(ร่าง) ระเบียบ กองทัพบก
ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก
พ.ศ.๒๕๕๔

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพบกเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองทัพบก ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก พ.ศ.๒๕๕๔”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ บรรดาระเบียบและคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับระเบียบนี้ให้ใช้ระเบียบนี้แทน โดยยึดถือให้อยู่ภายใต้ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และกรอบนโยบายด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกระทรวงกลาโหมที่ได้ประกาศขึ้น

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานข้าราชการและลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพบก

ข้อ ๕ คำนิยามในระเบียบนี้

(๑) ระบบสารสนเทศ (Information System) หมายความว่า ระบบข่าวสารของกองทัพบก ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบสื่อสาร มาช่วยในการสร้างสารสนเทศของกองทัพบก และสามารถนำสารสนเทศมาใช้ในการวางแผน การบริหาร การพัฒนา ควบคุม รวมทั้งแนวทางหรือระเบียบปฏิบัติในการใช้อุปกรณ์เหล่านี้ ซึ่งมีองค์ประกอบดังนี้

(๑.๑) ระบบคอมพิวเตอร์(Computer System) หมายถึง ระบบที่ประกอบด้วย ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (People ware)

(๑.๒) เครือข่ายคอมพิวเตอร์ (Computer Network) หมายความว่า การติดต่อสื่อสาร หรือการรับ-ส่งข้อมูลระหว่างระบบสารสนเทศภายในกองทัพบกและหน่วยงานอื่นๆ ที่เกี่ยวข้องกับกองทัพบก

(๑.๓) สารสนเทศ (Information) ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือ ภาพกราฟฟิกที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจ และอื่น ๆ

(๒) จดหมายอิเล็กทรอนิกส์ (Electronic Mail: E-mail) หมายถึง การรับส่งข้อมูลผ่านอินเทอร์เน็ตหรืออินทราเน็ต โดยชื่อที่ใช้ในการรับส่งจดหมายอิเล็กทรอนิกส์ จะมีรูปแบบซึ่งประกอบไปด้วย ๒ ส่วน คือ ชื่อผู้ใช้ และชื่อโดเมน เช่น user@rta.mi.th เป็นต้น

(๓) ผู้ใช้งาน (User) หมายถึง ข้าราชการ พนักงานราชการ และลูกจ้างของกองทัพบกที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศกองทัพบก รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพบก

(๔) ผู้ดูแลระบบ (System Administrator) หมายถึง นายทหารสัญญาบัตรที่ปฏิบัติงานในระบบสารสนเทศของกองทัพบกหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลระบบสารสนเทศของหน่วยงานนั้นๆ

(๕) ผู้ดูแลเครือข่าย (Network Administrator) หมายถึง นายทหารสัญญาบัตรที่ปฏิบัติงานในระบบสารสนเทศของกองทัพบกหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลเครือข่ายสารสนเทศของหน่วยงานนั้นๆ

(๖) ผู้ดูแลฐานข้อมูล (Database Administrator) หมายถึง นายทหารสัญญาบัตรที่ปฏิบัติงานในระบบสารสนเทศของกองทัพบกหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลฐานข้อมูล

(๗) ผู้บังคับบัญชา หมายถึง หัวหน้าหน่วยงานของผู้ปฏิบัติหน้าที่ในระบบสารสนเทศของกองทัพบก

(๘) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า ความมั่นคงและความปลอดภัยในบริบทของ การรักษาความลับ ความเชื่อถือได้ และความพร้อมใช้งานของข้อมูล สำหรับระบบสารสนเทศของ กองทัพบก

(๙) เหตุการณ์ด้านความมั่นคงปลอดภัย (Security incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของกองทัพบกหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรืออาจสร้างความเสียหายได้ในที่สุดซึ่งอาจส่งผลให้

(๙.๑) เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ เช่น ระบบงานสารสนเทศของหน่วยเกิดการหยุดชะงัก เป็นต้น

(๙.๒) เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของกองทัพบก

(๙.๓) เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กำหนดไว้

(๙.๔) เกิดภาพลักษณ์ที่ไม่ดีต่อกองทัพบกหรือทำให้สูญเสียชื่อเสียง เช่น การไปโพสต์ข้อความพาดพิงถึงกองทัพบกในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของกองทัพบก เป็นต้น

(๙.๕) ตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัย ได้แก่ โปรแกรมไม่พึงประสงค์ การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน การแจ้งเตือนของระบบป้องกันการบุกรุก ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต การใช้ทรัพยากรของหน่วยงานผิดวัตถุประสงค์ เช่น การใช้เครือข่ายของหน่วยงานเพื่อกระทำการที่ขัดต่อ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อกระทำการที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา เพื่อทำการส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ เป็นต้น ระบบถูกโจมตีจนไม่สามารถให้บริการได้ ระบบ อุปกรณ์ ฮาร์ดแวร์ หรือทรัพย์สินในระบบสารสนเทศอื่นๆ ถูกขโมย การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของกองทัพบก การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่นๆ ที่เป็นการละเมิดระเบียบฉบับนี้

(๙.๖) ตัวอย่างของเหตุการณ์ที่เป็นจุดอ่อน ได้แก่ ประตูศูนย์คอมพิวเตอร์ไม่สามารถปิดให้สนิทได้ ระบบงานสารสนเทศของหน่วยมีช่องทางอื่นในการเข้าสู่ระบบได้โดยไม่ผ่านการพิสูจน์ตัวตน ตามปกติ เจ้าหน้าที่รักษาความปลอดภัยของหน่วยไม่เข้มงวดหรือละเลยการปฏิบัติหน้าที่ บุคคลภายนอกสามารถเดินตามเจ้าหน้าที่เข้าห้องระบบสารสนเทศของหน่วยโดยไม่มีการแลกบัตรผ่าน บุคคลภายนอกไม่ได้ลงชื่อก่อนเข้าศูนย์คอมพิวเตอร์ของหน่วย เจ้าหน้าที่ไม่มีการระบุตัวตนก่อนที่จะเข้าถึงห้องระบบสารสนเทศของหน่วยนั้น

(๙.๗) เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ที่เป็นจุดอ่อนจำเป็นต้องได้รับรายงานจากผู้ใช้งานเพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสมได้ผลและทันกาล

(๑๐) ทรัพย์สินทางปัญญา หมายถึง ผลงานอันเกิดจากความคิดสร้างสรรค์ของมนุษย์ ทรัพย์สินทางปัญญาเป็นทรัพย์สินอีกชนิดหนึ่งที่นอกเหนือจากสังหาริมทรัพย์นั่นคือทรัพย์สินที่สามารถเคลื่อนย้ายได้ เช่น นาฬิกา รถยนต์ โต๊ะ เป็นต้น และอสังหาริมทรัพย์ คือทรัพย์สินที่ไม่สามารถเคลื่อนย้ายได้ เช่น บ้าน ที่ดิน เป็นต้น ซึ่งทรัพย์สินทางปัญญา ได้แก่

(๑๐.๑) ลิขสิทธิ์ (Copyright)

(๑๐.๒) สิทธิบัตร (Patent)

(๑๐.๓) เครื่องหมายการค้า (Trademark)

(๑๐.๔) แบบผังภูมิของวงจรรวม (Layout - Designs of Integrated Circuit)

(๑๐.๕) ความลับทางการค้า (Trade Secrets)

(๑๐.๖) สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

(๑๑) สินทรัพย์ หมายถึง สิ่งของที่จำเป็นทั้งมวลสำหรับกองทัพบก ทั้งที่มีไว้เพื่อการดำรงอยู่ และการปฏิบัติของหน่วยภายในกองทัพบก ทั้งให้เป็นไปตามระเบียบกองทัพบกว่าด้วย ความรับผิดชอบในสิ่งอุปกรณ์ พ.ศ.๒๕๓๕ ตามคำจัดความ ข้อ ๔ ว่าด้วยสิ่งอุปกรณ์ของกองทัพบก

(๑๒) สิทธิของผู้ใช้งาน (user access right) หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของกองทัพบก หรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของกองทัพบก

(๑๓) การเข้าถึง (access) หมายถึง ความสามารถในการเข้าไป อันอาจทำให้สามารถจะอ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใดๆ หรือได้อ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใดๆ สำหรับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ สารสนเทศ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์และวิธีการทางกายภาพ

(๑๔) การควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (access control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๑๕) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบของกองทัพบกสูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่างๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูกบุกรุกหรือโจมตีทางช่องโหว่ และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่างๆ

(๑๖) ภัยคุกคาม (threats) หมายถึง เหตุการณ์ต่างๆ ที่เป็นไปได้หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจส่งผลกระทบหรือสร้างความเสียหายต่อระบบสารสนเทศของกองทัพบก

(๑๗) ช่องโหว่ (vulnerabilities) หมายถึง จุดอ่อนของทรัพย์สินหรือมาตรการ ที่เป็นช่องทางเกิดปัจจัยเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อทรัพย์สินหรือต่อระบบสารสนเทศของกองทัพบก

ข้อ ๖ **เสนาธิการทหารบก** ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกองทัพบก (CIO) เป็นผู้รับผิดชอบระบบสารสนเทศในภาพรวมของกองทัพบก รวมถึงการละเมิดมาตรการต่างๆ จนความเสียหายของระบบสารสนเทศที่เกิดขึ้นตามระเบียบนี้ โดยมอบหมายให้ **เจ้ากรมการทหารสื่อสาร** เป็นผู้รักษาการให้เป็นไปตามระเบียบนี้ และให้กำหนดการทบทวนระเบียบนี้ ให้มีความทันสมัย อย่างต่อเนื่อง โดยมีวงรอบปีงบประมาณละ ๑ ครั้ง

ข้อ ๗ ระเบียบนี้แบ่งออกเป็น ๒๓ หมวด ดังนี้

หมวด ๑
กล่าวทั่วไป

ข้อ ๘ ความมุ่งหมายของระเบียบนี้

(๑) เพื่อให้เกิดความเชื่อมั่นและมีระบบการรักษาความมั่นคงปลอดภัยการใช้งานในระบบสารสนเทศของกองทัพบกดำเนินงานไปได้อย่างมีประสิทธิภาพ และประสิทธิผล

