(สำเนา) หน่วยรับ

บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สบค.โทร.๒-๐๖๕๗)

ที่ กห ๐๖๐๙.๔/๙๖๔ **วันที่** ๗ ส.ค.๖๓

เรื่อง ขออนุมัติใช้ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

เรียน ผบ.ทอ.

๑. ตามแผนการปฏิบัติงาน ทสส.ทอ. ปี ๖๓ กำหนดให้มีการทบทวนและปรับปรุงระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๕๒ ซึ่งเป็นการดำเนินงานตามแนวทางที่กำหนดไว้ในแนวความคิดการปฏิบัติการในมิติไซเบอร์ ทอ. เพื่อให้ระเบียบ ทอ.ฯ มีความทันสมัยสอดคล้องกับกฎหมายที่เกี่ยวข้อง ภารกิจของหน่วยขึ้นตรง และมาตรฐานสากลในปัจจุบัน นั้น

๒. ทสส.ทอ.ดำเนินการร่างระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ เรียบร้อยแล้ว ดังนี้

๒.๑ กรอบแนวทางการจัดทำเนื้อหา ประกอบด้วย

๒.๑.๑ การกำหนดบทบาทและหน้าที่การปฏิบัติด้านไซเบอร์ และด้านเทคโนโลยีสารสนเทศ โดยไม่ขัดต่อกฎหมายที่เกี่ยวข้องในปัจจุบัน เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ เป็นต้น

๒.๑.๒ มาตรฐานสากลด้าน Information Security Management ISO/IEC27001 : 2013 ซึ่งเป็นเวอร์ชันที่ใช้งานในปัจจุบัน เป็นกรอบการจัดทำเนื้อหาในเอกสาร เนื่องด้วยระเบียบ ทอ.ฯ ฉบับปัจจุบัน (ฉบับ พ.ศ.๒๕๕๒) ได้จัดทำเนื้อหาโดยใช้มาตรฐาน ISO/IEC27001 : 2005 ซึ่งเป็นเวอร์ชันที่ถูกยกเลิกการใช้งานไปแล้ว

๒.๒ ร่างระเบียบ ทอ.ฯ มีเนื้อหา จำนวน ๑๓ หมวด สรุปได้ดังนี้

๒.๒.๑ หมวด ๑ ทั่วไป เกี่ยวกับความมุ่งหมาย และแนวทางการบริหารจัดการความมั่นคงปลอดภัย

๒.๒.๒ หมวด ๒ โครงสร้างการบริหารจัดการความมั่นคงปลอดภัย เกี่ยวกับบทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย และอุปกรณ์พกพาและการปฏิบัติงานจากระยะไกล

๒.๒.๓ หมวด ๓ การรักษาความมั่นคงปลอดภัยด้านบุคคล เกี่ยวกับก่อนการบรรจุเข้าปฏิบัติงาน ระหว่างดำรงสถานภาพการปฏิบัติงาน และการสิ้นสุดสถานภาพและการเปลี่ยนหน้าที่ปฏิบัติงาน

๒.๒.๔ หมวด ๔ การบริหารจัดการทรัพย์สิน เกี่ยวกับความรับผิดชอบต่อทรัพย์สิน การจัดชั้นความลับของสารสนเทศ และการจัดการสื่อบันทึกข้อมูล

๒.๒.๕ หมวด ๕ การควบคุมการเข้าถึง เกี่ยวกับหลักการการควบคุมการเข้าถึง การบริหารจัดการผู้ใช้งานในการเข้าถึงระบบสารสนเทศ หน้าที่ความรับผิดชอบของผู้ใช้งาน และการควบคุมการเข้าถึงสารสนเทศและโปรแกรมประยุกต์

๒.๒.๖ หมวด ๖ การเข้ารหัสสารสนเทศ

๒.๒.๗ หมวด ๗ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เกี่ยวกับพื้นที่ควบคุมความมั่นคงปลอดภัย และความมั่นคงปลอดภัยของอุปกรณ์

๒.๒.๘ หมวด ๘ ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน เกี่ยวกับขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ การป้องกันโปรแกรมประสงค์ร้าย การสำรองข้อมูล การบันทึกข้อมูลเหตุการณ์และการเฝ้าระวัง การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ และการบริหารจัดการช่องโหว่ทางเทคนิค

๒.๒.๙ หมวด ๙ ...

๒.๒.๙ หมวด ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล เกี่ยวกับการบริหารจัดการการรักษาความปลอดภัยเครือข่ายสารสนเทศ และการถ่ายโอนสารสนเทศ

๒.๒.๑๐ หมวด ๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบ เกี่ยวกับการกำหนดความต้องการด้านความมั่นคงปลอดภัยระบบสารสนเทศ และความมั่นคงปลอดภัยสำหรับกระบวนการในการสนับสนุนและการพัฒนาระบบ

๒.๒.๑๑ หมวด ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก เกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก และการบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก

๒.๒.๑๒ หมวด ๑๒ การบริหารจัดการสถานการณ์ (Incident) ความมั่นคงปลอดภัยสารสนเทศ

๒.๒.๑๓ หมวด ๑๓ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๓. ทสส.ทอ.พิจารณาแล้ว เพื่อให้การดำเนินการรักษาความปลอดภัยระบบสารสนเทศ ทอ. เป็นไปด้วยความเรียบร้อยและเกิดความปลอดภัยสูงสุด จึงเห็นควรยกเลิก ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๕๒ และใช้ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ (ตามแนบ)

จึงเรียนมาเพื่อพิจารณาอนุมัติตามข้อ ๓ และลงชื่อในระเบียบ ทอ.ฯ ที่แนบให้ต่อไป

(ลงชื่อ) พล.อ.ท.ประยูร ธรรมาธิวัฒน์
จก.ทสส.ทอ.

(ลงชื่อ) พล.อ.ท.ธนศักดิ์ เมตะนันท์
รอง เสธ.ทอ.(ยก.)
๑๐ ส.ค.๖๓

เรียน ผบ.ทอ.
กระผมพิจารณาแล้ว เห็นสมควรอนุมัติ ตามข้อ ๓ และลงชื่อในระเบียบ ทอ.ฯ ที่แนบ

(ลงชื่อ) พล.อ.อ.สุทธิพันธุ์ ต่ายทอง
เสธ.ทอ.
๒๔ ส.ค.๖๓

อนุมัติตามข้อ ๓, ลงชื่อแล้ว

(ลงชื่อ) พล.อ.อ.มานัต วงษ์วาทย์

ผบ.ทอ.

๓๑ ส.ค.๖๓

<u>การแจกจ่าย</u>

- นขต.ทอ.

สำเนาถูกต้อง

น.อ.

(นิวัติ เนียมพลอย)

ผอ.กคช.สบค.ทสส.ทอ.

๒ ก.ย.๖๓

จ.ท.ทศพล ฯ พิมพ์/ทาน

น.อ. ตรวจ

ระเบียบกองทัพอากาศ
ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ
พ.ศ.๒๕๖๓

โดยที่เป็นการสมควรแก้ไข ปรับปรุง ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศให้มีความทันสมัยและเหมาะสมยิ่งขึ้น จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ.๒๕๕๒

บรรดาระเบียบและคำสั่งอื่นใด ในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ การดำเนินการรักษาความปลอดภัยตามระเบียบนี้ให้ยึดถือและปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และฉบับแก้ไขเพิ่มเติม ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ และฉบับแก้ไขเพิ่มเติม และระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๖๐ เป็นมูลฐาน

ข้อ ๕ ระเบียบนี้ให้ใช้บังคับแก่หน่วยขึ้นตรงกองทัพอากาศ บุคคลในสังกัดกองทัพอากาศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับสารสนเทศและระบบสารสนเทศของกองทัพอากาศ

ข้อ ๖ ในระเบียบนี้

๖.๑ "สารสนเทศ" (Information) หมายความว่า สิ่งที่มีต้นกำเนิดจากข้อมูล เช่น ตัวอักษร ตัวเลข ข้อความ รูปภาพ เป็นต้น โดยการได้มาซึ่งสารสนเทศนั้นต้องมีการนำข้อมูลผ่านการประมวลผล การจัดระเบียบด้วยวิธีต่าง ๆ เช่น การประมวลผลด้วยระบบคอมพิวเตอร์ การประมวลผลภายในระบบสารสนเทศ เป็นต้น เพื่อให้ข้อมูลเหล่านั้นอยู่ในรูปแบบที่มีความหมาย ผู้ใช้งานสามารถเข้าใจได้ และนำไปใช้ประโยชน์ในการปฏิบัติงาน การบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๖.๒ "สารสนเทศที่กำหนดชั้นความลับ" หมายความว่า สารสนเทศในรูปข้อมูล หรือข่าวสารที่บันทึกไว้ในแบบใด ๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหาจำกัดการเข้าถึง หรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงสื่อบันทึกข้อมูลลับ รหัส และรหัสผ่านที่กำลังใช้อยู่ หรือเตรียมจะใช้ตลอดจนวัสดุ หรือเอกสารทุกอย่างที่บันทึกเรื่องดังกล่าว

๖.๓ "คอมพิวเตอร์" ...

๖.๓ “คอมพิวเตอร์” (Computer) หมายความว่า เครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์ที่มีส่วนเครื่อง (Hardware) ประกอบด้วย ๓ ส่วนหลัก คือ ส่วนนำเข้าข้อมูล (Input) ส่วนประมวลผล (Process) และส่วนแสดงผล (Output) และประกอบด้วยซอฟต์แวร์ควบคุมการทำงานหรือซอฟต์แวร์ระบบปฏิบัติการ (Operating System) เป็นอย่างน้อย ทั้งนี้เครื่องมือหรืออุปกรณ์อาจมีลักษณะเป็นคอมพิวเตอร์แบบตั้งโต๊ะ คอมพิวเตอร์แบบโน้ตบุ๊ก อุปกรณ์แบบพกพา เช่น แท็ปเล็ต เป็นต้น และโทรศัพท์แบบฉลาด (Smart Phone) ตลอดจนระบบคอมพิวเตอร์ฝังตัว (Embedded Computer) ที่มีความสามารถในการคำนวณอัตโนมัติตามคำสั่งที่ฝังอยู่ในตัวเครื่อง

๖.๔ “ระบบคอมพิวเตอร์” (Computer System) หมายความว่า อุปกรณ์ที่ประกอบด้วย ส่วนเครื่อง (Hardware) ส่วนซอฟต์แวร์จำนวน ๒ ส่วน ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ (Operating System) และซอฟต์แวร์ประยุกต์ (Application Software) เพื่อใช้เป็นระบบจัดทำข้อมูล เช่น ตัวเลข ข้อความ รูปภาพ เสียง หรืออยู่ในรูปอื่น ๆ เป็นต้น และใช้ประมวลผลข้อมูลเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้

๖.๕ “ระบบสารสนเทศ” (Information System) หมายความว่า ระบบที่ประกอบด้วย บุคคล ระบบคอมพิวเตอร์ ซอฟต์แวร์ ฐานข้อมูล เครือข่ายสารสนเทศ และกระบวนการ ได้แก่ วิธีการสร้างข้อมูล วิธีการประมวลผลข้อมูล วิธีการเก็บข้อมูล และวิธีการแสดงผล โดยทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อเปลี่ยนข้อมูลให้เป็นสารสนเทศและส่งการแสดงผลให้ผู้ใช้งานสามารถนำไปใช้ประโยชน์ในการปฏิบัติงานหรือสนับสนุนการปฏิบัติภารกิจของหน่วยงาน โดยระบบสารสนเทศของกองทัพอากาศแบ่งออกเป็น ๒ ประเภทหลัก คือ ระบบสารสนเทศเพื่อการสนับสนุน (Support Information System : SIS) เช่น ระบบสารสนเทศเพื่อการบริหาร (Management Information System : MIS) ของหน่วยงาน เป็นต้น และระบบสารสนเทศเพื่อการยุทธ (Combat Information System : CIS) เช่น ระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link : TDL) ระบบบัญชาการและควบคุมทางอากาศ (Air Command and Control System : ACCS) เป็นต้น

๖.๖ “เครือข่ายสารสนเทศ” (Information Network) หมายความว่า ระบบคอมพิวเตอร์และอุปกรณ์ที่เชื่อมต่อกันเป็นเครือข่ายด้วยอุปกรณ์เชื่อมต่อเครือข่ายและสื่อการเชื่อมต่อทั้งที่เป็นสื่อการเชื่อมต่อแบบใช้สายและไร้สาย เพื่อการรับส่งข้อมูลและสารสนเทศกันระหว่างระบบคอมพิวเตอร์ รวมถึงการรับส่งข้อมูลและสารสนเทศภายในระบบสารสนเทศเดียวกันหรือระหว่างระบบสารสนเทศที่ถูกนำมาใช้งานร่วมกัน ทั้งนี้ ให้รวมถึงเครือข่ายอินทราเน็ต (Intranet) และเครือข่ายอินเทอร์เน็ต (Internet) ของกองทัพอากาศ ด้วย

๖.๗ “โครงสร้างพื้นฐานสำคัญ” (Critialcal Infrastructure) หมายความว่า บรรดาหน่วยขึ้นตรงกองทัพอากาศ ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วย มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของกองทัพอากาศ

๖.๘ “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” (Critical Information Infrastructure) หมายความว่า ระบบสารสนเทศของหน่วยขึ้นตรงกองทัพอากาศซึ่งเป็นโครงสร้างพื้นฐานสำคัญของกองทัพอากาศใช้สนับสนุนการปฏิบัติภารกิจของกองทัพอากาศ หากระบบถูกรบกวนจะทำให้ไม่สามารถปฏิบัติภารกิจได้

๖.๙ “พื้นที่ใช้งานระบบสารสนเทศ” (Information System Workspaces) หมายความว่า พื้นที่ติดตั้งระบบคอมพิวเตอร์ เครือข่ายสารสนเทศ ระบบสารสนเทศ รวมทั้งพื้นที่เตรียมข้อมูลจัดเก็บในคอมพิวเตอร์ ห้องทำงานของบุคลากรทางคอมพิวเตอร์

๖.๑๐ “ไซเบอร์” ...

