ระเบียบกรมกิจการพลเรือนทหาร
ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ
พ.ศ. ๒๕๖๐

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกรมกิจการพลเรือนทหารเป็นไปด้วยความเรียบร้อยมีประสิทธิภาพ สอดคล้องกับนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙ จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกรมกิจการพลเรือนทหารว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๐”

ข้อ ๒ ระเบียบนี้จัดทำขึ้นเพื่อให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

ข้อ ๓ ระเบียบนี้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๔ บรรดาระเบียบ และคำสั่งอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ ๕ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานราชการและลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่ดำเนินการเกี่ยวกับระบบสารสนเทศ ของกรมกิจการพลเรือนทหาร

ข้อ ๖ ในระเบียบนี้

๖.๑ ระบบสารสนเทศ หมายความว่า ระบบจัดการข้อมูลของกรมกิจการพลเรือนทหารที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์ และระบบสื่อสาร มาช่วยในการประมวลผลข้อมูลที่มีอยู่ ให้อยู่ในรูปแบบของข้อมูลที่เป็นประโยชน์สูงสุด เพื่อเป็นข้อสรุปที่ใช้สนับสนุนการวางแผน การบริหาร การพัฒนาและควบคุม ซึ่งประกอบด้วย

๖.๑.๑ ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยต้องกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์เพื่อทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ประกอบด้วย ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล/สารสนเทศ (Data/Information) บุคลากร (Peopleware) และกระบวนการทำงาน (Documentation/Procedure)

๖.๑.๒ ระบบเครือข่าย หมายความว่า ระบบที่ใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร ทั้งในระบบอินทราเน็ตและระบบอินเทอร์เน็ต

๖.๑.๒.๑ ระบบอินทราเน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๖.๑.๒.๒ ระบบอินเทอร์เน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

/๖.๑.๓ สารสนเทศ...

๖.๑.๓ สารสนเทศ หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปแบบของ ตัวเลข ข้อความ หรือภาพกราฟิก ที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๖.๒ คอมพิวเตอร์ หมายความว่า เครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์ ที่มีความสามารถในการรับข้อมูลเข้า ประมวลผล แสดงผล บันทึก และส่งออกข้อมูล ซึ่งเป็นผลที่ได้จากการประมวลผลตามโปรแกรม โดยอาจมีลักษณะเป็นคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา ตลอดจนคอมพิวเตอร์อื่นๆ รวมถึง แท็ปเล็ตและสมาร์ทโฟน

ข้อ ๗ จัดให้มีการตรวจสอบและประเมินความมั่นคงปลอดภัยของระบบสารสนเทศตามรายละเอียดในระเบียบนี้ อย่างน้อยทุก ๖ เดือน

ข้อ ๘ คณะทำงานด้านเทคโนโลยีสารสนเทศกรมกิจการพลเรือนทหาร แต่งตั้งคณะทำงาน/เลขานุการ เพื่อกำกับดูแลการดำเนินการให้เป็นไปตามระเบียบนี้ โดยปฏิบัติหน้าที่ตามที่กำหนดในคำสั่งตั้งแต่เมื่อมีการละเมิดการรักษาความปลอดภัยตามระเบียบนี้ จะต้องดำเนินการตรวจสอบและแก้ไขในทันที พร้อมทั้งรายงานเหตุการณ์ที่เกิดขึ้นและการดำเนินการแก้ไข ให้ผู้บังคับบัญชาทราบตามลำดับชั้นจนถึงเจ้ากรมกิจการพลเรือนทหาร

ข้อ ๙ ให้ รองเจ้ากรมกิจการพลเรือนทหาร เป็นผู้รักษาการให้เป็นไปตามระเบียบนี้

/หมวด ๑ ..

หมวด ๑
กล่าวทั่วไป

ข้อ ๑๐ ระเบียบนี้จัดทำขึ้นตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย มีจุดประสงค์เพื่อกำหนดทิศทาง รวมทั้งให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยระบบสารสนเทศของกรมกิจการพลเรือนทหาร ให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และประสิทธิผล มีความมั่นคงปลอดภัย โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพความพร้อมใช้งาน ต่อระบบสารสนเทศ สินทรัพย์สารสนเทศ และข้อมูลสำคัญในการปฏิบัติภารกิจ อันเป็นการลดความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศและลดความเสียหายต่าง ๆ ที่เกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัย และรักษาไว้ซึ่งความสามารถในการปฏิบัติภารกิจได้อย่างต่อเนื่อง รวมทั้งสอดคล้องกับกฎหมาย และระเบียบที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ในด้านการประกอบธุรกรรมทางอิเล็กทรอนิกส์ของกรมกิจการพลเรือนทหาร มีความจำเป็นอย่างยิ่งที่จะต้องมีระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ เพื่อขอบเขตและข้อกำหนดในการรักษาความปลอดภัยระบบสารสนเทศของกรมกิจการพลเรือนทหาร ตลอดจนผู้ใช้ระบบเทคโนโลยีสารสนเทศของกรมกิจการพลเรือนทหารให้เกิดความมั่นคงปลอดภัยสูงสุด ครอบคลุมการรักษาความปลอดภัยด้วยมาตรการด้านการป้องกัน (Preventive) มาตรการด้านการตรวจสอบ (Detective) และมาตรการด้านการแก้ไข (Corrective) ในเรื่องดังต่อไปนี้

๑๐.๑ การรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ (Hardware)

๑๐.๒ การรักษาความปลอดภัยด้านซอฟต์แวร์ (Software)

๑๐.๓ การรักษาความปลอดภัยระบบเครือข่ายสารสนเทศและสื่อสารข้อมูล (Data Communication and Network System)

๑๐.๔ การรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการปฏิบัติงานระบบสารสนเทศ (Procedure)

๑๐.๕ การรักษาความปลอดภัยด้านบุคลากรสารสนเทศ (Personnel)

๑๐.๖ การรักษาความปลอดภัยทางด้านกายภาพ สถานที่และสภาวะแวดล้อม (Physical and Environmental)

ข้อ ๑๑ นิยามศัพท์ต่าง ๆ ที่ไม่ได้กำหนดไว้ท้ายระเบียบ ให้ยึดถือตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

/หมวด ๒...

หมวด ๒

การรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ (Hardware)

ข้อ ๑๒ เครื่องคอมพิวเตอร์และอุปกรณ์ของระบบสารสนเทศ ได้แก่ เครื่องคอมพิวเตอร์ทุกชนิดและทุกขนาด อุปกรณ์ทั้งปวงที่มีการใช้งานร่วมกันระหว่างระบบงานต่าง ๆ อุปกรณ์ศูนย์กลางการประมวลผล อุปกรณ์ควบคุมการทำงานต่างๆ และอุปกรณ์อื่นๆ ที่อยู่ในความดูแลของกรมกิจการพลเรือนทหาร

ข้อ ๑๓ ให้มีการจัดหมวดหมู่และการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ดังนี้

๑๓.๑ จัดหมวดหมู่ กำหนดชั้นความลับและระดับความสำคัญ

๑๓.๒ กำหนดวิธีป้องกันรักษาความปลอดภัยที่เหมาะสมประจำอุปกรณ์

๑๓.๓ จัดทำป้ายชื่อ ชั้นความลับ และลำดับการเคลื่อนย้ายกำกับอุปกรณ์ทุกชนิด

๑๓.๔ บัญชีอุปกรณ์ทั้งหมดต้องจัดรวบรวมไว้ด้วยกัน โดยจัดทำอย่างน้อย ๒ ชุด และจัดเก็บในที่ที่เหมาะสมกับชั้นความลับที่กำหนดไว้

๑๓.๕ จัดให้มีการตรวจสอบบัญชีทุก ๖ เดือน และจัดทำสรุปนำเรียนเจ้ากรมกิจการพลเรือนทหาร ภายใน ๑๕ วันทำการ

ข้อ ๑๔ การติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ

๑๔.๑ จะต้องจัดให้มีสถานที่เฉพาะ ในการติดตั้งอุปกรณ์เหล่านี้ โดยมีระบบการรักษาความปลอดภัยที่ดีและระบบสภาพแวดล้อมให้เหมาะสมต่ออุปกรณ์ และหน้าที่ของอุปกรณ์นั้น