(๒) เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้มีส่วนเกี่ยวข้องได้แก่ ผู้บังคับบัญชา กำลังพลของหน่วย ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกองทัพบก เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศของกองทัพบก

(๓) เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบสารสนเทศของกองทัพบกยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไปสู่สากล

(๔) เพื่อเป็นมาตรการในการรักษาความปลอดภัยระบบสารสนเทศของกองทัพบก สำหรับการพิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการ รั่วไหลหรือรู้ไปถึง หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่ ป้องกันการจารกรรมทั้งจากบุคคลภายในและภายนอกส่วนราชการ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่เครื่องคอมพิวเตอร์ อุปกรณ์สารสนเทศ เครื่องใช้สำนักงาน อาคาร สถานที่ และเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ เป็นต้น

ข้อ ๙ หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการและแต่งตั้งผู้รับผิดชอบระบบสารสนเทศของส่วนราชการเพิ่มเติมได้โดยให้สอดคล้องและไม่ขัดแย้งกับระเบียบนี้

ข้อ ๑๐ เหตุผลในการประกาศใช้ระเบียบนี้ คือ วางแนวนโยบายและแนวปฏิบัติของกองทัพบก ในการรักษาความปลอดภัยระบบสารสนเทศของกองทัพบกเกี่ยวกับระบบคอมพิวเตอร์ระบบสื่อสารสารสนเทศ ระบบเครือข่ายสารสนเทศ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอก ที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศ ของกองทัพบก

ข้อ ๑๑ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พรบ.ข้อมูลข่าวสารของ ทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

หมวด ๒
การจัดทำโครงการและการจัดหาระบบงาน คอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์
(Application, Computer and Device Project Development and Acquisition)

ข้อ ๑๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องควบคุมการจัดหาระบบงานคอมพิวเตอร์ และอุปกรณ์เครือข่ายและคอมพิวเตอร์ดังนี้

(๑) ต้องเป็นผู้ให้ความเห็นชอบในการจัดทำโครงการด้านระบบสารสนเทศของหน่วยงานภายในต่างๆ ของกองทัพบกเพื่อให้มีความเหมาะสมและเกิดประโยชน์สูงสุดแก่กองทัพบก

(๒) ต้องเป็นผู้ให้ความเห็นชอบสำหรับการจัดหาระบบงาน คอมพิวเตอร์ อุปกรณ์เครือข่ายหรืออุปกรณ์คอมพิวเตอร์ของหน่วยงานภายในของกองทัพบก

(๓) ไม่อนุญาตให้หน่วยงานภายในต่างๆ ของกองทัพบกดำเนินการด้วยตนเองโดยไม่ผ่านความเห็นชอบจากหน่วยรับผิดชอบตามสายงานหรือหน่วยงานที่ได้รับมอบหมายจากผู้บังคับบัญชา

หมวด ๓
การควบคุมการเข้าถึงหรือการใช้งานระบบสารสนเทศ
(Access Control)

ข้อ ๑๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงาน โดยกำหนดเป็นมาตรการทั้ง ๔ ด้าน ดังนี้

(๑) ด้านการเข้าถึงระบบสารสนเทศทั่วไป

(๑.๑) ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบข้อมูลและ/หรือผู้รับผิดชอบระบบงาน ตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

(๑.๒) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่กองทัพบก กำหนดเพื่อขอสิทธิ์ในการเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน

(๑.๓) ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(๒) ด้านการเข้าถึงระบบเครือข่ายสารสนเทศ

(๒.๑) ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบระบบเครือข่ายของกองทัพบกตามสิทธิและความจำเป็นในการเข้าถึงเครือข่ายก่อนที่จะเข้าใช้งาน

(๒.๒ ผู้ดูแลเครือข่ายสารสนเทศของกองทัพบก มีหน้าที่ตรวจสอบการอนุมัติและกำหนดการอนุญาตในการผ่านเข้าสู่เครือข่ายสารสนเทศของกองทัพบก ตามสิทธิ์และความจำเป็นในการปฏิบัติงานเท่านั้น

(๒.๓) ผู้ดูแลเครือข่ายสารสนเทศของกองทัพบก จะต้องจัดให้มีการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน ล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่นๆ อีกด้วย

(๓) ด้านการเข้าถึงระบบปฏิบัติการ

(๓.๑) ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบระบบปฏิบัติ ซึ่งเป็นทรัพสินของกองทัพบก จึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะระบบปฏิบัติงานที่กองทัพบกจัดหามาอย่างถูกต้องตามกฎหมายเท่านั้น

(๓.๒) ผู้รับผิดชอบระบบปฏิบัติงาน มีหน้าหน้าที่ตรวจสอบสิทธิ์อนุญาตให้เข้าใช้งานระบบปฏิบัติงานของผู้ใช้ และควบคุมการใช้งานให้เป็นไปตามสิทธิ์และตามความจำเป็นในการใช้งาน รวมถึงการบันทึกการใช้งานของผู้ใช้ ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน รวมถึงล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่นๆ อีกด้วย

(๔) ด้านการเข้าถึงโปรแกรมประยุกต์ (application)

(๔.๑) ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบโปรแกรมประยุกต์ ซึ่งเป็นทรัพย์สินของกองทัพบก จึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะโปรแกรมประยุกต์ที่กองทัพบกจัดหามาอย่างถูกต้องตามกฎหมายเท่านั้น

(๔.๒) ผู้รับผิดชอบโปรแกรมประยุกต์ มีหน้าหน้าที่ตรวจสอบสิทธิ์อนุญาตให้เข้าใช้งานโปรแกรมประยุกต์ของผู้ใช้ และควบคุมการใช้งานให้เป็นไปตามสิทธิ์และตามความจำเป็นในการใช้งาน รวมถึงการบันทึกการใช้งานของผู้ใช้ ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน รวมถึงล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่นๆ อีกด้วย

ข้อ ๑๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ดังนี้

(๑) การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ที่ปฏิบัติงานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในกองทัพบก เป็นต้น

(๑.๑) ขั้นตอนการลงทะเบียนเจ้าหน้าที่ (user registration)

(๑.๑.๑) หน่วยต้นสังกัดของเจ้าหน้าที่ใหม่ แจ้งข้อมูลการขอลงทะเบียนเจ้าหน้าที่ใหม่เป็นลายลักษณ์อักษรตามสายการบังคับบัญชา ให้ผู้รับผิดชอบระบบสารสนเทศของกองทัพบก

(๑.๑.๒) ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาข้อมูลการขอลงทะเบียนของเจ้าหน้าที่ใหม่ โดยตรวจสอบให้ถูกต้องว่าเป็นเจ้าหน้าที่ของกองทัพบกอย่างแท้จริง และได้รับสิทธิ์ในการใช้งานตามคำร้องขอลงทะเบียนอย่างถูกต้อง

(๑.๑.๓) ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาอนุมัติให้ลงทะเบียนเจ้าหน้าที่ใหม่ และแจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชาและเจ้าหน้าที่ใหม่ทราบต่อไป

(๑.๒) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน

(๑.๒.๑) หน่วยต้นสังกัดของเจ้าหน้าที่ แจ้งข้อมูลการขอยกเลิกสิทธิ์การใช้งานเป็นลายลักษณ์อักษรตามสายการบังคับบัญชา ให้ผู้รับผิดชอบระบบสารสนเทศของกองทัพบก

(๑.๒.๒) ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาข้อมูลการขอยกเลิกสิทธิ์การใช้งานของเจ้าหน้าที่ โดยตรวจสอบให้ถูกต้องว่าเป็นเจ้าหน้าที่ของกองทัพบกอย่างแท้จริง และได้รับการยกเลิกสิทธิ์ในการใช้งานตามคำร้องอย่างถูกต้อง

(๑.๒.๓) ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาอนุมัติให้ยกเลิกสิทธิ์การใช้งานของเจ้าหน้าที่ และแจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชาและเจ้าหน้าที่นั้นทราบต่อไป

(๒) กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

(๓) กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน และถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของผู้ใช้งานต่อไป

(๔) จำกัดการใช้งานบัญชีชื่อผู้ใช้งานแบบกลุ่มซึ่งมีการใช้งานร่วมกัน กล่าวคือ อนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้นและผู้ใช้งานบัญชีแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน

(๕) ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

(๖) จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอเข้าใช้ระบบงานสารสนเทศเพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

(๗) ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

(๗.๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบงานสารสนเทศแยกตามหน่วยงานภายในของกองทัพบก

(๗.๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาที่รับผิดชอบระบบสารสนเทศของหน่วยเพื่อดำเนินการทบทวนว่ามีรายชื่อที่ออกสิทธิเข้าถึงระบบสารสนเทศไปแล้วหรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

(๗.๓) ผู้บังคับบัญชาของหน่วยแจ้งหรืออนุมัติรายชื่อของผู้มีสิทธิในระบบงานสารสนเทศที่ได้รับการแก้ไขให้ถูกต้องแล้ว

(๗.๔) ผู้ดูแลระบบงานสารสนเทศของหน่วยดำเนินการแก้ไขข้อมูลผู้มีสิทธิให้ถูกต้องตามที่ได้รับแจ้งหรือได้รับการอนุมัติ

ข้อ ๑๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่ดังนี้

(๑) ผู้ดูแลระบบ ที่รับผิดชอบระบบนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติโดยต้องกำหนดไว้เป็นลายลักษอักษรอย่างชัดเจน เช่น กำหนดเป็นเอกสารการบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน เป็นต้น

(๒) การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตามเอกสารหรือตามระเบียบที่ทางกองทัพบกกำหนดขึ้น

(๓) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา

(๓.๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๓.๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓.๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

ข้อ ๑๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดวิธีการบริหารจัดการ การเข้าถึงข้อมูลตามระดับชั้นความลับ

(๑) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๒) ผู้ดูแลฐานข้อมูลหรือเจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๓) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

(๔) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะผู้ใช้งานควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

(๕) มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสารหรือตามระเบียบที่ทางกองทัพบกกำหนดขึ้น