๖.๑๐ "ไซเบอร์" (Cyber) หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

๖.๑๑ "ภัยคุกคาม" (Threat) หมายความว่า อันตรายที่อาจเกิดขึ้นกับสารสนเทศโดยบุคคล (Person) สิ่งต่าง ๆ (Thing) หรือเหตุการณ์ (Event) ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูลของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นตามความต้องการของภัยคุกคาม นั้น

๖.๑๒ "ภัยคุกคามทางไซเบอร์" (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ ที่ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมประสงค์ร้ายโดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๖.๑๓ "ช่องโหว่" (Vulnerability) หมายความว่า จุดอ่อนหรือข้อบกพร่องใด ๆ ของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งหากมีภัยคุกคามในรูปแบบที่เหมาะกัน สามารถถูกนำไปใช้ประโยชน์เพื่อก่อให้เกิดความเสียหายต่อสารสนเทศและข้อมูล

๖.๑๔ "ความเสี่ยง" (Risk) หมายความว่า โอกาสที่เอื้อให้ภัยคุกคามต่าง ๆ สร้างความเสียหายในรูปแบบที่เหมาะกับช่องโหว่ ที่มีอยู่ในระบบคอมพิวเตอร์และระบบสารสนเทศ และความรุนแรงที่เกิดจากภัยนั้น ซึ่งความเสียหายประเภทเดียวกันอาจมีระดับความเสี่ยงไม่เท่ากัน ในแต่ละพื้นที่ใช้งานระบบสารสนเทศ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่าในพื้นที่ แต่ละแห่งควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่นเพียงใด

๖.๑๕ "ประเมินความเสี่ยง" (Risk Assessment) หมายความว่า กระบวนการวิเคราะห์ภัยคุกคามต่าง ๆ และความอ่อนแอของระบบคอมพิวเตอร์และระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความมั่นคงปลอดภัยของสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมให้สารสนเทศต่อไป

๖.๑๖ "การรักษาความมั่นคงปลอดภัยสารสนเทศ" หมายความว่า การดำเนินการเพื่อให้สารสนเทศ มีคุณสมบัติดังนี้ มีการรักษาความลับ (Confidentiality) มีการรักษาความน่าเชื่อถือ (Integrity) และมีสภาพพร้อมใช้งาน (Availability)

๖.๑๗ "การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

๖.๑๘ "ผู้ปฏิบัติหน้าที่ด้านระบบสารสนเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ" หมายความว่า ผู้ที่เกี่ยวข้องกับการจัดการระบบสารสนเทศในด้านต่าง ๆ เช่น ผู้บริหารระบบ (System Administrator) ผู้บริหารฐานข้อมูล (Database Administrator) ผู้บริหารเครือข่าย (Network Administrator) และนักเขียนโปรแกรม (Programmer) เป็นต้น

๖.๑๙ "เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์" หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๖.๒๐ "โปรแกรม...

๖.๒๐ “โปรแกรมประสงค์ร้าย” (Malware) หมายความว่า โปรแกรมคอมพิวเตอร์ที่ทำงานในลักษณะโจมตีระบบ ทำให้ระบบเสียหายรวมไปถึงการจารกรรมข้อมูลบนเครื่องคอมพิวเตอร์ของผู้ใช้งานตลอดจนโปรแกรมประเภทขโมยข้อมูล และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรมเบราว์เซอร์ แบ่งออกได้หลากหลายประเภท เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) และการแอบดักจับข้อมูล (Spyware) เป็นต้น

๖.๒๑ การใช้คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้องกับระเบียบนี้ ให้อ้างอิงจากผนวก ข

ข้อ ๗ ให้เจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ รักษาการให้เป็นไปตามระเบียบนี้

หมวด ๑
ทั่วไป

ส่วนที่ ๑
ความมุ่งหมาย

ข้อ ๘ ระเบียบนี้มีความมุ่งหมายเพื่อ

๘.๑ กำหนดหลักการ และมาตรการป้องกันระบบสารสนเทศของกองทัพอากาศเพื่อรักษาไว้ซึ่งคุณสมบัติที่มั่นคงปลอดภัยของระบบสารสนเทศ ได้แก่ การรักษาความลับ (Confidentiality) ความครบถ้วนสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ

๘.๒ รักษาความต่อเนื่องในการดำเนินการให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศของกองทัพอากาศ

ส่วนที่ ๒
แนวทางการบริหารจัดการความมั่นคงปลอดภัย

ข้อ ๙ การกำหนดมาตรการ หรือระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศนั้น ระบบสารสนเทศและการดำเนินการกับสารสนเทศที่เกี่ยวข้องต้องผ่านการประเมินความเสี่ยง (Risk Assessment) ช่องโหว่ (Vulnerability) ภัยคุกคาม (Threat) เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับระบบสารสนเทศ โดยการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Management Plan) รองรับเพื่อมุ่งเน้นให้มีแผนปฏิบัติการที่สามารถแปลงเป็นมาตรการป้องกันที่มีความเข้มแข็ง (Robustness) ต่อภัยคุกคามทางไซเบอร์ได้อย่างแท้จริง และกำหนดให้มีการปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ ๑๐ แนวทางการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ต้องดำเนินการให้ถึงระดับที่สมดุลกับความเสี่ยงที่ประเมินได้

ข้อ ๑๑ ต้องดำเนินการตรวจสอบ ทบทวน และประเมินแนวทางบริหารความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย ๑ ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญที่มีผลกระทบต่อระบบสารสนเทศ

ข้อ ๑๒ การรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการตามระเบียบนี้เป็นพื้นฐาน ควบคู่กับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกองทัพอากาศ เพื่อรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานให้สามารถสนับสนุนการปฏิบัติภารกิจของกองทัพอากาศได้อย่างต่อเนื่อง

หมวด ๒ ...

หมวด ๒
โครงสร้างการบริหารจัดการความมั่นคงปลอดภัย

ส่วนที่ ๑
บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย

ข้อ ๑๓ เพื่อให้การดำเนินงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศเป็นไปอย่างมีประสิทธิภาพ จึงแบ่งมอบบทบาทและหน้าที่ความรับผิดชอบ ไว้ในส่วนนี้

๑๓.๑ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีหน้าที่รับผิดชอบกำหนดมาตรการ แนวทางปฏิบัติ ประเมิน ตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ของกองทัพอากาศ ให้เป็นไปตามความมุ่งหมายของระเบียบนี้ และเป็นหน่วยงานในการประสานการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ กับหน่วยงานภายนอกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ รวมทั้งให้มีหน้าที่ดังต่อไปนี้

๑๓.๑.๑ ประเมินความมั่นคงปลอดภัยของระบบสารสนเทศและการดำเนินการกับสารสนเทศ เพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

๑๓.๑.๒ พัฒนาหลักการ และกระบวนการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และส่งเสริมความร่วมมือกับหน่วยงานภายนอกที่เกี่ยวข้อง

๑๓.๑.๓ สนับสนุนและส่งเสริมให้มีการศึกษาหลักสูตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ อย่างต่อเนื่อง

๑๓.๑.๔ ให้มีการฝึกอบรม สัมมนาและดูงาน เกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

๑๓.๑.๕ ตรวจสอบให้มีการปฏิบัติตามระเบียบนี้

๑๓.๑.๖ แจ้งผลการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ (Information System Security Audit) รวมทั้งพิจารณาให้คำแนะนำ ติดตามและประเมินผลตามนโยบายและระเบียบนี้

๑๓.๒ ศูนย์ไซเบอร์กองทัพอากาศ มีหน้าที่รับผิดชอบ ปฏิบัติการตามกระบวนการป้องกัน ป้องปราม และตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการปฏิบัติอื่น ๆ ที่กำหนดไว้ในระเบียบนี้

๑๓.๓ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ มีหน้าที่รับผิดชอบ ดำรงรักษาสถานภาพการใช้งานระบบสารสนเทศและการสื่อสาร และสนับสนุนระบบรวมถึงอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ของกองทัพอากาศ ให้เป็นไปตามความมุ่งหมายของระเบียบนี้

๑๓.๔ ให้หน่วยขึ้นตรงกองทัพอากาศ ดำเนินการจัดโครงสร้างบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศภายในหน่วยงาน ดังนี้

๑๓.๔.๑ แต่งตั้งนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๑๓.๔.๒ แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ประกอบด้วย

๑๓.๔.๒.๑ หัวหน้า หรือรองหัวหน้าหน่วยขึ้นตรงกองทัพอากาศ เป็นประธาน

๑๓.๔.๒.๒ หัวหน้าส่วน...

๑๓.๔.๒.๒ หัวหน้าส่วนราชการของหน่วย เป็นกรรมการ

๑๓.๔.๒.๓ นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เป็นกรรมการและเลขานุการ

๑๓.๔.๒.๔ ผู้ดูแลระบบ ได้แก่ ผู้ดูแลเครือข่ายสารสนเทศ ผู้ดูแลระบบสารสนเทศของหน่วย (กรณีหน่วยขึ้นตรงมีระบบสารสนเทศภายในหน่วย) และผู้ดูแลระบบสารสนเทศของระบบงานของกองทัพอากาศ (กรณีหน่วยขึ้นตรงรับผิดชอบระบบงานของกองทัพอากาศ) เป็นกรรมการ

๑๓.๔.๒.๕ ผู้เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และบุคคลตามผนวก ก ตามความเหมาะสม เป็นกรรมการ

๑๓.๔.๓ คณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ มีหน้าที่

๑๓.๔.๓.๑ จัดทำแผนบริหารจัดการความเสี่ยงการดำเนินการเกี่ยวกับสารสนเทศและระบบสารสนเทศของหน่วย และของระบบงานของกองทัพอากาศ ตามแนวทางข้อ ๙ (กรณีหน่วยขึ้นตรงรับผิดชอบระบบงานของกองทัพอากาศ)

๑๓.๔.๓.๒ จัดทำมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้สอดคล้องกับ ข้อ ๑๓.๔.๓.๑ และข้อกำหนดในระเบียบนี้

๑๓.๔.๓.๓ จัดทำแผนที่เกี่ยวข้อง ดังนี้

๑๓.๔.๓.๓ (๑) แผนการสำรองข้อมูลและสารสนเทศ

๑๓.๔.๓.๓ (๒) แผนฟื้นฟูระบบสารสนเทศ

๑๓.๔.๓.๓ (๓) แผนป้องกันภัยธรรมชาติ

๑๓.๔.๓.๓ (๔) แผนป้องกันอัคคีภัย

๑๓.๔.๓.๓ (๕) แผนเผชิญเหตุ (Contingency Plan)

๑๓.๔.๓.๓ (๖) แผนป้องกันภัยที่หน่วยงานนั้นพิจารณาว่าควรจัดทำตามสภาพแวดล้อม

๑๓.๔.๔ นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ มีหน้าที่รับผิดชอบ ดำเนินการให้เป็นไปตามระเบียบนี้และมาตรการที่กำหนดในข้อ ๑๓.๔.๓.๒

ส่วนที่ ๒
อุปกรณ์พกพาและการปฏิบัติงานจากระยะไกล

ข้อ ๑๔ เพื่อรักษาความมั่นคงปลอดภัยระบบสารสนเทศในการปฏิบัติงานจากภายนอกกองทัพอากาศและการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๑๕ หน่วยขึ้นตรงกองทัพอากาศต้องกำหนดให้มีมาตรการรองรับ การนำอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น คอมพิวเตอร์แบบโน้ตบุ๊ก แท็ปเล็ต Smart Phone และอุปกรณ์สื่อสารเคลื่อนที่อื่น ๆ เป็นต้น จากภายนอกมาใช้งานโดยเชื่อมต่อกับเครือข่ายสารสนเทศภายในหน่วยงาน ด้วยการลงทะเบียนขอใช้อุปกรณ์ดังกล่าวก่อนอนุญาตให้ใช้งาน เพื่อบริหารจัดการความเสี่ยงที่มาจากอุปกรณ์ดังกล่าว และควรคำนึงถึงความเสี่ยงของการทำงานในสภาพแวดล้อมที่ไม่ได้รับการป้องกัน

ข้อ ๑๖ ในกรณีที่จำเป็นต้องอนุญาตให้มีการปฏิบัติงานจากภายนอกกองทัพอากาศให้ปฏิบัติตามข้อกำหนดที่เกี่ยวข้องในหมวด ๕ เพื่อให้มีการตรวจพิสูจน์ตัวตนและควบคุมการทำงานจากระยะไกลโดยการแบ่งระหว่างระบบที่เชื่อมต่อเครือข่ายอินเทอร์เน็ตกับเครือข่ายอินทราเน็ต และการใช้งาน

เครือข่ายส่วน...

เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) โดยต้องมีการยืนยันตัวตนผู้ใช้งานแบบสองวิธีเป็นอย่างน้อย เพื่อเข้าสู่ระบบอินทราเน็ตของกองทัพอากาศ

หมวด ๓
การรักษาความมั่นคงปลอดภัยด้านบุคคล

ข้อ ๑๗ เพื่อกำหนดให้บุคคลมีบทบาทและหน้าที่ความรับผิดชอบในการปฏิบัติงานให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศที่ตนเองเข้าไปเกี่ยวข้อง ตลอดจนควบคุมการปฏิบัติของบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศ จึงไม่ให้สิทธิ์บุคคลอื่นใดที่จะอ้างยศ ตำแหน่ง หรืออำนาจ เพื่อขอทราบ หรือให้ได้มาซึ่งสารสนเทศที่ตนไม่ได้รับอนุญาต หรือขอยกเว้นการปฏิบัติตามระเบียบนี้

ส่วนที่ ๑
ก่อนการบรรจุเข้าปฏิบัติงาน

ข้อ ๑๘ ให้หน่วยขึ้นตรงกองทัพอากาศตรวจสอบความไว้วางใจบุคคลโดยละเอียดผ่านกรมข่าวทหารอากาศ และให้หัวหน้าหน่วยนั้นรับรองความไว้วางใจบุคคล ก่อนที่จะมอบหมายให้บุคคลใดปฏิบัติหน้าที่เกี่ยวกับสารสนเทศ โดยยึดถือผลการตรวจสอบประวัติ และพฤติการณ์ของบุคคลนั้นเป็นแนวทางการพิจารณาตามที่เห็นสมควร ในกรณีจำเป็นเร่งด่วนหัวหน้าหน่วยอาจรับรองความไว้วางใจบุคคลให้เข้าถึงสารสนเทศที่มีชั้นความลับไม่เกินชั้นความลับที่ขอรับรอง โดยมีเงื่อนไขว่าหากผลการตรวจสอบปรากฏว่าผู้นั้นมีประวัติหรือพฤติการณ์ไม่เหมาะสม ให้ผู้ที่ได้รับการมอบหมายพ้นจากการปฏิบัติหน้าที่เกี่ยวกับสารสนเทศทันที บุคคลที่ไม่เกี่ยวข้องกับสารสนเทศโดยตรง เข้ามาทำงานเป็นประจำภายในพื้นที่ใช้งานระบบสารสนเทศ เช่น เจ้าหน้าที่รับส่งหนังสือราชการ พนักงานทำความสะอาด เป็นต้น ต้องทำการตรวจสอบประวัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และฉบับแก้ไขเพิ่มเติม และให้กำหนดช่วงเวลาทำงานที่แน่นอนของบุคคลดังกล่าว ในระหว่างนั้นต้องมีเจ้าหน้าที่ประจำพื้นที่ใช้งานระบบสารสนเทศควบคุมดูแลอยู่ด้วยอย่างน้อย ๑ คน

ข้อ ๑๙ ให้นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ดำเนินการดังนี้

๑๙.๑ ชี้แจงเรื่องการรักษาความปลอดภัยตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และฉบับแก้ไขเพิ่มเติม และการปฏิบัติที่เกี่ยวข้องในมาตรการที่กำหนดในข้อ ๑๓.๔.๓.๒ และในระเบียบนี้แก่บุคคลที่จะปฏิบัติหน้าที่เกี่ยวกับสารสนเทศ

๑๙.๒ จัดทำทะเบียนความไว้วางใจของบุคคลตามระดับความไว้วางใจที่แต่ละบุคคลได้รับอนุมัติ และจัดเก็บเป็นหลักฐานเพื่อรับการตรวจสอบและประเมินด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๑๙.๓ แจ้งให้ทราบวัตถุประสงค์ของการนำข้อมูลส่วนบุคคลไปใช้งาน โดยดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ระเบียบ คำสั่ง แนวปฏิบัติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของกองทัพอากาศ

ส่วนที่ ๒ ...

ส่วนที่ ๒
ระหว่างดำรงสถานภาพการปฏิบัติงาน

ข้อ ๒๐ เพื่อให้บุคคลที่ปฏิบัติงาน ทั้งจากภายในและภายนอกกองทัพอากาศมีความตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยระบบสารสนเทศ จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๒๑ นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ต้องผ่านการอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ รวมทั้งจะต้องไม่ได้รับมอบหมายให้รับผิดชอบภารกิจอื่นที่เป็นอุปสรรค หรือเป็นภัยต่อความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

ข้อ ๒๒ นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ต้องชี้แจงให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับสารสนเทศได้ทราบถึงความเสียหายต่อความมั่นคงของชาติ ทัณฑ์ทางวินัยในการเปิดเผยความลับของทางราชการ รวมทั้งโทษตามกฎหมายในการเปิดเผยความลับของทางราชการแก่บุคคลผู้ไม่มีหน้าที่เกี่ยวข้องทราบ

ข้อ ๒๓ เมื่อบุคคลใดจะเข้าปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ลงชื่อในใบบันทึกรับรองการรักษาความลับเมื่อเข้ารับตำแหน่งหรือหน้าที่ (รปภ.๑๗) หรือใบรับรองการรักษาความลับตามที่กำหนดไว้ในระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และฉบับแก้ไขเพิ่มเติมในข้อที่เกี่ยวข้อง

ข้อ ๒๔ ให้มีการกำหนดมาตรการ ควบคุม ดูแล และตรวจสอบสิทธิ์การเข้าถึงระบบสารสนเทศ โดยบุคคลที่จะเข้าใช้ระบบสารสนเทศจะต้องได้รับอนุญาตจากผู้ดูแลรับผิดชอบที่เกี่ยวข้องก่อน และการเข้าถึงระบบสารสนเทศต้องคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก บุคคลที่ไม่มีอำนาจหน้าที่รับผิดชอบจะอนุญาตให้บุคคลอื่นเข้าถึงระบบสารสนเทศไม่ได้

ข้อ ๒๕ หากบุคคลมีพฤติการณ์ไม่น่าไว้วางใจหรืออาจเป็นภัยต่อระบบสารสนเทศ ให้ผู้ดูแลรับผิดชอบที่เกี่ยวข้อง รายงานถึงนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศโดยทันที เพื่อดำเนินการตามมาตรการรักษาความปลอดภัยและข้อกฎหมายที่เกี่ยวข้องต่อไป

ส่วนที่ ๓
การสิ้นสุดสถานภาพและการเปลี่ยนหน้าที่ปฏิบัติงาน

ข้อ ๒๖ เมื่อบุคคลใดพ้นจากการปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ และจัดทำรายชื่อบุคคลดังกล่าวเก็บไว้เป็นหลักฐานเพื่อการตรวจสอบ และให้ลงชื่อในใบรับรองการรักษาความลับเมื่อพ้นตำแหน่งหรือหน้าที่ (รปภ.๑๘) ตามที่กำหนดไว้ในระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และฉบับแก้ไขเพิ่มเติม ในข้อที่เกี่ยวข้อง เพื่อปกป้องระบบสารสนเทศซึ่งเป็นผลมาจากการสิ้นสุดสถานภาพหรือการเปลี่ยนหน้าที่ปฏิบัติงานของบุคคลที่เกี่ยวข้องกับสารสนเทศ

หมวด ๔ ....

หมวด ๔
การบริหารจัดการทรัพย์สิน

ส่วนที่ ๑
ความรับผิดชอบต่อทรัพย์สิน

ข้อ ๒๗ เพื่อกำหนดให้มีการระบุทรัพย์สินที่เกี่ยวข้องกับการดำเนินการกับระบบสารสนเทศ รวมทั้งทรัพย์สินที่เป็นองค์ประกอบในระบบสารสนเทศ และกำหนดความรับผิดชอบในการป้องกันทรัพย์สินที่เหมาะสม จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๒๘ หน่วยขึ้นตรงกองทัพอากาศต้องจัดทำบัญชีหรือทะเบียนเฉพาะทรัพย์สินประเภทอุปกรณ์คอมพิวเตอร์ รวมถึงอุปกรณ์อื่นที่เกี่ยวข้องกับการประมวลผลสารสนเทศของหน่วยหรือของระบบงาน และอุปกรณ์เชื่อมต่อเครือข่ายสารสนเทศ โดยจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับทรัพย์สิน ซึ่งทรัพย์สินทั้งหมดต้องมีการระบุผู้ถือครองหรือผู้รับผิดชอบ รวมถึงมีหลักฐานเอกสารการรับทรัพย์สินไปถือครองหรือรับผิดชอบ และมีการปรับปรุงบัญชีให้เป็นปัจจุบัน

ข้อ ๒๙ หน่วยขึ้นตรงกองทัพอากาศต้องกำกับดูแลการใช้ทรัพย์สินให้เป็นไปตามกำหนดกฎเกณฑ์ในการใช้ทรัพย์สินอย่างเหมาะสมเพื่อให้เกิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๓๐ เมื่อสิ้นสุดการใช้งานหรือความรับผิดชอบต่อทรัพย์สิน ผู้ถือครองหรือผู้รับผิดชอบทรัพย์สินต้องส่งคืนทรัพย์สิน พร้อมมีเอกสารหลักฐานการส่งคืนทรัพย์สิน

ข้อ ๓๑ การเคลื่อนย้ายทรัพย์สินเข้า-ออก พื้นที่ของหน่วยงาน หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะแวดล้อมการใช้งานทรัพย์สินเปลี่ยนแปลงไปจะต้องแจ้งและขออนุญาตต่อนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ก่อนการเคลื่อนย้ายทุกครั้ง

ส่วนที่ ๒
การจัดชั้นความลับของสารสนเทศ

ข้อ ๓๒ เพื่อให้มั่นใจได้ว่าสารสนเทศได้รับการปกป้องตามระดับความสำคัญของสารสนเทศที่มีต่อหน่วยขึ้นตรงกองทัพอากาศและกองทัพอากาศ จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๓๓ การกำหนดชั้นความลับของสารสนเทศ ให้เป็นไปตามกฎหมาย หรือระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ และฉบับแก้ไขเพิ่มเติม และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และฉบับแก้ไขเพิ่มเติม หรือกฎหมายและระเบียบอื่นที่เกี่ยวข้อง

ข้อ ๓๔ ต้องมีการจัดทำป้ายชื่อของข้อมูล โดยต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับฉลากเอกสารข้อมูล ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

ข้อ ๓๕ ก่อนนำทรัพย์สินประเภทอุปกรณ์คอมพิวเตอร์หรือทรัพย์สินใด ๆ ที่เกี่ยวข้องกับสารสนเทศหรือการประมวลผลสารสนเทศ ไปซ่อมบำรุง หรือจำหน่ายขายซากให้บุคคลภายนอกกองทัพอากาศ หรือนำกลับไปใช้งานในภารกิจใหม่ภายหลังจากใช้งานในภารกิจอื่น ๆ มาแล้ว ต้องทำลายข้อมูลก่อนมีการดำเนินการดังกล่าว รวมถึงการโอนสิทธิ์การถือครองทรัพย์สินในลักษณะอื่น ๆ ต้องทำลาย

ข้อมูลทั้งหมดที่มีชั้นความลับตั้งแต่ “ลับ” ขึ้นไปที่อยู่ในทรัพย์สินดังกล่าวไม่ให้สามารถกู้คืนมาใช้งานได้อีก ในกรณีที่นำทรัพย์สินดังกล่าวไปซ่อมภายนอกกองทัพอากาศ และมีการเปลี่ยนชิ้นส่วน เพื่อทดแทนชิ้นส่วนที่ชำรุดเสียหาย ให้นายทหารรักษาความมั่นปลอดภัยระบบสารสนเทศดำเนินการนำชิ้นส่วนดังกล่าวกลับมาดำเนินการให้ถูกต้องตามกระบวนการของทางราชการต่อไป

