิวเตอร์ ซึ่งเป็นแม่ข่ายบริการแก่หน่วยต่าง ๆ ของส่วนราชการ

๑.๒ ควบคุมและตรวจสอบการใช้งานระบบ

๑.๓ ตรวจสอบ ควบคุม ดูแล การบำรุงรักษาระบบ

๑.๔ รักษาความปลอดภัยระบบ เช่น รักษาความลับ ความคงสภาพและความพร้อมใช้งาน

๒. ผู้บริหารฐานข้อมูล (Database Administrator) มีความรู้ด้านการจัดการฐานข้อมูลระบบคอมพิวเตอร์เป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๒.๑ ควบคุมดูแลฐานข้อมูล เช่น การรวบรวม การเพิ่ม การเปลี่ยนแปลง การลบ การจัดโครงสร้าง การใช้งาน การเก็บ และการเรียกดู

๒.๒ เลือก ตัดตอน และกำหนดรูปแบบข้อมูลที่เก็บในแฟ้มข้อมูล

๒.๓ รักษาความปลอดภัยฐานข้อมูล เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้ฐานข้อมูล

๒.๔ ตรวจสอบฐานข้อมูล และวิเคราะห์ข้อมูล

๒.๕ ควบคุม และบริการการใช้งานฐานข้อมูล

๓. ผู้บริหารเครือข่าย (Network Administrator) มีความรู้ด้านฮาร์ดแวร์ การสื่อสารข้อมูลและอุปกรณ์ในระบบเครือข่ายเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๓.๑ กำหนดเลขที่อยู่ไอพี (IP Address) ให้คอมพิวเตอร์ในเครือข่ายของส่วนราชการโดยประสานกับส่วนราชการหรือผู้บริหารระบบเครือข่ายคอมพิวเตอร์ของกองทัพอากาศ

๓.๒ กำหนดบัญชีผู้ใช้ (Account) และรหัสผ่าน (Password) ของผู้ใช้ภายในเครือข่ายที่รับผิดชอบ

๓.๓ ดูแลการใช้เครือข่ายคอมพิวเตอร์ภายในส่วนราชการ

๓.๔ ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวกับระบบเครือข่าย

๓.๕ รักษาความปลอดภัยระบบเครือข่าย เช่น รักษาความลับ ความคงสภาพกำหนดการเข้ารหัส และความพร้อมใช้งานให้ระบบเครือข่าย

๔. ผู้เขียน...

๔. ผู้เขียนโปรแกรม (Programmer) มีความรู้เรื่องระบบคอมพิวเตอร์ การเขียนโปรแกรมคอมพิวเตอร์และฐานข้อมูลเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๔.๑ เขียนและพัฒนาโปรแกรมที่ได้รับมอบหมาย

๔.๒ จัดหาข้อมูลเพื่อทดสอบโปรแกรม

๔.๓ ดูแลบำรุงรักษาโปรแกรมที่พัฒนา

๔.๔ รักษาความปลอดภัยโปรแกรม เช่น รักษาความลับ ความคงสภาพและความพร้อมใช้งานให้โปรแกรม

ผนวก ข

คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง

๑. Account ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: บัญชีผู้ใช้

อธิบายความหมาย

: เป็นสัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกัน มีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกัน เพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชี หรือกลุ่มคนที่สามารถเข้าถึงระบบได้ บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (Password)

๒. Application ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: การประยุกต์

อธิบายความหมาย

: งานที่ทำด้วยโปรแกรมคอมพิวเตอร์ หรือระบบคอมพิวเตอร์เพื่อให้ได้ผลลัพธ์ตามที่ต้องการ เช่น งานออกแบบโครงสร้างทางวิศวกรรม งานพยากรณ์ทางธุรกิจ งานด้านการจัดการสถานพยาบาล เป็นต้น การประยุกต์ มีความหมายรวมถึงโปรแกรมประยุกต์ หรือโปรแกรมใช้งาน (Application Program) และซอฟต์แวร์ประยุกต์ (Application Software)