(๖) มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกองทัพบก เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๑๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการควบคุมการเข้าใช้งานระบบจากภายนอก หน่วยงานที่มีระบบสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งเอาไว้ภายในหน่วยของตนเอง เพื่อดูแลรักษาความปลอดภัยของระบบภายในจากการเข้าถึงระบบจากภายนอกโดยมีแนวทางปฏิบัติ ดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของกองทัพบก ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของกองทัพบก การควบคุมบุคคลที่เข้าสู่ระบบของกองทัพบกจากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

(๓) ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกองทัพบกอย่างเพียงพอและต้องได้รับอนุมัติจากผู้บังคับบัญชา

(๔) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(๕) การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ(Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ข้อ ๑๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกดังนี้

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของกองทัพบก ต้องผ่านการพิสูจน์ตัวตนจากระบบของกองทัพบกโดยมีแนวทางปฏิบัติดังนี้

(๑) การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

(๒) การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

(๓) การเข้าสู่ระบบสารสนเทศของกองทัพบกจากอินเทอร์เน็ตนั้น จะมีการตรวจสอบผู้ใช้งานด้วย

(๔) การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

หมวด ๔
การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

ข้อ ๑๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดวิธีการบริหารจัดการรหัสผ่าน (user password management) และการใช้งานรหัสผ่าน (password use)ของเจ้าหน้าที่ให้มีความมั่นคงปลอดภัย และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) โดยมีแนวทางปฏิบัติ ดังนี้

(๑) วิธีการบริหารจัดการรหัสผ่าน

(๑.๑) ต้องเก็บรักษารหัสผ่านที่ได้รับให้เป็นความลับ

(๑.๒) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๑.๓) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๑.๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๑.๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(๑.๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๑.๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๑.๘) การกำหนดรหัสผ่านเริ่มต้นให้กับเจ้าหน้าที่ให้ยากต่อการเดา และกำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกันอีกด้วย

(๑.๙) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑.๑๐) เมื่อเจ้าหน้าที่ของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้หน่วยแจ้งผู้รับผิดชอบระบบสารสนเทศทันที เพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิของผู้ที่ลาออกออกจากระบบทันทีที่ได้รับแจ้ง

(๑.๑๑) การส่งมอบรหัสผ่านให้กับเจ้าหน้าที่ต้องเป็นไปอย่างปลอดภัยโดยใส่ซองปิดผนึก และประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และ แนบเอกสารการได้รับอนุญาตจากผู้บังคับบัญชา รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

(๒) การใช้งานรหัสผ่าน

(๒.๑) ผู้ใช้งานต้องใช้งานรหัสผ่านของตนเองหรือตามที่ได้รับอนุมัติเท่านั้น

(๒.๒) ผู้ใช้งานรหัสผ่านต้องปฏิบัติให้เป็นไปตามวิธีการบริหารจัดการรหัสผ่านอย่างเคร็งครัด

(๒.๓) กรณีต้องการยกเลิกหรือเปลี่ยนแปลงรหัสผ่านให้แจ้งเป็นลายลักษณ์อักษรตามสายการบังคับบัญชาให้ผู้รับผิดชอบดำเนินการต่อไป

(๒.๔) ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่าน

(๒.๕) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

(๒.๖) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่า การกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

(๒.๗) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกองทัพบก และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(๒.๗.๑) คอมพิวเตอร์โน๊ตบุ๊ค (Notebook) ต้องทำการพิสูจน์ตัวตนในระดับไบออส (BIOS) ก่อนการใช้งาน

(๒.๗.๒) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒.๗.๓) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒.๗.๔) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๒.๗.๕) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๒.๗.๖) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

(๓) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

(๓.๑) ผู้ดูแลระบบ (System Administrator) เป็นผู้รับผิดชอบในการทบทวนสิทธิ์การถึงของผู้ใช้งาน

(๓.๒) วงรอบการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานให้ทบทวนทุกๆ ๖ เดือน หรือเมื่อการเกิดการเปลี่ยนแปลงสิทธิ์ของผู้ใช้ ได้แก่ การลาออก การย้ายหน่วย เป็นต้น อีกทั้งการทบทวนสิทธิ์ต้องพิจารณาถึงพฤติกรรมการทำงานของผู้ใช้ รวมทั้งถ้ามีการเปลี่ยนแปลงของระบบงานใหม่ จะต้องมีการทบทวนสิทธิ์การใช้งานทุกครั้งอีกด้วย

(๓.๓) การทบทวนสิทธิ์ผู้ดูแลระบบ จะต้องแจ้งรายงานการทบทวนสิทธิ์ เป็นลายลักษณ์อักษรให้ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกอนุมัติให้ดำเนินการต่อไป

หมวด ๕
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and environmental security)

ข้อ ๒๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการรักษาความปลอดภัยทางกายภาพ (Physical security management)

(๑) กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นใช้งาน

(๒) พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในโดยเฉพาะศูนย์สารสนเทศกลาง (Data Center) ให้ติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

(๓) มีระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

(๔) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบยังใช้งานได้ตามปกติ

(๕) บุคลากรของกองทัพบกควรปิดประตูและหน้าต่างให้ล็อคอยู่เสมอ

(๖) ถ้าตรวจพบอุปกรณ์สารสนเทศ ที่ถูกละทิ้งโดยไม่มีผู้ใช้อยู่ในบริเวณใกล้เคียงให้รีบแจ้งผู้รับผิดชอบ ดำเนินการเก็บอุปกรณ์ดังกล่าวในสถานที่ปลอดภัย เพื่อป้องกันการโจรกรรม หรือลักลอบขโมยข้อมูลจากผู้ไม่ประสงค์ดีต่อไป

ข้อ ๒๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดการควบคุมการเข้า-ออก (Physical entry controls) ดังนี้

(๑) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

(๒) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๓) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๔) สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๕) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๖) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๗) มีการพิสูจน์ตัวตน เช่น การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะในศูนย์สารสนเทศกลาง (Data Center)

(๘) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญโดยเฉพาะศูนย์สารสนเทศกลาง (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๙) บุคคลภายนอก เช่น เจ้าหน้าที่บริษัท, นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่นๆต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๑๐) ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๑๑) ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๒) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

ข้อ ๒๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบสิ่งอุปกรณ์โดยบุคคลภายนอก (Public access, delivery, and loading areas) ดังนี้

(๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายสิ่งอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

(๓) จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในระบบสารสนเทศของหน่วย

(๔) ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

(๕) ตรวจนับและลงทะเบียนหรือขึ้นบัญชีคุมสิ่งอุปกรณ์ที่ส่งมอบโดยผู้ถูกจ้าง ผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการสิ่งอุปกรณ์ของกองทัพบก

ข้อ ๒๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการจัดวางและการป้องกันอุปกรณ์ (Equipment Sitting and Protection) ดังนี้

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในห้องศูนย์สารสนเทศกลาง (Data Center) ให้น้อยที่สุด

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่ความมั่นคงปลอดภัย

(๓) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในศูนย์สารสนเทศกลาง (Data Center)

(๔) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติหรือไม่

ข้อ ๒๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ดังนี้

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

(๑.๑) ระบบสำรองกระแสไฟฟ้า (UPS)

(๑.๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

(๑.๓) ระบบระบายอากาศ

(๑.๔) ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๒๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดและควบคุมการเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security) ดังนี้

(๑) เครือข่ายของกองทัพบกในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณเพื่อทำให้เกิดความเสียหายและป้องกันสัตว์ต่างๆ กัดสาย เช่น หนู เป็นต้น

(๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๓) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๔) จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๕) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ ๒๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการบำรุงรักษาอุปกรณ์ (Equipment Maintenance) ดังนี้

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วย

(๖) ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๗) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๒๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องควบคุมและกำหนดขั้นตอนการนำสิ่งอุปกรณ์ของกองทัพบกออกนอกหน่วยงาน (Removal of Property) ดังนี้

(๑) ให้มีการขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วย

(๒) บันทึกข้อมูลการนำสิ่งอุปกรณ์ของกองทัพบกออกนอกหน่วย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๒๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบกออกไปใช้งานนอก

(๒) ไม่ทิ้งสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบกไว้โดยลำพังในที่สาธารณะ

(๓) ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๒๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องควบคุมการจำหน่ายสิ่งอุปกรณ์หรือการนำสิ่งอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment) ดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในสิ่งอุปกรณ์ก่อนที่จะดำเนินการจำหน่ายสิ่งอุปกรณ์ดังกล่าว และดูแนวทางปฏิบัติในการทำลายสื่อบันทึกข้อมูลในหมวด ๘

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวด ๖
การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ
(Communications and Operations Management)

ข้อ ๓๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures) ดังนี้

(๑) จัดทำขั้นตอนปฏิบัติอย่างเป็นลายลักษณ์อักษรสำหรับภารกิจการปฏิบัติงานกับระบบเทคโนโลยีสารสนเทศดังต่อไปนี้

(๑.๑) การปฏิบัติงานในห้องเครื่องคอมพิวเตอร์ที่ให้บริการหรือศูนย์สารสนเทศกลาง (Data Center)

(๑.๒) การเปิดและปิดระบบงานเช่น การเปิด-ปิดเครื่อง เปิด-ปิดระบบงาน เปิด-ปิดระบบให้บริการ เป็นต้น

(๑.๓) การสำรองข้อมูล

(๑.๔) การบำรุงรักษาอุปกรณ์

(๑.๕) การจัดการกับสื่อบันทึกข้อมูล เช่น การทำป้ายชื่อบ่งชี้ การลบ ทั้งการป้องกันการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง เป็นต้น

(๑.๖) การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้น

(๑.๗) การประมวลผลข้อมูล เช่น ขั้นตอนในการนำข้อมูลเข้าระบบงานประมวลผล และแสดงผล เป็นต้น

(๑.๘) การใช้งานโปรแกรมอรรถประโยชน์ต่างๆ (Utilities)

(๑.๙) การรายงานและการจัดการกับปัญหาที่เกิดขึ้น

(๑.๑๐) การจัดการกับการทำงานล้มเหลวและความผิดพลาดของระบบคอมพิวเตอร์ ระบบงาน และระบบเครือข่าย