ส่วนที่ ๓
การจัดการสื่อบันทึกข้อมูล

ข้อ ๓๖ เพื่อป้องกันสารสนเทศที่จัดเก็บในสื่อบันทึกข้อมูลโดยการเปิดเผยที่ไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บไว้ในสื่อบันทึกข้อมูล จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๓๗ การจัดเก็บสื่อบันทึกข้อมูล เช่น ซีดีรอม และอื่น ๆ เป็นต้น ที่เป็นสื่อในลักษณะถอดแยกและเคลื่อนย้ายได้ โดยมีสารสนเทศที่กำหนดชั้นความลับบันทึกไว้ในสื่อดังกล่าว ต้องแสดงชั้นความลับไว้บนสื่อบันทึกข้อมูลนั้น และให้พิทักษ์รักษาตามชั้นความลับนั้น และให้เก็บในกล่อง หรือหีบห่อ ซึ่งมีเครื่องหมายแสดงชั้นความลับนั้น ๆ

ข้อ ๓๘ ห้ามมิให้ผู้ใดมีการใช้งานสื่อบันทึกข้อมูลที่ถอดย้ายได้ (Removable Storage Devices) ในพื้นที่ใช้งานระบบสารสนเทศที่มีชั้นความลับ และที่เกี่ยวข้องกับงานด้านยุทธการ

ข้อ ๓๙ เมื่อหมดความต้องการในการใช้งานสื่อบันทึกข้อมูลที่มีชั้นความลับ ต้องมีการกำจัดหรือทำลายทิ้งโดยปฏิบัติตามกระบวนการทำลายข้อมูลของทางราชการ ภายใต้สิ่งแวดล้อมที่ได้มีการควบคุม

ข้อ ๔๐ การจัดส่งสื่อบันทึกข้อมูล ต้องมีวิธีการจัดส่งให้มีความมั่นคงปลอดภัยจากการถูกเปิดเผยต่อผู้ที่ไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือการทำให้เกิดความเสียหายระหว่างจัดส่ง

หมวด ๕
การควบคุมการเข้าถึง

ส่วนที่ ๑
หลักการการควบคุมการเข้าถึง

ข้อ ๔๑ เพื่อควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศให้มีความมั่นคงปลอดภัย จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๔๒ นโยบายควบคุมการเข้าถึง

๔๒.๑ กำหนดให้มีการควบคุมการใช้งานสารสนเทศและระบบสารสนเทศเพื่อควบคุมการเข้าถึง ให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๔๒.๒ ผู้ใช้งานสารสนเทศและระบบสารสนเทศจะต้องได้รับอนุญาตจากผู้บังคับบัญชาตามความจำเป็นในการปฏิบัติงาน และต้องถูกกำหนดสิทธิ์การเข้าถึงให้เหมาะสมกับการปฏิบัติงานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนให้เริ่มเข้าใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามวาระการปฏิบัติงาน

๔๒.๓ การแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงสารสนเทศและระบบสารสนเทศเป็นหน้าที่ของผู้ดูแลระบบสารสนเทศเท่านั้น

๔๒.๔ ต้องมีการ...

๔๒.๔ ต้องมีการบันทึกและติดตามการใช้งานสารสนเทศและระบบสารสนเทศและเฝ้าระวังการละเมิดความปลอดภัย

๔๒.๕ ต้องมีการจัดทำทะเบียนบันทึกรายละเอียด การเข้าถึง การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๔๒.๖ การเข้าถึงเครือข่ายและบริการเครือข่าย ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

๔๒.๖.๑ ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศและสถานภาพความพร้อมใช้งานของเครือข่าย ทั้งนี้ให้มีการควบคุม ดังนี้

๔๒.๖.๑.๑ ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย เช่น Secure Socket Layer (SSL) เป็นต้น

๔๒.๖.๑.๒ จำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth ในช่วงเวลาทำการ เช่น การรับส่งไฟล์ขนาดใหญ่ ฟังเพลงออนไลน์ ดูทีวีออนไลน์ หรือเล่นเกมออนไลน์ เป็นต้น ยกเว้นกรณีที่ได้รับอนุญาตเพื่อการปฏิบัติงาน

๔๒.๖.๒ เครือข่ายสารสนเทศต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสมเพื่อรักษาความมั่นคงปลอดภัยต่อสารสนเทศและระบบสารสนเทศ ทั้งนี้ให้ครอบคลุมองค์ประกอบดังนี้

๔๒.๖.๒.๑ อุปกรณ์ที่เชื่อมต่อกับเครือข่ายสารสนเทศทั้งหมดต้องได้รับการตั้งค่าให้มีความปลอดภัยและมีการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับเครือข่าย

๔๒.๖.๒.๒ ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรมและได้รับการติดตั้งโดยผู้ที่มีความชำนาญที่ผ่านการพิจารณาอนุมัติแล้ว

๔๒.๖.๒.๓ อุปกรณ์เชื่อมต่อเครือข่าย เช่น Router Firewall Switch และ Wireless Access Point เป็นต้น ต้องได้รับการตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัย และต้องมีอุปกรณ์สำรองไฟฟ้า (UPS) สนับสนุนให้พร้อมใช้งานอยู่เสมอ

๔๒.๖.๒.๔ IP Address ต้องได้รับการลงทะเบียน แจกจ่ายและบริหารจัดการจากส่วนกลางโดยกรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ

๔๒.๖.๒.๕ การเปลี่ยนแปลงเครือข่ายหรืออุปกรณ์เชื่อมต่อเครือข่ายต้องได้รับการควบคุมโดยนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ หรือกรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ ทั้งนี้ขึ้นอยู่กับเครือข่ายที่อยู่ในขอบเขตความรับผิดชอบ

๔๒.๖.๒.๖ เครือข่ายสารสนเทศต้องได้รับการออกแบบ และตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวตามความต้องการใช้งานในอนาคต (Scalable)

๔๒.๖.๓ ข้อตกลงการให้บริการเครือข่ายสารสนเทศต้องระบุถึงรายละเอียดและข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัย ระดับการให้บริการและการบริหารจัดการบริการเครือข่ายทั้งหมด หากการบริการเครือข่ายนั้นได้รับการดำเนินการโดยหน่วยงานภายนอก ต้องมีการระบุถึงสิทธิ์ของกองทัพอากาศที่สามารถติดตามตรวจสอบและตรวจประเมินการทำงานของหน่วยงานภายนอกด้วย

ส่วนที่ ๒ ...

ส่วนที่ ๒

การบริหารจัดการผู้ใช้งานในการเข้าถึงระบบสารสนเทศ

ข้อ ๔๓ การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์การเข้าถึงระบบสารสนเทศตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์ เช่น เมื่อลาออก เกษียณอายุราชการ หรือเมื่อเปลี่ยนตำแหน่งงาน เป็นต้น โดยผู้ใช้งานต้องได้รับการพิจารณาอนุมัติตามขั้นตอน อย่างเคร่งครัด

ข้อ ๔๔ การจัดการสิทธิ์ผู้ใช้งาน ต้องมีการกำหนดวิธีการในการบริหารจัดการสิทธิ์ ทั้งการให้สิทธิ์และการยกเลิกสิทธิ์ สำหรับผู้ใช้งานทุกประเภท

ข้อ ๔๕ การบริหารจัดการสิทธิ์การเข้าถึงระบบสารสนเทศ

๔๕.๑ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงสารสนเทศและระบบสารสนเทศแต่ละส่วนอย่างชัดเจน รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

๔๕.๒ ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งก่อนเข้าถึงระบบสารสนเทศ

๔๕.๓ การเข้าสู่ระบบ (Log in) ที่มีความมั่นคงปลอดภัย ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง

๔๕.๔ ต้องจัดให้มีระบบบริหารจัดการรหัสผ่าน (Password) หรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านทุก ๆ ๑๘๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๔๖ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน ต้องมีกระบวนการจัดการซึ่งเป็นความลับ

ข้อ ๔๗ การทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ต้องดำเนินการตามระยะเวลาที่กำหนดไว้

ข้อ ๔๘ การถอนหรือการปรับปรุงสิทธิ์การเข้าถึงของกำลังพลกองทัพอากาศและบุคคลภายนอกต่อระบบสารสนเทศ ต้องถูกยกเลิกสิทธิ์เมื่อสิ้นสุดสถานภาพการปฏิบัติงาน การจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงสิทธิ์ให้ถูกต้องอยู่เสมอ

ส่วนที่ ๓

หน้าที่ความรับผิดชอบของผู้ใช้งาน

ข้อ ๔๙ การใช้ข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน ต้องมีการปฏิบัติเพื่อรักษาความลับ ดังนี้

๔๙.๑ การเก็บรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ต้องเป็นความลับ

๔๙.๒ เมื่อเข้าใช้งานระบบครั้งแรก ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่าน (Password) เริ่มต้นเป็นรหัสผ่านของผู้ใช้งานทันที

ส่วนที่ ๔ ...

ส่วนที่ ๔

การควบคุมการเข้าถึงสารสนเทศและโปรแกรมประยุกต์

ข้อ ๕๐ การจำกัดการเข้าถึงสารสนเทศ

๕๐.๑ ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน และลบ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๕๐.๒ บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator เป็นต้น ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๕๐.๓ บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามระเบียบนี้ อย่างเคร่งครัดก่อนที่จะได้รับอนุญาตให้เข้าถึงสารสนเทศ

ข้อ ๕๑ การใช้โปรแกรมประยุกต์

๕๑.๑ การใช้โปรแกรมประยุกต์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยระบบสารสนเทศ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

๕๑.๒ ต้องกำหนดการควบคุมการใช้โปรแกรมประยุกต์สำหรับระบบสารสนเทศเพื่อป้องกันการใช้งานโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่ ให้ทำการแยกโปรแกรมประยุกต์ออกจากโปรแกรมระบบงาน และ จำกัดการใช้งานให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

ข้อ ๕๒ การควบคุมการเข้าถึงซอร์สโค้ด (Source Code) ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึงซอร์สโค้ดของระบบที่ใช้งานจริงหรือให้บริการ เช่น ต้องเก็บซอร์สโค้ดไว้ในที่ที่ปลอดภัย ไม่ควรเก็บซอร์สโค้ดไว้ในเครื่องที่ใช้งานจริง และต้องไม่เก็บซอร์สโค้ดที่อยู่ในระหว่างทดสอบรวมไว้กับซอร์สโค้ดที่ใช้งานได้จริงแล้ว เป็นต้น

หมวด ๖

การเข้ารหัสสารสนเทศ

ข้อ ๕๓ การส่งสารสนเทศที่มีชั้นความลับผ่านเครือข่ายสารสนเทศ จะต้องได้รับอนุมัติจากเจ้าของ ผู้มีสิทธิ์และอำนาจในสายงาน ที่กำหนดชั้นความลับนั้นก่อน เมื่อได้รับอนุมัติแล้ว สารสนเทศที่กำหนดชั้นความลับจะต้องถูกส่งด้วยการเข้ารหัส (Encryption) โดยมาตรฐานที่ได้รับการรับรองแล้วจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ผู้มีสิทธิ์และอำนาจในสายงานสามารถกำหนดระเบียบปฏิบัติของการเข้าใช้ที่สอดคล้องกับระเบียบนี้

ข้อ ๕๔ หากมีการใช้เครือข่ายไร้สายทั้งในด้านยุทธการและธุรการต้องมีการป้องกันทั้งการพิสูจน์ทราบและการเข้ารหัสที่ได้รับการยืนยันความปลอดภัยจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ โดยต้องมีการขึ้นทะเบียนอุปกรณ์เชื่อมต่อแบบไร้สาย (WiFi Access Point) เพื่อตรวจสอบการใช้งานด้วย

ข้อ ๕๕ ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ที่จัดเก็บในระบบฐานข้อมูลต้องได้รับการจัดระดับการป้องกัน ผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความมั่นคงปลอดภัย และข้อมูล ข่าวสาร สารสนเทศที่กำหนดชั้นความลับต้องมีการเข้ารหัสข้อมูลที่จัดเก็บในระบบฐานข้อมูลโดยใช้รูปแบบการเข้ารหัสตามมาตรฐานที่กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศกำหนด

ข้อ ๕๖ กุญแจเพื่อ...

