# ระเบียบกองทัพบก

## ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก

พ.ศ. ๒๕๖๗

# สารบัญ

ระเบียบกองทัพบก
ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก
พ.ศ. ๒๕๖๗

---

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพบกเป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ โดยอาศัยอำนาจตามความใน มาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมาตรา ๕ วรรคหนึ่ง และมาตรา ๒๔ วรรคหนึ่ง แห่งพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. ๒๕๕๑ และข้อ ๙ ของข้อบังคับกระทรวงกลาโหมว่าด้วยการสั่งการและประชาสัมพันธ์ พ.ศ. ๒๕๒๗ ผู้บัญชาการทหารบก จึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองทัพบก ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก พ.ศ. ๒๕๖๗”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิกระเบียบกองทัพบก ว่าด้วยการรักษาความปลอดภัยกองทัพบก (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และบรรดาระเบียบและคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน โดยยึดถือให้อยู่ภายใต้กฎ ระเบียบ กฎหมายที่เกี่ยวข้องดังนี้

๓.๑ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๓.๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๓.๔ ระเบียบกองทัพบกว่าด้วยการรักษาความปลอดภัยกองทัพบก พ.ศ. ๒๕๖๓

๓.๕ พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓

๓.๖ ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓

๓.๗ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ ฉบับที่ ๔ พ.ศ. ๒๕๖๔

๓.๘ พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

๓.๙ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานข้าราชการ และลูกจ้างที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพบก

## หมวด ๑
## กล่าวทั่วไป

ข้อ ๕ คำนิยามในระเบียบนี้

๕.๑ ระบบสารสนเทศ (Information System) หมายถึง ระบบข่าวสารของกองทัพบก ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบสื่อสาร มาช่วยในการสร้างสารสนเทศของกองทัพบก และสามารถนำสารสนเทศมาใช้ในการวางแผน การบริหาร การพัฒนา ควบคุม รวมทั้งแนวทางหรือระเบียบปฏิบัติ ในการใช้อุปกรณ์เหล่านี้ ซึ่งมีองค์ประกอบดังนี้

๕.๑.๑ ระบบคอมพิวเตอร์ (Computer System) หมายถึง ระบบที่ประกอบด้วย ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware)

๕.๑.๒ เครือข่ายคอมพิวเตอร์ (Computer Network) หมายถึง การติดต่อสื่อสาร หรือการรับ - ส่งข้อมูลระหว่างระบบสารสนเทศภายในกองทัพบกและหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับกองทัพบก

๕.๑.๓ สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการสกัดข้อมูล ให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือ ภาพกราฟฟิก ที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจ และอื่น ๆ

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

๕.๓ ผู้ใช้งาน (User) หมายถึง ข้าราชการ พนักงานราชการ และลูกจ้างของกองทัพบก ที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศกองทัพบก รวมถึงบุคคลภายนอกที่หน่วยงานอนุญาตให้เข้ามาดำเนินการ เกี่ยวกับระบบสารสนเทศของกองทัพบก

๕.๔ ผู้ดูแลระบบ (System Administrator) หมายถึง นายทหารสัญญาบัตรที่ปฏิบัติงาน ในระบบสารสนเทศของกองทัพบกหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลระบบสารสนเทศของหน่วยงานนั้น ๆ

๕.๕ ผู้ดูแลเครือข่าย (Network Administrator) หมายถึง นายทหารสัญญาบัตรที่ปฏิบัติงาน ในระบบสารสนเทศของกองทัพบกหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลเครือข่ายสารสนเทศ ของหน่วยงานนั้น ๆ

๕.๖ ผู้ดูแลฐานข้อมูล (Database Administrator) หมายถึง นายทหารสัญญาบัตร ที่ปฏิบัติงานในระบบสารสนเทศของกองทัพบกหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลฐานข้อมูล

๕.๗ ผู้บังคับบัญชา หมายถึง หัวหน้าหน่วยงานของผู้ปฏิบัติหน้าที่ในระบบสารสนเทศ ของกองทัพบก

๕.๘ ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า ความมั่นคงและความปลอดภัย ในบริบทของ การรักษาความลับ ความเชื่อถือได้ และความพร้อมใช้งานของข้อมูล สำหรับระบบสารสนเทศของกองทัพบก

๕.๙ ทรัพย์สินสารสนเทศ หมายความว่า

๕.๙.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๕.๙.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใดที่มีใช้ในระบบ

๕.๙.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๕.๑๐ ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) หมายความว่า การป้องกันทรัพย์สินสารสนเทศ จากการเข้าถึง ใช้เปิดเผย ขัดขวาง เปลี่ยนแปลง แก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้ โดยมิชอบ

๕.๑๑ ความมั่นคงปลอดภัยด้านกายภาพ (Physical Security) หมายความว่า การจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ป้องกัน ทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

๕.๑๒ เหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของกองทัพบกหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรืออาจสร้างความเสียหายได้ในที่สุดซึ่งอาจส่งผลให้

๕.๑๒.๑ เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ เช่น ระบบสารสนเทศของหน่วยเกิดการหยุดชะงัก เป็นต้น

๕.๑๒.๒ เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของกองทัพบก

๕.๑๒.๓ เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่าง ๆ ที่กำหนดไว้

๕.๑๒.๔ เกิดภาพลักษณ์ที่ไม่ดีต่อกองทัพบกหรือทำให้สูญเสียชื่อเสียง เช่น การไปโพสต์ข้อความพาดพิงถึงกองทัพบกในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของกองทัพบก เป็นต้น