๑๔.๒ การติดตั้งอุปกรณ์เหล่านี้ จะต้องติดตั้ง ณ สถานที่เฉพาะที่จัดเตรียมระบบสภาพแวดล้อมไว้อย่างเหมาะสม ถูกต้องตามหลักวิชา โดยคำนึงถึงความสะดวกในการเข้าถึงการใช้งานและการรักษาความปลอดภัยเป็นสำคัญ

ข้อ ๑๕ จัดให้มีการควบคุมการเข้าถึงอุปกรณ์ต่าง ๆ ให้เหมาะสมกับชั้นความลับและความสำคัญ ดังนี้

๑๕.๑ กำหนดผู้รับผิดชอบกำกับดูแลทางกายภาพ (Physical) และทางตรรกะ (Logical) ในเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ตามห้วงเวลาที่กำหนด

๑๕.๒ กำหนดรหัสป้องกัน และระบบกลั่นกรองการเข้าถึงอุปกรณ์เหล่านั้น

๑๕.๓ บันทึกการเข้าถึงอุปกรณ์ต่าง ๆ ตามรหัสป้องกันที่ได้กำหนดไว้ สามารถพิสูจน์ทราบผู้เป็นเจ้าของรหัสได้

๑๕.๔ จัดเก็บบันทึกการเข้าถึงอุปกรณ์ต่าง ๆ ไว้อย่างเป็นระบบสามารถตรวจสอบได้ง่าย

๑๕.๕ กำหนดแนวทางปฏิบัติ เมื่อเกิดเหตุละเมิด

๑๕.๖ สรุปนำเรียนเจ้ากรมกิจการพลเรือนทหาร ทุกเดือน และรวบรวมจัดทำเป็นสรุปรายงานในรอบ ๑ ปี

๑๕.๗ กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงและใช้งานสารสนเทศ (ผนวก ก)

ข้อ ๑๖ การรักษาความปลอดภัยด้านกระบวนการซ่อมบำรุงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบกรณีที่เป็นเครื่องคอมพิวเตอร์ที่มีหน่วยความจำ ให้ดำเนินการเพื่อรักษาความปลอดภัยดังนี้

๑๖.๑ การซ่อมบำรุงระดับโรงงาน

๑๖.๑.๑ ทำการสำรอง หรือจดบันทึกข้อมูลที่จัดเก็บไว้ในหน่วยความจำของเครื่องได้แก่

/(๑) เนื้อหา...

(๑) เนื้อหาข้อมูลที่จัดเก็บ

(๒) รหัส/หมายเลข ที่กำหนดประจำเครื่อง

๑๖.๑.๒ ทำการล้างข้อมูลที่จัดเก็บไว้ในหน่วยความจำของเครื่อง

๑๖.๑.๓ เมื่อได้รับเครื่องคืนแล้วให้ดำเนินการดังนี้

(๑) ตรวจสอบความครบถ้วนของระบบโปรแกรมในเครื่อง

(๒) ตรวจสอบหากมีโปรแกรมเพิ่มเติมหรือแปลกปลอม

(๓) เปลี่ยนรหัสผ่านที่ใช้สำหรับปฏิบัติงานใหม่ทั้งหมด

๑๖.๒ การซ่อมบำรุงระดับหน่วย

๑๖.๒.๑ ห้ามผู้ใช้เครื่องดำเนินการถอดเปลี่ยนหรือซ่อมแก้ไขเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบโดยพลการ

๑๖.๒.๒ ทำการสำรองข้อมูลที่จำเป็นไว้ทั้งหมด

๑๖.๒.๓ จดบันทึกข้อมูลที่เกี่ยวข้องกับการใช้งานระบบต่างๆ และระบบเครือข่ายของทางราชการ

๑๖.๒.๔ เมื่อได้รับเครื่องคืนแล้วให้ดำเนินการตามข้อ ๑๖.๑.๓

๑๖.๒.๕ จัดให้มีการปรนนิบัติบำรุง (Maintenance) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบตามเวลาและวิธีการที่ถูกต้องตามหลักวิชาและคู่มือประจำเครื่อง

๑๖.๓ จัดทำประวัติการซ่อมบำรุงในทุกระดับพร้อมรายชื่อผู้ทำการซ่อมบำรุง เพื่อตรวจสอบได้เมื่อเกิดเหตุละเมิดการรักษาความปลอดภัย หรือการรั่วไหลของข้อมูล

๑๖.๔ จัดทำบัญชีของอุปกรณ์ที่สามารถทดแทนกันได้พร้อมที่ตั้งของอุปกรณ์เหล่านั้น

๑๖.๕ ให้ดำเนินการซ่อมบำรุงตามแนวทางการซ่อมบำรุงคอมพิวเตอร์และอุปกรณ์ประกอบตามที่กรมการสื่อสารทหารกำหนด

ข้อ ๑๗ การทำระบบสำรองและคืนสภาพ (Full Backup and Recovery)

๑๗.๑ จัดทำแผนการทำสำรองและคืนสภาพที่มีประสิทธิภาพและเหมาะสม สามารถดำเนินการคืนสภาพได้ในทันทีตามที่กำหนด ครอบคลุมการทำงานของอุปกรณ์ทุกรายการ ให้กลับทำงานได้เต็มภารกิจของกรมกิจการพลเรือนทหาร และดำเนินการทดสอบการคืนสภาพอย่างน้อยปีละ ๒ ครั้ง โดยสอดคล้องกับระดับความสำคัญของระบบงาน

๑๗.๒ จัดเก็บสื่อบันทึกข้อมูลสำรองตามวิธีปฏิบัติในข้อ ๑๖.๑.๑ โดยนำสื่อดังกล่าวเก็บในสถานที่อื่นนอกพื้นที่เดียวกับต้นฉบับ

๑๗.๓ จัดเก็บสื่อบันทึกทะเบียนประวัติการทำสำรองและคืนสภาพไว้อย่างสมบูรณ์โดยให้มีข้อมูลครบถ้วนและทันสมัยตลอดเวลา แล้วจัดเก็บไว้ในที่ที่เหมาะสมและปลอดภัยแต่สามารถนำมาตรวจสอบได้

ข้อ ๑๘ เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบที่จะติดตั้งเข้าสู่ระบบสารสนเทศของกรมกิจการพลเรือนทหาร จะต้องมีคุณลักษณ์ขั้นต่ำตามมาตรฐานที่กำหนด

ข้อ ๑๙ อุปกรณ์คอมพิวเตอร์ในระบบเครือข่ายภายในของกรมกิจการพลเรือนทหารทุกรายการต้องได้รับการกำหนดผู้รับผิดชอบ ผู้มีสิทธิใช้งาน และวิธีการรักษาความปลอดภัยประจำเครื่องคอมพิวเตอร์และอุปกรณ์ตามแบบฟอร์ม

ข้อ ๒๐ คณะทำงานด้านเทคโนโลยีสารสนเทศของกรมกิจการพลเรือนทหารรับทราบและให้ความเห็นชอบการตรวจสอบอุปกรณ์ที่นำมาติดตั้งใหม่ทุกครั้ง สำหรับอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่แล้วให้ตรวจสอบทุกรอบ ๓ เดือน หรือมีเหตุอันควรให้ตรวจสอบ และรายงานให้เจ้ากรมกิจการพลเรือนทหารทราบ

/ข้อ ๒๑ การเคลื่อนย้าย...