๓. Computer Network ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: เครือข่ายคอมพิวเตอร์, ข่ายงานคอมพิวเตอร์

อธิบายความหมาย

: เป็นคำกล่าวโดยทั่ว ๆ ไปของการเชื่อมต่อสื่อสารกันระหว่างระบบคอมพิวเตอร์ตั้งแต่ ๒ ระบบขึ้นไป หรือระหว่างเครื่องคอมพิวเตอร์กับเครื่องปลายทาง (Terminals) ทั้งหลาย เพื่อให้สามารถนำข้อมูล โปรแกรมรวมทั้งอุปกรณ์รอบข้างมาใช้งานร่วมกันได้ โดยมีอุปกรณ์ในระบบสื่อสารเป็นตัวเชื่อมโยง

๔. Decryption / Encryption ยังไม่มีการกำหนดไว้ในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: การถอดรหัสลับ / เพื่อการเข้ารหัสลับ

อธิบายความหมาย

: การถอดรหัสลับ (Decryption)

(๑) กระบวนการนำข้อความ (Message) ที่ผ่านการเข้ารหัสลับ (Encrypted) แล้วมาแปลงกลับให้เป็นข้อความดั้งเดิม (Original Meaningful Message) หรือข้อความธรรมดา (Plaintext) เป็นความหมายที่ตรงกันข้ามกับคำว่า การเข้ารหัสลับ

(๒) กระบวน...

(๒) กระบวนการที่ตรงข้าม คือ การแปลงข้อความที่เข้ารหัสลับแล้วให้กลับไปอยู่ในรูปแบบปกติ คำที่มีความหมายเหมือนกันคือ เข้ารหัส (Encode) และถอดรหัส (Decode) หรือ เข้ารหัส (Encipher) และถอดรหัส (Decipher) ซึ่งใช้แทนคำว่า เข้ารหัส (Encrypt) และถอดรหัส (Decrypt) และเรียกระบบที่มีการเข้ารหัสลับและถอดรหัสลับว่า ระบบการเข้ารหัสลับ (Cryptosystem)

: การเข้ารหัสลับ (Encryption)

(๑) เป็นขบวนการเข้ารหัสให้ข้อความเพื่อทำให้ไม่ทราบความหมายที่แท้จริงของข้อความดังกล่าว

(๒) กระบวนการเข้ารหัส (Encode) หรือการเข้ารหัสลับ (Encryption) ให้แก่ข้อมูล (Data) ใด ๆ ก็ตามซึ่งต้องการรหัสเฉพาะเจาะจง (Specific Code) หรือ กุญแจ (Key) สำหรับการแปลงให้กลับมาเป็นข้อมูลดั้งเดิม (Original data)

(๓) เป็นการเข้ารหัสข้อมูลสื่อสาร (Communication Data)

๕. Decryption Key / Encryption Key ยังไม่มีการกำหนดไว้ในศัพท์คอมพิวเตอร์ฉบับราชบัณฑิตยสถาน

: กุญแจเพื่อการถอดรหัสลับ / กุญแจเพื่อการเข้ารหัสลับ

อธิบายความหมาย

: เป็นคำศัพท์สำหรับการเข้ารหัสแบบกุญแจสาธารณะ (Public Key System) ประกอบด้วยไฟล์คอมพิวเตอร์คู่หนึ่ง คือ กุญแจสาธารณะ (Public Key) ใช้ในการเข้ารหัสลับ ซึ่งไฟล์สำหรับการเข้ารหัสคือ Encryption Key และ กุญแจลับ (Secret Key) ใช้เมื่อถอดรหัสลับ ซึ่งไฟล์สำหรับการถอดรหัสคือ Decryption Key