๕.๑๒.๕ ตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัย ได้แก่ โปรแกรมไม่พึงประสงค์ การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน การแจ้งเตือนของระบบป้องกันการบุกรุก ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต การใช้ทรัพยากรของหน่วยงานผิดวัตถุประสงค์ เช่น การใช้เครือข่ายของหน่วยงานเพื่อกระทำการที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เพื่อกระทำการที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา เพื่อทำการส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ เป็นต้น ระบบถูกโจมตีจนไม่สามารถให้บริการได้ ระบบ อุปกรณ์ ฮาร์ดแวร์ หรือทรัพย์สินในระบบสารสนเทศอื่น ๆ ถูกขโมย การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของกองทัพบก การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่น ๆ ที่เป็นการละเมิดระเบียบฉบับนี้

๕.๑๒.๖ ตัวอย่างของเหตุการณ์ที่เป็นจุดอ่อน ได้แก่ ประตูศูนย์คอมพิวเตอร์ไม่สามารถปิดให้สนิทได้ ระบบสารสนเทศของหน่วยมีช่องทางอื่นในการเข้าสู่ระบบได้โดยไม่ผ่านการพิสูจน์ตัวตนตามปกติ เจ้าหน้าที่รักษาความปลอดภัยของหน่วยไม่เข้มงวดหรือละเลยการปฏิบัติหน้าที่ บุคคลภายนอกสามารถเดินตามเจ้าหน้าที่เข้าห้องระบบสารสนเทศของหน่วยโดยไม่มีการแลกบัตรผ่าน บุคคลภายนอกไม่ได้ลงชื่อก่อนเข้าศูนย์คอมพิวเตอร์ของหน่วย เจ้าหน้าที่ไม่มีการระบุตัวตนก่อนที่จะเข้าถึงห้องระบบสารสนเทศของหน่วยนั้น

๕.๑๒.๗ เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ที่เป็นจุดอ่อน จำเป็นต้องได้รับรายงานจากผู้ใช้งานเพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสมได้ผลและทันท่วงที

๕.๑๓ ทรัพย์สินทางปัญญา หมายถึง ผลงานอันเกิดจากความคิดสร้างสรรค์ของมนุษย์ ทรัพย์สินทางปัญญาเป็นทรัพย์สินอีกชนิดหนึ่งที่นอกเหนือจากสังหาริมทรัพย์นั่นคือทรัพย์สินที่สามารถเคลื่อนย้ายได้ เช่น นาฬิกา รถยนต์ โต๊ะ เป็นต้น และอสังหาริมทรัพย์ คือทรัพย์สินที่ไม่สามารถเคลื่อนย้ายได้ เช่น บ้าน ที่ดิน เป็นต้น ซึ่งทรัพย์สินทางปัญญา ได้แก่

๕.๑๓.๑ ลิขสิทธิ์ (Copyright)

๕.๑๓.๒ สิทธิบัตร (Patent)

๕.๑๓.๓ เครื่องหมายการค้า (Trademark)

๕.๑๓.๔ แบบผังภูมิของวงจรรวม (Layout - Designs of Integrated Circuit)

๕.๑๓.๕ ความลับทางการค้า (Trade Secrets)

๕.๑๓.๖ สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

๕.๑๔ สินทรัพย์ หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่า ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อกองทัพบก

๕.๑๕ สิ่งอุปกรณ์สายสื่อสาร หมายถึง เครื่องมือสื่อสารและระบบติดต่อสื่อสาร เครื่องคอมพิวเตอร์ เครื่องมือเครื่องใช้และอุปกรณ์ประกอบในระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ รวมทั้งชุดคำสั่งหรือโปรแกรม และอื่น ๆ ให้เป็นไปตามตามระเบียบกองทัพบกว่าด้วยความรับผิดชอบในสิ่งอุปกรณ์ พ.ศ. ๒๕๕๕ ตามคำจัดความ ข้อ ๔.๑๕ ว่าด้วยสิ่งอุปกรณ์สายสื่อสาร

๕.๑๖ สิทธิของผู้ใช้งาน (User Access Right) หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของกองทัพบก หรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของกองทัพบก

๕.๑๗ การเข้าถึง (Access) หมายถึง ความสามารถในการเข้าไป อันอาจทำให้สามารถอ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใด ๆ หรือได้อ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใด ๆ สำหรับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ สารสนเทศ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์และวิธีการทางกายภาพ

๕.๑๘ การควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๕.๑๙ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบของกองทัพบกสูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่าง ๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูกบุกรุกหรือโจมตีทางช่องโหว่และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่าง ๆ

๕.๒๐ ภัยคุกคาม (Threats) หมายถึง เหตุการณ์ต่าง ๆ ที่เป็นไปได้หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจส่งผลกระทบหรือสร้างความเสียหายต่อระบบสารสนเทศของกองทัพบก

๕.๒๑ ช่องโหว่ (Vulnerabilities) หมายถึง จุดอ่อนของทรัพย์สินหรือมาตรการที่เป็นช่องทางเกิดปัจจัยเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อทรัพย์สินหรือต่อระบบสารสนเทศของกองทัพบก

๕.๒๒ การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหารและความสงบเรียบร้อยภายในประเทศ

๕.๒๓ ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๕.๒๔ ไซเบอร์ (Cyber) หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

๕.๒๕ เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident) หมายถึง เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๕.๒๖ การเข้ารหัส (Encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ จะต้องมี โปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๕.๒๗ การยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน

๕.๒๘ ระบบ SSL (Secure Socket Layer) หมายถึง เทคโนโลยีการเข้ารหัสข้อมูลเพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน

๕.๒๙ ระบบ VPN (Virtual Private Network) หมายถึง เครือข่ายคอมพิวเตอร์เสมือนส่วนตัวโดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๕.๓๐ หน่วยงานของรัฐ (Government Agency) หมายถึง ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

๕.๓๑ โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure : CI) หมายถึง บรรดาหน่วยงาน หรือ องค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กรซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงาน หรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้นมีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

๕.๓๒ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) หมายถึง คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐ หรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

๕.๓๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure Operator) หมายถึง หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจ หรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งมาตรา ๔๙ ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ กำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) ด้านความมั่นคงของรัฐ

(๒) ด้านบริการภาครัฐที่สำคัญ

(๓) ด้านการเงินการธนาคาร

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(๕) ด้านการขนส่งและโลจิสติกส์

(๖) ด้านพลังงานและสาธารณูปโภค

(๗) ด้านสาธารณสุข

(๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

๕.๓๔ หน่วยงานควบคุมหรือกำกับดูแล (Regulator) หมายถึง หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๕.๓๕ ทีมรับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer Emergency Response Team : CERT) หมายถึง หน่วยงานรับมือเหตุภัยคุกคามที่อยู่ภายใต้สถาบันวิศวกรรมซอฟต์แวร์ (Software Engineering Institute - SEI) แห่งมหาวิทยาลัย Carnegie Mellon ในสหรัฐอเมริกา และเนื่องจาก CERT เป็นเครื่องหมายการค้าจดทะเบียน ดังนั้น ศูนย์ที่ทำหน้าที่ประสานและรับมือเหตุภัยคุกคามด้านความมั่นคงทางไซเบอร์ที่จัดตั้งขึ้นใหม่ และต้องการใช้ชื่อที่มีคำว่า CERT จะต้องยื่นขอใบอนุญาตเสียก่อน เช่น ประเทศไทยมี Thai CERT

๕.๓๖ ทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security Incident Response Team: CSIRT) หรือทีมรับมือสถานการณ์ที่เกี่ยวกับคอมพิวเตอร์ (Computer Incident Response Teams : CIRT) หมายถึง ศูนย์ประสานการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่สามารถรับมือและแก้ไขเหตุภัยคุกคามซึ่งประกอบด้วยบุคลากรที่มีความรู้และทักษะในการรับมือเหตุภัยคุกคาม ให้ความช่วยเหลือผู้รับบริการในการฟื้นตัวจากการเจาะระบบ นอกจากนี้ในการดำเนินการเชิงรุก CSIRT สามารถให้บริการตรวจสอบและประเมินช่องโหว่ของระบบสารสนเทศและความเสี่ยงต่าง ๆ รวมทั้งสร้างความตระหนักและให้ความรู้แก่ผู้เกี่ยวข้องในการพัฒนาและปรับปรุง การบริการเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์

ข้อ ๖ ผู้บัญชาการทหารบก ในฐานะผู้บริหารระดับสูงสุดกองทัพบก (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบระบบสารสนเทศในภาพรวมของกองทัพบก รวมถึงการละเมิดมาตรการต่าง ๆ อันทำให้เกิดความเสียหายของระบบสารสนเทศที่เกิดขึ้นตามระเบียบนี้

ข้อ ๗ เสนาธิการทหารบก ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) ของ ทบ. เป็นผู้ขับเคลื่อนการพัฒนาด้านดิจิทัลโดยส่งเสริมและผลักดันให้มีการปรับรูปแบบการบริการและการทำงานภาครัฐให้มีความทันสมัย รวดเร็ว โปร่งใส เชื่อมโยงอย่างเป็นเครือข่ายทั้งภายในและภายนอกอย่างมีมาตรฐาน มั่นคงปลอดภัยและคำนึงถึงความเป็นส่วนบุคคล เพื่อการพัฒนาที่ต่อเนื่องและยั่งยืน

ข้อ ๘ ให้ รองเสนาธิการทหารบก (๓) ในฐานะผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief Information Security Officer : CISO) ของ ทบ. เป็นผู้บริการระดับสูงด้านการรักษาความปลอดภัยให้กับโครงสร้าง เครือข่าย ข้อมูล และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยที่ส่งผลกระทบต่อ ทบ. ทั้งทางตรงและทางอ้อม และเป็นผู้รักษาการให้เป็นไปตามระเบียบนี้ โดยมีคณะทำงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทบ. และคณะทำงานดำเนินการตรวจสอบและประเมินความมั่นคงปลอดภัยไซเบอร์ ทบ. เป็นทีมงานขับเคลื่อน รวมทั้งทบทวนระเบียบนี้ให้มีความทันสมัยอย่างต่อเนื่องตามความเหมาะสม

ข้อ ๙ คณะทำงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศกองทัพบก มีผู้อำนวยการสำนักปฏิบัติการ กรมยุทธการทหารบก เป็นหัวหน้าคณะทำงาน มีบทบาทในการกำหนดแนวทางและมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามแนวทางและมาตรฐานที่กำหนด และดำเนินการตามบทบาทหน้าที่ที่กำหนด