ข้อ ๒๑ การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เข้า - ออก พื้นที่งานระบบสารสนเทศของกรมกิจการพลเรือนทหาร หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะการทำงานของอุปกรณ์เปลี่ยนแปลงไป จะต้องได้รับอนุญาตตามลำดับชั้น และมีการตรวจสอบความปลอดภัยก่อนเคลื่อนย้ายทุกครั้ง

ข้อ ๒๒ เครื่องคอมพิวเตอร์ที่มีข้อมูลชั้นความลับต้องติดเครื่องหมายแสดงชั้นความลับไว้

ข้อ ๒๓ การรักษาความปลอดภัยสื่อที่ใช้ในการบันทึกข้อมูล

๒๓.๑ กำหนดวิธีปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูล เพื่อป้องกันข้อมูลมิให้รั่วไหลหรือถูกทำลาย

๒๓.๑.๑ ให้ติดป้ายชื่อไว้ที่สื่ออย่างชัดเจน แสดงชั้นความลับของข้อมูลที่เก็บหากเป็นกรณีที่รวบรวมเก็บในกล่องหรือหีบห่อ ให้แสดงไว้ที่กล่องหรือหีบห่อนั้นๆ ด้วย

๒๓.๑.๒ กำหนดบุคคลที่มีสิทธิใช้งานและระดับการเข้าถึงสื่อบันทึกข้อมูลนั้นๆ

๒๓.๑.๓ จัดเก็บสื่อบันทึกข้อมูลไว้ในสถานที่และสภาวะแวดล้อมที่เหมาะสมปลอดภัย

๒๓.๑.๔ จัดทำทะเบียนสื่อบันทึกข้อมูลไว้อย่างเป็นระเบียบและครบถ้วนสามารถตรวจสอบได้

๒๓.๒ กรณีสื่อบันทึกที่สามารถถอดแยกได้ (Removable Computer Media) อาทิ สื่อข้อมูลแบบพกพา เทปบันทึกข้อมูล

๒๓.๒.๑ ให้ลบข้อมูลที่มิได้ใช้งานทิ้งทันทีที่หมดความต้องการใช้

๒๓.๒.๒ กำหนดสิทธิของบุคคลที่ถอดแยกได้

ข้อ ๒๔ ติดตั้งซอฟต์แวร์ป้องกันภัยคุกคามในเครื่องคอมพิวเตอร์ทุกชุดตามที่คณะทำงานด้านเทคโนโลยีสารสนเทศกรมกิจการพลเรือนทหารกำหนด และห้ามถอนการติดตั้ง (Uninstall) หากเครื่องคอมพิวเตอร์ใดมีการลบซอฟต์แวร์ป้องกันภัยคุกคามโดยเจตนาหรือโดยประมาท ผู้ใช้ประจำเครื่องนั้นและผู้ดำเนินการจะต้องเป็นผู้รับผิดชอบในความเสียหายที่เกิดขึ้น เนื่องจากจะเกิดผลเสียต่อเนื่องไปยังเครื่องอื่นที่เชื่อมโยง ในเครือข่ายของระบบคอมพิวเตอร์ที่ใช้งานอยู่

ข้อ ๒๕ ให้บันทึกการเข้าติดตั้งใหม่ หรือปรับแต่ง หรือเปลี่ยนแปลงองค์ประกอบของอุปกรณ์คอมพิวเตอร์ทุกครั้ง ทั้งทางตรรกะและทางกายภาพ (Logical and Physical Configuration Setup)

/หมวด ๓...

หมวด ๓

การรักษาความปลอดภัยด้านซอฟต์แวร์ (Software)

ข้อ ๒๖ โปรแกรมประยุกต์ คือกลุ่มของโปรแกรมหรือโปรแกรมคำสั่งต่าง ๆ ที่จัดทำขึ้นเพื่อใช้ในการปฏิบัติงานของหน่วย

ข้อ ๒๗ โปรแกรมประยุกต์ที่ใช้ในราชการจะต้องเป็นไปตามมาตรฐานที่กำหนด (Program Specification) เป็นที่ยอมรับตามหลักวิชาการทั่วไป

ข้อ ๒๘ หน่วยขึ้นตรงกรมกิจการพลเรือนทหารจะต้องกำหนดผู้รับผิดชอบหรือผู้บริหารจัดการระบบงาน กำหนดผู้ใช้และสิทธิในการเข้าถึง/แก้ไขข้อมูล และปรับปรุงให้ทันสมัยตามวงรอบการโยกย้าย เป็นลายลักษณ์อักษร โดยหัวหน้าหน่วยขึ้นตรงกรมกิจการพลเรือนทหาร เป็นผู้ลงนาม และแจ้งให้ผู้มีรายชื่อรับทราบด้วยทุกครั้ง

ข้อ ๒๙ การกำหนดสิทธิการเรียกใช้ระบบงานเพื่อทำการแก้ไขข้อมูลให้เป็นไปตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ.๒๕๕๙ ว่าด้วยการดำเนินกรรมวิธีข้อมูลอัตโนมัติระบบเทคโนโลยีสารสนเทศ โดยมีสายงานต่าง ๆ หรือหน่วยงานที่เป็นเจ้าของระบบงานและข้อมูลนั้น ๆ เป็นผู้กำหนดผู้ใช้และสิทธิในการเข้าถึง/แก้ไขข้อมูล

ข้อ ๓๐ การบริหารจัดการฐานข้อมูล

๓๐.๑ จัดให้มีผู้บริหารจัดการฐานข้อมูล (Database Administrator – DBA) เป็นผู้รับผิดชอบฐานข้อมูลที่อยู่ในความรับผิดชอบของกรมกิจการพลเรือนทหาร ในการควบคุมกำกับดูแลทางเทคนิค การกำหนดสิทธิทางเทคนิคในการแก้ไขทางกายภาพของฐานข้อมูลที่ใช้งานทั้งสิ้น

๓๐.๒ แต่งตั้งผู้ประสานงานด้านข้อมูลกรณีที่ใช้ข้อมูลร่วมกับส่วนราชการอื่น

ข้อ ๓๑ การแก้ไขฐานข้อมูลในระบบ ทำได้โดยเจ้าหน้าที่ที่ได้รับอนุมัติจากผู้บริหารจัดการฐานข้อมูลในข้อ ๓๐.๑ เท่านั้น โดยมีผู้มีหน้าที่รับผิดชอบลงนามและเก็บเป็นหลักฐานประวัติของฐานข้อมูลทุกครั้งที่มีการแก้ไข

ข้อ ๓๒ มีการทำระบบสำรองต้นฉบับโปรแกรมประยุกต์ (Source Code) ทุกโปรแกรมตามวงรอบทุก ๒ เดือน และทุกครั้งที่มีการแก้ไขโปรแกรม และจัดเก็บไว้ในที่ปลอดภัยและเหมาะสม

ข้อ ๓๓ ผู้พัฒนาโปรแกรม ต้องพัฒนาตามหลักวิชาการที่ยอมรับโดยทั่วไป รวมทั้งแสดงรายละเอียดที่จำเป็นต่อการรักษาความปลอดภัยไว้ที่ต้นฉบับโปรแกรมประยุกต์ (Source Code) ได้แก่ ชื่อผู้เขียน วัน เดือน ปี ที่เขียนหรือปรับปรุง วัตถุประสงค์ ระดับการป้องกัน

สำหรับข้อมูลที่จำเป็นต้องใช้ในการพัฒนา เช่น ความสัมพันธ์ที่สามารถเชื่อมโยงไปถึงโปรแกรม หรือข้อมูลลับอื่น ๆ ผู้ที่ได้รับอนุญาตให้นำโปรแกรมไปใช้งานได้ ให้เพิ่มเติมไว้ในเอกสารคู่มือ

ข้อ ๓๔ ผู้พัฒนาโปรแกรมเป็นผู้รับผิดชอบต่อการรักษาความลับของโครงสร้างข้อมูลความลับของตรรกะที่ใช้ในโปรแกรม ความถูกต้องของโปรแกรม และทำการพัฒนาโปรแกรมให้ตรงตามวัตถุประสงค์ของทางราชการ โดยใช้เฉพาะซอฟต์แวร์ที่ได้รับอนุญาตหรือลิขสิทธิ์เท่านั้น เป็นเครื่องมือในการพัฒนาโปรแกรม

ข้อ ๓๕ การวิเคราะห์พัฒนาและบำรุงรักษาระบบสารสนเทศ ให้เจ้าของระบบงาน ผู้มีสิทธิและอำนาจในสารสนเทศรับทราบว่าผู้ใดเป็นผู้มีหน้าที่ในการวิเคราะห์พัฒนา และบำรุงรักษาโปรแกรมประยุกต์ของระบบสารสนเทศนั้น

ข้อ ๓๖ การรักษาความปลอดภัยระบบงานให้ปฏิบัติดังนี้

/ ๓๖.๑ การพัฒนา...