ข้อ ๕๖ กุญแจเพื่อการเข้าและถอดรหัสลับ (Encryption and Decryption Key) ทุกชนิดที่ใช้ในการเข้ารหัสสารสนเทศให้จัดเป็นสารสนเทศที่กำหนดชั้นความลับ “ลับ” ขึ้นไป ต้องจำกัดการเข้าถึงเท่าที่จำเป็น โดยมีขนาดของกุญแจ (จำนวน bit) ที่เหมาะสมและควรเปลี่ยนตามวาระ ดังนี้

๕๖.๑ ตามห้วงระยะเวลาอย่างน้อย ๓ เดือนต่อหนึ่งครั้ง หรือหากเกี่ยวข้องกับงานด้านยุทธการ ให้กำหนดระยะเวลาตามความจำเป็น

๕๖.๒ เมื่อมีการเปลี่ยนเจ้าหน้าที่ที่เกี่ยวข้องกับการเข้ารหัส ให้ดำเนินการพร้อมทั้งสั่งยกเลิกกุญแจเพื่อเข้าและถอดรหัสลับ (Encryption and Decryption Key) เดิม

๕๖.๓ เมื่อความลับรั่วไหลหรือสงสัยว่าความลับรั่วไหล ให้ยกเลิกกุญแจเพื่อเข้าและถอดรหัสลับ (Encryption and Decryption Key) ทันที

หมวด ๗
ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ส่วนที่ ๑
พื้นที่ควบคุมความมั่นคงปลอดภัย

ข้อ ๕๗ เพื่อป้องกันไม่ให้มีการเข้าถึงอาคาร สถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศและพื้นที่ใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาต ซึ่งจะก่อให้เกิดความเสียหาย และการแทรกแซงต่อสารสนเทศ และโครงสร้างพื้นฐานและอุปกรณ์ประมวลผลสารสนเทศ เพิ่มเติมจากการปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และฉบับแก้ไขเพิ่มเติม และระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๖๐ จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๕๘ ให้หน่วยขึ้นตรงกองทัพอากาศกำหนดให้ อาคาร สถานที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศอื่นใด เป็นพื้นที่หวงห้าม โดยพิจารณาตามความสำคัญว่าจะต้องพิทักษ์รักษาสิ่งที่เป็นความลับของสารสนเทศ โดยให้กำหนดเป็น “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ” แล้วแต่กรณี

๕๘.๑ พื้นที่ใช้งานระบบสารสนเทศในส่วนที่เป็นหน่วยแสดงผล ต้องปลอดภัยจากการได้ยินและการมองเห็นของผู้ไม่มีอำนาจหน้าที่ที่จะเข้าถึง รวมถึงการบันทึกภาพจากกล้องวงจรปิด โดยให้กำหนดมาตรการควบคุมบุคคลก่อนจะเข้าพื้นที่หวงห้ามอีกชั้นหนึ่งด้วย

๕๘.๒ ให้หน่วยพิจารณากำหนดมาตรการป้องกันเพิ่มเติมให้เหมาะสม เช่น ห้ามนำอุปกรณ์สื่อสาร ถ่ายภาพ หรือสื่อบันทึกข้อมูลที่ถอดย้ายได้ (Removable Storage Device) เข้าไปภายใน “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ” เป็นต้น

ข้อ ๕๙ หน่วยขึ้นตรงกองทัพอากาศต้องจัดทำแผนผังแสดงตำแหน่ง และชนิดของพื้นที่ใช้งานสารสนเทศ โดยระบุประเภทพื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน

ข้อ ๖๐ หน่วยขึ้นตรงกองทัพอากาศต้องดูแลรักษาสภาพแวดล้อมพื้นที่ใช้งานระบบสารสนเทศให้เป็นระเบียบ เหมาะสมเพื่อดำรงรักษาสถานภาพความพร้อมใช้งานของระบบ

ข้อ ๖๑ การควบคุมการเข้า-ออก บริเวณพื้นที่ใช้งานระบบสารสนเทศ โดยให้ผ่านเข้า-ออกได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น และมีแนวทางปฏิบัติ ดังนี้

๖๑.๑ ต้องกำหนดบุคคลที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออกในแต่ละพื้นที่อย่างชัดเจน

๖๑.๒ บุคคลจะได้...

๖๑.๒ บุคคลจะได้รับสิทธิ์ให้เข้า-ออกสถานที่ได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๖๑.๓ หากมีบุคคลอื่นใดที่ไม่ใช่ผู้มีหน้าที่ปฏิบัติงานขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยขึ้นตรงต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกข้อมูลของบุคคลและการขอเข้า-ออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่อนุญาตให้เข้าพื้นที่) พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย ๑ ปี

๖๑.๔ บุคคลภายนอกต้องทำการแลกบัตรผู้มาติดต่อโดยใช้บัตรที่หน่วยงานของรัฐออกให้ เช่น บัตรประจำตัวประชาชน ใบขับขี่ หนังสือเดินทาง เป็นต้น ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่

๖๑.๕ ผู้ปฏิบัติงานของหน่วยและบุคคลภายนอกต้องติดบัตรผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่ ทั้งนี้ บัตรประจำตัวประชาชน และบัตรผู้มาติดต่อ ไม่อนุญาตให้โอนกรรมสิทธิ์หรือหยิบยืมใช้งาน

๖๑.๖ ผู้ปฏิบัติงานของหน่วยต้องไม่เปิดประตูเข้าพื้นที่ทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่โดยเด็ดขาด

๖๑.๗ ผู้ปฏิบัติงานต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่ติดบัตรเจ้าหน้าที่หรือบัตรผู้มาติดต่อ

๖๑.๘ ผู้ปฏิบัติงานต้องติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สำนักงาน

ข้อ ๖๒ การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ

๖๒.๑ หน่วยขึ้นตรงกองทัพอากาศต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้สำนักงาน ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สำนักงานหรือห้องจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตูและหน้าต่างของสำนักงานหรือห้องต้องใส่กุญแจเสมอเมื่อไม่มีคนอยู่ และเครื่องโทรสารหรือเครื่องถ่ายเอกสารต้องตั้งแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

๖๒.๒ ผู้ปฏิบัติงานต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงานเพื่อให้มั่นใจว่า ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อคอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๖๒.๓ ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้บนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยไม่มีผู้เฝ้าดูแลอย่างเด็ดขาด

๖๒.๔ ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม

๖๒.๕ เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

ข้อ ๖๓ การปฏิบัติ...

ข้อ ๖๓ การปฏิบัติงานในพื้นที่ควบคุมการปฏิบัติงาน

๖๓.๑ ต้องมีการควบคุมการปฏิบัติงานของบุคคลภายนอกในบริเวณพื้นที่ควบคุม เช่น การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณนั้น เป็นต้น

๖๓.๒ หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

ข้อ ๖๔ การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับส่งสิ่งของ หน่วยขึ้นตรงต้องมีการจำกัดพื้นที่การเข้าถึงของบุคคลภายนอก หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการปฏิบัติงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น พื้นที่เก็บและจัดส่งสินค้าจะต้องถูกแยกออกจากพื้นที่ปฏิบัติงาน เป็นต้น

ข้อ ๖๕ การปฏิบัติในเวลาฉุกเฉิน

๖๕.๑ อาคารและสถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศที่จัดให้มีเวรยามรักษาการณ์เพื่อพิทักษ์รักษาระบบสารสนเทศโดยเฉพาะแล้ว ให้ถือว่าเป็นการปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๖๐

๖๕.๒ ให้หน่วยขึ้นตรงกองทัพอากาศ จัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนป้องกันอัคคีภัยของระบบสารสนเทศ และแผนเผชิญเหตุ (Contingency Plan) เป็นต้น โดยเตรียมอุปกรณ์สนับสนุนในการเคลื่อนย้ายสารสนเทศและทำลายระบบสารสนเทศไว้ให้พร้อมที่จะปฏิบัติได้ทันท่วงที และชี้แจงให้เจ้าหน้าที่ผู้เกี่ยวข้อง เข้าใจวิธีและขั้นตอนปฏิบัติ โดยยึดแนวทางปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๖๐

๖๕.๓ หากสถานการณ์รุนแรงจนไม่สามารถพิทักษ์รักษาระบบสารสนเทศให้ปลอดภัยได้ ให้ทำการเคลื่อนย้ายสารสนเทศและทำลายระบบสารสนเทศตามขั้นตอนปฏิบัติที่ได้จัดทำไว้ในแผนตามข้อ ๖๕.๒

๖๕.๔ เพื่อมิให้ส่วนใดส่วนหนึ่งของสารสนเทศที่กำหนดชั้นความลับตกไปอยู่ในความครอบครองของฝ่ายตรงข้าม หรือผู้ไม่มีอำนาจหน้าที่ ให้ทำลายสารสนเทศที่มีชั้นความลับสูงสุดก่อนและตามลำดับจากมากไปน้อย

๖๕.๕ ให้หน่วยขึ้นตรงกองทัพอากาศ กำหนดมาตรการการป้องกันอัคคีภัย พร้อมจัดเตรียมอุปกรณ์ในการดับเพลิง สำหรับระบบคอมพิวเตอร์ กำหนดมาตรการป้องกันภัยธรรมชาติ พร้อมจัดเตรียมอุปกรณ์ป้องกันภัยธรรมชาติสำหรับระบบคอมพิวเตอร์ จัดเตรียมสถานที่ วัสดุ อุปกรณ์ที่จำเป็นสำหรับการฟื้นฟูระบบ รวมทั้งสถานที่เก็บรักษาสำรองข้อมูลที่ปลอดภัย

ส่วนที่ ๒
ความมั่นคงปลอดภัยของอุปกรณ์

ข้อ ๖๖ การจัดตั้งและการป้องกันอุปกรณ์ ต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัย รวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

ข้อ ๖๗ การดูแลการใช้งานอุปกรณ์ ต้องกำหนดให้มีระบบกระแสไฟฟ้าสำรอง เช่น ใช้ Uninterruptible Power Supply (UPS) เป็นต้น และต้องมีการตรวจสอบระบบไฟฟ้าสำรอง อย่างน้อยปีละ ๒ ครั้ง

ข้อ ๖๘ การบำรุง...

ข้อ ๖๘ การบำรุงรักษาอุปกรณ์ ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ ๑ ครั้ง เป็นต้น

ข้อ ๖๙ ต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ของหน่วยงาน เช่น เครื่องคอมพิวเตอร์พกพา โทรศัพท์มือถือ เป็นต้น เมื่อถูกนำไปใช้งานนอกหน่วย จะต้องปฏิบัติตามมาตรการหรือระเบียบขั้นตอนในการใช้งาน การยืมหรือคืนอุปกรณ์

ข้อ ๗๐ ต้องกำหนดให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้เพื่อป้องกันการรั่วไหล หรือการเปิดเผยข้อมูลดังกล่าวก่อนนำอุปกรณ์ไปแจกจ่ายหรือการนำกลับมาใช้งานใหม่

ข้อ ๗๑ การป้องกันอุปกรณ์ของผู้ใช้งานในขณะที่ไม่มีผู้เฝ้าดูแล ผู้ใช้งานต้องป้องกันไม่ให้ผู้ไม่มีสิทธิ์ สามารถเข้าถึงอุปกรณ์ ระบบสารสนเทศ และระบบคอมพิวเตอร์

ข้อ ๗๒ ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

หมวด ๘
ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

ส่วนที่ ๑
ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ

ข้อ ๗๓ เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๗๔ การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร

๗๔.๑ ต้องจัดทำคู่มือ และ/หรือ ขั้นตอนการปฏิบัติงานสารสนเทศ เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ เป็นต้น

๗๔.๒ คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนการปฏิบัติงานนั้น ๆ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗๕ เมื่อมีการเปลี่ยนแปลงเครือข่ายสารสนเทศ ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ สภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ เช่น ระบบปรับอากาศ น้ำ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ เป็นต้น ต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง โดยต้องมีข้อมูลอย่างน้อย ได้แก่ วันที่ทำการเปลี่ยนแปลงเจ้าของข้อมูล และผู้ดูแลระบบ วิธีการเปลี่ยนแปลง ผลของการเปลี่ยนแปลง (สำเร็จหรือล้มเหลว)

ข้อ ๗๖ การจัดการขีดความสามารถของระบบสารสนเทศ เป็นการติดตามการใช้งานทรัพยากรของระบบสารสนเทศเพื่อใช้ในการพยากรณ์และปรับปรุงระบบเพื่อให้รองรับความต้องการของกองทัพอากาศในอนาคต

๗๖.๑ ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมของทรัพยากรแต่ละชนิด

๗๖.๒ ต้องมีการ...