๖. Hardware ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ๑. ส่วนเครื่อง, ฮาร์ดแวร์

: ๒. ส่วนอุปกรณ์, ฮาร์ดแวร์

อธิบายความหมาย

: ระบบคอมพิวเตอร์ส่วนที่เป็นอุปกรณ์ทางกายภาพ เช่น อิเล็กทรอนิกส์ แม่เหล็ก และเครื่องจักรกล แสดงให้เห็นถึงความแตกต่างของฮาร์ดแวร์และซอฟต์แวร์ ซึ่งเป็นองค์ประกอบของระบบคอมพิวเตอร์เช่นเดียวกัน

๗. Log File ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: แฟ้มลงบันทึกเข้าออก

อธิบายความหมาย

: เป็นการบันทึกการปฏิบัติทั้งหมดของอุปกรณ์ที่เกี่ยวข้องกับการประมวลผลข้อมูล (Data Processing Equipment) จะบันทึกงานทุกงานหรือการดำเนินการ (Run) ตามลำดับที่เกิดขึ้น เวลาเริ่มต้นและสิ้นสุดของแต่ละงาน รวมทั้งกิจกรรมที่ทำ ทั้งนี้เพื่อนำมาตรวจสอบความถูกต้องของการใช้งานได้ในภายหลัง

๘. Malicious Code ยังไม่กำหนดความหมายไว้ในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: โปรแกรมประสงค์ร้าย

อธิบายความหมาย

: โปรแกรมหรือส่วนของโปรแกรมที่สร้างขึ้น และเผยแพร่โดยผู้มีเจตนาร้ายมุ่งทำลายอย่างใดอย่างหนึ่งต่อสิ่งที่เป็นเป้าหมาย โดยทั่วไปโปรแกรมประสงค์ร้ายจะแบ่งตามลักษณะ การแพร่กระจาย และการกระทำได้ ๕ ประเภท คือ

๘.๑ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นโปรแกรมหรือส่วนของโปรแกรมที่ผู้เขียนมีวัตถุประสงค์ในการทำลายอย่างใดอย่างหนึ่ง หนทางเข้าสู่ระบบคอมพิวเตอร์โดยการเกาะติดกับโปรแกรมที่ใช้งานทั่ว ๆ ไปภายในระบบคอมพิวเตอร์และทำให้โปรแกรมเป้าหมายที่อาศัยอยู่นั้นกลายเป็นโปรแกรมประสงค์ร้ายด้วย ไวรัสคอมพิวเตอร์แพร่กระจายโดยสำเนาตัวเอง (Copy) ไปเกาะติดกับโปรแกรมต่าง ๆ เพื่อให้โปรแกรมเหล่านั้นนำพาไปยังส่วนต่าง ๆ ของระบบเพื่อจะได้แพร่กระจายไปสู่โปรแกรมอื่น ๆ ที่ยังไม่มีโปรแกรมไวรัสเกาะอยู่ ซึ่งการแพร่กระจายจะเป็นลักษณะทวีคูณ ทำลายเป้าหมายได้ทุกรูปแบบตามเจตนาของผู้เขียนโปรแกรม ไวรัสคอมพิวเตอร์มักจะแบ่งประเภทตามแหล่งที่อาศัยภายในระบบหรือโปรแกรมที่จะกระทำการโดยเฉพาะ เช่น ไวรัสในส่วนการปลุกเครื่อง (Boot Sector Virus) มาโครไวรัส (Macro Virus) เป็นต้น ไวรัสคอมพิวเตอร์จะกระทำการ (Active) ได้ก็ต่อเมื่อโปรแกรมเป้าหมายที่โปรแกรมไวรัสอาศัยอยู่มีการดำเนินการ (Run/Process)

๘.๒ หนอน (Worm) เป็นโปรแกรมที่สามารถสำเนาตัวเอง (Copy) ให้แพร่กระจายในระบบเครือข่าย และสามารถกระทำการ (Active) ต่าง ๆ ได้โดยลำพัง ไม่ต้องอาศัยโปรแกรมอื่น ๆ ในการนำพาไปยังส่วนต่าง ๆ ของระบบ ทำลายระบบโดยการสำเนาตัวเองเพิ่มขึ้นเรื่อย ๆ จนระบบไม่สามารถทำงานต่อไปได้

๘.๓ ตัวลวง...