๓๖.๑ การพัฒนาโปรแกรมประยุกต์

๓๖.๑.๑ มีการจัดทำและเสนอความต้องการเป็นลายลักษณ์อักษร ลงนามโดยผู้อำนวยการกอง นำเรียนเจ้ากรมกิจการพลเรือนทหาร เพื่อขออนุมัติการจัดทำโปรแกรมระบบงาน

๓๖.๑.๒ ผู้พัฒนาระบบ จัดทำระบบตามที่วางแผนและออกแบบไว้ และสาธิตโปรแกรมต้นแบบ (Prototype) ให้เจ้าของระบบพิจารณาความถูกต้องตรงความต้องการ และอนุมัติให้ดำเนินการในรายละเอียด

๓๖.๒ ต้องจัดให้มีรหัสผ่านในการเข้าสู่ระบบงานอย่างน้อย ๑ ระดับ

๓๖.๓ ระบบงานหรือโปรแกรมประยุกต์จะต้องถูกออกแบบให้ผู้ใช้ระบบงานสามารถเรียกดู หรือเปลี่ยนแปลงข้อมูลได้เฉพาะในส่วนที่ได้รับสิทธิเท่านั้น

๓๖.๔ จัดทำเอกสารประกอบระบบงาน หรือโปรแกรมประยุกต์ตามมาตรฐานที่กำหนด ครอบคลุมถึงการเสนอความต้องการ การกำหนดข้อมูลต่าง ๆ การเคลื่อนไหวของข้อมูล คุณสมบัติของโปรแกรมต่าง ๆ รายละเอียดการทำงานของโปรแกรมข้อมูลเข้าและข้อมูลออก

๓๖.๕ จัดทำเอกสารข้อปฏิบัติด้านการรักษาความปลอดภัยของระบบงานที่พัฒนาแล้วส่งมอบให้ผู้ใช้งานและผู้มีสิทธิในสารสนเทศนั้น ๆ เพื่อรับทราบการปฏิบัติพร้อมกับเอกสารประกอบระบบงาน

ข้อ ๓๗ การจัดทำการรักษาความปลอดภัย การพัฒนาโปรแกรมประยุกต์ให้ปฏิบัติดังนี้

๓๗.๑ ผู้พัฒนาระบบต้องไม่เข้าสู่ระบบที่ใช้งานเป็นประจำ แต่ให้จัดทำข้อมูลสมมุติที่ครอบคลุมทุกเงื่อนไขของข้อมูลจริง เพื่อใช้ในการทดสอบโปรแกรมโดยเฉพาะ และต้องทดสอบโปรแกรมการใช้ร่วมกับเจ้าของระบบอย่างน้อย ๓ ครั้ง

๓๗.๒ ผู้พัฒนาระบบต้องทดสอบความปลอดภัย (Security Acceptance Test) ก่อนติดตั้งใช้งานจริง (Production)

๓๗.๓ โปรแกรมประยุกต์ที่บันทึก หรือแก้ไขข้อมูลต้องมีตรรกะตรวจสอบข้อมูลให้ถูกต้อง (Data Validation) ครบถ้วนสมบูรณ์และจะต้องให้ผู้มีสิทธิบันทึกหรือแก้ไขข้อมูล สามารถดำเนินการได้เฉพาะส่วนของข้อมูลที่ตนเองมีสิทธิเกี่ยวข้องเท่านั้น

๓๗.๔ ผู้บริหารจัดการระบบงาน (Application Administrator) ต้องจัดทำบัญชีรายชื่อของผู้มีสิทธิเข้าถึงระบบงาน มีการตรวจสอบความทันสมัยและถูกต้องของบัญชีตามวงรอบ ๓ เดือน และทุกวงรอบการโยกย้าย โดยต้องยกเลิกรายชื่อผู้ที่หมดสิทธิ์ออกด้วย

๓๗.๕ การแก้ไขโปรแกรมต่าง ๆ จะต้องมีการร้องขอจากผู้มีสิทธิในการปรับแก้ระบบงานนั้น ๆ ก่อนเสมอ

๓๗.๖ เมื่อมีการแก้ไขคำสั่งในโปรแกรมประยุกต์ใช้งานจริง (Production) ต้องแยกดำเนินขั้นตอนการทดสอบให้เรียบร้อยก่อนนำไปใช้งานจริง และบันทึกรายละเอียดคำขอแก้ไขไว้

๓๗.๗ จะต้องปรับปรุงเอกสารประกอบระบบงาน โดยแนบท้ายด้วยการเปลี่ยนแปลงปรับปรุงตามระยะเวลาต่าง ๆ เพื่อให้เอกสารประกอบระบบงานมีความถูกต้อง และทันสมัยอยู่ตลอดเวลา

๓๗.๘ ไม่เก็บต้นฉบับโปรแกรมประยุกต์ (Source Code) ที่อยู่ในระหว่างทดสอบ (Testing) ไว้ในพื้นที่เดียวกับโปรแกรมประยุกต์ที่ใช้งานจริง (Production)

๓๗.๙ กรณีซอฟต์แวร์ที่จัดหา ต้องตรวจสอบก่อนติดตั้งใช้งานจริง เพื่อป้องกันคำสั่งที่ไม่ประสงค์ดี (Malicious Code) แฝงมา

/ข้อ ๓๘ การเข้าถึง...

ข้อ ๓๘ การเข้าถึงฐานข้อมูล ให้เจ้าของระบบงานผู้มีสิทธิและอำนาจในสารสนเทศรับทราบว่าผู้ใดเป็นผู้มีสิทธิทางเทคนิคในการเข้าถึงฐานข้อมูลจริงได้

ข้อ ๓๙ การรักษาความปลอดภัยฐานข้อมูล

๓๙.๑ ผู้บริหารจัดการฐานข้อมูล (Database Administrator - DBA) ต้องไม่ใช้ชื่อผู้ใช้และรหัสผ่านแบบโดยปริยาย (Default Username/Password)

๓๙.๒ ต้องจัดทำบัญชีรายชื่อของผู้มีสิทธิทางเทคนิค ในการเข้าถึงฐานข้อมูลแต่ละระดับและกำหนดรหัสผ่านให้เป็นรายบุคคล ดำเนินการตรวจสอบแก้ไขบัญชีให้ทันสมัย ถูกต้องทุกวงรอบ ๓ เดือน และวงรอบการโยกย้าย โดยต้องยกเลิกรายชื่อผู้ที่หมดสิทธิออกด้วย

๓๙.๓ ต้องเก็บรักษาความลับชั้น “ลับมาก” ของชื่อผู้ใช้และรหัสผ่านของตนเอง โดยเคร่งครัดและรับผิดชอบหากมีการรั่วไหลด้วยรหัสของตน

๓๙.๔ ให้มีการจัดทำสำเนาฐานข้อมูลทุกระบบ ๓ รุ่นวงรอบ (Generation) วงรอบละ ๑ สัปดาห์ และจัดเก็บไว้ในที่ปลอดภัย/เหมาะสม

๓๙.๕ ห้ามใช้ฐานข้อมูลจริง และ/หรือ ฐานข้อมูลสำรองจริงที่ได้จัดทำสำเนาไว้ในการทดลองการพัฒนาโปรแกรม การฝึก หรือการศึกษาโดยเด็ดขาด

๓๙.๖ ห้ามทำการพิมพ์ หรือสำเนาข้อมูลไว้เพื่อการอื่น ที่ไม่ใช่เพื่อให้กรณีการฟื้นฟูระบบหรือตามความต้องการของผู้เป็นเจ้าของระบบงาน

๓๙.๗ การแลกเปลี่ยนสารสนเทศและซอฟต์แวร์

๓๙.๗.๑ จัดทำข้อมูลตกลงระหว่างส่วนราชการ หรือองค์กรที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร ในการแลกเปลี่ยนข้อมูล/สารสนเทศ/และซอฟต์แวร์ (Information and Software Exchange Agreement)

๓๙.๗.๒ กำหนดการจัดส่งสื่อบันทึกข้อมูล (Media Transit) โดยเลือกใช้การนำสารทางทหาร มีการบรรจุหีบห่อสื่อที่ปลอดภัย

ข้อ ๔๐ โปรแกรมอื่น ๆ ซึ่งจัดให้มีขึ้นเพื่อใช้ในการปฏิบัติราชการรวมทั้งแฟ้มข้อมูลต่าง ๆ ที่เกี่ยวข้อง

๔๐.๑ จะต้องมีระบบรักษาความปลอดภัยที่เหมาะสมและดีที่สุดเท่าที่สามารถดำเนินการได้

๔๐.๒ มีการปรับปรุงให้ทันสมัยตลอดเวลา

๔๐.๓ แฟ้มข้อมูลต่าง ๆ ที่ใช้ในการทำงาน หรือเป็นผลพวงของการทำงานจะต้องจัดให้มีชั้นความลับที่เหมาะสม และดำเนินการต่อแฟ้มข้อมูลเหล่านั้นให้สอดคล้องกับชั้นความลับที่กำหนดไว้

