บันทึกข้อความ

ส่วนราชการ สส.ทหาร (สผอ.สส.ทหาร โทร. ๐ ๒๕๖๕ ๕๔๙๐, โทร.ทหาร ๕๐๑๑๖๕๙)
ที่ กห ๐๓๐๗/๒๓๙๑ **วันที่** ๕ ก.ย.๕๙
เรื่อง ขออนุมัติประกาศ นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ.๒๕๕๙

เรียน ผบ.ทสส.

สิ่งที่ส่งมาด้วย ๑. ร่างประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ.๒๕๕๙
๒. สำเนาประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓
๓. สำเนาหนังสือ บก.ทท. ที่ กห ๐๓๐๐/๓๔๖๗ ลง ๙ ธ.ค.๕๘
๔. สำเนาหนังสือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ ทก ๐๒๐๙.๔/๓๗๙๒ ลง ๒๙ มี.ค.๕๙

๑. **สส.ทหาร ขออนุมัติประกาศ นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ.๒๕๕๙ ให้ส่วนราชการใน บก.ทท. ยึดถือและปฏิบัติตามนโยบายฯ เพื่อลดความเสี่ยงจากภัยคุกคามของระบบสารสนเทศ บก.ทท.** รายละเอียดตามสิ่งที่ส่งมาด้วย ๑

๒. ข้อเท็จจริง

๒.๑ **คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้ออกประกาศเรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ซึ่งกำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานและส่งให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อพิจารณาให้ความเห็นชอบก่อนการประกาศใช้** รายละเอียดตามสิ่งที่ส่งมาด้วย ๒

๒.๒ **บก.ทท. (สส.ทหาร) ได้จัดทำร่างนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. และแบบประเมิน ส่งให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร พิจารณาให้ความเห็นชอบร่างนโยบายฯ** ดังกล่าว **เพื่อให้ส่วนราชการใน บก.ทท. ยึดถือและปฏิบัติตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท.** รายละเอียดตามสิ่งที่ส่งมาด้วย ๓

๒.๓ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ในฐานะฝ่ายเลขานุการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีหนังสือแจ้งให้ทราบว่า **คณะกรรมการฯ มีมติเห็นชอบต่อร่างนโยบายฯ และแจ้งเพิ่มเติมว่า การพิจารณาให้ความเห็นชอบดังกล่าว เป็นเพียงมาตรการขั้นต่ำที่ช่วยลดความเสี่ยงจากภัยคุกคามของระบบสารสนเทศ เพื่อให้เกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ หน่วยงานต้องให้ความสำคัญ และจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยในทางปฏิบัติ รวมทั้งควรปรับปรุงมาตรการ เพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม** รายละเอียดตามสิ่งที่ส่งมาด้วย ๔ **ซึ่งตามร่างนโยบายฯ นี้ ได้จัดให้มีการตรวจสอบและประเมินผลอย่างน้อย ปีละ ๑ ครั้ง**

๓. ข้อพิจารณา **ร่างประกาศฯ ตามข้อ ๑ เป็นการกำหนดขอบเขตและข้อกำหนดในการรักษาความปลอดภัยระบบสารสนเทศ ให้กับส่วนราชการใน บก.ทท. และผู้ใช้งานระบบเทคโนโลยีสารสนเทศของ บก.ทท. ได้ยึดถือปฏิบัติ เพื่อเป็นการลดความเสี่ยงจากภัยคุกคามที่มีต่อระบบสารสนเทศ และลดความเสียหายต่าง ๆ**

/ที่จะเกิด...

ที่จะเกิดขึ้น จากเหตุละเมิดความมั่นคงปลอดภัย อันเป็นการรักษาไว้ซึ่งความสามารถในการปฏิบัติภารกิจของ บก.ทท. ได้อย่างต่อเนื่อง ทั้งนี้ ร่างประกาศฯ ดังกล่าว ได้ผ่านความเห็นชอบจาก คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้ว จึงเห็นสมควรประกาศ นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ.๒๕๕๙ ให้ส่วนราชการใน บก.ทท. ยึดถือปฏิบัติต่อไป

๔. ข้อเสนอ เห็นควรดำเนินการดังนี้

๔.๑ อนุมัติให้ประกาศ นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ.๒๕๕๙ เพื่อให้ส่วนราชการใน บก.ทท. ยึดถือและปฏิบัติ ตามข้อ ๑

๔.๒ ให้ สส.ทหาร ดำเนินการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ กับทั้งปรับปรุงมาตรการต่าง ๆ ที่เกี่ยวข้อง เพื่อให้ระบบสารสนเทศ บก.ทท. มีความมั่นคงปลอดภัยในทางปฏิบัติ

๔.๓ ให้ สบ.ทหาร สำเนาประกาศฯ แจ้งส่วนราชการใน บก.ทท. ทราบ และยึดถือเป็นแนวทางปฏิบัติ

จึงเรียนมาเพื่อพิจารณา หากเห็นสมควรกรุณาอนุมัติตามข้อ ๔ และลงนามในร่างประกาศฯ ที่แนบ

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)

จก.สส.ทหาร

-อนุมัติตามข้อ ๔
-ลงนามแจ้ง

พล.อ.

ผบ.ทสส.

๑๕ ก.ย.๕๙

เรียน ผบ.ทสส.

เห็นสมควรอนุมัติ และลงนามในร่างประกาศฯ

พลร. อิทธิ

รอง เสธ.ทหาร (๗)

๘ ก.ย. ๕๙

พล.อ.

เสธ.ทหาร

๑๖ ก.ย.๕๙

พล.อ.

รอง ผบ.ทสส.(๑)

๑๕ ก.ย.๕๙

ประกาศกองบัญชาการกองทัพไทย

เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย

พ.ศ.๒๕๕๙

เพื่อให้การรักษาความมั่นคงปลอดภัยสารสนเทศของ กองบัญชาการกองทัพไทย เป็นไปอย่างเหมาะสม มีประสิทธิภาพและประสิทธิผล และมีความมั่นคงปลอดภัย โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพความพร้อมใช้งาน ต่อระบบสารสนเทศ สินทรัพย์สารสนเทศ และข้อมูลสำคัญในการปฏิบัติภารกิจ อันเป็นการลดความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศ และลดความเสียหายต่างๆ ที่เกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัย และรักษาไว้ซึ่งความสามารถในการปฏิบัติภารกิจได้อย่างต่อเนื่อง รวมทั้งสอดคล้องกับกฎหมาย และระเบียบที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศและด้านการประกอบธุรกรรมทางอิเล็กทรอนิกส์ กองบัญชาการกองทัพไทย มีความจำเป็นอย่างยิ่งที่จะต้องมีนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อกำหนดขอบเขตและข้อกำหนดในการรักษาความปลอดภัยระบบสารสนเทศให้กับหน่วยขึ้นตรง ตลอดจนผู้ใช้งานระบบเทคโนโลยีสารสนเทศของ กองบัญชาการกองทัพไทย จึงกำหนดนโยบาย ดังนี้

๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

๑.๑ กองบัญชาการกองทัพไทย จัดให้มีนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information Technology Security Policy) เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของ กองบัญชาการกองทัพไทย ให้สอดคล้องกับข้อกำหนดการบริหารราชการ กฎหมายเทคโนโลยีสารสนเทศและกฎระเบียบที่เกี่ยวข้องและประกาศใช้อย่างเป็นลายลักษณ์อักษรและลงนามอนุมัติโดยผู้บัญชาการทหารสูงสุด รวมทั้งประกาศและเผยแพร่ ให้กำลังพลและผู้เกี่ยวข้องรับทราบและถือปฏิบัติรวมทั้งส่วนราชการใน กองบัญชาการกองทัพไทย สามารถจัดทำนโยบายเป็นของตนเองได้ โดยไม่ขัดต่อนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย

๑.๒ ผู้บัญชาการทหารสูงสุด ในฐานะผู้บริหารระดับสูง (Chief Executive Officer : CEO) กองบัญชาการกองทัพไทย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย

๑.๓ เสนาธิการทหาร กองบัญชาการกองทัพไทย ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) กองบัญชาการกองทัพไทย เป็นผู้รับผิดชอบด้านสารสนเทศในภาพรวมของ กองบัญชาการกองทัพไทย

๑.๔ เจ้ากรมการสื่อสารทหาร กองบัญชาการกองทัพไทย มีหน้าที่รับผิดชอบในการดำเนินการจัดทำและทบทวนปรับปรุงนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมถึงแนวนโยบาย และ/หรือแนวปฏิบัติที่เกี่ยวข้องให้เป็นปัจจุบันอยู่เสมอ และการประกาศให้บุคลากรและผู้เกี่ยวข้องทั้งหมดทราบ ให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย ได้

/๑.๕ คณะทำงาน...

๑.๕ คณะทำงานพัฒนาคุณภาพการบริหารจัดการภาครัฐ กองบัญชาการกองทัพไทย หมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ (IT 6) เป็นผู้พิจารณาทบทวนปรับปรุงนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย ให้เป็นปัจจุบันอยู่เสมอ โดยทบทวนปรับปรุงอย่างน้อยปีละ ๑ ครั้ง หรือตามรอบระยะเวลาที่กำหนด โดยการปฏิบัตินั้นให้คำนึงถึงความเพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อสภาวะโดยรวมของหน่วย ภารกิจ ข้อบังคับ กฎหมาย หรือสภาพแวดล้อมทางเทคนิค โดยให้คำนึงถึงความเหมาะสม ความเพียงพอ และประสิทธิผลการบังคับใช้

๒. การจัดโครงสร้างส่วนราชการ เพื่อรักษาความปลอดภัยสารสนเทศ (Security Organization) เพื่อการบริหารจัดการควบคุมและกำหนดรูปแบบการติดตั้งและใช้งานระบบการรักษาความปลอดภัยสารสนเทศ ให้ครอบคลุมและมีประสิทธิภาพ ดังนี้

๒.๑ ต้องกำหนดนิยามและกระบวนการต่าง ๆ ในการรักษาความปลอดภัยที่ชัดเจน รวมถึงต้องประสานงานส่วนราชการที่มีส่วนเกี่ยวข้องตามแผนนโยบายรักษาความปลอดภัยของ กองบัญชาการกองทัพไทย

๒.๒ ต้องจัดตั้งคณะหรือกลุ่มผู้ทำงานหลักเพื่อบริหารและจัดการความปลอดภัยสำหรับสารสนเทศของส่วนราชการ

๒.๓ ต้องกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานทางด้านความปลอดภัยสารสนเทศของส่วนราชการไว้อย่างชัดเจน

๒.๔ ต้องกำหนดสิทธิการใช้งานระบบสารสนเทศทั้งระบบปัจจุบันที่มีอยู่แล้วและที่จะนำเข้ามาใช้งานใหม่

๒.๕ ต้องระบุลักษณะของการเข้าใช้งานผ่านทางเครือข่าย การใช้งานในสำนักงานโดยตรง

๒.๖ ต้องระบุเหตุความจำเป็นในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศอย่างชัดเจน

๒.๗ ต้องควบคุมหน่วยงานภายนอกที่ปฏิบัติงานอยู่ในสำนักงานของส่วนราชการในการใช้งานระบบสารสนเทศและทรัพยากรสารสนเทศอื่น ๆ ให้เป็นไปอย่างปลอดภัย (รวมทั้งในสัญญาที่ทำไว้กับหน่วยงานนั้นจะต้องระบุข้อกำหนดในการใช้งานไว้อย่างชัดเจน)

๓. การสร้างความมั่นคงปลอดภัยด้านควบคุมการเข้าถึงและการใช้งานสินทรัพย์สารสนเทศ

๓.๑ ต้องบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management) โดยระบุประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลหรือสารสนเทศ รวมทั้งการระบุความเป็นเจ้าของหรือผู้ดูแลสินทรัพย์สารสนเทศ

๓.๒ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านควบคุมการเข้าถึงและการใช้งานสินทรัพย์สารสนเทศ (Access Control Policy) กำหนดการเข้าถึงและควบคุมการเข้าถึงดังต่อไปนี้

๓.๒.๑ ข้อกำหนดการใช้งานตามภารกิจ

๓.๒.๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๓.๒.๓ การควบคุมการเข้าถึงเครือข่าย

๓.๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๒.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

๓.๒.๖ การควบคุมการเข้าถึงจากการใช้งานจากภายนอก

๓.๒.๗ การควบคุมการใช้งานสารสนเทศ

/๓.๒.๘ จัดให้มี...

๓.๒.๘ จัดให้มีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy or Privacy Policy) ในกรณีที่ดำเนินการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม

๔. การสร้างความมั่นคงปลอดภัยด้านบุคลากร

๔.๑ ต้องกำหนดคุณสมบัติ และหน้าที่ความรับผิดชอบของบุคลากรด้านเทคโนโลยีสารสนเทศ

๔.๒ ต้องจัดอบรมให้ความรู้วิธีปฏิบัติแก่บุคลากร ความตระหนักรู้ เพื่อสร้างความปลอดภัยให้กับระบบสารสนเทศและเครือข่ายของส่วนราชการ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของส่วนราชการด้วย

๔.๓ ต้องพิจารณาลงโทษทางวินัยและดำเนินการตามกฎหมาย ในกรณีที่มีการฝ่าฝืน หรือละเมิดนโยบายความปลอดภัยหรือระเบียบปฏิบัติเพื่อความปลอดภัยของส่วนราชการ

๕. ความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) มาตรการ และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security) สำหรับพื้นที่ควบคุมและสถานที่สำคัญในการให้บริการสารสนเทศ ศูนย์ข้อมูล ศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงาน ให้ยึดถือตามแนวปฏิบัติในการควบคุมการเข้าถึงและใช้งานสารสนเทศ (ผนวก ข) รวมทั้งการรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศและอุปกรณ์ในการให้บริการสารสนเทศ

๖. การสร้างความมั่นคงปลอดภัยด้านการปฏิบัติงาน

๖.๑ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการบริหารจัดการด้านการสื่อสารและการปฏิบัติงาน (Communications and Operations Management) ของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๒ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

๖.๓ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ (Information Security Incident Management) การสร้างความมั่นคงปลอดภัยด้านการบริหารความต่อเนื่องในการปฏิบัติภารกิจ

๖.๔ ต้องมีระบบสำรอง ศูนย์ข้อมูลสำรองหรือศูนย์คอมพิวเตอร์สำรอง ที่เหมาะสมสำหรับหน่วยงานและให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสมต่อภารกิจหลักของหน่วยงาน รวมทั้งนโยบายการสำรองข้อมูล (Back-up Policy) เพื่อรองรับการดำเนินการตามภารกิจในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์หรือในกรณีที่ระบบหลักหรือศูนย์ข้อมูลหลักหรือศูนย์คอมพิวเตอร์หลักไม่สามารถให้บริการในระยะเวลาที่เหมาะสมต่อความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๖.๕ ต้องจัดการการบริหารความต่อเนื่องในการปฏิบัติภารกิจของหน่วยงาน (Business Continuity Management : BCM) โดยมีเนื้อหาครอบคลุม ดังนี้

/๖.๕.๑ ต้องจัดทำ...