๘.๓ ตัวลวง หรือ ม้าโทรจัน (Trojan Horse) เป็นโปรแกรม หรือส่วนของโปรแกรมที่ถูกนำมาซ่อนไว้ในโปรแกรมใช้งานโปรแกรมใดโปรแกรมหนึ่งภายในระบบโดยผู้ใช้ไม่ทราบและคิดว่าเป็นโปรแกรมที่ใช้งานตามปกติ มักกระทำโดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องกับการบำรุงรักษาโปรแกรม เช่น โปรแกรมม้าโทรจันที่แทรกมากับบท (คำสั่ง) ลงบันทึกเข้า (Login Script) ที่รอให้บริการแก่ผู้ใช้ที่ต้องการเข้าสู่ระบบใดระบบหนึ่ง โดยการใส่บัญชีผู้ใช้และรหัสผ่าน ซึ่งนอกจากทำหน้าที่ตรวจสอบความถูกต้องแท้จริงในการเข้าระบบของผู้ใช้แล้วยังแอบสำเนาบัญชีผู้ใช้และรหัสผ่านดังกล่าวเก็บไว้ใช้ประโยชน์ส่วนตัวในภายหลัง

ม้าโทรจันไม่สามารถเคลื่อนย้ายหรือสำเนาตัวเองได้ บางครั้งใช้เป็นที่พรางตัวของโปรแกรมประสงค์ร้ายอื่น ๆ มักเป็นไปในลักษณะของการเชิญชวนให้เกิดความสนใจและนำโปรแกรมดังกล่าวบรรจุเข้าในระบบ ซึ่งผู้ใช้เองที่นำม้าโทรจันเข้าสู่ระบบโดยไม่เจตนา เช่น เกมส์คอมพิวเตอร์ (Computer Game) โปรแกรมอรรถประโยชน์ (Utility Program) ภาพอนาจาร (Nude) เป็นต้น ซึ่งโปรแกรมเหล่านี้เมื่อบรรจุเข้าระบบได้แล้วก็อาจแพร่ไวรัสหรือโปรแกรมประสงค์ร้ายอื่น ๆ ได้

๘.๔ กับดัก (Trap Door) เป็นโปรแกรมที่สร้างให้มีหนทางลับหรืออภิสิทธิ์ในการเข้าสู่ระบบ โปรแกรมหรือข้อมูลเป้าหมายได้เฉพาะบุคคล และตลอดเวลาที่ต้องการ โดยปกติมีวัตถุประสงค์ให้ผู้ควบคุมระบบใช้เป็นทางเข้าเพื่อดูแล บำรุงรักษา หรือตรวจสอบระบบ เช่น โปรแกรมของเครื่องรับจ่ายเงินอัตโนมัติ (Automatic Teller Machine) กำหนดให้รหัสผ่าน ๙๙๙๙ เป็นรหัสผ่านที่สามารถเข้าถึงการบันทึกเข้าออก (Log) ของรายการเปลี่ยนแปลง (Transaction) ยอดเงินฝากเข้าลูกค้า

กับดักกระทำได้โดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องในช่วงที่กำลังพัฒนาโปรแกรมซึ่งอาจสร้างทางลับเพื่อหาประโยชน์อย่างใดอย่างหนึ่งจากระบบในภายหลังจากตัวอย่างข้างต้นเมื่อสามารถเข้าสู่แฟ้มบันทึกเข้าออก (Log File) ของรายการเปลี่ยนแปลงได้แล้วอาจสร้างโปรแกรมให้มีการโอนเงินหลังจุดทศนิยมจากรายการเปลี่ยนแปลงมาสะสมไว้ในบัญชีลับบัญชีใดบัญชีหนึ่งได้