๔๐.๔ กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ ที่ไม่ได้กำหนดไว้ท้ายระเบียบ ให้ยึดถือตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

ข้อ ๔๑ รายละเอียดของโปรแกรมใด ๆ และแฟ้มข้อมูลต่าง ๆ ที่อยู่ในเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ เป็นข้อมูลที่จัดเป็นความลับ จะต้องให้รู้เฉพาะผู้ที่มีความจำเป็นต้องรู้เท่านั้น การให้ข้อมูลเหล่านี้กับบุคคลภายนอกใด ๆ จะต้องอยู่ภายใต้ความควบคุมอย่างใกล้ชิด และจะต้องขออนุมัติต่อเจ้ากรมกิจการพลเรือนทหารก่อนดำเนินการเสมอ

ข้อ ๔๒ จัดทำแผนการแก้ไข แผนเตรียมรับสถานการณ์ เมื่อเกิดการละเมิดการรักษาความปลอดภัยขึ้น โดยจัดทำแผนแต่ละสถานการณ์เพื่อใช้เป็นคู่มือเบื้องต้นในการแก้ไข

ข้อ ๔๓ การเผยแพร่โปรแกรมระบบงานที่หน่วยพัฒนาขึ้น โปรแกรมระบบงานใด ๆ ที่จัดให้มีการพัฒนาขึ้นโดยกรมกิจการพลเรือนทหารนั้น หากเห็นว่าเป็นประโยชน์ต่อส่วนรวม และกรมกิจการพลเรือนทหาร สามารถนำไปเผยแพร่ประชาสัมพันธ์ หรือนำไปใช้ต่อได้ ทั้งนี้จะต้องได้รับความเห็นชอบจาก คณะทำงานฯ ตามข้อ ๘ และผู้บังคับบัญชาตามลำดับชั้นก่อนจึงดำเนินการได้

/หมวด ๔..

หมวด ๔

การรักษาความปลอดภัยระบบสื่อสารข้อมูลและระบบเครือข่าย

(Data Communication and Network System)

ข้อ ๔๔ ระบบสื่อสารข้อมูล (Data Communication) หมายความว่า ระบบที่ใช้เพื่อการนำข้อมูลจากจุดต้นทาง ไปยังจุดปลายทาง ตามที่ได้กำหนดไว้ โดยประกอบด้วยอุปกรณ์ต่าง ๆ และโปรแกรมคำสั่งที่ใช้ควบคุมการทำงานของอุปกรณ์เหล่านั้น

ข้อ ๔๕ ระบบเครือข่าย (Network) หมายความว่า การเชื่อมโยงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบที่แยกกันอยู่อย่างอิสระเข้าเป็นเครือข่ายเดียวกัน โดยระบบสื่อสารข้อมูล เพื่อใช้ในการสารสนเทศ ทำการแบ่งปันการใช้ทรัพยากร เช่น ข้อมูลและอุปกรณ์ต่อพ่วงอื่น ๆ

๔๕.๑ ระบบเครือข่ายกองบัญชาการกองทัพไทย ทุกหน่วยในส่วนราชการกองบัญชาการกองทัพไทยใช้ในการปฏิบัติงานร่วมกัน โดยมีกรมการสื่อสารทหารรับผิดชอบการดำเนินการ

๔๕.๒ ระบบเครือข่ายภายในของกรมกิจการพลเรือนทหาร ซึ่งกรมกิจการพลเรือนทหาร รับผิดชอบดำเนินการและบริหารดูแล ใช้เพื่อการปฏิบัติงานภายในหน่วย

ข้อ ๔๖ การเชื่อมโยงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบเข้ากับระบบเครือข่ายกองบัญชาการกองทัพไทย จะต้องได้รับการพิจารณาอนุมัติจากกรมการสื่อสารทหารก่อนดำเนินการทุกครั้ง

ข้อ ๔๗ การจัดทำระบบสื่อสารข้อมูล จะต้องได้รับการพิจารณาอนุมัติจากเจ้ากรมกิจการพลเรือนทหาร โดยผ่านความเห็นชอบจากคณะทำงานด้านเทคโนโลยีสารสนเทศกรมกิจการพลเรือนทหาร ก่อนดำเนินการทุกครั้ง โดยมีการกำหนดขั้นตอนและหน้าที่ความรับผิดชอบการปฏิบัติอย่างชัดเจน

๔๗.๑ กำหนดพิสูจน์การใช้งานของเจ้าหน้าที่ให้สามารถใช้เฉพาะเครือข่ายที่อนุญาตเท่านั้น จำกัดการใช้เส้นทางบนเครือข่ายเพื่อมิให้เจ้าหน้าที่สามารถใช้ออกเส้นทางอื่นได้

๔๗.๒ กำหนดข้อปฏิบัติของเจ้าหน้าที่ในการใช้งานเครือข่ายคอมพิวเตอร์ (ผนวก ก)

ข้อ ๔๘ การใช้ระบบสื่อสารข้อมูลในเครือข่ายสารสนเทศ

๔๘.๑ กรณีที่มีผลกระทบต่อการเชื่อมโยงเป็นส่วนรวมทำให้ไม่สามารถใช้งานเครือข่ายสารสนเทศได้ให้รีบประสานผู้รับผิดชอบเพื่อทำการแก้ไขโดยด่วน พร้อมทั้งรายงานข้อขัดข้องและการดำเนินการแก้ไขให้คณะทำงานด้านเทคโนโลยีสารสนเทศกรมกิจการพลเรือนทหารทราบทันที

๔๘.๒ จะต้องกำหนดรหัสผ่าน ในการเข้าปรับปรุงเปลี่ยนแปลงหรือจัดการการทำงานของอุปกรณ์สื่อสารข้อมูล และให้ใช้ได้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้นโดยปฏิบัติตามแนวทางเดียวกับหัวข้อรหัสผ่าน (หมวด ๕)

๔๘.๓ ในกรณีที่ต้องให้บุคคลอื่นภายนอกดำเนินการเกี่ยวกับระบบสื่อสารข้อมูลต้องจัดเจ้าหน้าที่ร่วมดำเนินการ และรับทราบทุกขั้นตอนทุกครั้ง และต้องได้รับการอนุญาตจากคณะทำงานด้านเทคโนโลยีสารสนเทศกรมกิจการพลเรือนทหารก่อนดำเนินการทุกครั้ง

ข้อ ๔๙ การดำเนินการเกี่ยวกับโปรแกรมคำสั่งต่าง ๆ และอุปกรณ์ในระบบสื่อสารข้อมูล

๔๙.๑ การย้าย เปลี่ยนแปลงที่ตั้ง การตั้งโปรแกรมคำสั่ง หรือมีการกระทำใด ๆ ต่ออุปกรณ์สื่อสารข้อมูล จะต้องได้รับการอนุมัติและกำกับดูแลในคณะทำงานด้านเทคโนโลยีสารสนเทศกรมกิจการพลเรือนทหาร

๔๙.๒ จัดให้มีเครื่องมืออุปกรณ์หรือระบบเข้า – ถอดรหัสข้อมูล ตามมาตรฐานกองบัญชาการกองทัพไทย เพื่อรักษาความลับของข้อมูล

/๔๙.๓ จัดให้มี...

๔๙.๓ จัดให้มีเครื่องมืออุปกรณ์ หรือระบบตรวจสอบเส้นทางการสื่อสารข้อมูลในเครือข่ายตลอดเวลา และมีการบันทึกข้อผิดพลาดที่เกิดขึ้นทุกครั้ง

๔๙.๔ จะต้องมีการทดสอบเครื่องอุปกรณ์ต่าง ๆ ทุก ๖ เดือน และรายงานผลต่อเจ้ากรมกิจการพลเรือนทหาร ทราบภายใน ๑ สัปดาห์

/ผนวก ก ...