๖.๕.๑ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ประกอบด้วยแผนรองรับการดำเนินงานอย่างต่อเนื่อง (Business Continuity Plan : BCP) และแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (IT Contingency Plan : ITCP) ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๖.๕.๒ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๖.๕.๓ ต้องทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ รวมถึงการทบทวนและปรับปรุงแผนเตรียมพร้อมกรณีฉุกเฉิน โดยความถี่ของการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อย ๑ ครั้งต่อปี

๗. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายและข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๑ ต้องประเมินความเสี่ยงด้านสารสนเทศ (Information Security Risk Assessment) และทบทวนการประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ตามรอบระยะเวลาที่หน่วยงานกำหนด หรือ อย่างน้อยปีละ ๒ ครั้ง โดยอ้างอิงหลักเกณฑ์การประเมินความเสี่ยงที่เหมาะสมหรือที่หน่วยงานจัดทำขึ้น ซึ่งครอบคลุมปัจจัยเสี่ยงทั้งปัจจัยภายในและภายนอก ตามกระบวนงานที่สำคัญของภารกิจหลักและสินทรัพย์สารสนเทศที่เกี่ยวข้อง

๗.๒ ต้องตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนด (Compliance) อย่างสม่ำเสมอ รวมถึงการตรวจสอบด้านความมั่นคงปลอดภัยระบบสารสนเทศที่สำคัญต่อการปฏิบัติภารกิจหลัก (Information System / Information Security Audit) โดยการตรวจสอบของผู้ตรวจสอบภายในหน่วยงาน (Internal Auditor) ทั้งนี้จะตรวจสอบจากผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เฉพาะในกรณีที่จำเป็นเท่านั้น เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๗.๓ ต้องประเมินตนเองด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Self - Assessment) ของหน่วยงานสม่ำเสมอตามแนวปฏิบัติและในการรักษาความมั่นคงปลอดภัย และกระบวนงานที่สำคัญตามภารกิจของหน่วยงานต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงานโดยครอบคลุมหัวข้ออย่างน้อยตามกฎระเบียบที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๘. การปฏิบัติการตามข้อกำหนดทางด้านกฎหมาย คำสั่ง นโยบาย และระเบียบการรักษาความปลอดภัยสารสนเทศ (Compliance)

เพื่อให้หัวหน้างานสารสนเทศ และนายทหารพระธรรมนูญ คำนึงถึงการปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อป้องกันการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญาและข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ โดยมีแนวนโยบาย ให้ดำเนินการให้สอดคล้องให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และมาตรฐานการรักษาความปลอดภัย

/๙. รายละเอียด...

๙. รายละเอียดเพิ่มเติมตามผนวก ท้ายประกาศ

ข้อแนะนำและแนวปฏิบัติในการดำเนินการตามรายละเอียดเพิ่มเติม มีวัตถุประสงค์เพื่อให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย เป็นมาตรการและแนวทางในการรักษาความปลอดภัยด้านสารสนเทศให้อยู่ในระดับที่มีความมั่นคงปลอดภัยสูงสุด ให้ข้าราชการ ลูกจ้าง และพนักงานราชการใน กองบัญชาการกองทัพไทย และหน่วยงานภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ กองบัญชาการกองทัพไทย ยึดถือและปฏิบัติ ตามผนวกท้ายประกาศอย่างเคร่งครัด หากดำเนินการแก้ไขปรับปรุงแนวปฏิบัติอื่น ๆ ให้สามารถเพิ่มเป็นภาคผนวกได้

ประกาศ ณ วันที่ ๑๙ กันยายน พ.ศ.๒๕๕๙

พลเอก

(สมหมาย เกาฏีระ)
ผู้บัญชาการทหารสูงสุด

กรมการสื่อสารทหาร

ผนวก ก : คำนิยาม
ผนวก ข : แนวปฏิบัติในการควบคุมการเข้าถึงและใช้งานสารสนเทศ
ผนวก ค : แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ
ผนวก ง : แนวปฏิบัติในการใช้งานระบบสารสนเทศและระบบสำรองของสารสนเทศ
ผนวก จ : แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน
ผนวก ฉ : แนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ผนวก ช : แนวปฏิบัติในการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ

ผนวก ก คำนิยาม

ประกอบ ประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

คำนิยาม

คำนิยามที่ใช้ในนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศฉบับนี้ประกอบด้วย

๑. "ระบบสารสนเทศ" หมายความว่า ระบบจัดการข้อมูลที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสาร มาช่วยในการสร้างสารสนเทศ เพื่อนำมาใช้ในการวางแผน การบริหาร การพัฒนาและควบคุม ซึ่งประกอบด้วย

๑.๑ "ระบบคอมพิวเตอร์"หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยต้องกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑.๒ "ระบบเครือข่าย"หมายความว่าระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กร ทั้งในระบบ Intranet และ ระบบ Internet ได้

๑.๒.๑ ระบบอินทราเน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑.๒.๒ ระบบอินเทอร์เน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๑.๓ "สารสนเทศ"หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๒. "คอมพิวเตอร์" หมายความว่า เครื่องมือ หรืออุปกรณ์อิเล็กทรอนิกส์ ที่มีความสามารถในการรับข้อมูลเข้าประมวลผลตามโปรแกรมและแสดง บันทึก ส่งออกข้อมูล ซึ่งเป็นผลที่ได้จากการประมวลผลนั้น โดยอาจมีลักษณะเป็นคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา ตลอดจนคอมพิวเตอร์อื่นๆ รวมถึง แท็ปเล็ต และสมาร์ทโฟน

๓. "พื้นที่ใช้งานระบบสารสนเทศ" หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ หรือพื้นที่เตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งพื้นที่โต๊ะทำงานที่มีคอมพิวเตอร์ส่วนบุคคลติดตั้งประจำโต๊ะทำงาน

๔. "ผู้บังคับบัญชา" หมายความว่า ผู้ที่มีอำนาจและหน้าที่ในการปกครองบังคับบัญชาหน่วย

๕. "ผู้ใช้งาน" หมายความว่า ข้าราชการ พนักงานราชการ และลูกจ้างของกองบัญชาการกองทัพไทย รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองบัญชาการกองทัพไทย ที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศ

๖. "ผู้ดูแลระบบ" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลระบบงานสารสนเทศของหน่วยนั้นๆ

๗. "ผู้ดูแลเครือข่าย" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบให้เป็นผู้ดูแลเครือข่ายสารสนเทศของหน่วยนั้นๆ

/๘. "ผู้ดูแล...

๘. "ผู้ดูแลฐานข้อมูล"หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบให้เป็นผู้ดูแลฐานข้อมูล

๙. "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ หรือเพื่อการเข้าถึงเข้าใช้สารสนเทศและสินทรัพย์สารสนเทศ

๑๐. "สินทรัพย์"หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้แก่เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ และหมายรวมถึงสิ่งใดก็ตามที่มีคุณค่าในระบบสารสนเทศ เป็นต้น

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

๑๒. "การควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับ การเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๑๓. "จดหมายอิเล็กทรอนิกส์" หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพกราฟิก ภาพเคลื่อนไหว และเสียงที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้

๑๔. "บัญชีผู้ใช้บริการ"หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์หรือใช้บริการในระบบเครือข่ายของหน่วย

๑๕. "รหัสผ่าน" หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๖. "การพิสูจน์ยืนยันตัวตน" หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานทั่วไปแล้ว จะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๑๗. "โปรแกรมประสงค์ร้าย" หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่ง และหรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์ หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

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

๑๙. "ไฟร์วอลล์" หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๒๐. "ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การรักษาไว้ซึ่งความปลอดภัยด้านการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความพร้อมใช้งานของข้อมูล (availability)

/สำหรับระบบ...

สำหรับระบบสารสนเทศใน กองบัญชาการกองทัพไทย รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๒๑. "เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า เหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศของหน่วยหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน ซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ โดยผลที่เกิดขึ้นอาจทำให้เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญการละเมิดต่อกฎหมาย ระเบียบข้อบังคับหรือข้อกำหนดต่าง ๆ การทำให้ภาพลักษณ์และชื่อเสียงเสื่อมเสียซึ่งตัวอย่างเหตุการณ์ด้านความมั่นคงปลอดภัย เช่น โปรแกรมประสงค์ร้าย การพบจุดอ่อนในซอฟต์แวร์ระบบงานหรือฮาร์ดแวร์ที่ใช้งานการแจ้งเตือนของระบบป้องกันการบุกรุก ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลงหรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต การใช้เครือข่ายของหน่วยเพื่อกระทำการที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ระบบสารสนเทศถูกโจมตีจนไม่สามารถให้บริการได้ การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย ทรัพย์สินในระบบสารสนเทศถูกขโมย หรือการแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของ กองบัญชาการกองทัพไทย

๒๒. "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่าเหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบสารสนเทศสูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่าง ๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูกบุกรุกหรือโจมตีทางช่องโหว่ และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่าง ๆ

ตรวจถูกต้อง

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)
จก.สส.ทหาร

ผนวก ข แนวปฏิบัติในการควบคุมการเข้าถึงและใช้งานสารสนเทศ
ประกอบ ประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

วัตถุประสงค์

๑. เพื่อให้มีแนวปฏิบัติ และมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์ เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้งาน ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของ กองบัญชาการกองทัพไทย

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ กองบัญชาการกองทัพไทย ได้รับรู้เข้าใจและสามารถปฏิบัติ ตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ซึ่งได้กำหนดแนวทางปฏิบัติ ดังนี้

๒.๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๒.๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน ให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ

๒.๑.๒.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

๒.๑.๒.๑(๑) อ่านอย่างเดียว

๒.๑.๒.๑(๒) สร้างข้อมูล

๒.๑.๒.๑(๓) ป้อนข้อมูล

๒.๑.๒.๑(๔) แก้ไข

๒.๑.๒.๑(๕) อนุมัติ

๒.๑.๒.๑(๖) ไม่มีสิทธิ

๒.๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

๒.๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศของ กองบัญชาการกองทัพไทย จะต้องได้รับการพิจารณาอนุญาตจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร หรือผู้ที่ได้รับมอบหมาย

๒.๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

/๒.๑.๓.๑ จัดแบ่ง...

๒.๑.๓.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น ๓ ประเภท คือ

๒.๑.๓.๑(๑) ข้อมูลลับ หรือ ข้อมูลสารสนเทศด้านการบริหาร หมายถึง ข้อมูลซึ่งเปิดเผยให้แก่ผู้ที่ได้รับอนุญาตแล้วเท่านั้น และจะไม่เปิดเผยแก่บุคคลภายนอก หากข้อมูลถูกเปิดเผยทั้งหมดหรือเพียงบางส่วนให้กับผู้ที่ไม่ได้รับอนุญาตอาจก่อให้เกิดความเสียหายแก่ กองบัญชาการกองทัพไทย

๒.๑.๓.๑(๑.๑) นโยบาย

๒.๑.๓.๑(๑.๒) ข้อมูลยุทธศาสตร์

๒.๑.๓.๑(๑.๓) ข้อมูลกำลังพล

๒.๑.๓.๑(๑.๔) ข้อมูลงบประมาณ การเงิน และการบัญชี

๒.๑.๓.๑(๒) ข้อมูลใช้ภายใน หรือ ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน หมายถึง ข้อมูลสำหรับใช้ในการดำเนินภารกิจภายในของ กองบัญชาการกองทัพไทย ซึ่งสามารถถูกเปิดเผยแก่บุคคลภายนอกที่ได้รับอนุญาต ทั้งนี้ข้อมูลใช้ภายในจะต้องถูกเปิดเผยเพื่อการดำเนินภารกิจของกองบัญชาการกองทัพไทย เท่านั้น

๒.๑.๓.๑(๒.๑) ข้อมูลการดำเนินงานตามภารกิจของ กองบัญชาการกองทัพไทย

๒.๑.๓.๑(๒.๒) ข้อมูลกฎ ระเบียบ กฎหมาย

๒.๑.๓.๑(๒.๓) ข้อมูลการติดต่อสื่อสารภายใน กองบัญชาการกองทัพไทย

๒.๑.๓.๑(๒.๔) ข้อมูลติดตามการดำเนินงานตามภารกิจของกองบัญชาการกองทัพไทย

๒.๑.๓.๑(๒.๕) ข้อมูลติดตามการใช้จ่ายงบประมาณ

๒.๑.๓.๑(๒.๖) ข้อมูลรายงานผลการปฏิบัติงาน

๒.๑.๓.๑(๓) ข้อมูลเปิดเผยได้ หรือ ข้อมูลสารสนเทศด้านการให้บริการ หมายถึง ข้อมูลที่สามารถเปิดเผยแก่บุคคลทั่วไปโดยไม่ก่อให้เกิดความเสียหายแก่ กองบัญชาการกองทัพไทย

๒.๑.๓.๒ จัดแบ่งลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ออกเป็น ๔ ระดับ คือ

๒.๑.๓.๒(๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๒.๑.๓.๒(๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๒.๑.๓.๒(๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๒.๑.๓.๒(๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

/๒.๑.๓.๓ จัดแบ่ง...

๒.๑.๓.๓ จัดแบ่งระดับชั้นการเข้าถึง ออกเป็น ๓ ระดับ คือ

๒.๑.๓.๓(๑) ระดับชั้นสำหรับผู้บริหาร หมายถึง การเข้าถึงเฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ์ ข้อมูลที่มีระดับชั้นการเข้าถึงนี้ ได้แก่ ข้อมูลใช้ภายในและข้อมูลลับ ที่เข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์เท่านั้น

๒.๑.๓.๓(๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป หมายถึง การเข้าถึงได้ทุกกลุ่มผู้ใช้งาน ข้อมูลที่มีระดับชั้นการเข้าถึงนี้ ได้แก่ ข้อมูลเปิดเผยได้

๒.๑.๓.๓(๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย หมายถึง การเข้าถึงได้เฉพาะผู้มีสิทธิ์ในการจัดการระบบสารสนเทศ ข้อมูลที่มีระดับชั้นการเข้าถึงนี้ ได้แก่ ข้อมูลใช้ภายในที่เป็นข้อมูลค่าคอนฟิกกูเรชั่น (Configuration) ของระบบสารสนเทศต่าง ๆ ซึ่งเข้าถึงได้เฉพาะผู้ดูแลระบบสารสนเทศ เท่านั้น

๒.๑.๓.๔ ผู้ดูแลระบบ ต้องติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๒.๑.๓.๕ ผู้ดูแลระบบ ต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ และการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๒.๑.๓.๖ ผู้ดูแลระบบ ต้องบันทึกการผ่านเข้า – ออกสถานที่ตั้งของระบบสารสนเทศ เพื่อเป็นหลักฐานในการตรวจสอบ

๒.๑.๓.๗ การกำหนดเวลาที่ได้เข้าถึงระบบสารสนเทศ ออกเป็น ๒ ระบบ คือ

๒.๑.๓.๗(๑) ระบบงานบริการ E - Service (Front Office) สำหรับผู้ใช้งานภายนอก สามารถเข้าถึงได้ตลอดเวลา

๒.๑.๓.๗(๒) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายใน สามารถเข้าถึงได้ ตามที่หน่วยงานกำหนดให้

๒.๑.๓.๘ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๒.๑.๓.๘(๑) ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

๒.๑.๓.๘(๒) โทรศัพท์ หรือ โทรสาร (เข้าถึงได้ในเวลาราชการ)

๒.๑.๓.๘(๓) หนังสือ หรือ บันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)

๒.๑.๓.๘(๔) ระบบอินทราเน็ต (เข้าถึงได้ทุกช่วงเวลา)

๒.๑.๓.๘(๕) ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

๒.๑.๓.๘(๖) ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

๒.๑.๓.๘(๗) เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา)

๒.๑.๓.๘(๘) การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และ ในช่วงเวลาพิเศษเป็นรายครั้ง)

๒.๑.๔ การบริหารสิทธิ์ของผู้ใช้งานในการใช้งานระบบ โดยมีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Mission Requirements for Access Control) ดังนี้

/๒.๑.๔.๑ ผู้ดูแล...