๘.๕ ระเบิด (Bomb) เป็นโปรแกรมที่มีเจตนาร้ายอย่างใดอย่างหนึ่ง จะดำเนินการเมื่อมีเหตุการณ์ตรงตามเงื่อนไขเกิดขึ้น ได้แก่ เงื่อนไขเวลา วันที่ หรือเงื่อนไขอื่น ๆ เช่น โปรแกรมกำหนดให้จัดรูปแบบจานบันทึกแบบแข็ง (Format Hard Disk) เมื่อมีผู้เข้าใช้ระบบที่มีบัญชีผู้ใช้ขึ้นต้นด้วยอักษร “ S” ครบ ๕๐ ครั้ง เป็นต้น

อย่างไรก็ตามปัจจุบันโปรแกรมประสงค์ร้ายได้มีการพัฒนาความสามารถในการทำลาย และการหลบหลีกการตรวจจับของโปรแกรมป้องกันต่าง ๆ อยู่เสมอ ดังนั้นในอนาคตจะปรากฏโปรแกรมประสงค์ร้ายในรูปแบบที่มีการผสมผสานกันหลาย ๆ ประเภทมากยิ่งขึ้น

๙. Password ความหมาย ในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: รหัสผ่าน

อธิบายความหมาย

: เป็นชุดของตัวอักษรหรือคำพิเศษ (Special Word) หรือวลี (Phase) ซึ่งให้สิทธิในการเข้าถึงระบบแก่ผู้ใช้แต่ละคน นอกจากนี้รหัสผ่านยังเป็นเครื่องมือรักษาความปลอดภัยที่ใช้แสดงต่อระบบคอมพิวเตอร์เพื่อให้การรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้ และตรวจสอบสิทธิในการใช้งานระบบ (Access to its Resources) ดังนั้นจึงต้องมีการกำหนดระเบียบปฏิบัติให้ผู้ใช้สามารถจัดการรหัสผ่านของตนเองได้อย่างปลอดภัยและถูกต้อง

๑๐. Program ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ๑. โปรแกรม, ชุดคำสั่ง

: ๒. สร้างโปรแกรม

อธิบายความหมาย

: เป็นชุดคำสั่งที่ต่อเนื่องกันเป็นลำดับเพื่อให้คอมพิวเตอร์ประมวลผลในลักษณะที่ต้องการ อาจอยู่ในรูปของการเขียนโปรแกรมด้วยภาษาระดับสูง (High-Level) ซึ่งต้องผ่านการแปลความหมายให้เป็นรหัสจุดหมาย (Object Code) ก่อน คอมพิวเตอร์จึงประมวลผลได้ หรืออาจอยู่ในรูปของรหัสจุดหมาย (Object Code) ซึ่งสามารถสั่งให้คอมพิวเตอร์ประมวลผลได้โดยตรง โปรแกรมคอมพิวเตอร์โดยทั่วไป แบ่งเป็น ๒ ประเภท คือ

- โปรแกรมระบบ (System Program) ได้แก่ โปรแกรมระบบปฏิบัติการ (Operating System Program) โปรแกรมบรรจุ (Loader, Loading Program) ตัวแปลโปรแกรม หรือโปรแกรมแปลโปรแกรมหรือคอมไพเลอร์ (Compiler) เป็นต้น โปรแกรมเหล่านี้ช่วยอำนวยความสะดวกในการใช้งานคอมพิวเตอร์

- โปรแกรมประยุกต์ หรือโปรแกรมใช้งาน (Application Program) เป็นโปรแกรมที่สร้างขึ้นโดยมีวัตถุประสงค์เพื่อการใช้งานในลักษณะใดลักษณะหนึ่งโดยเฉพาะ เช่น โปรแกรมประมวลผลคำ (Word Processing) - สารบรรณ - ธุรการ โปรแกรมทางธุรกิจ - การเงิน - การธนาคาร โปรแกรมเกี่ยวกับงานวิจัย - การศึกษา - การพยากรณ์ โปรแกรมควบคุมการทำงานของอุปกรณ์ - เครื่องมือเฉพาะอย่าง เป็นต้น โปรแกรมเหล่านี้มักจะเขียนด้วยภาษาระดับสูง และใช้ประโยชน์เพียงกลุ่มผู้ใช้บางกลุ่มเท่านั้น รวมทั้งต้องมีการปรับปรุงเปลี่ยนแปลงโปรแกรมเพื่อให้ใช้งานได้ทันสมัยอยู่เสมอ