ผนวก ก

ข้อปฏิบัติของเจ้าหน้าที่ในการใช้งานระบบเครือข่ายภายใน

ข้อ ๑ เจ้าหน้าที่มีสิทธิ์ใช้ระบบเครือข่ายภายในหรือบุคคลหนึ่งใด ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดดังกล่าว ซึ่งก่อหรืออาจก่อให้เกิดความเสียหายแก่กรมกิจการพลเรือนทหารหรือบุคคลหนึ่งบุคคลใด กรมกิจการพลเรือนทหารจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่เจ้าหน้าที่ที่ฝ่าฝืนตามความเหมาะสม

ข้อ ๒ เจ้าหน้าที่พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

ข้อ ๓ เจ้าหน้าที่พึงใช้ข้อความสุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่าย ไม่ส่ง Mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น

ข้อ ๔ เจ้าหน้าที่มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่น เข้าใช้ระบบเครือข่ายภายในจากบัญชีผู้ใช้ของตนเอง

ข้อ ๕ เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคลเจ้าหน้าที่จะต้องใช้รหัสผ่านส่วนบุคคลตามข้อกำหนดในระเบียบนี้ สำหรับการใช้งานเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองใช้งานอยู่

ข้อ ๖ เจ้าหน้าที่จะต้องไม่ใช้ระบบเครือข่ายภายในโดยมีวัตถุประสงค์ดังต่อไปนี้

๑) เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๒) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๓) เพื่อการพาณิชย์

๔) เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่ กรมกิจการพลเรือนทหารหรือของบุคคลอื่น

๕) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของ กรมกิจการพลเรือนทหารหรือของบุคคลอื่น

๖) เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ หรือผู้มีสิทธิในข้อมูลดังกล่าว

๗) เพื่อการบันทึกรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่ กรมกิจการพลเรือนทหาร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอก อันมีลักษณะเป็นการละเมิดกฎหมายหรือสิทธิของบุคคลอื่น

๘) เพื่อขัดขวางการใช้งานระบบเครือข่ายภายในของกรมกิจการพลเรือนทหาร หรือของเจ้าหน้าที่อื่นของกรมกิจการพลเรือนทหารหรือเพื่อให้ระบบเครือข่ายภายในของกรมกิจการพลเรือนทหารไม่สามารถใช้งานได้ตามปกติ

๙) เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของกรมกิจการพลเรือนทหาร ไปยังเว็บไซต์ (Website) ใดๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

/๑๐) เพื่อการอื่นใด ...

๑๐) เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของกรมกิจการพลเรือนทหารหรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่กรมกิจการพลเรือนทหาร

ข้อ ๗ เพื่อความปลอดภัยในการใช้ระบบเครือข่ายภายในโดยส่วนรวมเจ้าหน้าที่จะต้อง

๑) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

๒) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม ในเครื่องคอมพิวเตอร์ของกรมกิจการพลเรือนทหาร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้นหรือเครือข่ายคอมพิวเตอร์กรมกิจการพลเรือทหาร

๔) ปิดเครื่องคอมพิวเตอร์ที่ตนเองครอบครองใช้งาน เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้น เป็นเครื่องบริการ (Server) ที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

๕) ตรวจสอบข้อมูลที่ได้รับจากภายนอกกรมกิจการพลเรือนทหารทุกครั้งด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ที่องค์กรจัดให้และหากตรวจพบ ไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใด จะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด

๖) ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

๗) ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์หรือคณะกรรมการพัฒนาระบบสารสนเทศ กรมกิจการพลเรือนทหาร ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ของเจ้าหน้าที่รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์หรือคณะทำงานฯ ดังกล่าวด้วย

๘) ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่อง คอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ แล้วแต่กรณี

๙) ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายภายในก่อนได้รับอนุญาต

๑๐) คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานระบบเครือข่ายภายในที่เป็นของ กรมกิจการพลเรือนทหาร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่กรมกิจการพลเรือนทหาร ภายในกำหนด ๗ วัน นับแต่วันพ้นสภาพการเป็นเจ้าหน้าที่

/หมวด ๕ ...

หมวด ๕

การรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการปฏิบัติงานระบบสารสนเทศ
(Procedure)

ข้อ ๕๐ จัดให้มีคำแนะนำการใช้ระบบงานพร้อมเอกสารประกอบระบบงานให้เจ้าหน้าที่ผู้เกี่ยวข้องเพื่อปฏิบัติตามโดยเคร่งครัด

ข้อ ๕๑ กระบวนการตรวจสอบบันทึกเหตุการณ์ในระบบ (Audit Logging Procedures)

๕๑.๑ เจ้าหน้าที่ที่ได้รับมอบหมายทำการตรวจสอบระบบเป็นประจำ อย่างน้อยวันละ ๑ ครั้ง เพื่อช่วยในการควบคุมและแก้ไขความเสียหายที่อาจเกิดขึ้น โดยจะตรวจสอบจากข้อมูลบันทึกเหตุการณ์ต่าง ๆ (Log Event) และทำการบันทึกข้อมูลที่จำเป็น เพิ่มเติมเพื่อเป็นรายงานในการอ้างอิงต่อไป

๕๑.๒ ในกรณีเกิดเหตุการณ์ไม่ปกติเกี่ยวกับความมั่นคงของระบบ ให้เจ้าหน้าที่ผู้ดูแลระบบ รายงานผู้รับผิดชอบ เพื่อให้สามารถแก้ไขสถานการณ์ได้ทันท่วงที

ข้อ ๕๒ การเริ่มใช้ระบบงานใหม่

๕๒.๑ ต้องจัดทำข้อมูลให้สมบูรณ์ถูกต้องก่อนเริ่มใช้ระบบ

๕๒.๒ จัดให้มีการอบรมการใช้และบำรุงรักษาระบบงาน แก่เจ้าหน้าที่ผู้เกี่ยวข้องก่อนเริ่มใช้งานระบบงาน

๕๒.๓ ต้องมีการทำงานคู่ขนานอย่างน้อย ๒ วงรอบ ก่อนการใช้งานระบบงานจริง

๕๒.๔ จะต้องทำเอกสารรับและส่งมอบระบบงาน โดยมีการลงนามในเอกสารและส่งมอบก่อนที่จะเริ่มใช้ระบบงานใหม่ สำเนาเอกสารอีก ๑ ชุด แนบไว้ที่เอกสารประกอบการพัฒนาระบบงาน

ข้อ ๕๓ การดูแลระบบงาน

๕๓.๑ ต้องมีเจ้าหน้าที่ผู้รับผิดชอบโดยตรงในระบบงานนั้น ๆ และจะต้องมีผู้รับผิดชอบรองลงไปไม่น้อยกว่า ๒ คน

๕๓.๒ จะต้องมีการประเมินระบบการทำงานของระบบงานทุก ๖ เดือน และจัดทำสรุปเพื่อนำเรียนเจ้ากรมกิจการพลเรือนทหาร

ข้อ ๕๔ การจัดเก็บเอกสารเกี่ยวกับระบบงาน

๕๔.๑ จะต้องจัดเก็บเอกสารประกอบระบบงานทั้งหมดของแต่ละระบบไว้ด้วยกันโดยจัดทำไว้อย่างน้อย ๒ ชุด จัดเก็บไว้ที่กองสารสนเทศ ๑ ชุด และผู้รับผิดชอบระบบ ๑ ชุด

๕๔.๒ เอกสารย่อย อาจจัดทำสำเนาเก็บไว้สำหรับเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อใช้ในการทำงานได้ตามความเหมาะสม

๕๔.๓ มีการกำหนดชั้นความลับของเอกสารดังกล่าวให้เหมาะสมตามชั้นความลับระบบงาน

๕๔.๔ ดำเนินการเอกสารระบบงานตามระเบียบกองบัญชาการทหารสูงสุดว่าด้วยการเก็บเอกสาร พ.ศ.๒๕๒๒ และแก้ไขเพิ่มเติม

ข้อ ๕๕ จัดทำสถานภาพการสำรองข้อมูลไว้โดยละเอียด และสรุปนำเรียน เจ้ากรมกิจการพลเรือนทหาร ทุก ๑ ปี

ข้อ ๕๖ การดำเนินการด้านรหัสผ่าน (Password)

๕๖.๑ กำหนดระดับบุคคล/หน่วยงาน ที่สามารถเข้าถึงและ/หรือแก้ไขข้อมูลตามสิทธิและอำนาจหน้าที่

/๕๖.๒ กำหนดชื่อ...