(๑.๑๑) การกู้คืนระบบงานและระบบเครือข่าย

(๒) กำหนดผู้รับผิดชอบและผู้มีอำนาจในการควบคุมการดำเนินการในการจัดทำเอกสารขั้นตอนการปฏิบัติข้างต้น และให้มีการปรับปรุงเอกสารอย่างสม่ำเสมอ

ข้อ ๓๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบเทคโนโลยีสารสนเทศดังนี้

(๑) กำหนดขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงต่อระบบเทคโนโลยีสารสนเทศของกองทัพบก เช่น ซอฟต์แวร์ ฮาร์ดแวร์ของระบบงาน ซอฟต์แวร์ระบบปฏิบัติการ เป็นต้น ควรมีขั้นตอนการดำเนินการดังต่อไปนี้

(๑.๑) ระบุและบันทึกระดับผลกระทบและความเร่งด่วนของการเปลี่ยนแปลงที่ขออนุมัติ เช่น มากหรือน้อย เป็นต้น

(๑.๒) บันทึกรายละเอียดการดำเนินการที่เกี่ยวข้องเพื่อใช้เป็นหลักฐาน

(๑.๓) กำหนดให้มีการวางแผนการดำเนินการ

(๑.๔) กำหนดให้มีการทดสอบตามความจำเป็น

(๑.๕) กำหนดให้มีการแจ้งผู้ที่เกี่ยวข้องทั้งหมด

(๑.๖) กำหนดให้มีการวางแผนหรือขั้นตอนปฏิบัติสำหรับการถอยหลังกลับสำหรับกรณีที่ทำแล้วไม่สำเร็จ

(๑.๗) กำหนดผู้มีอำนาจในการอนุมัติให้ดำเนินการในการปรับปรุงหรือแก้ไขขั้นตอนปฏิบัติดังกล่าว

ข้อ ๓๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties) ดังนี้

(๑) กำหนดให้การปฏิบัติงานที่มีความสำคัญ แยกหน้าที่ความรับผิดชอบออกจากกันและมีผู้ปฏิบัติงานมากกว่าหนึ่งคน

(๒) ป้องกันไม่ให้งานที่มีความสำคัญสามารถดำเนินการได้ตั้งแต่ต้นจนจบได้ด้วยบุคคลเพียงคนเดียว

(๓) ให้ผู้บังคับบัญชามีการสอดส่องดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย

(๔) ให้มีการจัดเก็บหลักฐานที่สามารถใช้ตรวจสอบได้ในภายหลัง สำหรับงานที่มีความเสี่ยง

ข้อ ๓๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Test, and Operational Facilities) ดังนี้

(๑) ให้พิจารณาการแยกเครื่องคอมพิวเตอร์ของระบบงานและมาตรการเพื่อใช้ในการแยกเครื่องคอมพิวเตอร์สำหรับการพัฒนา การทดสอบและการให้บริการออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงานที่มีต่อกัน

(๒) กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องคอมพิวเตอร์ที่ใช้สำหรับการพัฒนาไปสู่เครื่องที่ใช้สำหรับการให้บริการ

(๓) ให้มีการป้องกันการเข้าถึงโปรแกรมอรรถประโยชน์ เช่น ซอฟต์แวร์ทูลและยูทิลิตี้ เป็นต้น ที่ใช้สำหรับการพัฒนาระบบงานโดยไม่ได้รับอนุญาตในการเข้าถึงโปรแกรมฯ ดังกล่าวบนเครื่องคอมพิวเตอร์สำหรับการพัฒนา

(๔) กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกันสำหรับระบบงานที่ใช้ในการพัฒนา ทดสอบและให้บริการจริง

ข้อ ๓๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดให้มีการตรวจสอบและติดตามการใช้ทรัพยากรของระบบและเครือข่ายคอมพิวเตอร์ ดังนี้

(๑) จัดทำแผนการตรวจสอบและติดตามทรัพยากรของระบบสารสนเทศ ดังนี้

(๑.๑) กำหนดประเภทของข้อมูลที่ใช้ในการตรวจสอบและติดตามการใช้ทรัพยากรของระบบ เช่น ร้อยละของการใช้ซีพียู ร้อยละของการใช้หน่วยความจำ ร้อยละของการใช้พื้นที่ฮาร์ดดิสก์ และร้อยละของปริมาณการใช้เครือข่าย เป็นต้น

(๑.๒) กำหนดค่าปริมาณการใช้ทรัพยากรสูงสุดบนระบบที่ยอมรับได้ ค่าต่างๆ เหล่านี้ใช้สำหรับเป็นจุดในการแจ้งเตือนว่าระบบสารสนเทศได้มีการใช้ทรัพยากรมาจนถึงค่าสูงสุดที่ยอมรับได้แล้วหรือไม่ เช่น กำหนดไว้ที่ร้อยละ ๘๐ ของการใช้ซีพียู เป็นต้น

(๑.๓) กำหนดความถี่ในการเข้าตรวจสอบปริมาณการใช้ทรัพยากรของระบบสารสนเทศ สำหรับระบบที่มีความสำคัญจากมากไปน้อย ให้กำหนดแผนการตรวจสอบและติดตามทรัพยากร

ของระบบด้วยความถี่ในการตรวจสอบจากสูงไปต่ำ เช่น ระบบที่มีความสำคัญมากควรมีความถี่ในการตรวจสอบสูงกว่าระบบที่มีความสำคัญปานกลางและน้อย เป็นต้น

(๒) ติดตามและตรวจสอบทรัพยากรของระบบตามแผนการตรวจสอบและติดตามทรัพยากรของระบบฯ ที่ได้กำหนดไว้เพื่อดูว่ายังมีทรัพยากรเพียงพอต่อการให้บริการหรือไม่

(๓) รายงานข้อมูลผลการติดตามการใช้ทรัพยากรของระบบสารสนเทศ เช่น สถิติปริมาณการใช้ซีพียู หน่วยความจำ ฮาร์ดดิสก์ และปริมาณเครือข่ายคอมพิวเตอร์ ให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

(๔) ประเมินความต้องการทรัพยากรของระบบสารสนเทศที่ต้องการเพิ่มเติมเพื่อนำไปใช้ในการวางแผนปรับปรุงประสิทธิภาพและขีดความสามารถของระบบต่อไป

หมวด ๗
การป้องกันชุดคำสั่งไม่พึงประสงค์
(Protection Against Malicious Code)

ข้อ ๓๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อป้องกันชุดคำสั่งไม่พึ่งประสงค์ดังนี้

(๑) ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้แฟ้มข้อมูล (File) อื่นที่กองทัพบกไม่อนุญาตให้ใช้งาน

(๒) ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอเพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

(๓) ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ให้กับระบบเทคโนโลยีสารสนเทศของกองทัพบก

(๔) ให้ผู้ดูแลระบบดำเนินการตรวจสอบชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ที่ให้บริการและอุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ในบริเวณจุดทางเข้า-ออกเครือข่ายอย่างสม่ำเสมอเพื่อดักจับชุดคำสั่งไม่พึ่งประสงค์ที่จะเข้าสู่ระบบ

(๕) กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับชุดคำสั่งไม่พึงประสงค์ได้แก่การรายงานการเกิดขึ้นของชุดคำสั่งไม่พึงประสงค์ การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่ตรวจพบ เป็นต้น

(๖) มีการติดตามข้อมูลข่าวสารเกี่ยวกับชุดคำสั่งไม่พึงประสงค์อย่างสม่ำเสมอ

(๗) ให้มีการสร้างความตระหนักเกี่ยวกับชุดคำสั่งไม่พึงประสงค์เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุชุดคำสั่งไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร รวมทั้งให้หน่วยมีการจัดการฝึกอบรมสร้างความตระหนักอย่างน้อยปีละ ๑ ครั้ง

หมวด ๘
การจัดการเข้าถึงข้อมูลสารสนเทศและโปรแกรมประยุกต์

ข้อ ๓๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการจัดการกับข้อมูลในแต่ละชั้นความลับ ดังนี้

(๑) กำหนดระดับชั้นความลับของข้อมูลซึ่งอย่างน้อยประกอบด้วย ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายใน และข้อมูลลับ

(๒) กำหนดแนวทางในการจัดหมวดหมู่ข้อมูลเป็นชั้นความลับที่เหมาะสมซึ่งควรพิจารณาจัดหมวดหมู่จาก

(๒.๑) แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับก็จะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับก็จะเป็นประเภทเปิดเผยได้ เป็นต้น

(๒.๒) วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านระบบงบประมาณของหน่วย ดังนั้นข้อมูลนี้จะอยู่ในประเภทลับ เป็นต้น

(๒.๓) จำนวนบุคคลที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

(๒.๔) ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการงบประมาณ ด้านการไม่ปฏิบัติตามกฎระเบียบข้อบังคับที่หน่วยกำหนดต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้นข้อมูลจะสามารถจัดอยู่ในประเภทใช้ภายในเท่านั้น หรือประเภทชั้นความลับ เป็นต้น

(๓) กำหนดขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับ ขั้นตอนฯ ควรประกอบด้วย การควบคุมการประมวลผล การควบคุมการเข้าถึง การจัดเก็บ การจัดการกับสื่อบันทึกข้อมูล การทำป้ายบ่งชี้ และการสื่อสารข้อมูลอย่างมั่นคงปลอดภัย

(๔) กำหนดให้มีการจำกัดการเข้าถึงข้อมูลสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๕) กำหนดมาตรการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลสำคัญที่ยังคงค้างอยู่บนสื่อบันทึกข้อมูลนั้น โดยอาจปฏิบัติตามแนวทางดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การตัดด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้การตัดด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตาม **มาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M** (ซึ่งมีการฟอร์แม็ตเป็นจำนวนหลายรอบ)

(๖) กำหนดมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

(๗) กำหนดมาตรการป้องกันข้อมูลสำคัญที่มีการสั่งพิมพ์ออกมาทางเครื่องพิมพ์เพื่อป้องกันการเข้าถึงโดยผู้อื่น

(๘) จัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

(๙) มาตรการในการนำวิธีการเข้ารหัสมาใช้กับข้อมูลชั้นความลับ ให้ปฏิบัติตาม ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ และระเบียบกองทัพบกว่าด้วยการรักษาความปลอดภัยทางการอักษรลับ พ.ศ.๒๕๑๕

ข้อ ๓๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System Documentation) ดังนี้