๑๑. Removable Storage Devices สื่อบันทึกข้อมูลที่เคลื่อนที่ได้ หมายถึง อุปกรณ์เชื่อมต่อใด ๆ ที่สามารถเก็บข้อมูลได้ เช่น External Hard Disk, USB Drive, เครื่องเล่น MP3, หรือ อื่น ๆ

๑๒. Software...

๑๒. Software ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ส่วนชุดคำสั่ง ซอฟต์แวร์

อธิบายความหมาย

: เป็นคำที่ใช้เรียกโปรแกรมหรือโปรแกรมคอมพิวเตอร์โดยทั่วไป ต้องการแสดงให้เห็นถึงความแตกต่างระหว่าง ฮาร์ดแวร์ และซอฟต์แวร์ซึ่งเป็นองค์ประกอบของระบบคอมพิวเตอร์

: เป็นคำสั่งที่อยู่ในรูปภาษาเครื่อง (Machine Language) ซึ่งเป็นภาษาระดับต่ำ (Low-Level) ที่หน่วยประมวลผลกลางของคอมพิวเตอร์สามารถเข้าใจและประมวลผลตามคำสั่งนั้นได้ทันที โดยทั่วไปมี ๒ ประเภท คือ ซอฟต์แวร์ระบบปฏิบัติการ (Operating System Software) และซอฟต์แวร์ประยุกต์ (Application Software)

แบบรายการตรวจติดตาม

การปฏิบัติตามระเบียบกองทัพอากาศ

ว่าด้วยรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

พ.ศ. ๒๕๕๒

แบบรายการตรวจติดตาม

การปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

พ.ศ. ๒๕๕๒

ชื่อหน่วยงาน	.....	ตรวจสำรวจเมื่อ วันที่...../...../.....

หมวดที่ ๑ กล่าวทั่วไป(ต้องมีการตั้งคณะกรรมการ ฯ ในข้อ ๑ หรือ ๒ ตามความเหมาะสม)

๑. แต่งตั้ง คณก. รักษาความปลอดภัยระบบสารสนเทศของระบบงาน (หากไม่มีให้ดูข้อ ๒)	๑.๑. น.รักษาความปลอดภัยระบบสารสนเทศของระบบงาน
◯ มี ชื่อระบบงาน.....	◯ มี ยศ ชื่อ.....เมื่อ.....
◯ ไม่มี	◯ ไม่มี
๒. แต่งตั้ง คณก. รักษาความปลอดภัยระบบสารสนเทศของหน่วย	๒.๑ น.รักษาความปลอดภัยระบบสารสนเทศ
◯ มี แต่งตั้งเมื่อ.....	◯ มี ยศ ชื่อ.....เมื่อ.....
◯ ไม่มี	◯ ไม่มี

๓. ผู้ปฏิบัติหน้าที่ด้านระบบสารสนเทศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ	◯ มี	◯ ไม่มี
◯ ผู้บริหารระบบ	◯ ผู้บริหารฐานข้อมูล	◯ ผู้บริหารเครือข่าย ◯ ผู้เขียนโปรแกรม

หมวดที่ ๒ การรักษาความปลอดภัยสภาพแวดล้อมของระบบสารสนเทศ และการจัดการด้านการรักษาความปลอดภัยระบบสารสนเทศ

๔. น.รักษาความปลอดภัยระบบสารสนเทศตามข้อ ๒.๑ เข้ารับการอบรมเกี่ยวกับการ รปภ. ระบบสารสนเทศ	◯ ผ่าน	◯ ไม่ผ่าน

๕. หน่วยงานจัดทำทะเบียนความไว้วางใจของผู้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศตามระดับความไว้วางใจ

๕.๑ การจัดทำทะเบียน ◯ เรียบร้อย ◯ ยังไม่ได้จัดทำ	๕.๒ สำเนาให้ ทสส.ทอ. ◯ เรียบร้อย ◯ ยังไม่ได้สำเนา