๒.๑.๔.๑ ผู้ดูแลระบบสารสนเทศอนุญาตให้ผู้ใช้งานมีสิทธิ์การใช้งานระบบสารสนเทศ ดังนี้

๒.๑.๔.๑(๑) กลุ่มข้าราชการ พนักงานราชการและลูกจ้าง ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ ระบบการจัดการสารสนเทศ (MIS : Management Information System) ระบบเครือข่ายไร้สาย ระบบอินทราเน็ต ระบบอินเทอร์เน็ต ระบบจดหมายอิเล็กทรอนิกส์ เป็นต้น

๒.๑.๔.๑(๒) กลุ่มบุคคลพลเรือน ได้แก่ www.rtarf.mi.th

๒.๑.๔.๒ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งาน ใช้งานระบบสารสนเทศได้แต่เพียงที่ได้รับอนุญาตเท่านั้น

๒.๑.๔.๓ ผู้ดูแลระบบสารสนเทศต้องให้สิทธิเฉพาะสำหรับการปฏิบัติงานในหน้าที่เฉพาะของผู้ใช้งาน และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร

๒.๑.๔.๔ ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน เพื่อให้มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากผู้ใช้งานตามปกติ

๒.๑.๔.๕ ผู้ดูแลระบบสารสนเทศกำหนดบัญชีชื่อผู้ใช้แยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน และถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของผู้ใช้งานต่อไป

๒.๑.๔.๖ ผู้ดูแลระบบสารสนเทศจำกัดการใช้งานบัญชีชื่อผู้ใช้งานแบบกลุ่มซึ่งมีการใช้งานร่วมกัน กล่าวคือ อนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้นและผู้ใช้งานบัญชีแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน

๒.๑.๔.๗ ผู้ดูแลระบบสารสนเทศต้องไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

๒.๑.๔.๘ ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๒.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายใน โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กองบัญชาการกองทัพไทย โดยกำหนดแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๒.๒.๑ การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

๒.๒.๑.๑ ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

๒.๒.๑.๒ ฝึกอบรมให้ความรู้ ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

/๒.๒.๒ การลง...

๒.๒.๒ การลงทะเบียนผู้ใช้งาน (User Registration) กำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานที่ปฏิบัติงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น ดังนี้

๒.๒.๒.๑ จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๒.๒.๒.๒ ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

๒.๒.๒.๓ จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

๒.๒.๒.๔ ตรวจสอบและมอบหมายสิทธิ ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒.๒.๒.๕ ตรวจสอบบัญชีผู้ใช้งาน โดยไม่ได้ดำเนินการลงทะเบียนผู้ใช้งานมาก่อน

๒.๒.๒.๖ จัดทำและแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๒.๒.๒.๗ ทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๒.๒.๒.๘ การอนุญาตให้เข้าถึงระบบสารสนเทศจะต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เท่านั้น

๒.๒.๒.๙ การยกเลิก เบิกถอน การอนุญาต ให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง

๒.๒.๒.๑๐ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบ ต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๒.๒.๓ ต้องบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๒.๒.๓.๑ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๒.๓.๒ ผู้ดูแลระบบ ต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ ตามหน้าที่รับผิดชอบ และตามความจำเป็นในการใช้งาน

๒.๒.๓.๓ ผู้ดูแลระบบ ต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๒.๒.๓.๔ ผู้ดูแลระบบ ต้องจัดเก็บเอกสารการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๒.๓.๕ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และต้องกำหนดสิทธิพิเศษที่ได้รับ ว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๒.๒.๔.๑ มีการเปลี่ยนรหัสผ่านให้มีความมั่นคงปลอดภัย

/๒.๒.๔.๒ การใช้...

๒.๒.๔.๒ การใช้งานบัญชีผู้ใช้งานและรหัสผ่านต้องแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๒.๒.๔.๓ การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกันและอนุญาตให้ ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่

๒.๒.๔.๔ ต้องส่งมอบบัญชีผู้ใช้งาน รหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่น ถ้าใช้พลนำสารส่งต้องใส่ซองปิดผนึกให้เรียบร้อย หรือส่งจดหมายอิเล็กทรอนิกส์ในการจัดส่งรหัสผ่านให้กับผู้ใช้งานโดยตรง และผู้ใช้งานต้องทำการลงชื่อเข้าใช้งานระบบงานครั้งแรกและทำการเปลี่ยนรหัสผ่านทันที หลังจากได้รับรหัสผ่านชั่วคราว

๒.๒.๔.๕ ต้องทำการลงนามยืนยันการได้รับรหัสผ่าน เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนจากผู้อื่น

๒.๒.๔.๖ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๒.๒.๔.๗ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้น จะต้องได้รับความเห็นชอบ และอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับว่าเข้าได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔.๘ ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน ให้แสดงเป็นเครื่องหมายดอกจัน (*) บนหน้าจอ

๒.๒.๔.๙ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง

๒.๒.๕ การทบทวนสิทธิการเข้าถึงผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิ การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน ปีละ ๑ ครั้ง หรือเมื่อเปลี่ยนแปลงโดยลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง ดังนี้

๒.๒.๕.๑ ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ๑ ครั้ง/ปี เป็นอย่างน้อย

๒.๒.๕.๒ ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง โดยสิทธิในระดับผู้ดูแลระบบต้องทบทวนด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๒.๒.๕.๓ ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อต้องเปลี่ยนแปลงจากการเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๒.๒.๕.๔ ผู้ดูแลระบบต้องกำหนดให้ทำการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

๒.๒.๖ การเพิกถอนสิทธิการเข้าถึงของผู้ใช้งาน

๒.๒.๖.๑ ผู้ดูแลระบบดำเนินการเพิกถอนสิทธิผู้ใช้งานที่พ้นสภาพการเป็นนักศึกษาและบุคลากรของ กองบัญชาการกองทัพไทย ยกเว้นกรณีเกษียณอายุราชการ

๒.๒.๖.๒ ผู้ดูแลระบบต้องกำหนดให้ถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

/๒.๓ การกำหนด...

๒.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กองบัญชาการกองทัพไทย เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต มีข้อปฏิบัติ ดังนี้

๒.๓.๑ วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่านการใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

๒.๓.๑.๑ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

๒.๓.๑.๒ ผู้ใช้งาน ต้องตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๒.๓.๑.๓ ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๒.๓.๑.๔ ผู้ใช้งาน ต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม

๒.๓.๑.๕ ผู้ใช้งาน ต้องหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วย

๒.๓.๑.๕(๑) กลุ่มอักขระที่เรียงกัน ตัวอย่าง ๑๒๓, abcd

๒.๓.๑.๕(๒) กลุ่มของตัวอักขระที่เหมือนกัน ตัวอย่าง ๑๑๑, aaa

๒.๓.๑.๖ ผู้ใช้งาน ต้องไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๒.๓.๑.๗ ผู้ใช้งาน ต้องเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๒.๓.๑.๘ ผู้ใช้งาน ต้องไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

๒.๓.๑.๙ ผู้ใช้งาน ต้องไม่กำหนดให้ทำการบันทึก หรือช่วยจำรหัสผ่านส่วนบุคคล

๒.๓.๑.๑๐ ผู้ใช้งาน ต้องไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

๒.๓.๑.๑๑ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผย หรือมีผู้อื่นล่วงรู้

๒.๓.๑.๑๒ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๒.๓.๑.๑๓ ผู้ใช้งาน ต้องตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำที่กำหนดไว้

๒.๓.๑.๑๔ ผู้ใช้งาน ต้องตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๒.๓.๑.๑๕ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๒.๓.๑.๑๖ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว และต้องทำทุก ๆ ๖ เดือน

๒.๓.๑.๑๗ ผู้ดูแลระบบ ต้องเปลี่ยนรหัสผ่านด้วยความถี่มากกว่าผู้ใช้งานทั่วไป และต้องทำทุก ๆ ๓ เดือน

/๒.๓.๒ การป้องกัน...

๒.๓.๒ การป้องกันอุปกรณ์ ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของ กองบัญชาการกองทัพไทย ในขณะที่ไม่มีผู้ดูแล ดังนี้

๒.๓.๒.๑ ต้องสร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

๒.๓.๒.๒ ต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศในส่วนที่เป็นระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์แบบพกพาโดยทันที เมื่อเสร็จสิ้นงาน

๒.๓.๒.๓ ผู้ใช้งาน ต้องล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน

๒.๓.๒.๔ ผู้ใช้งาน ป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๒.๓.๒.๕ กำหนดให้ตั้งล็อกหน้าจอเครื่องคอมพิวเตอร์ หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๒.๓.๓ การปฏิบัติตามนโยบายควบคุม การไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศประเภท เอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๒.๓.๓.๑ การกำหนดมาตรการป้องกันสินทรัพย์ของ กองบัญชาการกองทัพไทย และควบคุมไม่ให้ทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานการณ์ที่ไม่ปลอดภัย ครอบคลุม ดังนี้

๒.๓.๓.๑(๑) การจัดการบริเวณล้อมรอบ

๒.๓.๓.๑(๒) การควบคุมการเข้า – ออก

๒.๓.๓.๑(๓) การจัดบริการการเข้าถึงการส่งผลิตภัณฑ์โดยบุคคลภายนอก

๒.๓.๓.๑(๔) การวางอุปกรณ์

๒.๓.๓.๑(๕) ระบบและอุปกรณ์สนับสนุนการทำงาน

๒.๓.๓.๒ การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

๒.๓.๓.๒(๑) แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ

๒.๓.๓.๒(๒) กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ

๒.๓.๓.๒(๓) วัฒนธรรมองค์กร

๒.๓.๓.๓ กำหนดขอบเขตของการป้องกัน ดังนี้

๒.๓.๓.๓(๑) ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันสินทรัพย์ของกองบัญชาการกองทัพไทย

๒.๓.๓.๓(๒) ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๒.๓.๓.๓(๓) จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

๒.๓.๓.๓(๔) ล็อกเครื่องคอมพิวเตอร์ เมื่อไม่ใช้งาน

๒.๓.๓.๓(๕) ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน

/๒.๓.๓.๓(๖) ป้องกัน...

๒.๓.๓.๓(๖) ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

๒.๓.๓.๓(๗) ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต

๒.๓.๓.๓(๘) ต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒.๓.๓.๔ การทำลายสื่อบันทึกข้อมูลและอิเล็กทรอนิกส์

๒.๓.๓.๔(๑) ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์เป็นผู้ทำลายข้อมูล

๒.๓.๓.๔(๒) กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้

รูปแบบการทำลายสื่อบันทึกข้อมูล		ประเภทสื่อบันทึกข้อมูล			
		CD/DVD	Flash Drive	เทปบันทึกข้อมูล	Hard Drive
สามารถนำสื่อบันทึกกลับมาใช้ใหม่ได้	วิธีการทำลาย	-	Format	Format	Format โดยการเขียนทับข้อมูลเป็นจำนวนหลาย ๆรอบ
	ระยะเวลาการทำลาย	ทำลายก่อนนำกลับมาใช้ใหม่	ทำลายก่อนนำกลับมาใช้ใหม่	ทำลายก่อนนำกลับมาใช้ใหม่	ทำลายก่อนนำกลับมาใช้ใหม่
ไม่สามารถนำสื่อบันทึกกลับมาใช้ใหม่ได้	วิธีการทำลาย	ทุบ บดขยี้ให้เสียหาย หรือ เผาทำลาย	ทุบ บดขยี้ให้เสียหาย หรือ เผาทำลาย	ทุบ บดขยี้ให้เสียหาย หรือ เผาทำลาย	ทุบ บดขยี้ให้เสียหาย
	ระยะเวลาการทำลาย	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด

๒.๓.๔ การนำอุปกรณ์การเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

๒.๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

๒.๔.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒.๔.๑.๑ ต้องกำหนดระบบสารสนเทศที่ต้องทำการควบคุมการเข้าถึงโดยระบุเครือข่ายหรือบริการที่อนุญาตให้ทำการใช้งานได้

๒.๔.๑.๒ ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

/๒.๔.๑.๓ ผู้ดูแล...

๒.๔.๑.๓ ผู้ดูแลระบบเครือข่ายต้องกำหนดการใช้งานระบบสารสนเทศที่สำคัญ โดยมีระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ ๑ ครั้ง

๒.๔.๑.๔ ผู้ดูแลเครือข่ายต้องจัดให้มีการบันทึกการใช้งานของผู้ใช้งานตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัยและสิทธิการใช้งานของผู้ใช้งานอื่น ๆ

๒.๔.๑.๕ การใช้งานอินเทอร์เน็ตจะต้องถูกบันทึกการใช้งานไว้เป็นเวลา ๙๐ วัน

๒.๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก กองบัญชาการกองทัพไทย (User Authentication for External Connection) ต้องมีข้อปฏิบัติ หรือกระบวนการให้ทำการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก กองบัญชาการกองทัพไทย เข้าใช้งานเครือข่ายและระบบสารสนเทศของกองบัญชาการกองทัพไทย ได้ ดังนี้

๒.๔.๒.๑ ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

๒.๔.๒.๒ ตรวจสอบผู้ใช้งานทุกครั้ง ก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้รหัสผ่าน การใช้สมาร์ทการ์ด หรือการใช้ User Token ที่ใช้เทคโนโลยี PKI

๒.๔.๒.๓ การเข้าสู่ระบบสารสนเทศของ กองบัญชาการกองทัพไทย จากระบบอินเทอร์เน็ต ต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

๒.๔.๒.๔ การเข้าสู่ระบบจากระยะไกลเพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานและต้องมีการใช้งาน โปรโตคอล ที่มีการเข้ารหัสข้อมูล ได้แก่ SSL VPN

๒.๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

๒.๔.๓.๑ วิธีการพิสูจน์ตัวตนทุกครั้งต้องกำหนดหมายเลขเครือข่าย (IP Address) ให้กับอุปกรณ์เครือข่ายใด ๆ ที่เชื่อมต่ออยู่กับระบบเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้องในกรณีที่ไม่สามารถใช้หมายเลขเครือข่ายในการระบุถึงอุปกรณ์เครือข่ายได้ให้ใช้หมายเลขอุปกรณ์ (MAC Address) ในการระบุถึงอุปกรณ์เครือข่ายแทน

๒.๔.๓.๒ ควบคุมการใช้งานอย่างเหมาะสม

๒.๔.๓.๓ จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๒.๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

๒.๔.๔.๑ ป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านทางเครือข่าย

๒.๔.๔.๒ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

/๒.๔.๔.๓ ตรวจสอบ...