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

ข้อ ๓๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดนโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures) ดังนี้

(๑) จัดทำนโยบายหรือแนวทางการใช้อย่างเหมาะสมสำหรับการใช้งานระบบหรืออุปกรณ์ที่ใช้ในการสื่อสารข้อมูลระหว่างกองทัพบก เช่น ห้ามใช้เพื่อก่อความรำคาญแก่ผู้อื่น ทำให้ผู้อื่นสูญเสียชื่อเสียง ปลอมเป็นบุคคลอื่น เป็นต้น

(๒) มีวิธีการทางเทคนิคป้องกันข้อมูลสำคัญจากการถูกเข้าถึง ถูกเปลี่ยนแปลงแก้ไข ถูกสวมรอยโดยผู้อื่น ถูกเปิดเผยความลับ โดยไม่ได้รับอนุญาต

(๓) จัดทำแนวทางสำหรับการจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารโต้ตอบ และแนวทางควรสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่หน่วยต้องปฏิบัติตาม

ข้อ ๓๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements) ดังนี้

ควรจัดทำแนวทางข้อตกลงสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายในกับหน่วยงานภายนอกดังต่อไปนี้

(๑) กำหนดนโยบายขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง วิธีการรับ เป็นต้น

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบ

(๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิการเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ข้อ ๔๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดระบบงานสารสนเทศทางตามภารกิจที่ได้รับมอบที่มีการเชื่อมโยงถึงกัน พิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างหน่วยภายในกองทัพบก หรือหน่วยงานอื่นๆที่จะมาขอเชื่อมโยงกับกองทัพบก เป็นต้นดังนี้

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีกำลังพลใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลที่กำหนดชั้นความลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ข้อ ๔๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการหมดเวลาหรือหมดอายุการใช้งานระบบสารสนเทศ (Session Time-Out) ดังนี้

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดการติดต่อและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดการติดต่อและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานที่มีข้อมูลสำคัญ ระบบงานที่กำหนดชั้นความลับ เป็นต้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๓) แนวทางปฏิบัติดังนี้

(๓.๑) เมื่อผู้ใช้งานไม่ได้ใช้งานหรือว่างเว้นจากการใช้งานในระยะเวลา ๕ นาทีหรือตามที่ผู้รับผิดชอบกำหนด ให้มีการตัดการเชื่อมต่อการใช้งานออกจากระบบสารสนเทศโดยอัตโนมัติ

(๓.๒) ถ้ามีความพยายามเข้าสู่ระบบใหม่ ให้ยืนยันการใช้งานโดยใส่ชื่อผู้ใช้ (username) และรหัสผ่าน (password) หรือวิธีการที่ปลอดภัยในการยืนยันตัวบุคคลในทุกๆ ครั้ง

ข้อ ๔๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time) ดังนี้

(๑) กำหนดให้ระบบงานสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น

(๒) กำหนดให้ระบบงานสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วย) ระบบงานที่กำหนดชั้นความลับ เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อเพื่อป้องกันบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึงข้อมูลได้โดยง่าย

(๓) แนวทางปฏิบัติดังนี้

(๓.๑) การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพบก กำหนดให้ใช้งานได้ ๒ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หรือตามที่ผู้บังคับบัญชาเห็นสมควร

(๓.๒) การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพบก กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น

(๓.๓) การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพบก ถ้ากระทำในช่วงนอกเวลาทำงานตามปกติ ต้องได้รับอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ ๔๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดคุณสมบัติของการล็อกอิน (Login) ที่มีความมั่นคงปลอดภัยสำหรับระบบงานสารสนเทศ สำหรับเครื่องคอมพิวเตอร์ให้บริการหรืออุปกรณ์เครือข่ายคอมพิวเตอร์ที่หน่วยรับผิดชอบ ดังนี้

(๑) ไม่มีหรือไม่แสดงฟังก์ชั่น (Function) ให้การช่วยเหลือในระหว่างที่ทำการล็อกอิน (Login)

(๒) บันทึกความพยายามในการล็อกอินทั้งที่สำเร็จและไม่สำเร็จและแสดงประวัติการล็อกอิน ๓ ครั้งล่าสุด

(๓) ตัดการเชื่อมต่อหลังจากที่ทำการล็อกอินไม่สำเร็จเกินกว่า ๓ ครั้ง

(๔) เมื่อมีการใส่ข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความรวมๆ เช่น “ข้อมูลการล็อกอิน ไม่ถูกต้อง”

(๕) ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของกองทัพบก การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงาน หากมีการตรวจพบ อาจมีการลงโทษทางวินัยหรือดำเนินการทางกฎหมายตามความเหมาะสม กองทัพบกมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”

(๖) ไม่แสดงรายละเอียดของระบบใดๆ จนกว่าจะล็อกอินสำเร็จ

ข้อ ๔๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging) ของระบบงานภายในกองทัพบกดังนี้

จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งานข้อมูลโดยการจัดเก็บ Audit Log เป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้ เพื่อตรวจสอบว่าใครเข้ามาใช้งานระบบ การตรวจสอบการบุกรุกรวมไปถึงการตรวจสอบข้อผิดพลาดที่เกิดขึ้น โดยจัดทำรายงานเบื้องต้นสรุปข้อมูลว่า ใคร (Who) ทำอะไร (What) เมื่อไหร่ (When) ที่ไหน (Where) และอย่างไร (How) ดังนั้นข้อมูลที่ควรจัดเก็บมีดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้ระบบงาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบงาน

(๓) ข้อมูลวันเวลาที่ออกจากระบบงาน

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลชื่อเครื่องคอมพิวเตอร์ที่ใช้งาน

(๖) ข้อมูลการเข้าถึงระบบ (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลความพยายามในการเข้าถึงทรัพยากร เช่น ข้อมูลบัญชีผู้ใช้ฐานข้อมูลสำคัญของระบบงาน เป็นต้น ทั้งที่สำเร็จและไม่สำเร็จ

(๘) ข้อมูลการเปลี่ยนแปลงสิ่งแวดล้อมหรือการกำหนดค่า (Configuration) ของระบบงาน

(๙) ข้อมูลแสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบ เป็นต้น

(๑๐) ข้อมูลแสดงการใช้งานโปรแกรมประยุกต์ (Application Program)

(๑๑) ข้อมูลแสดงการเข้าถึงแฟ้มข้อมูล (File) และการกระทำกับแฟ้มข้อมูล (File) เช่น เปิด ปิด เขียน อ่านแฟ้มข้อมูล เป็นต้น

(๑๒) ข้อมูลไอพีแอดเดรสที่เข้าถึง

(๑๓) ข้อมูลโพรโตคอลของเครือข่ายที่ใช้งาน

(๑๔) ข้อมูลการแจ้งเตือนเกี่ยวกับการเข้าถึงระบบจากการบุกรุก

(๑๕) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

(๑๖) ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญๆ

(๑๗) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

หมวด ๙
การบริหารจัดการการเข้าถึงระบบเครือข่ายสื่อสารข้อมูล

ข้อ ๔๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดมาตรการทางเครือข่ายสื่อสารข้อมูล (Network Controls)

กำหนดมาตรการทางเครือข่ายสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่าย ระบบงาน หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

(๑) กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

(๒) กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานและอุปกรณ์ที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

(๓) กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

(๔) กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

(๕) กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

(๖) มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

(๗) มีการใช้ฮาร์ดแวร์หรือซอฟต์แวร์ สำหรับการบริหารจัดการเครือข่าย เพื่อระบุ เฝ้าตรวจ ติดตามสถานะ อุปกรณ์ในระบบสารสนเทศของกองทัพบก

ข้อ ๔๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการเข้าถึงระบบเครือข่ายดังนี้

(๑) ผู้ดูแลระบบ ต้องมีการออกแบบแบ่งระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น เขตภายใน (Internal Zone) เขตภายนอก (External Zone) เป็นต้น เพื่อเป็นการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

(๒) ผู้ดูแลระบบ ควรดำเนินการแยกและติดตั้ง เครื่องคอมพิวเตอร์ให้บริการไว้ในวงเครือข่ายที่แยกต่างหากจากวงเครือข่ายของผู้ใช้งาน และใช้ Firewall หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อจำกัดให้เฉพาะกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้น จึงจะสามารถเชื่อมต่อเข้าไปยังเครื่องคอมพิวเตอร์ให้บริการนั้นได้ และสำหรับแนวทางปฏิบัติการใช้งานของไฟร์วอลล์ (Firewall) ของกองทัพบก มีดังนี้

(๒.๑) ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

(๒.๒) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

(๒.๓) ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

(๒.๔) ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

(๒.๕) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

(๒.๖) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

(๒.๗) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

(๒.๘) การกำหนดระเบียบในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางกองทัพบกอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากกองทัพบกก่อน

(๒.๙) การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

(๒.๑๐) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

(๒.๑๑) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

(๒.๑๒) ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(๒.๑๓) การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

(๒.๑๔) ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตหรือเชื่อมต่อเครือข่ายภายในโดยทันที

(๓) การเข้าสู่ระบบเครือข่ายภายในของกองทัพบก โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี

(๔) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๕) ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

(๖) ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ เช่น ในการเชื่อมต่อเข้าสู่เครื่องคอมพิวเตอร์ให้บริการเพื่อบริหารจัดการระบบ ให้กำหนดเฉพาะชุดไอพีแอดเดรสของผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงเครื่องคอมพิวเตอร์ให้บริการนั้นได้

(๗) ผู้ดูแลระบบ ตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๘) กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๙) ระบบเครือข่ายทั้งหมดของหน่วยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วย ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ เป็นต้น

(๑๐) มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง และสำหรับแนวทางปฏิบัติการใช้งานของอุปกรณ์ป้องกันการบุกรุก (IDS/IPS) ดังนี้

(๑๐.๑) เป็นการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในของกองทัพบก ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

(๑๐.๒) ให้ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกองทัพบกและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ทั้งที่เชื่อมต่อสู่เครือข่ายภายนอก และเครือข่ายภายในทุกเส้นทาง

(๑๐.๓) ระบบทั้งหมดที่สามารถเข้าถึงได้จากเครือข่ายภายนอกหรือเครือข่ายสาธารณะต่างๆ จะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