ข้อ ๑๐ คณะทำงานดำเนินการตรวจสอบและประเมินความมั่นคงปลอดภัยไซเบอร์กองทัพบก มีผู้อำนวยการศูนย์ไซเบอร์กองทัพบก เป็นหัวหน้าคณะทำงาน มีบทบาทวางแผน อำนวยการ ประสานงาน กำกับดูแล และจัดเตรียมแผนการตรวจสอบและประเมินความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งดำเนินการตรวจสอบและประเมินตามแผน รวมทั้งวิเคราะห์ ติดตาม ตรวจสอบ แก้ไขและป้องกัน เพื่อพัฒนาและปรับปรุงแผนการตรวจสอบและประเมินต่าง ๆ ที่เกี่ยวข้องอย่างต่อเนื่องในภาพรวมของกองทัพบก

ข้อ ๑๑ ความมุ่งหมายของระเบียบนี้

๑๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีระบบการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกองทัพบกดำเนินงานไปได้อย่างมีประสิทธิภาพและประสิทธิผล

๑๑.๒ เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บังคับบัญชา กำลังพลของหน่วย ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกองทัพบก เป็นไปอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกองทัพบก

๑๑.๓ เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบสารสนเทศของกองทัพบกยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศไปสู่สากล

๑๑.๔ เพื่อเป็นมาตรการในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกองทัพบก สำหรับการพิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการรั่วไหลหรือรู้ไปถึงหรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่ ป้องกันการจารกรรม ทั้งจากบุคคลภายในและภายนอกส่วนราชการ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่เครื่องคอมพิวเตอร์ อุปกรณ์สารสนเทศ เครื่องใช้สำนักงาน อาคาร สถานที่ และเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ เป็นต้น

๑๑.๕ เพื่อเป็นการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. ๒๕๖๒ และนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ในฐานที่กองทัพบกเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ด้านความมั่นคงของรัฐ

๑๑.๖ เพื่อเป็นกรอบและแนวทางปฏิบัติให้กับหน่วยงานในกองทัพบก สามารถดำเนินการด้านระบบสารสนเทศและเทคโนโลยีดิจิทัลเป็นไปตามพระราชบัญญัติ กฎหมาย กฎ ระเบียบ ที่มีผลบังคับใช้ในปัจจุบันได้อย่างถูกต้อง

ข้อ ๑๒ หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของส่วนราชการ และแต่งตั้งผู้รับผิดชอบระบบสารสนเทศของส่วนราชการเพิ่มเติมได้โดยให้กำหนดบทบาทหน้าที่ให้สอดคล้อง ชัดเจนและไม่ขัดแย้งกับระเบียบนี้

ข้อ ๑๓ เหตุผลในการประกาศใช้ระเบียบนี้ เพื่อใช้เป็นแนวนโยบายและแนวปฏิบัติของกองทัพบกในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกองทัพบกเกี่ยวกับระบบคอมพิวเตอร์ระบบสื่อสารสารสนเทศ ระบบเครือข่ายสารสนเทศ สอดคล้องและเป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพบก

ข้อ ๑๔ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และระเบียบกองทัพบกว่าด้วยการรักษาความปลอดภัยกองทัพบก พ.ศ. ๒๕๖๓ หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

## หมวด ๒
## การจัดทำโครงการและการจัดหาระบบคอมพิวเตอร์และอุปกรณ์ประกอบ
## (Application, Computer and Device Project Development and Acquisition)

ข้อ ๑๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องควบคุมการจัดหาระบบงาน คอมพิวเตอร์ และอุปกรณ์เครือข่ายและคอมพิวเตอร์ดังนี้

๑๕.๑ ต้องเป็นผู้ให้ความเห็นชอบในการจัดทำโครงการด้านระบบสารสนเทศของหน่วยงานภายในต่าง ๆ ของกองทัพบก เพื่อให้มีความเหมาะสมและเกิดประโยชน์สูงสุดแก่กองทัพบก

๑๕.๒ ต้องเป็นผู้ให้ความเห็นชอบสำหรับการจัดหาระบบงาน คอมพิวเตอร์ อุปกรณ์เครือข่าย หรืออุปกรณ์คอมพิวเตอร์ของหน่วยงานภายในของกองทัพบก

๑๕.๓ ไม่อนุญาตให้หน่วยงานภายในต่าง ๆ ของกองทัพบกดำเนินการด้วยตนเองโดยไม่ผ่านความเห็นชอบจากหน่วยรับผิดชอบตามสายงานหรือหน่วยงานที่ได้รับมอบหมายจากผู้บังคับบัญชา

๑๕.๔ การจัดหาระบบคอมพิวเตอร์หรือแผนงาน/โครงการที่มีระบบคอมพิวเตอร์เป็นองค์ประกอบ ให้ยึดถือและดำเนินการตามหลักเกณฑ์และแนวทางดำเนินการด้านแผนงาน/โครงการด้านเทคโนโลยีสารสนเทศ การปฏิบัติการไซเบอร์และการสื่อสารของ ทบ. พ.ศ. ๒๕๖๖ หรือกรณีมีการปรับปรุงให้ยึดถือฉบับอนุมัติล่าสุด

ข้อ ๑๖ การเสนอแผนงาน/โครงการที่มีระบบคอมพิวเตอร์ของ ทบ. ให้เสนอตามสายบังคับบัญชาไปยังหน่วยงานรับผิดชอบโครงการรอง หลัก ไปยัง ยก.ทบ./ฝ่ายเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศการปฏิบัติการไซเบอร์และการสื่อสาร ทบ.