๒.๔.๔.๓ ตรวจสอบพอร์ตที่ไม่มีการใช้งานอย่างสม่ำเสมอ

๒.๔.๕ การแบ่งแยกเครือข่าย (Segregation in Network) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ

๒.๔.๕.๑ เครือข่ายสำหรับผู้ใช้งานภายใน

๒.๔.๕.๒ เครือข่ายสำหรับผู้ใช้งานภายนอก

๒.๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่ใช้ร่วมกันหรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๒.๔.๖.๑ ใช้ Monitoring Tools เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย

๒.๔.๖.๒ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๒.๔.๖.๓ ควบคุมไม่ให้ทำการเปิดให้บริการเครือข่าย โดยไม่ได้รับอนุญาต

๒.๔.๗ การควบคุมการจัดเส้นทางเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๒.๔.๗.๑ ควบคุมไม่ให้ทำการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address Plan)

๒.๔.๗.๒ กำหนดให้ทำการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๒.๔.๗.๓ ผู้ดูแลระบบเครือข่ายต้องกำหนดตารางการใช้เส้นทางบนระบบเครือข่าย (Network Routing Table) บนอุปกรณ์จัดเส้นทาง (Router) หรือ อุปกรณ์กระจายสัญญาณข้อมูล (Switch Layer 3) เพื่อบังคับผู้ใช้งานให้สามารถใช้เส้นทางเครือข่ายเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒.๔.๗.๔ ผู้ดูแลระบบเครือข่ายต้องกำหนดให้มีการใช้อุปกรณ์ ไฟร์วอลล์ เพื่อควบคุมเส้นทางบนระบบเครือข่าย

๒.๔.๗.๕ ผู้ดูแลระบบเครือข่ายต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากอุปกรณ์คอมพิวเตอร์ที่ใช้งานไปยังเครื่องแม่ข่ายที่ให้บริการต่าง ๆ โดยการเชื่อมต่อเข้าสู่เครื่องแม่ข่ายที่ให้บริการเพื่อบริหารจัดการระบบให้กำหนดเฉพาะชุดหมายเลขเครือข่ายของผู้ดูแลระบบสารสนเทศเท่านั้นที่สามารถเข้าถึงเครื่องแม่ข่ายให้บริการนั้นได้

๒.๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก ดังนี้

๒.๔.๘.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของ กองบัญชาการกองทัพไทย ต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๒.๔.๘.๒ การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องทำการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานโดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส

๒.๔.๘.๓ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกล ต้องได้รับการอนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ก่อนและทำการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

/๒.๔.๘.๔ ก่อนทำ...

๒.๔.๘.๔ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ กองบัญชาการกองทัพไทย อย่างเพียงพอ และต้องได้รับอนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร อย่างเป็นทางการ

๒.๔.๘.๕ ต้องควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๒.๔.๘.๖ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องไม่เปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อ เมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อทำการร้องขอที่จำเป็นเท่านั้น

๒.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ โดยมีแนวปฏิบัติ ดังนี้

๒.๕.๑ ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของ กองบัญชาการกองทัพไทย และกำหนดชื่อผู้ใช้งานและรหัสผ่าน ให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของ กองบัญชาการกองทัพไทย

๒.๕.๒ กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๒.๕.๒.๑ ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญ หรือความผิดพลาดต่าง ๆ ของระบบก่อนที่จะเข้าสู่ระบบจะเสร็จสมบูรณ์

๒.๕.๒.๒ ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๒.๕.๒.๓ จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๒.๕.๒.๔ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๒.๕.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

๒.๕.๓.๑ ผู้ใช้งาน ต้องมีชื่อผู้ใช้งานและรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของกองบัญชาการกองทัพไทย

๒.๕.๓.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงาน หรือด้านเทคนิค

๒.๕.๓.๓ สามารถใช้อุปกรณ์ควบคุมความปลอดภัย สมาร์ทการ์ด (RFID : Radio Frequency Identification) หรือเครื่องอ่านลายพิมพ์นิ้วมือเพิ่มเติมได้

/๒.๕.๔ การบริหาร...

๒.๕.๔ การบริหารจัดการรหัสผ่าน (Password Management System)

๒.๕.๔.๑ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของหน่วยงาน

๒.๕.๔.๒ การมอบบัญชีผู้ใช้งานให้กับผู้ใช้งานครั้งแรก ให้กำหนดรหัสผ่านชั่วคราวจากการสุ่มให้กับผู้ใช้งาน เมื่อผู้ใช้งานได้รับรหัสผ่านแล้ว ให้เปลี่ยนรหัสผ่านนั้นเป็นรหัสผ่านของตนเองที่เป็นไปตามแนวปฏิบัติการใช้งานรหัสผ่านอย่างปลอดภัย

๒.๕.๔.๓ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยให้ใช้วิธีการใส่ซองปิดผนึกหรือกระดาษคาร์บอน จากนั้นจึงส่งมอบให้ผู้ใช้งานโดยตรง

๒.๕.๔.๔ ผู้ใช้งานต้องตอบยืนยันการได้รับรหัสผ่าน

๒.๕.๔.๕ เมื่อมีผู้ใช้งานระบบสารสนเทศของหน่วยงานลาออก หรือไม่มีหน้าที่การรับผิดชอบในระบบที่ขอสิทธิในการใช้งาน ให้หน่วยงานแจ้งผู้ดูแลระบบสารสนเทศทันที เพื่อเปลี่ยนสิทธิการถอดถอนสิทธิของผู้ที่ลาออก ออกจากระบบทันทีที่ได้รับแจ้ง

๒.๕.๔.๖ ผู้ดูแลระบบสารสนเทศจัดทำระบบที่เอื้อให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านของตนเองได้ โดยกำหนดให้เปลี่ยนรหัสผ่านทุก ๑๘๐ วัน

๒.๕.๔.๗ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง กรณีผู้ใช้งานพิมพ์รหัสผิดเกิน ๓ ครั้ง ระบบต้องระงับการใช้งาน ผู้ใช้ต้องทำเรื่องขอรหัสใหม่จากผู้ดูแลระบบสารสนเทศ

๒.๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้ไม่ปลอดภัยให้ดำเนินการ ดังนี้

๒.๕.๕.๑ จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุม ในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๒.๕.๕.๒ อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๒.๕.๕.๓ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ใช้งานเป็นประจำ

๒.๕.๕.๔ จัดเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๒.๕.๕.๕ ถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๒.๕.๕.๖ ห้ามติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ ต้องใช้โปรแกรมที่ถูกต้องมีลิขสิทธิ์ เท่านั้น

๒.๕.๖ การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out) เมื่อว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time - Out) มีแนวปฏิบัติ ดังนี้

๒.๕.๖.๑ กำหนดหลักเกณฑ์การยุติ การใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

/๒.๕.๖.๒ ถ้าไม่...

๒.๕.๖.๒ ถ้าไม่ทำการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์ และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๒.๕.๖.๓ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูง ต้องกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่ใช้งานเป็นระยะเวลาตามที่กำหนด

๒.๕.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Imitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากขึ้น สำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๒.๕.๗.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอพพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง และต้องกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของ กองบัญชาการกองทัพไทย ตามปกติเท่านั้น

๒.๕.๗.๒ กำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๒.๕.๗.๓ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง และ/หรือ ระบบงานที่ใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อ

๒.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and Information Access control) ต้องควบคุม ดังนี้

๒.๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๒.๖.๑.๑ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานใหม่ปฏิบัติ ดังนี้

๒.๖.๑.๑(๑) การลงทะเบียนผู้ใช้งานใหม่

๒.๖.๑.๑(๒) การบริหารสิทธิของผู้ใช้งานในการใช้งานระบบ

๒.๖.๑.๑(๓) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๖.๑.๑(๔) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๒.๖.๑.๒ การเข้าถึงโปรแกรมประยุกต์ผ่านทางระบบเครือข่ายของ กองบัญชาการกองทัพไทย ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัย โดยใช้ชื่อผู้ใช้ และรหัสผ่าน

๒.๖.๑.๓ การเข้าถึงโปรแกรมประยุกต์ผ่านทางระบบเครือข่ายสาธารณะให้ใช้ช่องทางระบบเครือข่ายส่วนบุคคลเสมือน (VPN) และต้องมีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัยโดยใช้ชื่อผู้ใช้ และรหัสผ่าน

๒.๖.๑.๔ ผู้ดูแลระบบสารสนเทศต้องตัดเวลาการใช้งานเครื่องลูกข่าย เมื่อเครื่องลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลา ๓๐ นาที

๒.๖.๑.๕ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ระบบสารสนเทศจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ ใช้งานได้ ๒ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง ทั้งนี้จะต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้

/๒.๖.๑.๖ ผู้ดูแล...

๒.๖.๑.๖ ผู้ดูแลระบบสารสนเทศต้องบันทึกข้อมูลพฤติกรรมการใช้งานข้อมูลโดยการจัดเก็บ Audit Log เป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้งาน เพื่อตรวจสอบว่า ใครเข้ามาใช้งานระบบ การตรวจสอบการบุกรุก

๒.๖.๑.๗ กรณีในการจ้างพนักงานจากภายนอก (Outsource) เพื่อดำเนินการในเรื่องต่าง ๆ กำหนดมาตรการในการควบคุมการเข้าถึงโปรแกรมประยุกต์ และสารสนเทศ ดังนี้

๒.๖.๑.๗(๑) กำหนดให้มีเจ้าหน้าที่ผู้ควบคุมงานเพื่อคอยกำกับดูแลการดำเนินงานต่าง ๆ ของพนักงานจากภายนอก

๒.๖.๑.๗(๒) แจ้งให้พนักงานจากภายนอกรับทราบ และปฏิบัติตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย

๒.๖.๑.๗(๓) กำหนดให้พนักงานจากภายนอกลงนามในสัญญารักษาความลับ

๒.๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ กองบัญชาการกองทัพไทย ต้องดำเนินการ ดังนี้

๒.๖.๒.๑ จัดทำบัญชีรายชื่อระบบที่ไวต่อการรบกวน ได้แก่ ระบบสารสนเทศเพื่อการจัดการที่ประกอบด้วย ระบบไปรษณีย์อิเล็กทรอนิกส์ทางทหาร (Mil Mail) ระบบงานกำลังพล ระบบงานด้านการข่าว ระบบงานการเงินและหนี้สิน ระบบงานงบประมาณ ระบบงานครุภัณฑ์ และระบบสารบรรณอิเล็กทรอนิกส์ทหาร (Mil Doc)

๒.๖.๒.๒ แยกระบบซึ่งไวต่อการรบกวนออกจากระบบสารสนเทศอื่น ๆ โดยกำหนดให้สามารถใช้งานเฉพาะกลุ่มเท่านั้น และต้องกำหนดช่องทางและวิธีการในการเข้าถึง โดยจัดให้มีเครื่องแม่ข่ายควบคุมแยกต่างหาก การติดต่อกับเครื่องแม่ข่ายต้องผ่านระบบ Firewall การจำกัดการเข้าถึงเฉพาะการใช้เครือข่ายภายในเท่านั้น

๒.๖.๒.๓ จัดทำระบบสำรองของระบบสารสนเทศที่มีความสำคัญสูงต่อ กองบัญชาการกองทัพไทย

๒.๖.๒.๔ ผู้ดูแลระบบสารสนเทศต้องควบคุมอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานที่เกี่ยวข้องกับระบบดังกล่าว จากภายนอก กองบัญชาการกองทัพไทย (Mobile Computing and Teleworking) ให้สามารถเข้าถึงโดยผ่าน “ผ่าน อุปกรณ์สื่อสารเคลื่อนที่” หรือ “ผ่านการปฏิบัติงานจากภายนอก” ได้

๒.๖.๒.๕ ผู้ดูแลระบบสารสนเทศต้องมีเครื่องมือที่ใช้สำหรับตรวจสอบสภาพพร้อมใช้งานของระบบสารสนเทศซึ่งไวต่อการรบกวน

๒.๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต้องปฏิบัติ ดังต่อไปนี้

๒.๖.๓.๑ ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๒.๖.๓.๒ ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้การเผยแพร่เป็นการทั่วไป

๒.๖.๓.๓ เมื่อหมดความจำเป็น ต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้วให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

/๒.๖.๓.๔ เจ้าหน้าที่...

๒.๖.๓.๔ เจ้าหน้าที่ที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่รับคืนด้วย

๒.๖.๓.๕ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๒.๖.๔ การปฏิบัติงานจากภายนอก (Teleworking)

๒.๖.๔.๑ กำหนดการเข้าถึงโปรแกรมประยุกต์และสารสนเทศของ กองบัญชาการกองทัพไทย ได้ ๒ ช่องทาง คือ

๒.๖.๔.๑(๑) การเข้าถึงผ่านโปรแกรมประยุกต์และสารสนเทศที่เปิดให้ใช้งานจากภายนอกได้โดยตรง ได้แก่ จดหมายอิเล็กทรอนิกส์ และระบบเว็บไซต์ของ กองบัญชาการกองทัพไทย

๒.๖.๔.๑(๒) การเข้าถึงผ่านโปรแกรมประยุกต์และสารสนเทศผ่านระบบ VPN

๒.๖.๔.๒ ผู้ใช้งานได้รับสิทธิการเข้าใช้งานระบบสารสนเทศจากภายนอกผ่านช่องทางในข้อ ๒.๖.๔.๑(๑) สามารถเข้าใช้งานได้โดยการใช้ชื่อผู้ใช้และรหัสผ่านของตนเอง

๒.๖.๔.๓ ในกรณีที่ผู้ใช้งานเป็นพนักงานจากภายนอกหรือบุคคลภายนอกต้องได้รับการอนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร หรือผู้ที่ได้รับมอบหมายก่อนเข้าใช้งาน ซึ่งสามารถเข้าใช้งานได้โดยการใช้ชื่อผู้ใช้และรหัสผ่านที่ตนเองได้รับ

๒.๖.๔.๔ ผู้ดูแลระบบสารสนเทศ ต้องกำหนดสิทธิการเข้าถึงโปรแกรมประยุกต์และสารสนเทศให้ผู้ใช้งานเข้าถึงได้เพียงบริการที่ได้รับอนุญาตเท่านั้น

๒.๖.๔.๕ อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อเข้ากับโปรแกรมประยุกต์และระบบสารสนเทศผ่านช่องทางการปฏิบัติงานจากภายนอกองค์กร ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่ได้รับการปรับปรุงอยู่เสมอ

๒.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สายของ กองบัญชาการกองทัพไทย โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย และแนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ดังนี้

๒.๗.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ กองบัญชาการกองทัพไทย จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร หรือผู้ที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษร

๒.๗.๒ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๗.๓ ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๒.๗.๔ ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (AP : Access Point) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

/๒.๗.๕ ผู้ดูแล...