(๑๐.๔) ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

(๑๐.๕) โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

(๑๐.๖) มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

(๑๐.๗) มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

(๑๐.๘) IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

(๑๐.๙) เครื่องคอมพิวเตอร์ที่ให้บริการที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

(๑๐.๑๐) พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

(๑๐.๑๑) พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

(๑๐.๑๒) การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

(๑๐.๑๓) มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผนเผชิญเหตุที่เกิดขึ้น

(๑๐.๑๔) ผู้ดูแลระบบมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

(๑๐.๑๕) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดระเบียบของกองทัพบก การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของกองทัพบก จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมายต่อไป

(๑๑) การเข้าสู่ระบบงานเครือข่ายภายในหน่วย ผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

(๑๒) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ (IP Address) ภายใน (Local) ของระบบงานเครือข่ายภายในของหน่วย จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศของหน่วยได้โดยง่าย

(๑๓) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๔) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๕) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศของหน่วย และจะต้องจัดทำเป็นบัญชีไว้สำหรับระบุอุปกรณ์บนเครือข่ายได้

(๑๖) การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อยกว่า ๓ เดือน หรือไม่ต่ำกว่า ๙๐ วัน

(๑๗) มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

หมวด ๑๐
การควบคุมการพัฒนาหรือจัดหาระบบงาน
(Control of Application Development or Acquisition)

ข้อ ๔๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัยเพียงพอ ดังนี้

(๑) ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อยควรมี

(๑.๑) คุณสมบัติของการล็อกอินเข้าสู่ระบบงานที่มีความมั่นคงปลอดภัย ตามหมวด ๘

(๑.๒) การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับเข้าถึงระบบงานสารสนเทศตามหมวด ๔

(๑.๓) การเข้ารหัสข้อมูลสำคัญที่มีการรับ-ส่งข้อมูลระหว่างเครื่องผู้ใช้งานกับเครื่องคอมพิวเตอร์ให้บริการ

(๑.๔) การเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

(๑.๕) การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ - ๓๐ นาที เป็นต้น

(๑.๖) การบันทึกบัญชีชื่อผู้ใช้งานที่ล็อกอินเข้าระบบ หมายเลขไอพีแอดเดรส วันเวลาที่เข้าใช้ระบบ ความสำเร็จหรือไม่สำเร็จในการล็อกอินของผู้ใช้งาน

(๒) พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้

(๓) พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

(๔) กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบ นำเสนอแผนดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้ผู้บังคับบัญชาได้รับทราบเพื่อให้คำแนะนำในการปรับปรุงต่างๆ ที่จำเป็น แผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

(๔.๑) แผนการทดสอบ UAT (User Acceptance Test)

(๔.๒) แผนการทดสอบ System Integration Test

(๔.๓) แผนการทดสอบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Test)

(๕) ไม่อนุญาตการนำข้อมูลสำคัญของกองทัพบกไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชาระดับสูงก่อน และหากเป็นไปได้ ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

หมวด ๑๑
การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์ที่ให้บริการ (Server)

ข้อ ๔๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ (Control of operational software)

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของหน่วยเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วย

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๕) กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงาน เป็นต้น

(๖) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

(๗) ทำการปรับปรุงไลบรารี่สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกับทั้งหมดที่การติดตั้ง

(๘) ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จ จะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

(๙) ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

(๑๐) ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่นๆ

(๑๑) สำหรับซอฟต์แวร์ที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

(๑๒) ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

(๑๓) สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้

(๑๔) ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่างๆ (Patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

(๑๕) ตรวจสอบและปิดพอร์ต (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

(๑๖) จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

(๑๗) จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้น จึงจะสามารถเชื่อมต่อเพื่อเข้าสู่ระบบงานที่ทำการติดตั้งนั้น

ข้อ ๔๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes) ดังนี้

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้าน งบประมาณที่จำเป็นต้องใช้ ในกรณีที่กองทัพบกต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

หมวด ๑๒
การจ้างงานหน่วยงานภายนอกให้บริการด้านเทคโนโลยีสารสนเทศ
(Information Technology Service Delivery)

ข้อ ๕๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางการควบคุมการจ้างงานสำหรับการให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ดังนี้

(๑) จัดให้มีการควบคุมโครงการที่มีการจัดจ้างดำเนินการโดยหน่วยงานภายนอก

(๒) กำหนดให้มีการประเมินและจัดทำแผนการลด ความเสี่ยงสำหรับกรณีการเข้าถึงระบบงานหรือสารสนเทศโดยหน่วยงานภายนอก โดยปฏิบัติตามแนวทางการประเมินตามหมวด ๒๑

(๓) กำหนดให้มีการอ้างอิงข้อปฏิบัติที่เกี่ยวข้องในระเบียบของกองทัพบกฉบับนี้ไว้ในสัญญาจ้างเพื่อให้ผู้รับจ้างปฏิบัติตามอย่างเคร่งครัด

(๔) กำหนดให้มีการทำสัญญาการไม่เปิดเผยข้อมูลสำคัญที่ได้รับจากกองทัพบกให้แก่ผู้อื่น

(๕) สำหรับบริการต่างๆ ที่เป็นงานให้บริการตามวงรอบระยะเวลาที่กำหนดไว้ หรือตามคำร้องขอจากหน่วยงานผู้ว่าจ้าง เช่น บริการบำรุงรักษาฮาร์ดแวร์ บริการแก้ไขปัญหาฮาร์ดแวร์ บริการแก้ไขปัญหาระบบงาน บริการจ้างในลักษณะ Help Desk ให้กำหนดรายละเอียดการบริการหรือตามที่กองทัพบกกำหนด ลงไว้ในสัญญาจ้างดังนี้

(๕.๑) รายละเอียดของบริการ

(๕.๒) ระดับการให้บริการ (Service Level Agreement)

(๕.๓) ผู้รับผิดชอบในการเฝ้าระวังหรือติดตามการให้บริการ

(๕.๔) วิธีการติดตามการให้บริการ

(๕.๕) วงรอบระยะที่ชัดเจนของการทบทวนการปฏิบัติงาน เช่น ทุกๆ ๓ เดือน เป็นต้น

(๕.๖) รูปแบบของรายงานที่ต้องการและความถี่ในการจัดส่งรายงาน

(๖) กำหนดให้มีการติดตามการให้บริการตามข้อ (๕)อย่างสม่ำเสมอ และบันทึกผลการติดตามนั้นไว้ด้วย

(๗) ทบทวนการให้บริการตามข้อ (๕) จากผลการปฏิบัติงานในช่วงเวลาที่ผ่านมาหรือผลที่ได้บันทึกไว้ ร้องขอให้ผู้ให้บริการปรับปรุงการให้บริการเพิ่มเติมตามที่ต้องการ และ/หรือ แก้ไขสัญญาจ้างตามความเหมาะสมและจำเป็น

(๘) กรณีการจ้างพัฒนาซอฟต์แวร์หรือระบบงานโดยหน่วยงานภายนอก (Outsourced software development) ให้ปฏิบัติตามแนวทางดังนี้

(๘.๑) กำหนดให้มีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของซอฟต์แวร์หรือระบบงานที่จะทำการพัฒนา ขึ้นมาอย่างเป็นลายลักษณ์อักษร

(๘.๒) ควรพิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนาซอฟต์แวร์ที่มีการจัดจ้างดำเนินการจากผู้รับจ้างภายนอก

(๘.๓) ควรพิจารณากำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้รับจ้างภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้รับจ้างภายนอกนั้น

(๘.๔) ให้มีการตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์ในซอฟต์แวร์ต่างๆ ที่ถูกพัฒนาขึ้นก่อนดำเนินการติดตั้งหรือทดสอบการใช้งานจริง

หมวด ๑๓
การตรวจสอบการใช้งานระบบ
(Monitoring System Use)

ข้อ ๕๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่ใช้งานเพื่อกำหนดแนวทางในการเฝ้าระวังและดูแลระบบเหล่านั้น และกำหนดให้มีการเฝ้าระวังและดูแลระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกฎหมายระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่หน่วยต้องปฏิบัติตามอย่างสม่ำเสมอ โดยการตรวจสอบดังต่อไปนี้

(๑) ชื่อบัญชีผู้ใช้งาน

(๒) กิจกรรมการใช้งานและประเภทของกิจกรรม

(๓) วัน/เวลาที่เข้าถึง

(๔) แฟ้มข้อมูลหรือข้อมูลที่ถูกเข้าถึง

(๕) โปรแกรมทั่วไปและอรรถประโยชน์ต่างๆ (Utilities) ที่ถูกเรียกใช้งาน

(๖) การใช้บัญชีผู้ใช้งานในระดับสูง เช่น Supervisor, Root, Administrator เป็นต้น

(๗) การเปิด-ปิดการทำงานของระบบ

(๘) การถอดถอนหรือติดตั้งอุปกรณ์สำหรับนำเข้าและส่งออกข้อมูล (I/O) เช่น ฮาร์ดดิสก์ เป็นต้น

(๙) การใช้คำสั่งของผู้ใช้งานที่ได้รับการปฏิเสธโดยระบบ เช่น พยายามใช้คำสั่งทั้งที่ไม่มีสิทธิ การพยายามเข้าถึงระบบอย่างไม่ถูกต้อง เป็นต้น

(๑๐) ความพยายามในการเข้าถึงข้อมูลหรือทรัพยากรของระบบที่ได้รับการปฏิเสธโดยระบบ

(๑๑) การแจ้งเตือนจากไฟร์วอลล์หรือระบบป้องกันการบุกรุก

(๑๒) การแจ้งเตือนจากอุปกรณ์แจ้งเตือน (Console) ของผู้ดูแลระบ

(๑๓) การแจ้งเตือนเมื่อระบบทำงานผิดปกติ เช่น ฮาร์ดดิสก์เต็ม เป็นต้น

(๑๔) การแจ้งเตือนจากโปรแกรมบริหารจัดการเครือข่าย

(๑๕) การแจ้งเตือนการทำงานของระบบล้มเหลวหรือหยุดชะงัก

(๑๖) ความพยายามในการเปลี่ยนแปลงค่าการติดตั้งระบบ(Configuration) ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