ข้อ ๑๗ แผนงาน/โครงการที่มีระบบคอมพิวเตอร์ ต้องได้รับการลงนามรับรองจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ของ ทบ. ก่อนการดำเนินการด้านงบประมาณของ ทบ. ต่อไป

## หมวด ๓
## การควบคุมการเข้าถึงหรือการใช้งานระบบสารสนเทศ
## (Access Control)

ข้อ ๑๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงาน โดยกำหนดเป็นมาตรการทั้ง ๔ ด้าน ดังนี้

๑๘.๑ ด้านการเข้าถึงระบบสารสนเทศทั่วไป

๑๘.๑.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบข้อมูลและ/หรือผู้รับผิดชอบระบบงาน ตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๑๘.๑.๒ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่กองทัพบกกำหนด เพื่อขอสิทธิในการเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน

๑๘.๑.๓ ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๑๘.๒ ด้านการเข้าถึงระบบเครือข่ายสารสนเทศ

๑๘.๒.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบระบบเครือข่ายของกองทัพบก ตามสิทธิและความจำเป็นในการเข้าถึงเครือข่ายก่อนที่จะเข้าใช้งาน

๑๘.๒.๒ ผู้ดูแลเครือข่ายสารสนเทศของกองทัพบก มีหน้าที่ตรวจสอบการอนุมัติและกำหนดการอนุญาตในการผ่านเข้าสู่เครือข่ายสารสนเทศของกองทัพบก ตามสิทธิและความจำเป็นในการปฏิบัติงานเท่านั้น

๑๘.๒.๓ ผู้ดูแลเครือข่ายสารสนเทศของกองทัพบก จะต้องจัดให้มีการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิการใช้งาน ล่วงละเมิดสิทธิของผู้ใช้งานอื่น ๆ อีกด้วย

๑๘.๓ ด้านการเข้าถึงระบบปฏิบัติการ

๑๘.๓.๑ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบระบบปฏิบัติการ ซึ่งเป็นทรัพย์สินของกองทัพบก จึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะระบบปฏิบัติการที่กองทัพบกจัดหามาอย่างถูกต้องตามกฎหมายเท่านั้น

๑๘.๓.๒ ผู้รับผิดชอบระบบปฏิบัติการ มีหน้าที่ตรวจสอบสิทธิอนุญาตให้เข้าใช้งานระบบปฏิบัติการของผู้ใช้ และควบคุมการใช้งานให้เป็นไปตามสิทธิและตามความจำเป็นในการใช้งาน รวมถึงการบันทึกการใช้งานของผู้ใช้ ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิการใช้งาน รวมถึงล่วงละเมิดสิทธิของผู้ใช้งานอื่น ๆ อีกด้วย

๑๘.๔ ด้านการเข้าถึงโปรแกรมประยุกต์ (application)

๑๘.๔.๑ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบโปรแกรมประยุกต์ ซึ่งเป็นทรัพย์สินของกองทัพบก จึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะโปรแกรมประยุกต์ที่กองทัพบกจัดหามาอย่างถูกต้องตามกฎหมายเท่านั้น

๑๘.๔.๒ ผู้รับผิดชอบโปรแกรมประยุกต์ มีหน้าที่ตรวจสอบสิทธิอนุญาตให้เข้าใช้งานโปรแกรมประยุกต์ของผู้ใช้ และควบคุมการใช้งานให้เป็นไปตามสิทธิและตามความจำเป็นในการใช้งาน รวมถึงการบันทึกการใช้งานของผู้ใช้ ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิการใช้งาน รวมถึงล่วงละเมิดสิทธิของผู้ใช้งานอื่น ๆ อีกด้วย

ข้อ ๑๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ดังนี้

๑๙.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ที่ปฏิบัติงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในกองทัพบก เป็นต้น

๑๙.๑.๑ ขั้นตอนการลงทะเบียนเจ้าหน้าที่ (User Registration)

๑๙.๑.๑.๑ หน่วยต้นสังกัดของเจ้าหน้าที่ใหม่ แจ้งข้อมูลการขอลงทะเบียนเจ้าหน้าที่ใหม่เป็นลายลักษณ์อักษรตามสายการบังคับบัญชา ให้ผู้รับผิดชอบระบบสารสนเทศของกองทัพบก

๑๙.๑.๑.๒ ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาข้อมูลการขอลงทะเบียนของเจ้าหน้าที่ใหม่ โดยตรวจสอบให้ถูกต้องว่าเป็นเจ้าหน้าที่ของกองทัพบกอย่างแท้จริง และได้รับสิทธิในการใช้งานตามคำร้องขอลงทะเบียนอย่างถูกต้อง

๑๙.๑.๑.๓ ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาอนุมัติให้ลงทะเบียนเจ้าหน้าที่ใหม่ และแจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชาและเจ้าหน้าที่ใหม่ทราบต่อไป

๑๙.๑.๒ ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน

๑๙.๑.๒.๑ หน่วยต้นสังกัดของเจ้าหน้าที่ แจ้งข้อมูลการขอยกเลิกสิทธิการใช้งานเป็นลายลักษณ์อักษรตามสายการบังคับบัญชา ให้ผู้รับผิดชอบระบบสารสนเทศของกองทัพบก

๑๙.๑.๒.๒ ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาข้อมูลการขอยกเลิกสิทธิการใช้งานของเจ้าหน้าที่ โดยตรวจสอบให้ถูกต้องว่าเป็นเจ้าหน้าที่ของกองทัพบกอย่างแท้จริง และได้รับการยกเลิกสิทธิในการใช้งานตามคำร้องอย่างถูกต้อง