๗๖.๒ ต้องมีการวางแผนจัดการขีดความสามารถของระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต และสภาพการใช้งานทรัพยากรในปัจจุบัน รวมทั้งการเปลี่ยนแปลงของเทคโนโลยีในอนาคต

ข้อ ๗๗ ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ ในการพัฒนาและทดสอบระบบ รวมทั้งควรแยกระบบเครือข่ายของการพัฒนาออกจากระบบที่ใช้งานจริง ทั้งนี้เพื่อป้องกันปัญหาจากการแก้ไขระบบโดยผู้ที่ไม่ได้รับอนุญาตหรือเกิดจากความผิดพลาดในระหว่างการพัฒนาระบบ

ส่วนที่ ๒

การป้องกันโปรแกรมประสงค์ร้าย (Malware)

ข้อ ๗๘ เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบโน้ตบุ๊ก ต้องได้รับการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย ที่ได้รับการรับรองจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ และต้องเปิดใช้งานซอฟต์แวร์ตลอดเวลาที่ใช้งานเครื่อง

ข้อ ๗๙ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันโปรแกรมประสงค์ร้าย ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Malware Definition) อยู่เสมอ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเครื่องคอมพิวเตอร์ลูกข่ายแบบตั้งโต๊ะ และโน้ตบุ๊กทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันประสงค์ร้าย

ข้อ ๘๐ เอกสารการตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันโปรแกรมประสงค์ร้าย ต้องได้รับการจัดทำและทบทวนให้ทันสมัยตามวงรอบที่เหมาะสม อย่างน้อยทุก ๖ เดือน

ข้อ ๘๑ ห้ามผู้ใช้งานทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ตโดยปราศจากการตรวจสอบผ่านศูนย์ไซเบอร์กองทัพอากาศ หลังจากผ่านการตรวจสอบแล้ว ผู้ใช้งานต้องทำการสแกนด้วยซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย ก่อนการใช้งาน

ข้อ ๘๒ ไฟล์ทั้งหมดที่ดาวน์โหลดในหน่วยงานไม่ว่าจะเป็นไฟล์แนบของอีเมล สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาโปรแกรมประสงค์ร้ายก่อน

ข้อ ๘๓ ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมประสงค์ร้ายใด ๆ และนำเข้าสู่ระบบคอมพิวเตอร์ของหน่วยงาน

ข้อ ๘๔ ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย

ข้อ ๘๕ ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับส่งผ่านเครือข่ายสารสนเทศของหน่วยงานได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก นอกจากนี้ผู้ใช้งานต้องทำการสแกนโปรแกรมประสงค์ร้ายในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย ก่อนเปิดใช้งานเสมอ

ข้อ ๘๖ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้ครั้งคราวเท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมประสงค์ร้าย มีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

ส่วนที่ ๓ ...

ส่วนที่ ๓
การสำรองข้อมูล

ข้อ ๘๗ เพื่อกำหนดให้หน่วยขึ้นตรงกองทัพอากาศต้องสำรองข้อมูลการปฏิบัติภารกิจของหน่วย ให้สามารถนำกลับมาใช้ได้ในภายหลัง ในกรณีที่เกิดเหตุต่าง ๆ ที่ทำให้ข้อมูลสูญหายหรือถูกทำลาย เช่น ภัยจากการโจมตีทางไซเบอร์ ระบบล้มเหลว ภัยจากธรรมชาติ เป็นต้น จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๘๘ กำหนดให้หน่วยขึ้นตรงกองทัพอากาศมีการดำเนินการสำรองข้อมูล ดังนี้

๘๘.๑ ต้องกำหนดความถี่ในการทำการสำรองข้อมูลขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล

๘๘.๒ ต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพสามารถใช้งานได้ตลอดเวลา

๘๘.๓ ต้องมีการควมคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

๘๘.๔ ต้องกำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง

๘๘.๕ ต้องมีการทำเอกสารกระบวนการสำรองข้อมูลและมีการตรวจสอบเป็นวงรอบปฏิบัติประจำ

๘๘.๖ ต้องจัดให้มีทะเบียนการบันทึกข้อมูลที่ทำการสำรองไว้ และการเรียกคืนข้อมูลในแต่ละครั้ง

๘๘.๗ ข้อมูลสำรองต้องได้รับการทดสอบตามห้วงเวลาที่กำหนด เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

๘๘.๘ ต้องลงบันทึกการเก็บสื่อสำรองข้อมูลและสถานที่จัดเก็บ ต้องได้รับการตรวจสอบเป็นประจำทุกปี

๘๘.๙ สื่อที่ใช้สำรองข้อมูลต้องมีป้ายบอกรายละเอียด โดยมีรายละเอียดประกอบอย่างน้อย ได้แก่ ชื่อระบุ วันสร้างข้อมูลสำรอง ระดับความสำคัญของข้อมูล และรายละเอียดติดต่อผู้ดูแลข้อมูล

ส่วนที่ ๔
การบันทึกข้อมูลเหตุการณ์และการเฝ้าระวัง (Logging and Monitoring)

ข้อ ๘๙ เพื่อกำหนดให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศและมีความพร้อมรองรับกระบวนการตรวจพิสูจน์หลักฐานดิจิทัลจากหน่วยงานที่เกี่ยวข้อง จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๙๐ การบันทึกข้อมูลเหตุการณ์ ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

ข้อ ๙๑ การป้องกันข้อมูลเหตุการณ์ ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

ข้อ ๙๒ ข้อมูล...

ข้อ ๙๒ ข้อมูลเหตุการณ์ของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น รวมถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย

ข้อ ๙๓ การตั้งเวลาให้ถูกต้อง (Clock Synchronization) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในหน่วยงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ เพื่อความถูกต้องตรงกันในการตรวจสอบช่วงเวลาจากข้อมูลเหตุการณ์

ส่วนที่ ๕
การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ

ข้อ ๙๔ เพื่อให้ระบบที่ให้บริการสารสนเทศ สามารถให้บริการและมีการทำงานที่ถูกต้องดำรงสถานภาพความพร้อมใช้งานได้ตามวัตถุประสงค์ของระบบ กำหนดให้ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์ปรับปรุงระบบ และซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องที่ให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

ส่วนที่ ๖
การบริหารจัดการช่องโหว่ทางเทคนิค

ข้อ ๙๕ เพื่อป้องกันไม่ให้มีการใช้ประโยชน์จากช่องโหว่ของซอฟต์แวร์ในระบบสารสนเทศในการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ออกสื่อสาธารณะที่สามารถค้นหาข้อมูลช่องโหว่นั้นได้ จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๙๖ การบริหารจัดการช่องโหว่ทางเทคนิค ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

ข้อ ๙๗ การจำกัดการติดตั้งซอฟต์แวร์

๙๗.๑ ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ให้มีการละเมิด

๙๗.๒ ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ หรือซอฟต์แวร์ที่ไม่ได้รับอนุญาตจากหน่วยงานบนคอมพิวเตอร์ของหน่วยงานโดยเด็ดขาด

หมวด ๙ ...

หมวด ๙
ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

ส่วนที่ ๑
การบริหารจัดการการรักษาความปลอดภัยเครือข่ายสารสนเทศ

ข้อ ๙๘ เพื่อป้องกันข้อมูลในเครือข่ายสารสนเทศ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๙๙ การควบคุมเครือข่าย (Network Control) หน่วยขึ้นตรงกองทัพอากาศ ดำเนินการดังนี้

๙๙.๑ ต้องกำหนดผู้รับผิดชอบเครือข่าย รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดการรักษาความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

๙๙.๒ การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย

๙๙.๓ ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานที่เกี่ยวข้องทราบกรณีที่มีการเปลี่ยนแปลงแก้ไขเครือข่าย

๙๙.๔ บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของหน่วยงาน

ข้อ ๑๐๐ การรักษาความมั่นคงปลอดภัยของบริการเครือข่าย (Security of Network Service)

๑๐๐.๑ เครือข่ายสารสนเทศทั้งหมดของหน่วยขึ้นตรงกองทัพอากาศ ที่มีการเชื่อมต่อไปยังเครือข่ายอื่น ๆ ภายนอกกองทัพอากาศ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ เป็นต้น รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้ายด้วย

๑๐๐.๒ ต้องจำกัดจำนวนการเชื่อมต่อจากเครือข่ายภายนอกกองทัพอากาศเข้าระบบสารสนเทศของกองทัพอากาศ และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะการเชื่อมต่อกับเครือข่ายภายนอกเท่านั้น

๑๐๐.๓ ห้ามผู้ใช้งานติดตั้งโมเด็มหรืออุปกรณ์เชื่อมต่อเครือข่ายภายนอกกองทัพอากาศเข้ากับเครื่องคอมพิวเตอร์ของหน่วยงาน หรือต่อกับจุดใดก็ตามบนเครือข่ายของหน่วยงาน

๑๐๐.๔ ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์ และเครือข่ายของหน่วยงานกองทัพอากาศโดยเด็ดขาด

๑๐๐.๕ ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย เช่น Router Switch Hub และ Wireless Access Point เป็นต้น โดยไม่ได้รับอนุญาตเด็ดขาด

๑๐๐.๖ ห้ามเชื่อมต่อเครือข่ายสารสนเทศทางด้านยุทธการกับเครือข่ายอินเทอร์เน็ตหรือระบบอื่น ๆ ของหน่วยงานภายนอกกองทัพอากาศ ยกเว้นแต่ที่ได้รับการตรวจสอบและเห็นชอบจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ข้อ ๑๐๑ การจัดแบ่ง...

ข้อ ๑๐๑ การจัดแบ่งเครือข่ายภายในของกองทัพอากาศ

๑๐๑.๑ ต้องออกแบบเครือข่ายสารสนเทศตามกลุ่มของการให้บริการของระบบสารสนเทศ โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ มีการแบ่งเป็นพื้นที่ภายใน (Internal Zone) และ พื้นที่ภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๑๐๑.๒ ต้องจัดทำแผนผังเครือข่าย (Network Diagram) โดยมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ส่วนที่ ๒

การถ่ายโอนสารสนเทศ (Information Transfer)

ข้อ ๑๐๒ เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนกันระหว่างหน่วยงานภายในกองทัพอากาศและระหว่างกองทัพอากาศกับหน่วยงานภายนอก จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๑๐๓ หน่วยงานเจ้าของสารสนเทศ ผู้มีสิทธิ์และอำนาจในสายงานที่มีการติดต่อแลกเปลี่ยนสารสนเทศผ่านเครือข่ายสารสนเทศ เป็นผู้พิจารณาคุณสมบัติของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึง และดำเนินการกับสารสนเทศดังกล่าว รวมทั้งพิจารณาระดับของการป้องกันที่ต้องการ โดยหากมีการแลกเปลี่ยนสารสนเทศกับหน่วยงานนอกกองทัพอากาศ ต้องได้รับการตรวจสอบระดับความปลอดภัยที่เหมาะสมจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ข้อ ๑๐๔ หน่วยงานที่ต้องมีการถ่ายโอนสารสนเทศกับหน่วยงานภายนอก ต้องมีการจัดทำข้อตกลงในการถ่ายโอนแลกเปลี่ยนสารสนเทศ โดยยึดถือการรักษาความลับของสารสนเทศเป็นสำคัญ

หมวด ๑๐

การจัดหา การพัฒนา และการบำรุงรักษาระบบ

ส่วนที่ ๑

การกำหนดความต้องการด้านความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๑๐๕ เพื่อให้การบริหารจัดการสารสนเทศเป็นไปด้วยความปลอดภัยทั้งกระบวนการ ต้องมีการรวบรวมข้อกำหนดทางด้านความปลอดภัยและบรรจุข้อกำหนดเข้าไปในวงจรการพัฒนาระบบและรวมถึงสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๑๐๖ การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยระบบสารสนเทศ กำหนดให้ต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งานหรือจัดซื้อมาใช้งาน โดยหน่วยงานผู้รับผิดชอบระบบสารสนเทศ ทำการวิเคราะห์ระบบว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

๑๐๖.๑ มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสำรองข้อมูล และระบบเครือข่ายสำรอง เป็นต้น

๑๐๖.๒ มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมูล และระยะเวลาในการกู้คืนข้อมูล เป็นต้น

ข้อ ๑๐๗ ความมั่นคงปลอดภัยของการบริการสารสนเทศบนเครือข่ายสาธารณะ ต้องได้รับการป้องกันจากการถูกเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๑๐๘ การป้องกัน...