หมวด ๑๔
การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์คอมพิวเตอร์
(Use of Personal Computers and Computer Devices)

ข้อ ๕๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยอนุญาตให้ผู้ใช้ ใช้งานเป็นสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบก ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของกองทัพบกเท่านั้น

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วย ต้องเป็นโปรแกรมที่กองทัพบกได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๔) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งอุปกรณ์คอมพิวเตอร์ใดๆ เข้าไปในระบบและเครือข่ายคอมพิวเตอร์ของกองทัพบก

(๕) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกองทัพบกเท่านั้น

๖) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๗) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่อง

ข้อ ๕๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้รหัสผ่าน ดังนี้

(๑) ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารที่หน่วยที่รับผิดชอบระบบงานสารสนเทศเป็นผู้กำหนดขึ้น

ข้อ ๕๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการป้องกันจากโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ (Malware) ดังนี้

(๑) ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่น ๆ เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของกองทัพบก

(๒) ผู้ใช้งานควรตรวจสอบแฟ้ม (File) ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (E-mail) หรือแฟ้ม (File) ที่ได้รับ (Download) มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๓) ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นๆ เกิดความเสียหาย ถูกทำลาย แก้ไขเปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๕๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการสำรองข้อมูลและการกู้คืนดังนี้

(๑) ผู้ใช้งานคอมพิวเตอร์ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานคอมพิวเตอร์มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง(Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

หมวด ๑๕
การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer)

ข้อ ๕๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติการใช้งานทั่วไป ดังนี้

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่กองทัพบกอนุญาตให้ผู้ใช้ใช้งานเป็นสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบก ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของกองทัพบกเท่านั้น

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของกองทัพบกต้องเป็นโปรแกรมที่กองทัพบกได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

(๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา ปลายดินสอ เป็นต้น กดสัมผัสหน้าจอแสดงผลให้เป็นรอยขีดข่วนหรือทำให้จอแสดงผลของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๗) ไม่วางของที่มีน้ำหนักมากทับบนหน้าจอแสดงผลและแป้นพิมพ์

(๘) การเช็ดทำความสะอาดหน้าจอแสดงผลควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอแสดงผลมีรอยขีดข่วนได้

ข้อ ๕๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดความปลอดภัยทางด้านกายภาพ ดังนี้

(๑) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรเก็บเครื่องไว้ในสถานที่ที่มีอุปกรณ์ป้องกันขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

(๒) ผู้ใช้ไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อนความชื้นฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ ๕๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ ดังนี้

(๑) ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(๒) ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบงานสารสนเทศเป็นผู้กำหนดขึ้น

(๓) ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาหน้าจอแสดงผล(Screen Saver) โดยตั้งเวลาในกรณีไม่ได้ใช้งานในห้วงระยะเวลาขณะหนึ่ง เช่น ตั้งไว้ ๑๐ นาที เป็นต้น ให้ทำการปิดกั้นการใช้งาน (Lock) สำหรับหน้าจอแสดงผล หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

(๔) ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอแสดงผลเป็นเวลานาน

(๕) ห้ามบันทึกชื่อผู้ใช้งานและรหัสผ่านไว้บนสถานที่ที่พบเห็นได้ง่าย เช่น บันทึกไว้บนอุปกรณ์คอมพิวเตอร์ บันทึกไว้บนโต๊ะทำงาน เป็นต้น

ข้อ ๕๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้รหัสผ่าน ดังนี้

(๑) ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบงานสารสนเทศเป็นผู้กำหนดขึ้น

ข้อ ๖๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการสำรองข้อมูลและการกู้คืน ดังนี้

(๑) ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก ให้ปฏิบัติตามแนวทางการทำลายสื่อบันทึกข้อมูลในหมวด ๘

หมวด ๑๖
การใช้งานอินเทอร์เน็ต
(Use of the Internet)

ข้อ ๖๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตดังนี้

(๑) ให้ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS/IDS เป็นต้น

(๒) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาก่อนทำ การเชื่อมต่ออินเทอร์เน็ตเพื่อใช้งานโปรแกรมเข้าชมเว็บไซต์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่โปรแกรมเข้าชมเว็บไซต์ติดตั้งอยู่ก่อนการใช้งาน

(๓) ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกองทัพบก เพื่อหาประโยชน์ในเชิงธุรกิจ ส่วนตัวและการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

(๔) ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกองทัพบก โดยผ่านความเห็นชอบจากผู้บังคับบัญชา

(๕) ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับทางราชการและที่เกี่ยวข้องกับกองทัพบกโดยไม่ได้รับอนุญาตอย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต เช่น เอกสารที่กำหนดชั้นความลับ ร่างหนังสือประกาศหรือคำสั่งต่างๆ เอกสารการบรรยายสรุปที่เกี่ยวข้องกับความมั่นคงฯ เอกสารที่เป็นสื่ออิเล็กทรอนิกส์ต่างๆที่เกี่ยวข้องกับความมั่นคงฯ เป็นต้น

(๖) ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

(๗) การใช้งานกระดานสนทนา (Web Board) ของหน่วย ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลส่วนบุคคล และเป็นความลับของทางราชการ โดยไม่ได้รับอนุญาต รวมทั้งต้องไม่บันทึกข้อมูลที่เป็นการใส่ร้าย ให้ร้ายบุคคลอื่น และการบันทึกข้อมูลที่ผิดกฎหมายต่างๆ

(๘) หลังจากใช้งานอินเทอร์เน็ตเสร็จเรียบร้อยแล้ว ให้ทำการออกจากระบบ (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

(๙) ผู้ใช้ต้องปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

ข้อ ๖๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดมาตรการป้องกันและรักษาความปลอดภัยจากการเชื่อมต่ออินเทอร์เน็ตความเร็วสูงดังนี้

(๑) การขอเปิดใช้บริการเชื่อมต่ออินเตอร์เน็ตความเร็วสูง ผ่านโทรศัพท์เลขหมายเอกชน หน่วยผู้ขอใช้จะต้องเสนอขออนุมัติกองทัพบกผ่านกรมการทหารสื่อสารเพื่อพิจารณาความเหมาะสมและความจำเป็นในการใช้งานต่อไป

(๒) การเชื่อมต่ออินเตอร์เน็ตความเร็วสูง จะต้องไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ของทางราชการที่เชื่อมต่อกับเครือข่ายภายในกองทัพบก (Intranet) หรือเครื่องคอมพิวเตอร์ส่วนตัวที่มีข้อมูลข่าวสารของกองทัพบก ที่เป็นชั้นความลับ และ/หรือข้อมูลที่อาจส่งผลกระทบด้านความมั่นคงของประเทศโดยเด็ดขาด

ข้อ ๖๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ กรณีที่มีการให้บริการเข้าถึงระบบอินเทอร์เน็ตจากภายในหน่วยงาน โดยการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

หมวด ๑๗
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

ข้อ ๖๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์ ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกองทัพบกให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอเช่น การเปลี่ยนตำแหน่ง เปลี่ยนต้นสังกัด การลาออกจากราชการ การเกษียณอายุ เป็นต้น

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกองทัพบก

(๓) การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบงานสารสนเทศเป็นผู้กำหนดขึ้น

(๔) รหัสผ่านของจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

(๕) ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของกองทัพบก หรือ จดหมายอิเล็กทรอนิกส์ (E-mail) ของภาครัฐเพื่อใช้ในการติดต่องานราชการ

(๖) ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

(๗) ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน เป็นต้น

(๘) ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกองทัพบกหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกองทัพบก

(๙) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการ ออกจากระบบ(Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(๑๐) ผู้ใช้ควรทำการตรวจสอบเอกสารที่แนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบแฟ้มข้อมูลโดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดแฟ้มข้อมูลที่เป็น Executable File เช่น .exe, .com เป็นต้น

(๑๑) ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๑๒) ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(๑๓) ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

หมวด ๑๘
การใช้งานทรัพย์สินทางปัญญา
(Use of Intellectual Property)

ข้อ ๖๕ ผู้ใช้งานระบบสารสนเทศของกองทัพบกควรจะต้องปฏิบัติตามเงื่อนไขการใช้งานและไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น ดังนี้

(๑) ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของซอฟต์แวร์หรือทรัพย์สินทางปัญญาอื่นๆ ที่กองทัพบก หรือผู้ใช้งานมีใช้งานหรือครอบครอง

(๒) ห้ามทำซ้ำ เปลี่ยนแปลง หรือแก้ไขทรัพย์สินทางปัญญาไปสู่รูปแบบอื่นที่เป็นการละเมิดเงื่อนไขหรือข้อตกลงการใช้งาน

(๓) ห้ามสำเนาทั้งหมดหรือบางส่วนของหนังสือ บทความ เพลง ภาพยนตร์ รายงาน หรือเอกสารอื่นๆ ที่เป็นการละเมิดเงื่อนไขของเจ้าของทรัพย์สินทางปัญญา

หมวด ๑๙

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(Wireless LAN Access Control)

ข้อ ๖๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สายดังนี้

(๑) ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในกองทัพบกจะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

(๒) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

(๔) การระบุอุปกรณ์ที่จะเข้าใช้งานในเครือข่ายไร้สายของกองทัพบก นอกจากการลงทะเบียนการใช้งานแล้ว จะต้องแจ้งค่า MAC address ของเครื่อง หรืออุปกรณ์ที่จะเข้ามาใช้งาน เพื่อให้ผู้รับผิดชอบเครือข่ายไร้สายของกองทัพบก บันทึกเป็นหลักฐานการเข้าใช้งานต่อไป

หมวด ๒๐

ระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

(Backup System and Contingency Plan)

ข้อ ๖๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการคัดเลือกและจัดทำระบบสำรองและกู้คืนระบบ ดังนี้

(๑) กำหนดระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้

(๒) กำหนดผู้รับผิดชอบในการสำรองข้อมูล

(๓) กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

(๔) กำหนดความถี่ในการสำรองข้อมูลของระบบงาน เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรมีความถี่ในการสำรองข้อมูลมากขึ้น เป็นต้น