๑๙.๑.๒.๓ ผู้รับผิดชอบระบบสารสนเทศของกองทัพบกพิจารณาอนุมัติให้ยกเลิกสิทธิการใช้งานของเจ้าหน้าที่ และแจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชาและเจ้าหน้าที่นั้นทราบต่อไป

๑๙.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑๙.๓ กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน และถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของผู้ใช้งานต่อไป

๑๙.๔ จำกัดการใช้งานบัญชีชื่อผู้ใช้งานแบบกลุ่มซึ่งมีการใช้งานร่วมกัน กล่าวคือ อนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้น และผู้ใช้งานบัญชีแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน

๑๙.๕ ไม่อนุญาตให้ผู้ร้องขอใช้ระบบสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

๑๙.๖ จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอเข้าใช้ระบบสารสนเทศเพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

๑๙.๗ ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

๑๙.๗.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบสารสนเทศแยกตามหน่วยงานภายในของกองทัพบก

๑๙.๗.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาที่รับผิดชอบระบบสารสนเทศของหน่วยเพื่อดำเนินการทบทวนว่ามีรายชื่อที่ออกสิทธิเข้าถึงระบบสารสนเทศไปแล้วหรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๑๙.๗.๓ ผู้บังคับบัญชาของหน่วยแจ้งหรืออนุมัติรายชื่อของผู้มีสิทธิในระบบสารสนเทศที่ได้รับการแก้ไขให้ถูกต้องแล้ว

๑๙.๗.๔ ผู้ดูแลระบบสารสนเทศของหน่วยดำเนินการแก้ไขข้อมูลผู้มีสิทธิให้ถูกต้องตามที่ได้รับแจ้งหรือได้รับการอนุมัติ

ข้อ ๒๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่ดังนี้

๒๐.๑ ผู้ดูแลระบบที่รับผิดชอบระบบนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติโดยต้องกำหนดไว้เป็นลายลักษณ์อักษรอย่างชัดเจน เช่น กำหนดเป็นเอกสารการบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน เป็นต้น

๒๐.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตามเอกสารหรือตามระเบียบที่ทางกองทัพบกกำหนดขึ้น

๒๐.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา ควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา

๒๐.๓.๑ ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๒๐.๓.๒ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒๐.๓.๓ มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๒๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดวิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๒๑.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๒๑.๒ ผู้ดูแลฐานข้อมูลหรือเจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๒๑.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๒๑.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะผู้ใช้งานควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL และ VPN เป็นต้น

๒๑.๕ มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสารหรือตามระเบียบที่ทางกองทัพบกกำหนดขึ้น

๒๑.๖ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกองทัพบก เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๒๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการควบคุมการเข้าใช้งานระบบจากภายนอก หน่วยงานที่มีระบบสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งเอาไว้ภายในหน่วยของตนเอง เพื่อดูแลรักษาความปลอดภัยของระบบภายในจากการเข้าถึงระบบจากภายนอกโดยมีแนวทางปฏิบัติ ดังนี้

๒๒.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของกองทัพบก ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของกองทัพบก การควบคุมบุคคลที่เข้าสู่ระบบของกองทัพบกจากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๒๒.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๒๒.๓ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกองทัพบกอย่างเพียงพอและต้องได้รับอนุมัติจากผู้บังคับบัญชา

๒๒.๔ มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๒๒.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ข้อ ๒๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกดังนี้

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของกองทัพบก ต้องผ่านการพิสูจน์ตัวตนจากระบบของกองทัพบก โดยมีแนวทางปฏิบัติดังนี้

๒๓.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

๒๓.๒ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

๒๓.๓ การเข้าสู่ระบบสารสนเทศของกองทัพบกจากอินเทอร์เน็ตนั้น จะมีการตรวจสอบผู้ใช้งานด้วย

๒๓.๔ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัย จะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

## หมวด ๔
## การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน

ข้อ ๒๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดวิธีการบริหารจัดการรหัสผ่าน (User Password Management) และการใช้งานรหัสผ่าน (Password Use)ของเจ้าหน้าที่ให้มีความมั่นคงปลอดภัย และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) โดยมีแนวทางปฏิบัติ ดังนี้

๒๔.๑ วิธีการบริหารจัดการรหัสผ่าน

๒๔.๑.๑ ต้องเก็บรักษารหัสผ่านที่ได้รับให้เป็นความลับ

๒๔.๑.๒ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)

๒๔.๑.๓ ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๒๔.๑.๔ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๒๔.๑.๕ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

๒๔.๑.๖ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๒๔.๑.๗ เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๒๔.๑.๘ การกำหนดรหัสผ่านเริ่มต้นให้กับเจ้าหน้าที่ให้ยากต่อการเดาและกำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกันอีกด้วย

๒๔.๑.๙ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงานหลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๒๔.๑.๑๐ เมื่อเจ้าหน้าที่ของหน่วยงานลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้หน่วยแจ้งผู้รับผิดชอบระบบสารสนเทศทันที เพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ที่ลาออกออกจากระบบทันทีที่ได้รับแจ้ง

๒๔.๑.๑๑ การส่งมอบรหัสผ่านให้กับเจ้าหน้าที่ต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึก และประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และ แนบเอกสารการได้รับอนุญาตจากผู้บังคับบัญชา รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๒๔.๒ การใช้งานรหัสผ่าน

๒๔.๒.๑ ผู้ใช้งานต้องใช้งานรหัสผ่านของตนเองหรือตามที่ได้รับอนุมัติเท่านั้น

๒๔.๒.๒ ผู้ใช้งานรหัสผ่านต้องปฏิบัติให้เป็นไปตามวิธีการบริหารจัดการรหัสผ่านอย่างเคร่งครัด