๖. หน่วยงานมีการกำหนดให้อาคาร สถานที่ ซึ่งเป็นที่ตั้งและที่ใช้งาน ของระบบสารสนเทศ เป็นพื้นที่หวงห้าม	เขตหวงห้าม " เด็ดขาด หรือ เฉพาะ " ◯ มี ◯ ไม่มี

๗. หน่วยงานพิจารณากำหนดมาตรการป้องกันเพิ่มเติมตามความเหมาะสม

กำหนดมาตรการเรื่อง.....

.....

๘. การปฏิบัติเมื่อเกิดสถานการณ์ในเวลาฉุกเฉิน

๘.๑ อาคาร สถานที่ ของที่ตั้งระบบสารสนเทศมีการจัดให้มีเวร-ยามรักษาการณ์	◯ มี	◯ ไม่มี

๘.๒ หน่วยงานเจ้าของอาคาร สถานที่ มีการจัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินต่างๆ เช่น แผนเผชิญเหตุ (Contingency Planning)	◯ มีแผนรองรับ ◯ ไม่มีแผน
๘.๓ หากสถานการณ์ฉุกเฉินรุนแรงจนไม่สามารถดูแลรักษาระบบสารสนเทศได้ เช่น แผนการเคลื่อนย้าย หรือแผนการทำลายระบบสารสนเทศ	◯ มีแผนรองรับ ◯ ไม่มีแผน
๘.๔ การดำเนินการสำหรับการฟื้นฟูระบบสารสนเทศที่เกิดความเสียหาย	◯ มีแผนรองรับ ◯ ไม่มีแผน
๘.๕ การดำเนินการสำหรับการสำรองข้อมูลระบบสารสนเทศ	◯ มีแผนรองรับ ◯ ไม่มีแผน
๘.๖ การดำเนินการเมื่อประสบภัยธรรมชาติและอัคคีภัย	◯ มีแผนรองรับ ◯ ไม่มีแผน
๙. การกำหนดมาตรการป้องกันที่เหมาะสมกับสภาพแวดล้อมของระบบสารสนเทศโดยทำแผนจัดการความเสี่ยง (Risk Management Plan)	
โดยผ่าน ◯ การประเมินความเสี่ยง(risk assessment) ◯ ความอ่อนแอ(vulnerability) ◯ ภัย(threat) ◯ ยังไม่ได้กำหนด	
๑๐. หน่วยงานกำหนดรหัสผ่าน (password)ที่เหมาะสมสำหรับผู้ใช้ทุกระดับตามข้อกำหนด	◯ มีการกำหนดครบ ◯ บางส่วน
◯ ๑๐.๑ มีความยาวอย่างน้อย ๘ ตัวอักษร	
◯ ๑๐.๒ ประกอบด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลขและอักขระพิเศษ	
◯ ๑๐.๓ ต้องไม่มีข้อมูลเกี่ยวกับผู้ใช้ เช่น วันเกิด ชื่อเล่น หมายเลขโทรศัพท์ เป็นต้น	
◯ ๑๐.๔ เปลี่ยนรหัสผ่านตามช่วงเวลาที่กำหนด	
◯ ๑๐.๕ ไม่เปิดเผยรหัสผ่านให้แก่ผู้อื่น หรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตน	
◯ ๑๐.๖ รหัสผ่านสำหรับระบบสารสนเทศที่มีความสำคัญ ไม่ควรเป็นรหัสเดียวกับระบบสารสนเทศทั่วๆไป	
◯ ๑๐.๗ ไม่ใช้รหัสผ่านร่วมกับผู้อื่นโดยเด็ดขาด	
หมวดที่ ๓ การรักษาความปลอดภัยระบบคอมพิวเตอร์	
๑๑. การจัดทำรายการอุปกรณ์ สถานภาพการใช้งาน และกำหนดผู้ดูแลรับผิดชอบ	◯ จัดทำแล้ว ◯ ไม่ได้จัดทำ
๑๒. การจัดทำแผนผัง สถานที่ติดตั้งอุปกรณ์คอมพิวเตอร์และเครือข่าย	◯ จัดทำแล้ว ◯ ไม่ได้จัดทำ
๑๓. กำหนดมาตรการจัดเก็บสิ่งบันทึกข้อมูลเช่น ซีดีรอม ฯ ที่มีชั้นความลับ	◯ มีมาตรการ ◯ ไม่มีมาตรการ
๑๔. หน่วยงานมีผู้พัฒนาโปรแกรมเพื่อนำไปใช้ในระบบสารสนเทศ ดำเนินการพัฒนาโปรแกรมตามหลักวิชาการ และยินยอมให้ทำการตรวจสอบ รายละเอียดที่จำเป็นต่อการ รปภ.ระบบสารสนเทศ	◯ มีผู้พัฒนาและมีการตรวจสอบ ◯ ไม่มีผู้พัฒนาหรือไม่มีการตรวจสอบ
หมวดที่ ๔ การรักษาความปลอดภัยระบบสื่อสาร	
๑๕. การรับส่งข้อมูลสารสนเทศที่มีชั้นความลับผ่านระบบเครือข่ายคอมพิวเตอร์ จะต้องทำการเข้ารหัส (encryption) ตามมาตรฐานที่ได้รับการรับรองจาก ทสส.ทอ. ◯ มีการเข้ารหัส ◯ ยังไม่มีการเข้ารหัส	
๑๖. การใช้งานเครือข่ายไร้สายทั้งในด้านยุทธการ และธุรการ จะต้องมีการป้องกันทั้งการพิสูจน์ทราบและการเข้ารหัส โดยมีการขึ้นทะเบียนอุปกรณ์ (WiFi) เพื่อตรวจสอบและยืนยันความปลอดภัยจาก ทสส.ทอ. ◯ มีกระบวนการป้องกัน ◯ ยังไม่ได้ดำเนินการ	