(๕) ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

(๖) ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

(๗) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่

(๘) แนวทางปฏิบัติสำหรับการสำรองข้อมูล ดังนี้

(๘.๑) ผู้ดูแลระบบต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามแนวทางการสำรองข้อมูลของกองทัพบก

(๘.๒) การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

(๘.๓) การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรางข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

(๘.๔) ให้ผู้ดูแลระบบมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบและ/หรือผู้ดูแลเครือข่ายไม่สามารถปฏิบัติงานได้

(๘.๕) ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้รับผิดชอบระบบสารสนเทศของหน่วยทราบ

(๘.๖) ให้ผู้ดูแลระบบและผู้ดูแลเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสมพร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิดคือการสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

(๘.๗) การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

(๘.๘) แนวทางที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

(๘.๙) สำหรับความถี่ในการสำรองข้อมูลมีดังนี้

รายการ	**ข้อมูลที่ต้องสำรอง**	**ความถี่ในการสำรอง**
ระบบ E-mail	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลในส่วน Mailbox	๑ ครั้งต่อเดือน
Web Server	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลต่างๆ ที่เผยแพร่บนเว็บไซต์	๑ ครั้งต่อเดือน
Database Server	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ฐานข้อมูลที่มีความสำคัญ	๑ ครั้งต่อสัปดาห์
อุปกรณ์ Firewall	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูล Rule ของอุปกรณ์นั้น	๑ ครั้งต่อเดือน
อุปกรณ์ IDS/IPS	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูล Rule ของอุปกรณ์นั้น	๑ ครั้งต่อเดือน
อุปกรณ์ Server อื่นๆ	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลที่มีความสำคัญของระบบงานที่ถูกเก็บในอุปกรณ์ต่างๆ เหล่านั้น	๑ ครั้งต่อเดือน

(๘.๑๐) ผู้ดูแลระบบและผู้ดูแลเครือข่ายสารสนเทศ รับผิดชอบความถูกต้องและความสมบูรณ์ของข้อมูล ตามความถี่ในข้อ (๘.๙)

(๙) แนวทางปฏิบัติสำหรับการกู้คืนระบบ ดังนี้

(๙.๑) ในกรณีพบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบและ/หรือผู้ดูแลเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้รับผิดชอบระบบสารสนเทศของหน่วย หรือผู้ที่ได้รับมอบหมายทราบ

(๙.๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

(๙.๓) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันที พร้องทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

ข้อ ๖๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ดังนี้

(๑) กำหนดระบบงานที่มีความสำคัญทั้งหมดของกองทัพบก และจัดทำเป็นบัญชีรายชื่อของระบบงาน ดังกล่าวรวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

(๒) ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงที่พบ โดยให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

(๓) กำหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบงาน และข้อมูลในฐานข้อมูล เป็นต้น รวมถึงกำหนดความถี่ในการสำรองข้อมูล วิธีการสำรองข้อมูล เช่น แบบ Full Backup หรือแบบ Incremental Backup เป็นต้น สำหรับระบบงานที่มีความสำคัญเหล่านั้น

(๔) จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน(Contingency Plan) เพื่อรับมือกับภัยพิบัติ ที่อาจเกิดขึ้นได้ ทั้งวิธีการทางอิเล็กทรอนิกส์ และทางกายภาพ อีกทั้งให้กำหนดห้วงในการทดสอบแผนดังกล่าวในห้วงวงรอบ ๖ เดือน ของทุกๆ ปี โดยแผนฯ ต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๔.๑) การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

(๔.๒) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๔.๓) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

(๔.๔) การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(๔.๕) การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอกเช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่างๆ เช่น เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น

(๔.๖) การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(๕) ให้ทำการปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยมุ่งเน้นไปที่ระบบที่มีความสำคัญสูง

(๖) ให้ทำการสำรองข้อมูลตามชนิด ความถี่ และ วิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่าง สม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

(๗) ให้ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้นั้นว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ อย่างน้อยปีละ ๑ ครั้ง ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และ บันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

(๘) ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินรวมทั้งเมื่อมีการปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

หมวด ๒๑
การตรวจสอบและประเมินความเสี่ยง
ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ข้อ ๖๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยของข้อมูล ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่ตนเองรับผิดชอบอย่างสม่ำเสมอ ดังนี้

(๑) ตรวจสอบและประเมินด้านการบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศ

(๒) ตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม

(๓) ตรวจสอบและประเมินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลและการปฏิบัติการ

(๔) ตรวจสอบและประเมินการควบคุมการเข้าถึง

(๕) ตรวจสอบและประเมินด้านการพัฒนาระบบงานสารสนเทศ เช่น ด้านการจัดซื้อจัดจ้างพัฒนาระบบฯ รวมทั้งด้านการดูแลระบบงานสารสนเทศ เป็นต้น

(๖) ตรวจสอบและประเมินด้านความพร้อมการรับมือกับเหตุการณ์เฉพาะหน้า

(๗) ตรวจสอบความสอดคล้องกับระเบียบฉบับนี้และทางเทคนิคกับระเบียบฉบับนี้

ข้อ ๗๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดให้มีการประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ ซึ่งประกอบด้วยทรัพย์สิน ๕ หมวด ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบงาน ที่หน่วยรับผิดชอบอย่างน้อยปีละ ๑ ครั้ง โดยปฏิบัติตามแนวทางการประเมินดังนี้

(๑) กำหนดให้มีการจัดทำบัญชีทรัพย์สินสารสนเทศ

(๒) ระบุและประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ

(๓) จัดลำดับความเสี่ยงจากสูงมาต่ำ

(๔) จัดทำแผนการลดความเสี่ยงโดยคำนึงถึงการจัดการกับความเสี่ยงสูงก่อน

(๕) กำหนดให้มีการปฏิบัติตามแผนการลดความเสี่ยงที่กำหนดไว้และติดตามจนกระทั่งแล้วเสร็จ

(๖) ความรับผิดชอบในการตรวจสอบและประเมินความเสี่ยง

(๖.๑) กรณีการตรวจสอบภายในหน่วยงานของกองทัพบก (internal auditor)

(๖.๑.๑) ให้ผู้รับผิดชอบระบบสารสนเทศภายในกองทัพบก แต่งตั้งหน่วยงาน หรือคณะกรรมการสำหรับการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของกองทัพบก

(๖.๑.๒) วงรอบการตรวจสอบปีละ ๑ ครั้ง

(๖.๑.๓) ภายหลังการตรวจสอบ ให้รายงานผลการตรวจสอบให้หน่วยที่ได้รับการตรวจสอบ และผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

(๖.๒) กรณีผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor)

(๖.๒.๑) ให้ผู้รับผิดชอบระบบสารสนเทศภายในกองทัพบก พิจารณาจัดทำโครงการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของกองทัพบก

(๖.๒.๒) โดยให้มีการจัดจ้างดำเนินการในวงรอบรอบ ๑ ปีงบประมาณ

(๖.๒.๓) ภายหลังการตรวจสอบ ให้รายงานผลการตรวจสอบให้หน่วยที่ได้รับการตรวจสอบ และผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

หมวด ๒๒
การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๗๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่ตรวจพบให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

(๑) ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด ได้แก่ ระดับสูง ระดับกลาง หรือระดับต่ำ

(๒) แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

(๓) วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็น กรณีการบุกรุก การโจมตีระบบ หรือระบบได้รับความเสียหาย กรณีที่ไม่สามารถวิเคราะห์และแก้ไขโดยหน่วยงานเองได้ ให้ประสานงานขอความช่วยเหลือจากผู้ที่มีความรู้และความเชี่ยวชาญ เช่น ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (Thai CERT) หรือหน่วยงานภายนอกอื่นๆ เป็นต้น

(๔) กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

(๕) จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลาง ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงานดังนี้

(๕.๑) รายละเอียดเหตุการณ์

(๕.๒) วันเวลาที่เกิดขึ้น

(๕.๓) ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง

(๕.๔) สถานะของเหตุการณ์ในแต่ละช่วงเวลา

(๕.๕) ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา

(๕.๖) สาเหตุและวิธีการแก้ไข

(๕.๗) ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

หมวด ๒๓
หน้าที่และความรับผิดชอบ

ข้อ ๗๒ ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัติตามระเบียบนี้ โดยเฉพาะในกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามระเบียบกองทัพบกว่าด้วยการรักษาความปลอดภัยสารสนเทศของกองทัพบก พ.ศ.๒๕๕๔ ให้ผู้บังคับบัญชาสูงสุดในพื้นที่และรับผิดชอบระบบสารสนเทศของหน่วย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยมีแนวทางปฏิบัติดังนี้

(๑) ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือและหน่วยที่เกี่ยวข้องทราบ

(๒) สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

(๓) พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

(๔) ให้พิจารณาสั่งการลงโทษทางวินัยตามแบบธรรมเนียมทหารหรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้ จะโดยเจตนาหรือไม่เจตนา และการละเมิดนั้นจะเกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๗๓ ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบงานสารสนเทศ

เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการดังนี้

(๑) พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่างๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้ เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนหรือเกิดเสียหายอย่างใดหรือไม่

(๒) ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ ๗๔ ความรับผิดชอบของผู้ใช้งานต่อระเบียบฉบับนี้มีดังนี้

(๑) ปฏิบัติตามระเบียบฯ อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

(๒) ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของกองทัพบก

(๓) ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ของกองทัพบก

(๔) รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังผู้บังคับบัญชาและผู้รับผิดชอบระบบงานสารสนเทศโดยเร็วที่สุด

ข้อ ๗๕ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของของผู้บังคับบัญชาสามารถแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติหากจำเป็นให้รายงานหน่วยเหนือได้ตามความเหมาะสม

ข้อ ๗๖ ให้ส่วนราชการที่มีศูนย์สารสนเทศหรือศูนย์กรรมวิธีข้อมูลอัตโนมัติอยู่ในสังกัด สามารถออกระเบียบปลีกย่อยได้โดยไม่ขัดต่อระเบียบนี้

ประกาศ ณ วันที่ ตุลาคม พ.ศ. ๒๕๕๔

(ลงชื่อ) พลเอก
(ประยุทธ์ จันทร์โอชา)
ผู้บัญชาการทหารบก