๒๔.๒.๓ กรณีต้องการยกเลิกหรือเปลี่ยนแปลงรหัสผ่านให้แจ้งเป็นลายลักษณ์อักษรตามสายการบังคับบัญชาให้ผู้รับผิดชอบดำเนินการต่อไป

๒๔.๒.๔ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่าน

๒๔.๒.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๑๘๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๒๔.๒.๖ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๒๔.๒.๗ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกองทัพบก และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดย

๒๔.๒.๗.๑ คอมพิวเตอร์โน๊ตบุ๊ค (Notebook) ต้องทำการพิสูจน์ตัวตนในระดับไบออส (BIOS) ก่อนการใช้งาน

๒๔.๒.๗.๒ คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๒๔.๒.๗.๓ การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๒๔.๒.๗.๔ การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๒๔.๒.๗.๕ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๒๔.๒.๗.๖ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๒๔.๓ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๒๔.๓.๑ ผู้ดูแลระบบ (System Administrator) เป็นผู้รับผิดชอบในการทบทวนสิทธิการถึงของผู้ใช้งาน

๒๔.๓.๒ วงรอบการทบทวนสิทธิการเข้าถึงของผู้ใช้งานให้ทบทวน ทุก ๆ ๑ ปี หรือเมื่อการเกิดการเปลี่ยนแปลงสิทธิของผู้ใช้ ได้แก่ การลาออก การย้ายหน่วย เป็นต้น อีกทั้งการทบทวนสิทธิต้องพิจารณาถึงพฤติกรรมการทำงานของผู้ใช้ รวมทั้งถ้ามีการเปลี่ยนแปลงของระบบงานใหม่ จะต้องมีการทบทวนสิทธิการใช้งานทุกครั้งอีกด้วย

๒๔.๓.๓ การทบทวนสิทธิผู้ดูแลระบบ จะต้องแจ้งรายงานการทบทวนสิทธิเป็นลายลักษณ์อักษรให้ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกอนุมัติให้ดำเนินการต่อไป

## หมวด ๕
## การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
## (Physical and Environmental Security)

ข้อ ๒๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Physical Security)

๒๕.๑ กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

๒๕.๒ พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในโดยเฉพาะศูนย์เทคโนโลยีสารสนเทศกลาง (Data Center) ให้ติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

๒๕.๓ มีระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

๒๕.๔ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบยังใช้งานได้ตามปกติ

๒๕.๕ บุคลากรของกองทัพบกควรปิดประตูและหน้าต่างให้ล็อคอยู่เสมอ

๒๕.๖ ถ้าตรวจพบอุปกรณ์สารสนเทศ ที่ถูกละทิ้งโดยไม่มีผู้ใช้อยู่ในบริเวณใกล้เคียงให้รีบแจ้งผู้รับผิดชอบ ดำเนินการเก็บอุปกรณ์ดังกล่าวในสถานที่ปลอดภัย เพื่อป้องกันการโจรกรรม หรือลักลอบขโมยข้อมูลจากผู้ไม่ประสงค์ดีต่อไป

ข้อ ๒๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดการควบคุมการเข้า - ออก (Physical Entry Controls) ดังนี้

๒๖.๑ ให้มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

๒๖.๒ ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒๖.๓ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๒๖.๔ สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๒๖.๕ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๒๖.๖ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

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

๒๖.๘ จัดเก็บบันทึกการเข้า - ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญโดยเฉพาะศูนย์เทคโนโลยีสารสนเทศกลาง (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๒๖.๙ บุคคลภายนอก เช่น เจ้าหน้าที่บริษัท นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่น ๆ ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๒๖.๑๐ ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๒๖.๑๑ ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๒๖.๑๒ จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

ข้อ ๒๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบสิ่งอุปกรณ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas) ดังนี้

๒๗.๑ จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายสิ่งอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒๗.๒ จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๒๗.๓ จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในระบบสารสนเทศของหน่วย

๒๗.๔ ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

๒๗.๕ ตรวจนับและลงทะเบียนหรือขึ้นบัญชีคุมสิ่งอุปกรณ์ที่ส่งมอบโดยผู้ถูกจ้าง ผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการสิ่งอุปกรณ์ของกองทัพบก

ข้อ ๒๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการจัดวางและการป้องกันอุปกรณ์ (Equipment Sitting and Protection) ดังนี้

๒๘.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในห้องศูนย์เทคโนโลยีสารสนเทศกลาง (Data Center) ให้น้อยที่สุด

๒๘.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่ความมั่นคงปลอดภัย

๒๘.๓ ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในศูนย์เทคโนโลยีสารสนเทศกลาง (Data Center)

๒๘.๔ ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติหรือไม่

ข้อ ๒๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ดังนี้

๒๙.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

๒๙.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS)

๒๙.๑.๒ เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

๒๙.๑.๓ ระบบระบายอากาศ

๒๙.๑.๔ ระบบปรับอากาศ และควบคุมความชื้น

๒๙.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๒๙.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๓๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดและควบคุมการเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security) ดังนี้

๓๐.๑ เครือข่ายของกองทัพบกในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณเพื่อทำให้เกิดความเสียหายและป้องกันสัตว์ต่าง ๆ กัดสาย เช่น หนู เป็นต้น

๓๐.๒ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๓๐.๓ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๓๐.๔ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๓๐.๕ ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ ๓๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการบำรุงรักษาอุปกรณ์ (Equipment Maintenance) ดังนี้