๒.๗.๕ ผู้ดูแลระบบ ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๒.๗.๖ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๒.๗.๗ ผู้ดูแลระบบ ต้องเปลี่ยนค่าชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบ ต้องเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดา หรือเจาะรหัสได้โดยง่าย

๒.๗.๘ ผู้ดูแลระบบ ต้องกำหนดค่าใช้ (WEP : Wired Equipment Privacy) หรือ (WPA : Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

๒.๗.๙ ผู้ดูแลระบบ ต้องเลือกใช้วิธีการควบคุมหมายเลขอุปกรณ์ และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มีหมายเลขอุปกรณ์และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๒.๗.๑๐ ผู้ดูแลระบบ ต้องติดตั้งไฟร์วอลล์ (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน กองบัญชาการกองทัพไทย

๒.๗.๑๑ ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ (VPN : Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๒.๗.๑๒ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์ หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ทราบโดยทันที

๒.๘ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) ดังนี้

๒.๘.๑ การกำหนดบริเวณที่ต้องทำการรักษาความมั่นคงปลอดภัย

๒.๘.๑.๑ ให้ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยภายในกองบัญชาการกองทัพไทย ต้องจำแนกและกำหนดพื้นที่ของเครื่องแม่ข่าย อุปกรณ์เครื่องแม่ข่าย ระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม และให้กำหนดพื้นที่รักษาความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย กองบัญชาการกองทัพไทย มีจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้น โดยการกำหนดพื้นที่ดังกล่าว อาจแบ่งออกได้เป็น

๒.๘.๑.๑(๑) พื้นที่ทำงาน

๒.๘.๑.๑(๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย

๒.๘.๑.๑(๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย

/๒.๘.๑.๒ ให้ ศูนย์...

๒.๘.๑.๒ ให้ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

๒.๘.๑.๒(๑) จัดทำ "ทะเบียนผู้มีสิทธิเข้า - ออกพื้นที่" เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๒.๘.๑.๒(๒) กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า - ออกพื้นที่ โดยจัดทำเป็นเอกสาร "บันทึกการเข้า - ออกพื้นที่"

๒.๘.๑.๒(๓) จัดให้มีเจ้าหน้าที่ เพื่อทำหน้าที่ตรวจสอบประวัติการเข้า - ออกพื้นที่เป็นประจำทุกวัน และต้องปรับปรุงรายการผู้มีสิทธิเข้า - ออกพื้นที่ ปีละ ๑ ครั้งเป็นอย่างน้อย

๒.๘.๑.๒(๔) บุคคลภายนอกเข้ามาติดต่อต้องลงชื่อขออนุญาตการเข้า - ออกในแบบฟอร์มการเข้า - ออก ให้ถูกต้องและจะต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๘.๑.๒(๕)บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

๒.๘.๑.๒(๖) ประกาศห้ามผู้ไม่มีส่วนเกี่ยวข้องเข้าพื้นที่ เว้นแต่ได้รับอนุญาตให้รับทราบทั่วกัน

๒.๘.๑.๒(๗) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายใน กองบัญชาการกองทัพไทย จะต้องได้รับอนุญาตจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

๒.๘.๑.๒(๘) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของ กองบัญชาการกองทัพไทย ที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดับเพลิง ระบบปรับอากาศ และควบคุมความชื้น และต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ ให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๒.๘.๑.๒(๙) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๒.๘.๒ การเดินสายไฟสายสื่อสาร และสายเคเบิลอื่น ๆ ต้องดำเนินการ ดังนี้

๒.๘.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของ กองบัญชาการกองทัพไทย ในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒.๘.๒.๒ ป้องกันสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๒.๘.๒.๓ เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๒.๘.๒.๔ จัดทำป้ายชื่อสำหรับสายสัญญาณ และบนอุปกรณ์ เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๒.๘.๒.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

/๒.๘.๒.๖ ห้องที่...

๒.๘.๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงบุคคลภายนอก

๒.๘.๒.๗ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๒.๘.๓ การบำรุงรักษาอุปกรณ์ ต้องดำเนินการ ดังนี้

๒.๘.๓.๑ กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒.๘.๓.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๒.๘.๓.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบ หรือประเมินในภายหลัง

๒.๘.๓.๔ จัดเก็บบันทึกปัญหา และข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๒.๘.๓.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอก ที่มาทำการบำรุงรักษาอุปกรณ์ภายใน กองบัญชาการกองทัพไทย

๒.๘.๓.๖ จัดให้ทำการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๘.๔ การนำสินทรัพย์ของ กองบัญชาการกองทัพไทย ออกนอก กองบัญชาการกองทัพไทย ต้องดำเนินการ ดังนี้

๒.๘.๔.๑ ขออนุญาตก่อนนำอุปกรณ์ หรือสินทรัพย์นั้นออกไปใช้งานนอก กองบัญชาการ-กองทัพไทย

๒.๘.๔.๒ กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอก กองบัญชาการ-กองทัพไทย

๒.๘.๔.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอก กองบัญชาการกองทัพไทย

๒.๘.๔.๔ เมื่อนำอุปกรณ์ส่งคืน ต้องตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๒.๘.๔.๕ บันทึกข้อมูลการนำอุปกรณ์ของ กองบัญชาการกองทัพไทย ออกไปใช้งานนอก กองบัญชาการกองทัพไทย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๒.๘.๕ การจัดการอุปกรณ์ที่ใช้งานอยู่นอก กองบัญชาการกองทัพไทย ดังนี้

๒.๘.๕.๑ กำหนดมาตรการความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือสินทรัพย์ของ กองบัญชาการกองทัพไทย ออกไปใช้งาน

๒.๘.๕.๒ ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของ กองบัญชาการกองทัพไทย ไว้โดยลำพังในที่สาธารณะ

๒.๘.๕.๓ เจ้าหน้าที่มีความรับผิดชอบอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

๒.๘.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง ดังนี้

๒.๘.๖.๑ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

/๒.๘.๖.๒ มีมาตรการ...

๒.๘.๖.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้นได้

๒.๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ ดังนี้

๒.๘.๗.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๒.๘.๗.๒ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ โดยผู้เป็นเจ้าของระบบนั้น

๒.๘.๗.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ และระบบอินเทอร์เน็ต เพื่อป้องกันการเข้าถึง หรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๒.๙ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย ดำเนินการ ดังนี้

๒.๙.๑ การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๒.๙.๑.๑ ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของ กองบัญชาการกองทัพไทย เพื่อป้องกันความเสียหาย หรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

๒.๙.๑.๒ ให้ ผู้ดูแลระบบ ที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของ กองบัญชาการกองทัพไทย

๒.๙.๑.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ ต้องขออนุมัติให้ติดตั้งก่อนการดำเนินงาน

๒.๙.๑.๔ ไม่ติดตั้งรหัสต้นฉบับ (Source Code) ของระบบสารสนเทศ ในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

๒.๙.๑.๕ จัดเก็บรหัสต้นฉบับและคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๒.๙.๑.๖ ให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้อง ต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ทั้งซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ

๒.๙.๑.๗ ให้ผู้ที่เกี่ยวข้อง ต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๒.๙.๑.๘ จัดเก็บซอฟต์แวร์รุ่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม และขั้นตอนปฏิบัติ ที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้รุ่นเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

๒.๙.๑.๙ ระบุความต้องการทางสารสนเทศ สำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๒.๙.๒ การทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๒.๙.๒.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ ได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๒.๙.๒.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่ กองบัญชาการกองทัพไทย ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

/๒.๙.๓ การพัฒนา...

๒.๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๒.๙.๓.๑ ควบคุมการพัฒนาซอฟต์แวร์ที่จัดจ้างจากบุคคล หรือหน่วยงานภายนอก

๒.๙.๓.๒ ระบุว่าใครจะเป็นผู้มีสิทธิในสินทรัพย์ทางปัญญาสำหรับรหัสต้นฉบับ ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๒.๙.๓.๓ กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ ที่พัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๒.๙.๓.๔ ตรวจสอบโปรแกรมไม่ประสงค์ดี (Malware) ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๒.๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

๒.๙.๔.๑ การจัดทำบัญชีของระบบสารสนเทศ เพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ต้องดำเนินการบันทึก ดังต่อไปนี้

๒.๙.๔.๑(๑) ชื่อซอฟต์แวร์และรุ่นที่ใช้งาน

๒.๙.๔.๑(๒) สถานที่ติดตั้ง

๒.๙.๔.๑(๓) เครื่องที่ติดตั้ง

๒.๙.๔.๑(๔) ผู้ผลิตซอฟต์แวร์

๒.๙.๔.๑(๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๒.๙.๔.๒ จัดการช่องโหว่ที่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๒.๙.๔.๓ กระบวนการบริหารจัดการช่องโหว่ ของระบบสารสนเทศให้ ผู้ดูแลระบบดำเนินการ ดังนี้

๒.๙.๔.๓(๑) เฝ้าระวังติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ ตามความเหมาะสม

๒.๙.๔.๓(๒) กำหนดตำแหน่งข้อมูลข่าวสาร เพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของ กองบัญชาการกองทัพไทย

๒.๙.๔.๓(๓) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยง เมื่อได้รับการแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๒.๙.๔.๓(๔) ปิดการใช้งาน หรือควบคุมการเข้าพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๒.๙.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) ต้องบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

๒.๙.๕.๑ ข้อมูลบัญชีผู้ใช้งาน

๒.๙.๕.๒ ข้อมูลวันเวลาที่เข้าถึงระบบ

/๒.๙.๕.๓ ข้อมูล...

๒.๙.๕.๓ ข้อมูลวันเวลาที่ออกจากระบบ

๒.๙.๕.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๒.๙.๕.๕ ข้อมูลการบันทึกเข้าใช้งาน (Login) ทั้งที่สำเร็จและไม่สำเร็จ

๒.๙.๕.๖ ข้อมูลความพยายามในการเข้าถึงทรัพยากร ทั้งที่สำเร็จและไม่สำเร็จ

๒.๙.๕.๗ ข้อมูลการเปลี่ยนการทำงานพื้นฐาน (Configuration) ของระบบ

๒.๙.๕.๘ ข้อมูลแสดงการใช้งานแอพพลิเคชั่นโปรแกรมประยุกต์ (Application)

๒.๙.๕.๙ ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำการเปิด ปิด เขียน หรืออ่านกับไฟล์

๒.๙.๕.๑๐ ข้อมูลเลขที่อยู่ไอพีที่เข้าถึง IP (Internet Protocol)

๒.๙.๕.๑๑ ข้อมูลโพรโทคอลเครือข่ายที่ใช้ (Protocol)

๒.๙.๕.๑๒ ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

๒.๙.๕.๑๓ ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๒.๑๐ การควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่าย (Network System Control Room) เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูล และระบบข้อมูลของ กองบัญชาการกองทัพไทย โดยต้องกำหนดกระบวนการควบคุมการเข้า - ออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่าย ดังนี้

๒.๑๐.๑ ผู้ที่เกี่ยวข้อง บทบาท และหน้าที่รับผิดชอบ

๒.๑๐.๑.๑ หัวหน้างานระบบเครือข่ายและบริการระบบอินเทอร์เน็ต

๒.๑๐.๑.๑(๑) อนุมัติสิทธิการเข้า - ออก พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๑๐.๑.๑(๒) อนุมัติกระบวนการควบคุมการเข้า - ออก ห้องควบคุมระบบเครือข่าย

๒.๑๐.๑.๒ ผู้ดูแลห้องควบคุมระบบเครือข่าย

ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายใน ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร การปฏิบัติให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

๒.๑๐.๒ กระบวนการควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่ายผู้ดูแลห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่ มีแนวทางปฏิบัติ ดังนี้

๒.๑๐.๒.๑ ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้า - ออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคลากรภายใน เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูและระบบ (System Administrator) ที่ปฏิบัติหน้าที่ที่เกี่ยวข้องและต้องทำการบันทึก “ทะเบียนผู้มีสิทธิเข้า - ออกพื้นที่”

๒.๑๐.๒.๒ สิทธิในการเข้า – ออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร หรือผู้ที่

/ได้รับมอบ...

ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

๒.๑๐.๒.๓ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้า - ออกห้องควบคุมระบบเครือข่ายก็ต้องควบคุมอย่างรัดกุม

๒.๑๐.๒.๔ การเข้าถึงห้องควบคุมระบบเครือข่ายต้องลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า - ออกพื้นที่”

๒.๑๐.๓ แนวปฏิบัติการจัดทำเอกสารระบุสิทธิในการเข้าถึงพื้นที่การจัดทำเอกสารระบุสิทธิของผู้ใช้และ “หน่วยงานภายนอก” ในการเข้าถึงพื้นที่ มีดังนี้

๒.๑๐.๓.๑ กำหนดสิทธิผู้ใช้ ที่มีสิทธิผ่านเข้าออกและช่วงเวลาที่มีสิทธิในการผ่านเข้า - ออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๒.๑๐.๓.๒ การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องแลกบัตรบัตรประชาชน หรือใบอนุญาตขับขี่ หรือบัตรใด ๆ ที่ใช้ระบุตัวตนของบุคคลนั้น ๆ ที่ออกโดยหน่วยงานราชการ แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้า - ออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๒.๑๐.๓.๓ บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน กองบัญชาการกองทัพไทย

๒.๑๐.๓.๔ เจ้าหน้าที่ ที่บุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้า - ออก ในแบบฟอร์มการเข้า - ออกให้ถูกต้อง และต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๑๐.๓.๕ บุคคลภายนอก หรือผู้ติดต่อ ต้องคืนแบบฟอร์มการเข้า - ออก และบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่อพร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

๒.๑๐.๓.๖ ผู้ใช้จะได้รับสิทธิ ให้เข้า - ออกพื้นที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๒.๑๐.๓.๗ หากมีบุคคลอื่นที่ไม่ใช่ผู้ใช้ ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้ เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผล และความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่หน่วยงานราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ ต้องจดบันทึกบุคคลและการเข้า - ออก ไว้เป็นหลักฐานทั้งในกรณีที่อนุญาต และไม่อนุญาตให้เข้าพื้นที่

๒.๑๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๒.๑๑.๑ การใช้งานทั่วไป

๒.๑๑.๑.๑ ผู้ใช้งานต้องยอมรับทราบ กฎ ระเบียบ หรือนโยบายต่าง ๆ ที่กำหนดขึ้นโดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

๒.๑๑.๑.๒ เครื่องคอมพิวเตอร์ และเครือข่ายของ กองบัญชาการกองทัพไทย เป็นสมบัติของทางราชการ ผู้ใช้งานต้องใช้เพื่อประโยชน์ทางราชการเท่านั้น

/๒.๑๑.๑.๓ โปรแกรม...