ข้อ ๑๐๘ การป้องกันธุรกรรมของการบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับ-ส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

ส่วนที่ ๒

ความมั่นคงปลอดภัยสำหรับกระบวนการในการสนับสนุนและการพัฒนาระบบ

(Security in Development and Support Process)

ข้อ ๑๐๙ เพื่อให้มีมาตรการความมั่นคงปลอดภัยครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๑๑๐ ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบายหรือข้อกำหนดที่กองทัพอากาศกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนามีช่องโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้ เป็นต้น

ข้อ ๑๑๑ ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์ ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ และต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

ข้อ ๑๑๒ การทบทวนทางเทคนิคต่อระบบหลังจากการเปลี่ยนแปลงโครงสร้างการทำงานพื้นฐานของระบบ โดยเมื่อมีการเปลี่ยนแปลงเกิดขึ้นกับโครงสร้างการทำงานพื้นฐานของระบบ เช่น การแก้ไขปรับปรุง เป็นต้น ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ที่ใช้งานว่า ไม่เกิดผลกระทบต่อการทำงาน และความมั่นคงปลอดภัยของระบบที่ใช้โครงสร้างพื้นฐานนั้น

ข้อ ๑๑๓ การจำกัดการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการจำกัดการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

ข้อ ๑๑๔ หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย ต้องมีการกำหนดหลักการวิศวกรรมขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับการพัฒนาระบบ

ข้อ ๑๑๕ สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย ต้องมีการจัดทำหรือป้องกันสภาพแวดล้อมในการทำงานต่าง ๆ ให้มีความเหมาะสมและปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

ข้อ ๑๑๖ การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบ ในการทำสัญญาว่าจ้างการพัฒนาระบบของหน่วยงาน ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การตรวจสอบระบบโดยละเอียดก่อนติดตั้งเพื่อใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

ข้อ ๑๑๗ การทดสอบด้านความมั่นคงปลอดภัยของระบบ โปรแกรมหรือระบบที่พัฒนาขึ้นมาควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา

ข้อ ๑๑๘ การทดสอบ...

ข้อ ๑๑๘ การทดสอบเพื่อรับรองระบบ กำหนดให้มีแนวทาง ดังนี้

๑๑๘.๑ มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งระบบใหม่ และระบบที่ปรับปรุง

๑๑๘.๒ ต้องจัดให้มีเกณฑ์ในการรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสารหัวข้อ (Checklist) ที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มีการเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ

๑๑๘.๓ ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวด ๑๑
ความสัมพันธ์กับผู้ให้บริการภายนอก

ส่วนที่ ๑
ความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

ข้อ ๑๑๙ เพื่อให้มีการป้องกันทรัพย์สินของกองทัพอากาศ ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๑๒๐ หน่วยขึ้นตรงกองทัพอากาศจะต้องจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างหน่วยงานกับผู้ให้บริการภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร

ข้อ ๑๒๑ การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก ต้องระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่างหน่วยงานกับผู้ให้บริการภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศ รวมถึงการถอนหรือการปรับปรุงสิทธิ์การเข้าถึงระบบสารสนเทศตามข้อ ๔๘ เมื่อมีความจำเป็นต้องให้ผู้ให้บริการภายนอกนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศ

ข้อ ๑๒๒ ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่อุปทานของการให้บริการเทคโนโลยีสารสนเทศด้วย

ส่วนที่ ๒
การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก

ข้อ ๑๒๓ เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก จึงมีข้อกำหนดไว้ในส่วนนี้

ข้อ ๑๒๔ การติดตามและทบทวนบริการของผู้ให้บริการภายนอก ต้องจัดทำข้อตกลงกำหนดสิทธิ์สำหรับกองทัพอากาศ ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก รวมถึงมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

ข้อ ๑๒๕ การบริหาร...

ข้อ ๑๒๕ การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก กำหนดดังนี้

๑๒๕.๑ มีการจัดทำเอกสารวิธีปฏิบัติงานเรื่องการให้บริการของผู้ให้บริการภายนอก กำกับดูแลการเปลี่ยนแปลงรายละเอียดการให้บริการของผู้ให้บริการภายนอก ที่เกี่ยวข้องกับบริการในระบบสารสนเทศของกองทัพอากาศ

๑๒๕.๒ การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของระบบสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

หมวด ๑๒

การบริหารจัดการสถานการณ์ (Incident) ความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๒๖ เพื่อให้มีแนวทางดำเนินการที่สอดคล้องต่อเนื่องและมีประสิทธิภาพในการบริหารจัดการสถานการณ์ความมั่นคงปลอดภัยระบบสารสนเทศ ซึ่งรวมถึงการสื่อสาร วิธีการและช่องโหว่ของระบบสารสนเทศ จึงมีข้อกำหนดไว้ในหมวดนี้

ข้อ ๑๒๗ ให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ควบคุม กำกับ และกำหนดหน้าที่รับผิดชอบในการดำเนินการต่อสถานการณ์ความมั่นคงปลอดภัยระบบสารสนเทศเพื่อให้เกิดความสอดคล้องในการปฏิบัติระหว่างหน่วยงานของกองทัพอากาศในภาพรวม

ข้อ ๑๒๘ ศูนย์ไซเบอร์กองทัพอากาศ มีหน้าที่

๑๒๘.๑ เฝ้าระวังสถานการณ์ความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ โดยต้องมีการประเมิน และพิจารณาว่าเหตุการณ์ที่เกิดขึ้นเป็นสถานการณ์ที่ก่อให้เกิดความไม่มั่นคงปลอดภัย

๑๒๘.๒ ต้องมีการกำหนดขั้นตอนไว้รองรับกรณีเกิดสถานการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัยต่อระบบสารสนเทศและไซเบอร์

๑๒๘.๓ ต้องได้รับการตอบสนองต่อสถานการณ์ความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ เพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

๑๒๘.๔ ต้องบันทึกสถานการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของสถานการณ์ ปริมาณที่เกิดขึ้นและผลกระทบจากความเสียหาย เพื่อจะได้เรียนรู้จากสถานการณ์ที่เกิดขึ้นแล้วและเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๑๒๘.๕ ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหมาย หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางกฎหมายที่เกี่ยวข้อง เมื่อพบว่าสถานการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

ข้อ ๑๒๙ นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ต้องบันทึกช่องโหว่ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน ที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่และรายงานศูนย์ไซเบอร์กองทัพอากาศ

ข้อ ๑๓๐ บุคคลในสังกัดกองทัพอากาศ มีหน้าที่

๑๓๐.๑ รายงานเหตุละเมิดความมั่นคงปลอดภัย หรือการกระทำที่ไม่เหมาะสมที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในหน่วยงานต่อนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

ข้อ ๑๓๐.๒ รายงานการ...

๑๓๐.๒ รายงานการทำงานที่ผิดปกติ ข้อผิดพลาดหรือช่องโหว่ของซอฟต์แวร์ที่ตรวจพบ ต่อนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศทันที

๑๓๐.๓ รายงานเหตุละเมิดความมั่นคงปลอดภัยหรือช่องโหว่ ต่อนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศโดยตรง และห้ามดำเนินการใด ๆ ที่เกี่ยวข้องกับหลักฐานของการละเมิดความมั่นคงปลอดภัยนั้นด้วยตนเอง

หมวด ๑๓

การปฏิบัติเมื่อเกิดการละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๑๓๑ เพื่อให้มีแนวทางปฏิบัติเมื่อเกิดการละเว้นการปฏิบัติตามระเบียบนี้ การละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศ และลดความเสียหายที่เกิดขึ้นจากการกระทำที่ฝ่าฝืน หรือละเลยให้เหลือน้อยที่สุด พร้อมตรวจสอบ ค้นหาสาเหตุ และผลเสียหายเพื่อปรับปรุงมาตรการป้องกันการละเมิดที่จะเกิดขึ้นซ้ำอีก รวมทั้งกำหนดวิธีดำเนินการต่อผู้ละเมิดการรักษาความปลอดภัย จึงมีข้อกำหนดไว้ในหมวดนี้

ข้อ ๑๓๒ หน่วยขึ้นตรงกองทัพอากาศและข้าราชการในสังกัดกองทัพอากาศต้องปฏิบัติตามระเบียบนี้อย่างเคร่งครัด การละเว้นการปฏิบัติตามระเบียบนี้ให้ถือว่าเป็นการกระทำผิดวินัยทหารสังกัดกองทัพอากาศ

ข้อ ๑๓๓ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ มีดังนี้

๑๓๓.๑ เมื่อมีผู้ตรวจพบ หรือสงสัยว่ามีการละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ หรือมีสิ่งผิดปกติเกิดขึ้นในระบบสารสนเทศ ให้รายงานผู้บังคับบัญชา และแจ้งนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศทราบโดยเร็วที่สุด

๑๓๓.๒ ให้นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศดำเนินการ ดังนี้

๑๓๓.๒.๑ รายงานขั้นต้นต่อ ศูนย์ไซเบอร์กองทัพอากาศ เพื่อการค้นหาและตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensic) หากพบว่าเป็นการละเมิดความมั่นคงปลอดภัยต่อระบบสารสนเทศที่มีชั้นความลับให้แจ้ง กรมข่าวทหารอากาศทราบเพื่อดำเนินการด้านการรักษาความปลอดภัยต่อไป

๑๓๓.๒.๒ ลดความเสียหายเบื้องต้น โดยการระงับใช้ แก้ไข หรือยกเลิกระบบสารสนเทศที่สงสัยว่าถูกละเมิดนั้น

๑๓๓.๒.๓ สำรวจความเสียหายที่เกิดจากการละเมิด ให้ตรวจสอบสาเหตุและช่องโหว่ หรือข้อบกพร่องที่ก่อให้เกิดการละเมิดโดยให้มีผู้แทนจาก ศูนย์ไซเบอร์กองทัพอากาศและกรมข่าวทหารอากาศร่วมในการตรวจสอบสาเหตุด้วย

๑๓๓.๒.๔ รายงานเหตุการณ์ที่เกิดขึ้นให้ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ พร้อมทั้งแนวทางป้องกันมิให้เกิดการละเมิดซ้ำ

๑๓๓.๒.๕ หากปรากฏหลักฐาน หรือสงสัยว่าระบบสารสนเทศถูกจารกรรม ให้รายงานกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ เพื่อแก้ไขโดยเร็วที่สุด

ข้อ ๑๓๔ หน้าที่และความรับผิดชอบของศูนย์ไซเบอร์กองทัพอากาศ มีดังนี้

๑๓๔.๑ ปฏิบัติการตามข้อ ๑๒๘ ต่อเหตุการณ์ที่ตรวจพบหรือได้รับรายงานโดยมีหน่วยเกี่ยวข้องกับเหตุการณ์ ให้การสนับสนุนการปฏิบัติเป็นไปด้วยความเรียบร้อย

๑๓๔.๒ รายงานความ...

๑๓๔.๒ รายงานความก้าวหน้าการปฏิบัติต่อเหตุการณ์ให้ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบอย่างต่อเนื่อง

ข้อ ๑๓๕ หน้าที่และความรับผิดชอบของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีดังนี้

๑๓๕.๑ ตรวจสอบผลกระทบที่เกิด ขึ้นกับระบบสารสนเทศที่สำคัญของกองทัพอากาศและรายงานศูนย์ปฏิบัติการกองทัพอากาศ เพื่อพิจารณาดำเนินการในส่วนที่เกี่ยวข้อง

๑๓๕.๒ แจ้งให้หน่วยงานเจ้าของระบบสารสนเทศ ร่วมดำเนินการในส่วนที่เกี่ยวข้องโดยเร็วที่สุด

๑๓๕.๓ แต่งตั้งคณะกรรมการร่วมกับหน่วยงานที่มีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ เพื่อดำเนินการสืบสวนสอบสวนหาผู้กระทำผิดและผู้เกี่ยวข้องโดยเร็วที่สุด

๑๓๕.๔ แจ้งให้หน่วยงานต้นสังกัด พิจารณาลงโทษผู้รับผิดชอบและผู้กระทำผิดต่อการละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ตามกรณีที่ก่อให้เกิดความเสียหายต่อระบบหรือดำเนินการตามกระบวนการทางกฎหมายที่เกี่ยวข้อง

๑๓๕.๕ กำหนดแนวทางการแก้ไขข้อบกพร่อง และป้องกันมิให้เกิดเหตุการณ์ซ้ำขึ้นอีก

๑๓๕.๖ กำกับดูแลการแก้ไข เปลี่ยนแปลงระบบ แผนงาน และวิธีปฏิบัติได้ตามความจำเป็นและความเหมาะสม ในกรณีที่มีผลกระทบเป็นความเสียหายต่อระบบสารสนเทศของกองทัพอากาศอย่างร้ายแรง

ข้อ ๑๓๖ หน้าที่และความรับผิดชอบของหน่วยขึ้นตรงกองทัพอากาศที่มีผู้ละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

๑๓๖.๑ ลงโทษหรือลงทัณฑ์ทางวินัยกับผู้ละเมิด และผู้รับผิดชอบต่อการละเมิดดังกล่าว ตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำขึ้นอีก ในกรณีผู้ละเมิดเป็นบุคคลภายนอกกองทัพอากาศให้หน่วยเกี่ยวข้องดำเนินการตามกฎหมายต่อไป

๑๓๖.๒ หากก่อให้เกิดความเสียหายต่อทางราชการอย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ดำเนินการตามกระบวนการทางกฎหมายที่เกี่ยวข้อง