๑๗. ระบบเครือข่ายทางด้านยุทธการเชื่อมต่อกับระบบอินเทอร์เน็ต	◯ เชื่อมต่อ ◯ ไม่เชื่อมต่อ
หมวดที่ ๕ การรักษาความปลอดภัยสารสนเทศ	
๑๘. ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูล มีการจัดระดับการป้องกันผู้มีสิทธิเข้าไปใช้งาน หากเป็นข้อมูลที่มีชั้นความลับ ต้องมีการเข้ารหัสในการจัดเก็บที่เหมาะสม	
◯ มีการกำหนดสิทธิและเข้ารหัสข้อมูล ◯ มีการกำหนดสิทธิแต่ไม่ได้เข้ารหัสข้อมูล ◯ ไม่มีทั้งการกำหนดสิทธิและเข้ารหัส	
๑๙. หน่วยงานดำเนินการจัดให้มีแฟ้มลงบันทึกเข้าออกและการใช้งาน (audit log)	◯ มี log file ◯ ไม่มี
๒๐. หน่วยงานดำเนินการชี้แจงข้าราชการทุกคนให้รับทราบถึงวิธีการใช้ระบบสารสนเทศที่ปลอดภัยรวมถึงการตรวจสอบและลงโทษ กรณีการละเมิดการรักษาความปลอดภัยต่อระบบสารสนเทศของกองทัพอากาศ อันเกิดขึ้นจากการกระทำที่ฝ่าฝืน หรือละเลย ส่งผลกระทบเสียหายต่อกองทัพอากาศ	
◯ ดำเนินการชี้แจ้งอย่างต่อเนื่อง ◯ ดำเนินการชี้แจ้งแล้ว ◯ ยังไม่ได้ดำเนินการชี้แจง	

CIO หน่วย..... ลงชื่อ

( )

...../...../.....

หน.แผนกรักษาความปลอดภัยระบบสารสนเทศ ลงชื่อ

กคส.ทสส.ทอ. ( )

...../...../.....

จัดทำโดย

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