๒.๑๑.๑.๓ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ กองบัญชาการกองทัพไทย ต้องเป็นโปรแกรมที่ กองบัญชาการกองทัพไทย ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่าได้ติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรม หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

๒.๑๑.๑.๔ การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร หรือผู้รับจ้าง ในการบำรุงรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ที่ได้ทำสัญญากับ กองบัญชาการกองทัพไทย เท่านั้น

๒.๑๑.๑.๕ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๒.๑๑.๑.๖ ไม่วางสื่อแม่เหล็ก ไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ และ/หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

๒.๑๑.๑.๗ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน กรณีการตกจากโต๊ะทำงานหรือหลุดมือ

๒.๑๑.๑.๘ การใช้เครื่องคอมพิวเตอร์แบบพกพา เป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒.๑๑.๑.๙ ไม่วางสิ่งของทับบนหน้าจอและแป้นพิมพ์

๒.๑๑.๑.๑๐ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๒.๑๑.๑.๑๑ ต้องไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลวความชื้น จากอาหาร น้ำ กาแฟ และเครื่องดื่มต่างๆ

๒.๑๑.๑.๑๒ ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๒.๑๑.๑.๑๓ ห้ามมิให้ผู้ใช้งาน ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๒.๑๑.๑.๑๔ ผู้ใช้งาน ต้องให้ความร่วมมือและอำนวยความสะดวกแก่ ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ และเครือข่ายรวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

๒.๑๑.๑.๑๕ ผู้ใช้งาน จะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตน โดยไม่ได้รับอนุญาต โดยการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ ข้อความใด ๆ ที่ก่อให้เกิดความเสียหาย เสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพ หรือการเขียนข้อความ ที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ ของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว

/๒.๑๑.๑.๑๖ ผู้ใช้...

๒.๑๑.๑.๑๖ ผู้ใช้งานสัญญาว่า จะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คำแนะนำที่กองบัญชาการกองทัพไทย กำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม

๒.๑๑.๑.๑๗ หากผู้ใช้งานกระทำการล่วงละเมิด หรือ พยามยามจะล่วงละเมิด ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ในฐานะผู้ดูแลระบบคอมพิวเตอร์ และเครือข่ายของกองบัญชาการกองทัพไทย ขอสงวนสิทธิที่จะยกเลิกการใช้งาน หรือระงับการเชื่อมต่อ และ/หรือ การใช้งานใด ๆ ตามความเหมาะสม

๒.๑๑.๑.๑๘ ผู้ใช้งาน ต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒.๑๑.๑.๑๙ ผู้ใช้งาน ต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อกหน้าจอภาพ เมื่อไม่ใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๑๑.๑.๒๐ ในการเข้าใช้ระบบปฏิบัติการต้องใส่ชื่อผู้ใช้ (User) และ รหัสผ่าน (Password) ทุกครั้ง

๒.๑๑.๑.๒๑ ผู้ใช้งาน ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนในการเข้าใช้งาน เครื่องคอมพิวเตอร์ร่วมกัน

๒.๑๑.๑.๒๒ ผู้ใช้งาน ต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒.๑๑.๑.๒๓ ห้ามเปิด หรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

๒.๑๑.๑.๒๔ ห้ามผู้ใช้งาน ทำการติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๒.๑๑.๑.๒๕ ห้ามผู้ใช้งาน ทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟต์แวร์ที่ กองบัญชาการกองทัพไทย จัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น

๒.๑๑.๑.๒๖ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของ กองบัญชาการกองทัพไทย เพื่อประโยชน์ทางการค้า

๒.๑๑.๑.๒๗ ห้ามผู้ใช้งาน นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๒.๑๑.๑.๒๘ ห้ามผู้ใช้งาน ใช้ระบบสารสนเทศของ กองบัญชาการกองทัพไทย เพื่อควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒.๑๑.๒ การสำรองข้อมูลและการกู้คืน

๒.๑๑.๒.๑ ผู้ใช้งาน ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ (CD, DVD และ External Hard Disk)

๒.๑๑.๒.๒ ผู้ใช้งาน มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

/๒.๑๑.๒.๓ ผู้ใช้งาน...

๒.๑๑.๒.๓ ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Hard Disk ต้องไม่เป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

๒.๑๒ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๒.๑๒.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีการปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๒.๑๒.๒ เจ้าของข้อมูล ต้องทบทวนความเหมาะสมของสิทธิ ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ ปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๒.๑๒.๓ วิธีปฏิบัติ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๒.๑๒.๔ การรับส่งข้อมูล ข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล ดังนี้ SSL (Secure Socket Layer), VPN (Virtual Private Network) หรือ XML (Extensible Markup Language) encryption

๒.๑๒.๕ ให้นำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๒.๑๓ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail) กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ กองบัญชาการกองทัพไทย ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์ บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ไม่ละเมิดสิทธิ หรือกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่ เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำ ของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ ซึ่งมีแนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์ ดังนี้

๒.๑๓.๑ ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกองบัญชาการกองทัพไทย ให้เหมาะสมกับการเข้าใช้บริการ ของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งต้องทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ ในกรณีลาออก

๒.๑๓.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของ กองบัญชาการกองทัพไทย

๒.๑๓.๓ รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏ หรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์ (*) ในการพิมพ์แต่ละตัวอักษร แทนตัวอักษรนั้น

๒.๑๓.๔ ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๕ ครั้ง

๒.๑๓.๕ ผู้ดูแลระบบ ต้องกำหนดให้ ระบบจดหมายอิเล็กทรอนิกส์ ต้องบันทึกออกจากหน้าจอตัดการใช้งานผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้อย่างน้อย ๑๐ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้ และรหัสผ่านอีกครั้ง

/๒.๑๓.๖ ผู้ใช้งาน...

๒.๑๓.๖ผู้ใช้งาน ต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๑๓.๗ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุก ๓ - ๖ เดือน

๒.๑๓.๘ผู้ใช้งาน ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อกองบัญชาการกองทัพไทย หรือละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมายละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ กองบัญชาการกองทัพไทย

๒.๑๓.๙ข้อห้ามผู้ใช้ ต้องไม่ใช้ที่อยู่ จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน รับ - ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๒.๑๓.๑๐ ผู้ใช้งาน ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ กองบัญชาการกองทัพไทย เพื่อการทำงานของ กองบัญชาการกองทัพไทย เท่านั้น

๒.๑๓.๑๑ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการบันทึกออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒.๑๓.๑๒ ผู้ใช้งาน ต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File ที่มีนามสกุล .exe, .com

๒.๑๓.๑๓ ผู้ใช้งาน ต้องไม่เปิด หรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๑๓.๑๔ ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของ กองบัญชาการกองทัพไทย ทำให้เกิดความแตกแยกระหว่าง กองบัญชาการกองทัพไทย ผ่านทางจดหมายอิเล็กทรอนิกส์

๒.๑๓.๑๕ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๓.๑๖ ผู้ใช้งาน ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๑๓.๑๗ ผู้ใช้งาน ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๒.๑๓.๑๘ ผู้ใช้งาน ต้องโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตนเพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นต้องไม่จัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๒.๑๔ การใช้งานระบบอินเทอร์เน็ต (Use of the Internet) เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ โดยส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบ

/คอมพิวเตอร์...

คอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของ กองบัญชาการกองทัพไทย ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต มีดังนี้

๒.๑๔.๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย Proxy, Firewall และ IPS-IDS (Intrusion Prevention System) / (Intrusion Detection System) ที่ กองบัญชาการกองทัพไทย ได้จัดสรรไว้เท่านั้น ยกเว้นมีเหตุผลความจำเป็นและทำการขออนุญาตจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เป็นลายลักษณ์อักษร

๒.๑๔.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราว์เซอร์

๒.๑๔.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางระบบอินเทอร์เน็ต ต้องตรวจสอบไวรัส (Virus Scanning) ป้องกันไวรัสก่อนการรับ – ส่งข้อมูลทุกครั้ง

๒.๑๔.๔ ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ กองบัญชาการกองทัพไทย เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

๒.๑๔.๕ ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ กองบัญชาการกองทัพไทย

๒.๑๔.๖ ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับ กองบัญชาการกองทัพไทย

๒.๑๔.๗ ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ กองบัญชาการกองทัพไทย ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๑๔.๘ ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่ หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบอินเทอร์เน็ต

๒.๑๔.๙ ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัด ต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด อันจะทำให้ผู้อื่นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๑๔.๑๐ ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนระบบอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๒.๑๔.๑๑ ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Files ต่าง ๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดสินทรัพย์ทางปัญญา

๒.๑๔.๑๒ ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ กองบัญชาการกองทัพไทย รวมถึงการทำลายความสัมพันธ์ กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

/๒.๑๔.๑๓ หลังจาก...

๒.๑๔.๑๓ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๒.๑๕ การพัฒนาและการบริหารจัดการเว็บไซต์ (Web Site Develop and Management) เพื่อให้ผู้ดูแลและบริหารจัดการเว็บไซต์ (Web Master) ได้ทราบถึงกฎเกณฑ์ แนวทางปฏิบัติในการพัฒนาและการบริหารจัดการเว็บไซต์อย่างปลอดภัย และเป็นการป้องกันไม่ให้เกิดการละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และการคุกคามจากผู้ไม่ประสงค์ดี รบกวนจนไม่สามารถทำงานตามปกติได้ ผู้ดูแลและบริหารจัดการเว็บไซต์ต้องปฏิบัติตามแนวปฏิบัติ ดังนี้

๒.๑๕.๑ หมั่นตรวจสอบระบบที่ใช้ซอฟต์แวร์สำเร็จรูป (Content Management System) ซึ่งพัฒนาจากผู้พัฒนาภายนอก (Third Party) ได้แก่ Mambo, Joomla, WordPress PhP-nuke หรือ Drupal โดยการตรวจสอบข้อมูลจากเว็บไซต์ (Web Site) ของผู้พัฒนาเสมอว่ามีช่องโหว่ใดเกิดขึ้นกับระบบบ้าง และพิจารณาช่องโหว่ดังกล่าวว่า ดำเนินการใช้งานบนระบบหรือเว็บไซต์ของเราหรือไม่ เพื่อเป็นข้อมูลในการตัดสินใจปรับปรุง (Update) ซอฟต์แวร์แพคเกจนั้น

๒.๑๕.๒ ทำการปรับปรุง หรือ Patch เครื่องมือที่ใช้ในการพัฒนาเว็บไซต์ โดยเฉพาะการใช้ซอฟต์แวร์สำเร็จรูปในการพัฒนา รวมถึงปรับเปลี่ยนการใช้งานไม่ให้เป็นแบบ Default (Hardening) ในโฟลเดอร์ (Folder) หลักที่เกี่ยวข้อง คือ โฟลเดอร์ admin และ ไฟล์ที่ชื่อ login.html และ login.php รวมถึงการตั้งค่ารหัสผ่านให้เป็นชื่ออื่นที่ยากต่อการคาดเดา เนื่องจากเป็นส่วนที่ผู้ดูแลเว็บไซต์ (Web Master) ใช้งานแต่เพียงผู้เดียว

๒.๑๕.๓ ตรวจสอบผู้ให้บริการเครือข่ายระบบอินเทอร์เน็ต และผู้ให้บริการ Web Hosting ที่มีความน่าเชื่อถือและมีความตระหนักถึงความมั่นคงปลอดภัยของระบบ

๒.๑๕.๔ ตรวจสอบการรับและแสดงผลข้อมูลในหน้าเว็บไซต์ (Web Page) (Input/Output) และในทุกครั้งที่รับ - ส่ง ข้อมูลบนเว็บไซต์ เพื่อป้องกันการส่งค่าที่เป็นอันตรายต่อการบุกรุกเว็บไซต์

๒.๑๕.๕ ต้องไม่นำไฟล์หน้าเว็บไซต์ และ Script ของผู้อื่นมาดัดแปลงเป็นหน้าเว็บไซต์ของส่วนราชการ เนื่องจากอาจฝังชุดคำสั่งที่เป็นอันตราย หรือภัยคุกคามต่อข้อมูลเครื่องคอมพิวเตอร์และเครือข่ายของ กองบัญชาการกองทัพไทย

๒.๑๕.๖ ในทุกหน้าเว็บไซต์ที่พัฒนาขึ้น ต้องแบ่งแยกประเภทและชนิดของข้อมูลที่รับ-ส่งให้ชัดเจน เพื่อให้ง่ายต่อการพัฒนาฟังก์ชั่นสำหรับตรวจสอบ หากดำเนินการรับค่าหรือกรอกข้อมูล ผู้พัฒนาเว็บไซต์ต้องตรวจสอบว่าข้อมูลที่ได้รับจากผู้ใช้งานในแต่ละส่วนนั้น ตรงตามรูปแบบและข้อกำหนดของแต่ละประเภทก่อนนำไปประมวลผลและไม่ปล่อยให้ข้อมูลที่ส่งเข้ามา ประมวลผลโดยไม่ผ่านการตรวจสอบ

๒.๑๕.๗ ตรวจสอบประเภทหรือนามสกุลของไฟล์ (File Extension) ในส่วนที่ผ่านกระบวนการอัพโหลดไฟล์ (Upload) เพื่อป้องกันการอัพโหลดไฟล์สคริปต์อันตราย หรือไฟล์ที่จะก่อให้เกิดปัญหาบนเครื่องคอมพิวเตอร์แม่ข่าย (Web Server) ของเว็บไซต์ และผู้ดูแลเว็บไซต์ ต้องกำหนดขอบเขตและประเภทของไฟล์ที่อนุญาตให้สามารถอัพโหลดได้

๒.๑๕.๘ ต้องไม่กำหนดสิทธิในการอ่าน เขียน ไฟล์ต้นฉบับ (Source Code) ของเว็บไซต์ให้กับผู้อื่น รวมถึงหมั่นตรวจสอบและปรับปรุงไฟล์อยู่เสมอ เนื่องจากการปรับเปลี่ยนหน้าเว็บไซต์ (Web Defacement) ส่วนใหญ่เกิดขึ้นจากการที่ผู้อื่นใช้สิทธิของไฟล์สคริปต์อันตราย ซึ่งเป็นสิทธิของผู้ให้บริการเว็บไซต์ (Web Hosting) ที่ใช้ในการดำเนินการ ฉะนั้นต้องระมัดระวังการให้สิทธิไฟล์ต้นฉบับของเว็บไซต์

/๒.๑๕.๙ จัดการ...