๕๖.๒ กำหนดชื่อและรหัสผ่านให้แก่บุคคล/หน่วยงานใน ข้อ ๕๖.๑ เป็นรายบุคคล (Single Password) ห้ามใช้ร่วมกัน

๕๖.๓ กำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยการกำหนดวันหมดอายุทุก ๙๐ วัน ยกเว้นอุปกรณ์ หรือระบบงานที่ไม่สามารถกระทำได้ทางเทคนิค

๕๖.๔ การกำหนดรหัสผ่านต้องไม่ง่ายต่อการคาดเดา ไม่นำรหัสผ่านเดิมมาวนใช้ซ้ำอีก ไม่ใช้ตัวอักษรหรือตัวเลขที่เรียงกัน ไม่ใช้หมายเลขโทรศัพท์ ชื่อเล่น คำในพจนานุกรม ทะเบียนรถ บ้านเลขที่ วัน เดือนปีเกิด หรือเว้นว่างไว้

๕๖.๕ หากสงสัยว่าผู้อื่นรู้รหัสผ่านของตน ให้ดำเนินการเปลี่ยนรหัสผ่านทันที

๕๖.๖ ห้ามเก็บ (Save) รหัสผ่านไว้ในหน่วยความจำเพื่อใช้โดยปริยาย (Default)

๕๖.๗ การเปิดใช้รหัสผ่านต้องมีการปิดเมื่อเลิกใช้ทุกครั้ง

๕๖.๘ การมอบรหัสผ่านให้ผู้เป็นเจ้าของ ต้องดำเนินการในลักษณะชั้นความลับ ลับที่สุด ไม่จดหรือบันทึกรหัสผ่านไว้ในที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๕๖.๙ กรณีผู้ใช้ลืมรหัสผ่าน ต้องดำเนินการตามมาตรการตรวจสอบ และได้รับการยืนยัน จากผู้บังคับบัญชา ก่อนออกรหัสผ่านให้ใหม่

๕๖.๑๐ กรณีการฝึก/ศึกษา หรือเจ้าหน้าที่เทคนิคภายนอกองค์กรที่เกี่ยวข้องชั่วคราวจะได้รับชื่อและรหัสผ่านชั่วคราว และยกเลิกทันทีที่สิ้นสุดกำหนดการใช้งาน

ข้อ ๕๗ ห้ามนำซอฟต์แวร์หรือข้อมูลจากภายนอกที่ไม่ได้ผ่านการตรวจสอบไวรัสหรือภัยคุกคามมาติดตั้งหรือใช้งานโดยพลการ หากเกิดการละเมิด ผู้เป็นเจ้าหน้าที่ประจำเครื่องนั้น ๆ เป็นผู้รับผิดชอบในเบื้องต้น

ข้อ ๕๘ ผู้ใช้เครื่องคอมพิวเตอร์ส่วนบุคคล

๕๘.๑ ต้องทำการสำเนาข้อมูลเครื่องนั้น ๆ ด้วยตนเอง เพื่อสามารถกู้คืนสภาพได้โดยไม่ต้องทำเป็นส่วนรวม

๕๘.๒ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ครอบครองใช้งานประจำ เมื่อเสร็จสิ้นภารกิจหรือหยุดการใช้งานเกินกว่า ๑ ชั่วโมง ยกเว้นเครื่องให้บริการส่วนรวมที่ต้องเปิดตลอด ๒๔ ชั่วโมง

ข้อ ๕๙ ห้ามปรับแต่งหรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัสที่กำหนดให้ติดตั้งใช้งานบนเครื่องคอมพิวเตอร์โดยพลการ

/หมวด ๖...

หมวด ๖
การรักษาความปลอดภัยด้านบุคลากรสารสนเทศ (Personnel)

ข้อ ๖๐ ความมุ่งหมายเพื่อคัดเลือกบุคคลที่มีความเหมาะสม มาปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศและเพื่อกำหนดระดับความไว้วางใจในการปฏิบัติหน้าที่เกี่ยวกับข้อมูลที่เป็นความลับของทางราชการ ตลอดจนควบคุมบุคคลที่ไม่เกี่ยวข้องและบุคคลภายนอก

ข้อ ๖๑ ข้าราชการ ลูกจ้างและพนักงานราชการ กรมกิจการพลเรือนทหาร ต้องผ่านการอบรมในเรื่องระเบียบรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๖ ระเบียบรักษาความปลอดภัยระบบสารสนเทศกองทัพไทย พ.ศ.๒๕๔๗ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ และระเบียบนี้ เพื่อให้ทุกคนมีจิตสำนึกในการรักษาความปลอดภัย ปฏิบัติตามระเบียบรักษาความปลอดภัยฯ ได้อย่างถูกต้อง ช่วยกันสอดส่องดูแลมิให้ผู้ใดละเมิด และกำหนดให้มีการตรวจสอบการปฏิบัติงานของข้าราชการ ลูกจ้างและพนักงานราชการให้เป็นไปตามระเบียบและสอดคล้องกับนโยบายการรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๖๒ ตรวจสอบความไว้วางใจของข้าราชการ ลูกจ้างและพนักงานราชการ กรมกิจการพลเรือนทหารทุกนาย โดยตรวจสอบประวัติ และพฤติการณ์ของบุคคลก่อนมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศภายในกรมกิจการพลเรือนทหาร

ข้อ ๖๓ ทะเบียนความไว้วางใจบุคลากร

๖๓.๑ จัดทำทะเบียนความไว้วางใจของเจ้าหน้าที่เทคนิคและเจ้าหน้าที่ที่ระบบงานตามกลุ่มงาน หน้าที่ความรับผิดชอบ โดยจัดตามระดับชั้นความลับที่ได้รับอนุมัติ

๖๓.๒ จัดลงทะเบียนเจ้าหน้าที่ใหม่ และยกเลิกการใช้งานทันทีที่พ้นหน้าที่

๖๓.๓ ต้องทบทวนสิทธิ์ทุก ๖ เดือน และทุกครั้งที่มีการเปลี่ยนแปลง

ข้อ ๖๔ แต่งตั้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ กรมกิจการพลเรืองทหาร ดูแลรักษาความปลอดภัยระบบสารสนเทศกรมกิจการพลเรือนทหาร โดยมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมกิจการพลเรือนทหาร (รองเจ้ากรมกิจการพลเรือนทหาร (สายงานด้านสารสนเทศ)) เป็นหัวหน้าคณะทำงาน

ข้อ ๖๕ แต่งตั้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศประจำพื้นที่ของหน่วยอย่างน้อย ๑ นาย โดยกำหนดหน้าที่ความรับผิดชอบไว้อย่างชัดเจน

ข้อ ๖๖ ผู้ที่พ้นจากหน้าที่เกี่ยวกับระบบสารสนเทศ ได้ตัดชื่อออกจากทะเบียนความไว้วางใจและนำเรียนเจ้ากรมกิจการพลเรือนทหาร ทราบภายใน ๒ วันทำการ

ข้อ ๖๗ การปฏิบัติด้านการรักษาความปลอดภัยของผู้ใช้

เพื่อประโยชน์ในการรักษาความปลอดภัยในการใช้บริการ ผู้ขอใช้บริการจะต้องยึดถือและปฏิบัติตาม ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และระเบียบอื่น ๆ ที่เกี่ยวข้อง รวมทั้งปฏิบัติตามนโยบาย และคำชี้แจงตามที่กำหนดไว้อย่างเคร่งครัด

ข้อ ๖๘ การปฏิบัติด้านการรักษาความปลอดภัยของผู้ปฏิบัติงานชั่วคราว

/ให้จัดทำ ...