๑๓๖.๓ พิจารณาสารสนเทศที่มีชั้นความลับ รหัสประมวลลับ (Code) กุญแจเข้าและถอดรหัสที่อยู่ในความรับผิดชอบ หากได้รับความเสียหาย รั่วไหล หรือถูกดัดแปลง ต้องดำเนินการแก้ไขโดยเร็วที่สุด

๑๓๖.๔ กำหนดมาตรการหรือระเบียบปฏิบัติเพิ่มเติม เพื่อป้องกันและขจัดความเสียหายที่จะเกิดการละเมิดซ้ำ เช่น เปลี่ยนแปลงวิธีการปฏิบัติ ยกเลิกโปรแกรม และอื่น ๆ เป็นต้น

๑๓๖.๕ หากก่อให้เกิดความเสียหายต่อระบบสารสนเทศ และต้องเสียค่าใช้จ่ายในการกู้คืนมา ให้ส่วนราชการเรียกร้องค่าเสียหายส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้ระบบด้วย

ประกาศ ณ วันที่ ๓๑ สิงหาคม พ.ศ.๒๕๖๓

(ลงชื่อ) พลอากาศเอก มานัต วงษ์วาทย์

(มานัต วงษ์วาทย์)

ผู้บัญชาการทหารอากาศ

ผนวก ก ประกอบระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

หน้าที่การรักษาความมั่นคงปลอดภัยระบบสารสนเทศแบ่งตามบทบาท

๑. ผู้บริหาร หรือผู้ดูแลระบบ (System Administrator) มีความรู้ด้านฮาร์ดแวร์ ซอฟต์แวร์ระบบเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๑.๑ บริหารและดูแลอุปกรณ์คอมพิวเตอร์ ซึ่งเป็นแม่ข่ายบริการแก่หน่วยต่าง ๆ ของส่วนราชการ

๑.๒ ควบคุมและตรวจสอบการใช้งานระบบ

๑.๓ ตรวจสอบ ควบคุม ดูแล และบำรุงรักษาระบบ

๑.๔ รักษาความปลอดภัยระบบ เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานของระบบ เป็นต้น

๒. ผู้บริหารฐานข้อมูล (Database Administrator) มีความรู้ด้านการจัดการฐานข้อมูลระบบคอมพิวเตอร์เป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ ดังนี้

๒.๑ ควบคุมดูแลฐานข้อมูล เช่น การรวบรวม การเพิ่ม การเปลี่ยนแปลง การลบ การจัดโครงสร้าง การใช้งาน การเก็บ และการเรียกดูข้อมูล เป็นต้น

๒.๒ เลือก ตัดตอน และกำหนดรูปแบบข้อมูลที่เก็บในแฟ้มข้อมูล

๒.๓ รักษาความปลอดภัยฐานข้อมูล ได้แก่ รักษาความลับ ความคงสภาพ และความพร้อมใช้งานของฐานข้อมูล

๒.๔ ตรวจสอบฐานข้อมูล และวิเคราะห์ข้อมูล

๒.๕ ควบคุม และบริการการใช้งานฐานข้อมูล

๓. ผู้ดูแลเครือข่าย (Network Administrator) มีความรู้ด้านฮาร์ดแวร์ การสื่อสารข้อมูลและอุปกรณ์ในระบบเครือข่ายเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ ดังนี้

๓.๑ กำหนดเลขที่อยู่ไอพี (IP Address) ให้คอมพิวเตอร์ในเครือข่ายของส่วนราชการโดยประสานกับส่วนราชการหรือผู้บริหารระบบเครือข่ายคอมพิวเตอร์ของกองทัพอากาศ

๓.๒ กำหนดบัญชีผู้ใช้ (Account) และรหัสผ่าน (Password) ของผู้ใช้ภายในเครือข่ายที่รับผิดชอบ

๓.๓ ดูแลการใช้เครือข่ายคอมพิวเตอร์ภายในส่วนราชการ

๓.๔ ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวกับระบบเครือข่าย

๓.๕ รักษาความปลอดภัยระบบเครือข่าย ได้แก่ รักษาความลับ ความคงสภาพ กำหนดการเข้ารหัส และความพร้อมใช้งานของระบบเครือข่าย

๔. นักเขียนโปรแกรม (Programmer) มีความรู้เรื่องระบบคอมพิวเตอร์ การเขียนโปรแกรมคอมพิวเตอร์และฐานข้อมูลเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ ดังนี้

๔.๑ เขียนและพัฒนาโปรแกรมที่ได้รับมอบหมาย

๔.๒ จัดหาข้อมูลเพื่อทดสอบโปรแกรม

๔.๓ ดูแลบำรุงรักษาโปรแกรมที่พัฒนา

๔.๔ รักษาความปลอดภัยโปรแกรม ได้แก่ รักษาความลับ ความคงสภาพ และความพร้อม

ผนวก ข ประกอบระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง

๑. Account ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: บัญชีผู้ใช้

อธิบายความหมาย

: เป็นสัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกัน มีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกัน เพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชี หรือกลุ่มคนที่สามารถเข้าถึงระบบได้บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (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 ความหมายในภาษาไทยในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: การถอดรหัสลับ / เพื่อการเข้ารหัสลับ

อธิบายความหมาย

: การถอดรหัสลับ (Decryption)

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

(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) กระบวนการ...

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

๕. Decryption Key/Encryption Key ความหมายในภาษาไทยในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: กุญแจเพื่อการถอดรหัสลับ/กุญแจเพื่อการเข้ารหัสลับ

อธิบายความหมาย

: เป็นคำศัพท์สำหรับการเข้ารหัสแบบกุญแจสาธารณะ (Public Key System) ประกอบด้วย ไฟล์คอมพิวเตอร์คู่หนึ่ง 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 แม่เหล็กและเครื่องจักรกล เป็นต้น แสดงให้เห็นถึงความแตกต่างของฮาร์ดแวร์และซอฟต์แวร์ ซึ่งเป็นองค์ประกอบของระบบคอมพิวเตอร์เช่นเดียวกัน

๗. Log File ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: แฟ้มลงบันทึกเข้าออก

อธิบายความหมาย

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

๘. Malicious Code ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: โปรแกรมประสงค์ร้าย

อธิบายความหมาย

: โปรแกรมหรือส่วนของโปรแกรมที่สร้างขึ้น และเผยแพร่โดยผู้มีเจตนาร้ายมุ่งทำลายอย่างใดอย่างหนึ่งต่อสิ่งที่เป็นเป้าหมาย โดยทั่วไปโปรแกรมประสงค์ร้ายจะแบ่งตามลักษณะ การแพร่กระจายและการกระทำได้ ๕ ประเภท คือ

๘.๑ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นโปรแกรมหรือส่วนของโปรแกรมที่ผู้เขียนมีวัตถุประสงค์ในการทำลายอย่างใดอย่างหนึ่ง หนทางเข้าสู่ระบบคอมพิวเตอร์โดยการเกาะติดกับโปรแกรมที่ใช้งานทั่วไปภายในระบบคอมพิวเตอร์และทำให้โปรแกรมเป้าหมายที่อาศัยอยู่นั้น กลายเป็นโปรแกรมประสงค์ร้ายด้วย ไวรัสคอมพิวเตอร์แพร่กระจายโดยสำเนาตัวเอง (Copy) ไปเกาะติดกับโปรแกรมต่าง ๆ เพื่อให้โปรแกรมเหล่านั้นนำพาไปยังส่วนต่าง ๆ ของระบบเพื่อจะได้แพร่กระจายไปสู่โปรแกรมอื่นที่ยังไม่มีโปรแกรมไวรัสเกาะอยู่ ซึ่งการแพร่กระจายจะเป็นลักษณะทวีคูณ ทำลายเป้าหมายได้ทุกรูปแบบตามเจตนาของ

ผู้เขียน...

ผู้เขียนโปรแกรม ไวรัสคอมพิวเตอร์มักจะแบ่งประเภทตามแหล่งที่อาศัยภายในระบบ หรือโปรแกรมที่จะกระทำการโดยเฉพาะ เช่น ไวรัสในส่วนการปลุกเครื่อง (Boot Sector Virus) มาโครไวรัส (Macro Virus) เป็นต้น ไวรัสคอมพิวเตอร์จะกระทำการ (Active) ได้ก็ต่อเมื่อโปรแกรมเป้าหมายที่โปรแกรมไวรัสอาศัยอยู่มีการดำเนินการ (Run/Process)

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

๘.๓ ตัวลวง หรือ ม้าโทรจัน (Trojan Horse) เป็นโปรแกรม หรือส่วนของโปรแกรมที่ถูกนำมาซ่อนไว้ในโปรแกรมใช้งานโปรแกรมใดโปรแกรมหนึ่งภายในระบบโดยผู้ใช้ไม่ทราบและคิดว่าเป็นโปรแกรมที่ใช้งานตามปกติ มักกระทำโดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องกับการบำรุงรักษาโปรแกรม ได้แก่ โปรแกรมม้าโทรจันที่แทรกมากับบท (คำสั่ง) ลงบันทึกเข้า (Login Script) ที่รอให้บริการแก่ผู้ใช้ที่ต้องการเข้าสู่ระบบใดระบบหนึ่ง โดยการใส่บัญชีผู้ใช้และรหัสผ่าน ซึ่งนอกจากทำหน้าที่ตรวจสอบความถูกต้องแท้จริงในการเข้าระบบของผู้ใช้แล้วยังแอบสำเนาบัญชีผู้ใช้และรหัสผ่านดังกล่าวเก็บไว้ใช้ประโยชน์ส่วนตัวในภายหลัง ม้าโทรจันไม่สามารถเคลื่อนย้ายหรือสำเนาตัวเองได้ บางครั้งใช้เป็นที่พรางตัวของโปรแกรมประสงค์ร้ายอื่น ๆ มักเป็นไปในลักษณะของการเชิญชวนให้เกิดความสนใจและนำโปรแกรมดังกล่าวบรรจุเข้าในระบบ ซึ่งผู้ใช้เองที่นำม้าโทรจันเข้าสู่ระบบโดยไม่เจตนา เช่น เกมคอมพิวเตอร์(Computer Game) โปรแกรมประยุกต์ภาพอนาจาร (Nude) เป็นต้น ซึ่งโปรแกรมเหล่านี้เมื่อบรรจุเข้าระบบได้แล้วอาจแพร่ไวรัสหรือโปรแกรมประสงค์ร้ายอื่น 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 เป็นต้น กับดักกระทำได้โดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องในช่วงที่กำลังพัฒนาโปรแกรมซึ่งอาจสร้างทางลับเพื่อหาประโยชน์อย่างใดอย่างหนึ่งจากระบบในภายหลังจากตัวอย่างข้างต้น เมื่อสามารถเข้าสู่แฟ้มบันทึกเข้าออก (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 อย่างไรก็ตามปัจจุบันโปรแกรมประสงค์ร้ายได้มีการพัฒนาความสามารถในการทำลายและการหลบหลีกการตรวจจับของโปรแกรมป้องกันต่าง ๆ อยู่เสมอ ดังนั้นในอนาคตจะปรากฏโปรแกรมประสงค์ร้ายในรูปแบบที่มีการผสมผสานกันหลาย ๆ ประเภทมากยิ่งขึ้น

๙. Password ความหมาย ในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: รหัสผ่าน

อธิบายความหมาย

: เป็นชุดของตัวอักษรหรือคำพิเศษ (Special Word) หรือวลี (Phase) ซึ่งให้สิทธิ์ในการเข้าถึงระบบแก่ผู้ใช้แต่ละคนนอกจากนี้รหัสผ่านยังเป็นเครื่องมือรักษาความปลอดภัยที่ใช้แสดงต่อระบบคอมพิวเตอร์ เพื่อให้การรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้ และตรวจสอบสิทธิ์ในการใช้งานระบบ

(Access ...

(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

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

๑๐.๒ โปรแกรมประยุกต์ หรือโปรแกรมใช้งาน (Application Program) เป็นโปรแกรมที่สร้างขึ้นโดยมีวัตถุประสงค์เพื่อการใช้งานในลักษณะใดลักษณะหนึ่งโดยเฉพาะ เช่น โปรแกรมประมวลผลคำ (สารบรรณหรือธุรการ) โปรแกรมทางธุรกิจ (การเงินหรือการธนาคาร) โปรแกรมเกี่ยวกับงานวิจัย (การศึกษาหรือการพยากรณ์) โปรแกรมควบคุมการทำงานของอุปกรณ์ (เครื่องมือเฉพาะอย่าง) เป็นต้น โปรแกรมเหล่านี้มักจะเขียนด้วยภาษาระดับสูง และใช้ประโยชน์เพียงกลุ่มผู้ใช้บางกลุ่มเท่านั้น รวมทั้งต้องมีการปรับปรุงเปลี่ยนแปลงโปรแกรมเพื่อให้ใช้งานได้ทันสมัยอยู่เสมอ

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

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)