๒.๑๕.๙ จัดการสิทธิไฟล์ต้นฉบับของเว็บไซต์ ด้วยสิทธิผู้ใช้งานของตนเอง ไม่ใช้ผ่านหน้าเว็บไซต์อัพโหลดใด ๆ เพราะจะทำให้สิทธิของไฟล์ต่าง ๆ ที่อยู่บนระบบ เป็นของเครื่องคอมพิวเตอร์แม่ข่าย และหากไฟล์ใดจำเป็นต้องแก้ไข จึงเปิดใช้งานสิทธิ และระวังตรวจสอบไฟล์ว่าได้ถูกเปลี่ยนแปลงหรือไม่ เพื่อเป็นข้อมูลสำหรับการพิจารณาความผิดปกติที่อาจจะเกิดขึ้นกับเว็บไซต์

๒.๑๕.๑๐ ต้องลบไฟล์ หรือโฟลเดอร์ หรือ โฟลเดอร์ย่อย (Sub Folder) ต่าง ๆ ที่ไม่จำเป็นต่อการใช้งานและที่แปลกปลอมเข้ามาในเว็บไซต์

๒.๑๕.๑๑ ดำเนินการตรวจสอบหน้าเว็บไซต์ อย่างสม่ำเสมอว่ามีความแตกต่างไปจากที่ได้พัฒนาหรือไม่

๒.๑๕.๑๒ สำรองข้อมูลของเว็บไซต์ และไฟล์ต้นฉบับไว้ที่แหล่งบันทึกข้อมูลอื่น นอกเหนือจากบนเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้บริการอยู่ หากเว็บไซต์ถูกเปลี่ยนแปลงหรือแก้ไขข้อมูล จะได้สามารถดำเนินการกู้คืนข้อมูลได้อย่างรวดเร็วและสมบูรณ์

๒.๑๖ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๒.๑๖.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ ในรูปแบบและลักษณะตามที่ กองบัญชาการกองทัพไทย ได้กำหนดไว้เท่านั้น

๒.๑๖.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับ กองบัญชาการกองทัพไทย ผู้ใช้งานต้องแจ้ง ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๒.๑๗ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ให้ปฏิบัติดังต่อไปนี้

๒.๑๗.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๒.๑๗.๒ ห้ามผู้ดูแลระบบ แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของ กองบัญชาการกองทัพไทย (IT Auditor) หรือบุคคลที่ กองบัญชาการกองทัพไทย มอบหมาย

๒.๑๗.๓ กำหนดให้ต้องบันทึกการทำงานของระบบ บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก โดยบันทึกการเข้า - ออก ระบบบันทึกการพยายามเข้าสู่ระบบ เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกไว้ ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๒.๑๗.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ตรวจถูกต้อง

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)

จก.สส.ทหาร

ผนวก ค แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ
ประกอบ ประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

๑. การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายกองบัญชาการกองทัพไทย (Access Control)เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาติเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกองบัญชาการกองทัพไทย และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารได้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกองบัญชาการกองทัพไทยได้อย่างถูกต้อง

๑.๑ กระบวนการหลักในการควบคุมการเข้าถึงระบบ ดังนี้

๑.๑.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๑.๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๑.๑.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ การเข้าถึงข้อมูลและระบบข้อมูลได้

๑.๑.๔ ผู้ดูแลระบบ ต้องติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกองบัญชาการกองทัพไทย และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๑.๑.๕ ผู้ดูแลระบบ ต้องบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๑.๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑.๒.๑ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้ลงนามอนุมัติเอกสารดังกล่าวต้องดำเนินการจัดเก็บไว้เป็นหลักฐาน

๑.๒.๒ เจ้าของข้อมูล และ“เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๑.๒.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

/๑.๓ การบริหาร...

๑.๓ การบริหารจัดการการเข้าถึงของผู้ใช้

๑.๓.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของกองบัญชาการกองทัพไทยต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งานเมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน

๑.๓.๒ กำหนดสิทธิ การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ตโดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑.๓.๓ ผู้ใช้งาน ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๑.๔ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

๑.๔.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ใน “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๑.๔.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ใน“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๑.๔.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึงผู้ใช้ที่มีสิทธิสูงสุดต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ

๑.๔.๔ ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

๑.๔.๕ ต้องควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดให้ดำเนินการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๑.๔.๖ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๑.๔.๗ ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

๒. การบริหารจัดการการเข้าถึงระบบเครือข่าย

๒.๑ ผู้ดูแลระบบ ต้องออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่ดำเนินการใช้งานกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ ทั้งเขตภายใน (Internal Zone) และเขตภายนอก (External zone) เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๒.๒ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาติเท่านั้น

๒.๓ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน

๒.๔ ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

/๒.๕ ต้องกำหนด...

๒.๕ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไข หรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๒.๖ ระบบเครือข่ายทั้งหมดของกองบัญชาการกองทัพไทยที่เชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกกองบัญชาการกองทัพไทยต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet Filtering โดยการใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๒.๗ ต้องติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกองบัญชาการกองทัพไทย ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๒.๘ การเข้าสู่ระบบงานเครือข่ายภายในกองบัญชาการกองทัพไทย โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องลงชื่อเข้าใช้งาน(Login)และต้องพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๒.๙ หมายเลขไอพี (IP Address)ภายในของระบบงานเครือข่ายภายในของกองบัญชาการกองทัพไทยต้องดำเนินการป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

๒.๑๐ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๑๑ การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๑๒ การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เท่านั้น

๒.๑๓ ผู้ใช้งานที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัดเพื่อให้การเชื่อมต่ออุปกรณ์ต่างๆเป็นไปตามมาตรฐาน และไม่เกิดผลกระทบกับระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของกองบัญชาการกองทัพไทย

๒.๑๔ การขออนุญาตนำเครื่องคอมพิวเตอร์ เชื่อมต่อระบบเครือข่ายและขอหมายเลขไอพี และชื่อโดเมน (Domain Name) ของหน่วยงานใด ๆ หน่วยงานนั้นต้องทำหนังสือขออนุญาตส่งผ่านหน่วยงานต้นสังกัดมายังศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เพื่อพิจารณาดำเนินการ

๒.๑๕ ห้ามบุคคลใดกระทำการเคลื่อนย้าย หรือทำการใด ๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของ กองบัญชาการกองทัพไทย ได้

๒.๑๖ ในกรณีที่ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลักของ กองบัญชาการกองทัพไทย ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร จะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่ต้องแจ้งให้ทราบล่วงหน้าจนกว่าจะดำเนินการแก้ไขให้ทำงานได้เป็นปกติก่อน

/๒.๑๗ ห้ามทำ...

๒.๑๗ ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network)

๓. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๓.๑ กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๓.๒ มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีผู้ใช้งานเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องรีบดำเนินการแก้ไขรวมทั้งรายงานโดยทันที

๓.๓ เปิดใช้บริการ (Service)ของTelnet FTP หรือ Ping เท่าที่จำเป็นเท่านั้น ทั้งนี้หากบริการที่จำเป็นต้องใช้ มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๓.๔ ติดตั้งปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) ในเครื่องแม่ข่ายให้บริการเว็บไซต์ (webserver)อย่างสม่ำเสมอ

๓.๕ ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษา

๓.๖ การติดตั้งและเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ของ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เท่านั้น

๔. การบริหารจัดการการบันทึกและตรวจสอบ

๔.๑ กำหนดให้ต้องบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของการใช้งาน (Application Logs) บันทึกรายละเอียดของระบบป้องกันการบุกรุก บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๓ เดือน

๔.๒ ต้องตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๔.๓ มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๕. การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ต้องกำหนดให้ดำเนินการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายใน กองบัญชาการกองทัพไทย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๕.๑ การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายของ กองบัญชาการกองทัพไทย ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของกองบัญชาการกองทัพไทยจากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๕.๒ วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูล หรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ก่อน และดำเนินการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกองบัญชาการกองทัพไทย ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๕.๓ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับ กองบัญชาการกองทัพไทย อย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๕.๔ ต้องควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

/๕.๕ การอนุญาต...

๕.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ต้องเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อดำเนินการร้องขอที่จำเป็นเท่านั้น

๖. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของกองบัญชาการกองทัพไทยดังนี้

๖.๑ แสดงชื่อผู้ใช้งาน (Username)

๖.๒ ใส่รหัสผ่าน (Password)

๗. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control) การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ ได้แก่ ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เพื่อให้การควบคุมหน่วยงานภายนอกที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กองบัญชาการกองทัพไทย เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

๗.๑ แนวทางปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

๗.๑.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร กำหนดให้ต้องดำเนินการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับ หรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

๗.๑.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารของหน่วยงานภายนอก

๗.๑.๒.๑ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ และ การสื่อสารของ กองบัญชาการกองทัพไทย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

๗.๑.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

๗.๑.๒.๒(๑) เหตุผลในการขอใช้

๗.๑.๒.๒(๒) ระยะเวลาในการใช้

๗.๑.๒.๒(๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๗.๑.๒.๒(๔) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๗.๑.๓ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๗.๑.๓.๑ หน่วยงานภายนอกที่ทำงานให้กับ กองบัญชาการกองทัพไทย ทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายใน กองบัญชาการกองทัพไทย หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของ กองบัญชาการกองทัพไทย โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๗.๑.๓.๒ เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่ต้องเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

/๗.๑.๓.๓ สำหรับ...

๗.๑.๓.๓ สำหรับโครงการขนาดใหญ่หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของ กองบัญชาการกองทัพไทย ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๗.๑.๓.๔ กองบัญชาการกองทัพไทย มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจได้ว่า กองบัญชาการกองทัพไทย สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๗.๑.๓.๕ กำหนดให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งดำเนินการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ตรวจถูกต้อง

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)

จก.สส.ทหาร

ผนวก ง แนวปฏิบัติในการใช้งานระบบสารสนเทศและระบบสำรองของสารสนเทศ
ประกอบ ประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

เพื่อให้ระบบสารสนเทศของ กองบัญชาการกองทัพไทย ให้บริการได้อย่างต่อเนื่อง และใช้เป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับ กองบัญชาการกองทัพไทย อย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จึงได้กำหนดแนวทางปฏิบัติไว้ ดังนี้

๑. การสำรองข้อมูลและระบบคอมพิวเตอร์ ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทาง ดังต่อไปนี้

๑.๑ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของ กองบัญชาการกองทัพไทย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ ๑ ครั้ง

๑.๒ กำหนดให้สำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้นโดยให้มีวิธีการสำรองข้อมูล ดังนี้

๑.๒.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๑.๒.๒ มีขั้นตอนการปฏิบัติ การจัดทำ การสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๑.๒.๓ ให้ผู้ดูแลระบบคอมพิวเตอร์ และผู้ดูแลระบบเครือข่าย กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี ๒ ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑.๒.๔ การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล โดยมี วัน/เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก สำเร็จ/ไม่สำเร็จ

๑.๒.๕ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุ ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหา และสรุปผลการแก้ไขปัญหา และรายงานต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

๑.๒.๖ ตรวจสอบข้อมูลทั้งหมดระบบว่าได้สำรองข้อมูลไว้อย่างครบถ้วน ประกอบด้วย ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน (Configuration) ข้อมูลในฐานข้อมูล

๑.๒.๗ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยพิมพ์ชื่อบนสื่อเก็บข้อมูลสำรอง และสถานที่เก็บสื่อบันทึกข้อมูลสำรองกับ กองบัญชาการกองทัพไทย ต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลจัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติ ไฟไหม้ น้ำท่วม กับ กองบัญชาการกองทัพไทย

๑.๒.๘ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูลนอกสถานที่

๑.๒.๙ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๑.๒.๑๐ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

/๑.๒.๑๑ ตรวจสอบ...

๑.๒.๑๑ ตรวจสอบและทดสอบประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑.๒.๑๒ ให้ผู้ดูแลระบบคอมพิวเตอร์ มอบหมายหน้าที่การสำรองข้อมูลให้กับเจ้าหน้าที่คนอื่นเพื่อช่วยสำรองข้อมูล ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๑.๒.๑๓ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๑.๒.๑๔ นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

๑.๓ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณี ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑.๔ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่ ดังนี้

ลำดับ	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Mail Server	- ค่า Configure - ข้อมูล ในเมลบ๊อกซ์	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๒	Web Server	- ค่า Configure - ข้อมูลเผยแพร่บนเว็บไซต์	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๓	Database Server	- ค่า Configure - ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๔	Firewall Server	- ค่า Configure - ข้อมูล Rule ของ Firewall	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๕	Server ของระบบงานต่าง ๆ	- ค่า Configure - ข้อมูลบน Server อื่น ๆ	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน

หมายเหตุ ทุกรายการที่ปรากฏในตารางจะใช้วิธีสำรองข้อมูลแบบ Full Backup

๑.๕ ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าได้สำรองข้อมูล (Back up) ตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์ หรือไม่

๒. การกู้คืนระบบ

๒.๑ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์ หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึก และรายงานสรุปผลการปฏิบัติงานต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร หรือผู้ที่ได้รับมอบหมาย

๒.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Lastest Update) ที่ได้สำรองไว้ หรือตามความเหมาะสม เพื่อกู้คืนระบบ

/๒.๓ หากความ...

๒.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๒.๔ ต้องซักซ้อมการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

ตรวจถูกต้อง

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)

จก.สส.ทหาร

ผนวก จ แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน
ประกอบ ประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
ของ กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

วัตถุประสงค์

เพื่อลดความเสียหายที่จะเกิดแก่ระบบเทคโนโลยีสารสนเทศของ กองบัญชาการกองทัพไทย จากสถานการณ์ความไม่แน่นอน ภัยคุกคาม และภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ทั้งเครื่องแม่ข่ายระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ ภัยอันตรายที่เกิดขึ้นอาจทำให้ข้อมูลถูกเปิดเผย เปลี่ยนแปลง หรือสูญหาย ส่งผลกระทบต่อการปฏิบัติราชการ ดังนั้นเพื่อเป็นการลดภัยดังกล่าวที่จะเกิดขึ้นจึงมีความจำเป็นอย่างยิ่งที่กองบัญชาการกองทัพไทย จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยคุกคาม ซึ่งประกอบด้วย แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan) แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan) และแผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure) ได้กำหนดแนวปฏิบัติไว้ ดังนี้

๑. แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan)

๑.๑ ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๑.๒ ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยง กรณีไฟดับเป็นระยะเวลานาน ไฟไหม้ น้ำท่วม แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้าใช้ระบบงานได้

๑.๓ ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๑.๔ ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๑.๕ ต้องกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ และซอฟต์แวร์

๑.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติเมื่อเกิดเหตุเร่งด่วน

๑.๗ ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ โดยมุ่งเน้นไปที่ระบบที่มีความสำคัญสูง ปีละ ๑ ครั้ง

๒. แผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan) เพื่อแก้ไขระบบเทคโนโลยีสารสนเทศ ของ กองบัญชาการกองทัพไทย ที่เกิดจากภัยพิบัติให้ใช้งานได้อย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ ได้กำหนดบทบาทหน้าที่ ดังนี้

๒.๑. ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)

๒.๑.๑ กำหนดนโยบายให้ กองบัญชาการกองทัพไทย

๒.๑.๒ ให้คำปรึกษาแก่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ในฐานะการกำกับดูแล

๒.๑.๓ ดำเนินการจัดตั้งหน่วยปฏิบัติการสารสนเทศเฉพาะกิจ เพื่อรองรับการปฏิบัติภารกิจเฉพาะ ที่ต้องใช้ความชำนาญการพิเศษของกำลังพลจากส่วนราชการอื่น ๆ ภายใน กองบัญชาการกองทัพไทย

/๒.๒ ผู้อำนวยการ...