ให้จัดทำทะเบียนแยกกลุ่มต่างหาก โดยจะต้องผ่านการตรวจสอบความไว้วางใจเช่นเดียวกันก่อนจะได้รับอนุญาตให้ปฏิบัติงานชั่วคราว โดยเกี่ยวข้องเฉพาะเรื่องเป็นกรณีไป และให้ยกเลิกการอนุญาตทันที เมื่อครบกำหนดสิ้นสุดการขอใช้งาน

ข้อ ๖๙ การปฏิบัติด้านการรักษาความปลอดภัย ในการจัดจ้างองค์กร/เอกชนภายนอกมาปฏิบัติงาน (Outsourcing) จะต้องกำหนดให้ผู้รับจ้างต้องไม่นำข้อมูล เอกสาร ผลงานต่าง ๆ เอกสารการฝึกอบรมไปเผยแพร่หรือใช้ในกิจการที่ไม่เกี่ยวกับงานตามสัญญา และเจ้าหน้าที่ของผู้รับจ้างจะได้รับสิทธิ์ในฐานะผู้ปฏิบัติงานชั่วคราว โดยรายละเอียดเหล่านี้จะต้องระบุไว้ในสัญญาอย่างชัดเจน

ข้อ ๗๐ หากกำลังพลหรือบุคคลใดที่ได้รับอนุญาตปฏิบัติงานด้านสารสนเทศแล้วมีพฤติกรรมหรือข้อชวนสงสัย อันจะเป็นภัยต่อระบบสารสนเทศที่กรมกิจการพลเรือนทหารรับผิดชอบไม่ว่าจะโดยเจตนาหรือไม่ก็ตาม ให้ผู้มีหน้าที่กำกับดูแลระงับการอนุญาตชั่วคราว และสอบสวนให้ได้ความจริงก่อนพิจารณาตัดสิทธิ หรือให้สิทธิการปฏิบัติงานต่อไป

ข้อ ๗๑ ในกรณีที่เกิดเหตุการณ์ไม่ปกติ ข้าราชการ ลูกจ้างและพนักงานราชการ กรมกิจการพลเรือนทหารต้องปฏิบัติ ดังนี้

๗๑.๑ จัดให้มีการเฝ้าดูการปฏิบัติงานสารสนเทศของเจ้าหน้าที่เทคนิคและเจ้าหน้าที่ผู้ใช้ระบบงาน ให้เป็นไปตามวัตถุประสงค์ของกรมกิจการพลเรือนทหารและไม่ให้ใช้งานนอกเหนือจากสิทธิที่ตนได้รับ

๗๑.๒ รายงานเหตุการณ์ที่ละเมิดความมั่นคงความปลอดภัยซึ่งเกิดขึ้น (Security Incidents) ให้ผู้รับผิดชอบทราบโดยด่วน

๗๑.๓ รายงานจุดอ่อน ช่องโหว่ หรือภัยคุกคามที่พบในระบบสารสนเทศให้ผู้รับผิดชอบทราบโดยด่วน

๗๑.๔ ผู้ดูแลระบบ ต้องบันทึกเหตุการณ์ในกรณีที่เกิดเหตุการณ์ไม่ปกติต่าง ๆ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

ข้อ ๗๒ จัดให้มีกระบวนการทางวินัยเพื่อลงโทษข้าราชการ ลูกจ้างและพนักงานราชการที่ฝ่าฝืนหรือละเมิดระเบียบกรมกิจการพลเรือนทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๐ โดยจะได้รับโทษทางวินัยแล้วแต่กรณี

/หมวดที่ ๗...

หมวด ๗
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม
(Physical and Environment)

ข้อ ๗๓ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูล จัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๗๔ กำหนดให้ที่ตั้งของระบบสารสนเทศ และพื้นที่ที่ใช้งานระบบสารสนเทศภายในกรมกิจการพลเรือนทหาร

๗๔.๑ เป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๗๔.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่บริเวณที่มีการผ่านเข้า-ออกของบุคคลเป็นจำนวนมาก

๗๔.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๗๔.๔ จะต้องปิดล็อกหรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่อยู่

๗๔.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

๗๔.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกแถบบันทึกภาพในบริเวณดังกล่าวเป็นอันขาด

๗๔.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๗๕ เพื่อประโยชน์ในการรักษาความปลอดภัยทางด้านกายภาพของระบบให้ติดตั้งอุปกรณ์รักษาความปลอดภัย ณ สถานที่ตั้งระบบให้บริการ (Service System) ด้วยเทคโนโลยีที่เหมาะสมและทันสมัย

ข้อ ๗๖ การเข้าถึงหรือเข้าออกพื้นที่ ให้เจ้าหน้าที่ของกรมกิจการพลเรือนทหารซึ่งได้รับมอบหมายหรือได้รับอนุญาตเท่านั้น เป็นผู้มีสิทธิเข้าถึงหรือเข้าออกบริเวณพื้นที่ซึ่งติดตั้งอุปกรณ์

ข้อ ๗๗ ต้องกำหนดให้มีการป้องกันรักษาความปลอดภัยเครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบที่สามารถเคลื่อนย้ายได้ และหรืออยู่นอกพื้นที่ควบคุม เมื่อถูกนำไปใช้งานนอกสถานที่ต้องกำหนดการปฏิบัติในการใช้งาน การยืม/คืน และอื่น ๆ ให้สอดคล้องกับระเบียบว่าด้วยการรักษาความปลอดภัยอย่างรัดกุม

ข้อ ๗๘ ระบบไฟฟ้าและระบบปรับอากาศ จะต้องมีความปลอดภัยและเหมาะสมโดยจัดให้มีระบบไฟฟ้าสำรองเพื่อใช้งานเมื่อไฟฟ้าขัดข้อง และระบบปรับอากาศสำรองเพื่อควบคุมและรักษาอุณหภูมิและความชื้นของห้องให้คงที่

ข้อ ๗๙ ต้องมีการป้องกันรักษาความปลอดภัยระบบสายไฟและเคเบิล โดยเดินสายไฟฟ้าหรือสายเคเบิลผ่านทางช่องทางพิเศษที่จัดไว้ ซึ่งจะต้องเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย

ข้อ ๘๐ ต้องมีมาตรการป้องกันอัคคีภัยและภัยธรรมชาติ โดยจัดเตรียมอุปกรณ์ให้พร้อมใช้งานได้ตลอดเวลา ตลอดจนจัดเตรียมสถานที่ วัสดุอุปกรณ์ สำหรับการฟื้นฟูระบบ และสถานที่เก็บรักษาสำรองข้อมูลที่ปลอดภัยถ้ามี

/ ๘๐.๑ การป้องกัน...

๘๐.๑ การป้องกันอัคคีภัย

บริเวณพื้นที่ซึ่งติดตั้งและจัดวางอุปกรณ์ จะต้องมีการติดตั้งระบบดับเพลิง ซึ่งมีคุณสมบัติพิเศษในการดับเพลิงได้อย่างรวดเร็วและมีประสิทธิภาพ โดยไม่ก่อให้เกิดความเสียหายกับอุปกรณ์ประเภทไฟฟ้า อิเล็กทรอนิกส์ หรือคอมพิวเตอร์

๘๐.๒ การเก็บรักษาสื่อที่ใช้เก็บข้อมูล (Media Storage) จะต้องถูกจัดเก็บอย่างปลอดภัย และมีระบบสำรองข้อมูลที่มีประสิทธิภาพ

๘๐.๓ การทำลายสิ่งที่ไม่ใช้

สื่อแม่เหล็ก หรือสื่ออื่นที่ใช้ในการบันทึก หรือเก็บข้อมูลที่ไม่ใช้อีกต่อไปจะต้องดำเนินการเพื่อไม่ให้มีการนำสื่อข้างต้นกลับมาใช้หรือเรียกค้นข้อมูลได้อีก ทั้งนี้การทำลายสื่อแม่เหล็กหมายรวมถึงการเขียนข้อมูลทับ (Overwrite) การทำลายด้วยสนามแม่เหล็ก (Degauss) หรือการทำลายทิ้ง (Destruct) ก็ได้

ข้อ ๘๑ จะต้องมีแผนเตรียมรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนการพิทักษ์รักษาระบบสารสนเทศ แผนการเคลื่อนย้าย แผนการทำลายระบบสารสนเทศในเวลาฉุกเฉิน และแผนอื่น ๆ ตามที่ผู้บังคับบัญชากำหนด

ข้อ ๘๒ จัดให้มีเวร-ยามรักษาการณ์ และพิทักษ์รักษาระบบสารสนเทศ และมีการประชุมชี้แจงเจ้าหน้าที่รักษาการณ์ให้ทราบถึงขั้นตอนการตรวจการณ์ การพิสูจน์ทราบฝ่าย และการเข้าขัดขวางในพื้นที่รับผิดชอบอย่างสม่ำเสมอ และให้มีการกำกับดูแลอย่างเข้มงวด

ข้อ ๘๓ ให้ใช้ระเบียบนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ มีนาคม พ.ศ.๒๕๖๐

พลโท

(ชัยพฤกษ์ อัยยะภาคย์)
เจ้ากรมกิจการพลเรือนทหาร

สำนักประชาสัมพันธ์ กรมกิจการพลเรือนทหาร