๒.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

๒.๒.๑ เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๒.๒.๒ มีอำนาจสั่งการให้ทุกส่วนราชการหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๒.๒.๓ จัดประชุมหารือกับคณะกรรมการที่เกี่ยวข้อง

๒.๒.๔ ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผน ตามความเหมาะสม

๒.๒.๕ รายงานผลการปฏิบัติงานให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ทราบ

๒.๓ ผู้ประสานงาน และบริหาร กำกับดูแลสภาพความพร้อมของระบบเครือข่าย (หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต)

๒.๓.๑ วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

๒.๓.๒ มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่า ผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

๒.๓.๓ สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

๒.๓.๔ ทำหน้าที่แทน ผู้อำนวยการระงับเหตุฉุกเฉิน ตามที่ได้รับมอบหมาย หรือขณะที่ผู้อำนวยการระงับเหตุฉุกเฉิน ไม่อยู่

๒.๓.๕ ประสานงานกับหัวหน้าหน่วยงาน ช่างไฟฟ้า ช่างยานพาหนะ และหน่วยดับเพลิงที่เกี่ยวข้อง

๒.๓.๖ รายงานให้ ผู้อำนวยการระงับเหตุฉุกเฉิน ทราบถึงสถานการณ์ และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

๒.๓.๗ กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

๒.๓.๘ ตรวจสอบความเสียหายของสินทรัพย์ และอาคารที่เกิดเหตุ

๒.๔. ผู้ดูแลระบบเครือข่าย และผู้ช่วยดูแลระบบเครือข่าย (Network Administor and Staffs)

๒.๔.๑ กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

๒.๔.๒ พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่น ๆ มาช่วย

๒.๔.๓ ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

๒.๔.๔ ป้องกันชีวิตสินทรัพย์ และสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

๒.๔.๕ หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้ว ให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ทราบ อุปกรณ์ที่ต้องตรวจสอบ ดังนี้

๒.๔.๕.๑ ตรวจสอบระบบไฟร์วอลล์

๒.๔.๕.๒ ตรวจสอบ Virus, Worm และ Spyware

๒.๔.๕.๓ ตรวจสอบ UPS (Uninterrupt Power Supply)

๒.๔.๕.๔ ตรวจสอบ Transaction log files

๒.๔.๕.๕ ตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ

๒.๔.๕.๖ ตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ

๒.๔.๕.๗ ตรวจสอบความถูกต้องของไฟล์ข้อมูล

๒.๔.๕.๘ ตรวจสอบค่า Configuration ของระบบ

/๒.๔.๖ เตรียมเครื่อง...

๒.๔.๖ เตรียมเครื่องมืออุปกรณ์ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

๒.๔.๗ ทำการสำรองข้อมูลทุกวัน โดย วันอาทิตย์ - วันศุกร์ ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) และวันเสาร์ทำการสำรองข้อมูลทั้งระบบ (System)

๒.๔.๘ ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ ในสถานที่ที่ปลอดภัยโดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบโปรแกรม และแฟ้มข้อมูล Tape Backup รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรอง สำเนาคู่มือ

๒.๔.๙ นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๒.๕. หัวหน้าหน่วยงานที่เกิดเหตุ (On-Site Manager)

๒.๕.๑ แจ้งเหตุฉุกเฉินและเคลื่อนย้ายตนเอง และผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

๒.๕.๒ ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

๒.๕.๓ นำสินทรัพย์ที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีสินทรัพย์ที่จัดทำขึ้นมาและทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

๓. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณโดยปกติ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดเท่าที่จะทำได้ เนื่องจากเครื่องแม่ข่าย และอุปกรณ์กระจายสัญญาณต้องทำงานด้านบริการ (Service) แก่เครื่องลูกข่ายให้สามารถใช้งานได้ปกติ การกู้คืนระบบเครื่องแม่ข่าย และอุปกรณ์กระจายสัญญาณจำเป็นต้องทำอย่างรวดเร็ว เพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์ และแฟ้มข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน ซึ่งสามารถดำเนินการได้ ดังนี้

๓.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๓.๒ เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓.๓ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๓.๔ ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๓.๕ นำ BACKUP TAPE/CD-ROM/HARDDISK ที่ได้สำรองข้อมูลไว้ นำกลับมาใช้ (Restore)

๓.๖ ทีมกู้ระบบ (กองปฏิบัติการเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๓.๗ ต้องตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

/๓.๘ ต้องสำรอง...

๓.๘ ต้องสำรองข้อมูลตามชนิด ความถี่ และ วิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

๓.๙ ต้องทดสอบกู้คืนข้อมูลที่สำรองไว้นั้น ว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่อย่างน้อย ปีละ ๑ ครั้ง ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

ตรวจถูกต้อง

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)

จก.สส.ทหาร

ผนวก ฉ แนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ประกอบ ประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

การประเมินสถานการณ์ความเสี่ยง

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ ในระบบเทคโนโลยีสารสนเทศของ กองบัญชาการกองทัพไทย พบว่าความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของ กองบัญชาการกองทัพไทย สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

๑. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

ได้แก่ เจ้าหน้าที่ หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจ ในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงานและส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน โดย ศูนย์เทคโนโลยีสารสนเทศ กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ดังนี้

๑.๑ จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ และซอฟต์แวร์เบื้องต้น เพื่อลดความเสี่ยงด้านภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้ และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้านฮาร์ดแวร์ และซอฟต์แวร์ ได้อย่างมีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจากภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงานลดน้อยลง

๑.๒ นำเสนอนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อพิจารณาในการประชุมคณะทำงานการดำเนินการพัฒนาคุณภาพการบริหารจัดการภาครัฐ กองบัญชาการกองทัพไทย หมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ (PMQA : Public Sector Manangement Quality Awards)

๑.๓ จัดทำนโยบายว่าด้วยการใช้งานคอมพิวเตอร์ทั่วไป และการเข้าถึงระบบเครือข่ายอินเทอร์เน็ต เผยแพร่ผ่านเว็บไซต์ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

๒. ภัยที่เกิดจากซอฟต์แวร์ เป็นภัยที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) ซึ่งซอฟต์แวร์ประเภทนี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของ กองบัญชาการกองทัพไทย ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของ กองบัญชาการกองทัพไทย ใช้งานไม่ได้ ซึ่งแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากซอฟต์แวร์ ซึ่ง ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ได้ตระหนักถึงปัญหานี้จึงได้ดำเนินการ ดังนี้

๒.๑ ติดตั้งไฟร์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

/๒.๒ ต้องติดตั้ง...

๒.๒ ต้องติดตั้งซอฟต์แวร์ Trend Micro Server ที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่เป็นซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของ กองบัญชาการกองทัพไทย

๒.๓ แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านทางระบบอินทราเน็ต ของ กองบัญชาการกองทัพไทย ที่ http://mitd.rtarf.local/mitd/ อย่างต่อเนื่อง สม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากซอฟต์แวร์ ดังกล่าวให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกัน และแก้ไขปัญหาในเบื้องต้นได้ผ่านทาง http://mid6000.rtarf.local/km-sc/

๓. ภัยจากไฟไหม้ หรือระบบไฟฟ้า

จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ ระบบเทคโนโลยีสารสนเทศ ซึ่ง ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้ หรือระบบไฟฟ้าขัดข้อง ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการ ดังนี้

๓.๑ ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS : Uninterrupt Power Suppy) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย ในกรณีเกิดกระแสไฟฟ้าขัดข้อง โดยต้องสำรวจตรวจสอบระยะเวลาการสำรองไฟฟ้ากรณีที่เกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์ต้องสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

๓.๒ ติดตั้งอุปกรณ์ ตรวจจับควันกรณีที่เกิดเหตุการณ์ กระแสไฟฟ้าขัดข้อง หรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งต้องตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

๓.๓ ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์ เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (อัคคีภัย) โดยต้องตรวจสอบความพร้อมของอุปกรณ์ และทดลองใช้งานโดยสม่ำเสมอ

๔. ภัยจากน้ำท่วม (อุทกภัย)

เนื่องจากห้องควบคุมระบบเครือข่าย กองบัญชาการกองทัพไทย อยู่บริเวณชั้น ๑ ของอาคารซึ่งมีความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ ระบบเทคโนโลยีสารสนเทศ ซึ่ง กองบัญชาการกองทัพไทย ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้ภัยในลักษณะดังกล่าวเกิดขึ้นแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากน้ำท่วม (อุทกภัย) ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้นจึงได้ดำเนินการ ดังนี้

๔.๑ เฝ้าระวังภัยอันเกิดจากน้ำท่วม โดยติดตามจากพยากรณ์อากาศของ กรมอุตุนิยมวิทยา ตลอดเวลา

๔.๒ เมื่อเกิดน้ำขัง หรือเกิดรั่วซึมจากน้ำ และมีแนวโน้มว่าน้ำท่วมขังเพิ่มขึ้นเรื่อย ๆ มาถึงบริเวณหน้าอาคาร ให้ปิดเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครื่องแม่ข่ายทั้งหมด

๔.๓ ถอดเทปสำรองข้อมูล (Back up) ทั้งหมดไปเก็บไว้ในที่ปลอดภัย

๔.๔ ดำเนินการตัดระบบน้ำ และไฟฟ้าในห้องควบคุมปิดตัวตัดไฟ (Breaker) เครื่องปรับอากาศเพื่อป้องกันเครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

๔.๕ เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในชั้นที่สูงขึ้นไป

๔.๖ กรณีน้ำลดลงเรียบร้อยแล้ว ให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

/ ๔.๗ เมื่อระบบ...

๔.๗ เมื่อระบบไฟฟ้าใช้งานได้ตามปกติ ผู้ดูแลระบบ และเจ้าหน้าที่ผู้เกี่ยวข้อง ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์ทำหน้าที่แม่ข่ายมาติดตั้ง ณ ห้องควบคุมระบบเครือข่าย เพื่อให้ใช้งานได้ตามปกติ

๔.๘ ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายพร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบเครือข่ายว่าสามารถเชื่อมต่อ และให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

๔.๙ เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้วแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ การจัดเตรียมอุปกรณ์ที่จำเป็นในการเตรียมพร้อมรับภัยพิบัติ ที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ กองบัญชาการกองทัพไทย งานระบบเครือข่าย บริการอินเทอร์เน็ต งานระบบคอมพิวเตอร์และบริการซึ่ง ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร เป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ของ กองบัญชาการกองทัพไทย ต้องจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยต้องเตรียมอุปกรณ์ ดังนี้

๔.๙.๑ แผ่น Boot Disk
๔.๙.๒ แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
๔.๙.๓ แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
๔.๙.๔ แผ่นโปรแกรม Antivirus/Spyware
๔.๙.๕ แผ่น Driver ของอุปกรณ์ต่าง ๆ
๔.๙.๖ ระบบสำรองไฟฉุกเฉิน
๔.๙.๗ Hard Disk สำรองข้อมูล
๔.๙.๘ สำเนารายละเอียดการบันทึกค่าต่าง ๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้การตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ และเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ โดยอิงมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ได้กำหนดแนวปฏิบัติไว้ ดังนี้

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑.๑ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

๑.๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) ปีละ ๑ ครั้ง

๑.๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยสำนักงานตรวจสอบภายในทหาร เพื่อให้ กองบัญชาการกองทัพไทย ได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๒.๑ ต้องทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ ๑ ครั้ง

๒.๒ ต้องทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีละ ๑ ครั้ง

๒.๓ ต้องตรวจสอบและประเมินความเสี่ยง และให้จัดทำรายงานพร้อมข้อเสนอแนะ

/ ๒.๔ มีมาตรการ...

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ ดังนี้

๒.๔.๑ ต้องให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ แบบอ่านอย่างเดียว

๒.๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งต้องทำลาย หรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยต้องป้องกันเป็นอย่างดี

๒.๔.๓ ต้องทำการระบุ และจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๔.๔ ต้องเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวัน และเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๒.๔.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจสอบประเมินระบบสารสนเทศ ต้องกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และต้องจัดเก็บป้องกันเครื่องนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. ต้องรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ ปีละ ๑ ครั้ง ต่อคณะกรรมการพัฒนาสารสนเทศ และแจ้งคณะกรรมการบริหารความเสี่ยงของ กองบัญชาการกองทัพไทย เพื่อดำเนินการต่อไป

๔. ต้องแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตามตรวจสอบ และประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ตรวจถูกต้อง

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)

จก.สส.ทหาร

ผนวก ช แนวปฏิบัติในการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ
ประกอบ ประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
กองบัญชาการกองทัพไทย พ.ศ.๒๕๕๙

วัตถุประสงค์

เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศให้กับผู้ใช้งานของ กองบัญชาการกองทัพไทย และป้องกันการกระทำผิดโดยรู้เท่าไม่ถึงการณ์ เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัย โดยกำหนดแนวปฏิบัติไว้ดังนี้

๑. จัดฝึกอบรมการใช้ระบบสารสนเทศ ของ กองบัญชาการกองทัพไทย ปีละ ๑ ครั้ง หรือทุกครั้งที่ทำการปรับปรุง และเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และเผยแพร่ทางเว็บไซต์ของ กองบัญชาการกองทัพไทย

๓. จัดฝึกอบรมและสัมมนา การรักษาความปลอดภัยระบบสารสนเทศของ กองบัญชาการกองทัพไทย โดยการจัดอบรมและสัมมนาฯ ใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของ กองบัญชาการกองทัพไทย

๔. จัดประชุมสัมมนาเพื่อเผยแพร่ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน

๕. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่ายโดยปรับปรุงความรู้อยู่เสมอ

๖. ระดมการมีส่วนร่วมการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ และลงสู่ภาคปฏิบัติ โดยต้องสำรวจความต้องการผู้ใช้งานและติดตามประเมินผล

๗. เผยแพร่ความรู้ด้านการรักษาความปลอดภัยระบบสารสนเทศ ผ่านทางเว็บไซต์อินทราเน็ต http://mid6000.rtarf.local/km-sc/

ตรวจถูกต้อง

พล.ท.

(พิเชฏฐ์ แย้มแก้ว)
จก.สส.ทหาร