๓๑.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

๓๑.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๓๑.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๓๑.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๓๑.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วย

๓๑.๖ ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓๑.๗ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๓๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องควบคุมและกำหนดขั้นตอนการนำสิ่งอุปกรณ์ของกองทัพบกออกนอกหน่วยงาน (Removal of Property) ดังนี้

๓๒.๑ ให้มีการขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วย

๓๒.๒ บันทึกข้อมูลการนำสิ่งอุปกรณ์ของกองทัพบกออกนอกหน่วย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๓๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off - Premises)

๓๓.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบกออกไปใช้งานนอก

๓๓.๒ ไม่ทิ้งสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบกไว้โดยลำพังในที่สาธารณะ

๓๓.๓ ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๓๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องควบคุมการจำหน่ายสิ่งอุปกรณ์หรือการนำสิ่งอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment) ดังนี้

๓๔.๑ ให้ทำลายข้อมูลสำคัญในสิ่งอุปกรณ์ก่อนที่จะดำเนินการจำหน่ายสิ่งอุปกรณ์ดังกล่าว และดูแนวทางปฏิบัติในการทำลายสื่อบันทึกข้อมูลในหมวด ๘

๓๔.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

## หมวด ๖
## การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ
## (Communications and Operations Management)

ข้อ ๓๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures) ดังนี้

๓๕.๑ จัดทำขั้นตอนปฏิบัติอย่างเป็นลายลักษณ์อักษรสำหรับภารกิจการปฏิบัติงานกับระบบเทคโนโลยีสารสนเทศดังต่อไปนี้

๓๕.๑.๑ การปฏิบัติงานในห้องเครื่องคอมพิวเตอร์ที่ให้บริการหรือศูนย์เทคโนโลยีสารสนเทศกลาง (Data Center)

๓๕.๑.๒ การเปิดและปิดระบบเช่น การเปิด - ปิดเครื่องคอมพิวเตอร์, เปิด - ปิดระบบงานเทคโนโลยีสารสนเทศ และเปิด - ปิดระบบให้บริการและอำนวยความสะดวก เป็นต้น

๓๕.๑.๓ การสำรองข้อมูล

๓๕.๑.๔ การบำรุงรักษาอุปกรณ์

๓๕.๑.๕ การจัดการกับสื่อบันทึกข้อมูล เช่น การทำป้ายชื่อบ่งชี้ การลบทั้งการป้องกันการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง เป็นต้น

๓๕.๑.๖ การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้น

๓๕.๑.๗ การประมวลผลข้อมูล เช่น ขั้นตอนในการนำข้อมูลเข้าระบบงานประมวลผลและแสดงผล เป็นต้น

๓๕.๑.๘ การใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ (Utilities)

๓๕.๑.๙ การรายงานและการจัดการกับปัญหาที่เกิดขึ้น

๓๕.๑.๑๐ การจัดการกับการทำงานล้มเหลวและความผิดพลาดของระบบคอมพิวเตอร์ระบบงาน และระบบเครือข่าย

๓๕.๑.๑๑ การกู้คืนระบบงานและระบบเครือข่าย

๓๕.๒ กำหนดผู้รับผิดชอบและผู้มีอำนาจในการควบคุมการดำเนินการในการจัดทำเอกสารขั้นตอนการปฏิบัติข้างต้น และให้มีการปรับปรุงเอกสารอย่างสม่ำเสมอ

ข้อ ๓๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบเทคโนโลยีสารสนเทศดังนี้

๓๖.๑ กำหนดขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงต่อระบบเทคโนโลยีสารสนเทศของกองทัพบก เช่น ซอฟต์แวร์ ฮาร์ดแวร์ของระบบงาน ซอฟต์แวร์ระบบปฏิบัติการ เป็นต้น ควรมีขั้นตอนการดำเนินการดังต่อไปนี้

๓๖.๑.๑ ระบุและบันทึกระดับผลกระทบและความเร่งด่วนของการเปลี่ยนแปลงที่ขออนุมัติ เช่น มากหรือน้อย เป็นต้น

๓๖.๑.๒ บันทึกรายละเอียดการดำเนินการที่เกี่ยวข้องเพื่อใช้เป็นหลักฐาน

๓๖.๑.๓ กำหนดให้มีการวางแผนการดำเนินการ

๓๖.๑.๔ กำหนดให้มีการทดสอบตามความจำเป็น

๓๖.๑.๕ กำหนดให้มีการแจ้งผู้ที่เกี่ยวข้องทั้งหมด

๓๖.๑.๖ กำหนดให้มีการวางแผนหรือขั้นตอนปฏิบัติสำหรับการถอยหลังกลับสำหรับกรณีที่ทำแล้วไม่สำเร็จ

๓๖.๑.๗ กำหนดผู้มีอำนาจในการอนุมัติให้ดำเนินการในการปรับปรุงหรือแก้ไขขั้นตอนปฏิบัติดังกล่าว

ข้อ ๓๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties) ดังนี้

๓๗.๑ กำหนดให้การปฏิบัติงานที่มีความสำคัญ แยกหน้าที่ความรับผิดชอบออกจากกันและมีผู้ปฏิบัติงานมากกว่าหนึ่งคน

๓๗.๒ ป้องกันไม่ให้งานที่มีความสำคัญสามารถดำเนินการได้ตั้งแต่ต้นจนจบได้ด้วยบุคคลเพียงคนเดียว

๓๗.๓ ให้ผู้บังคับบัญชามีการสอดส่องดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย

๓๗.๔ ให้มีการจัดเก็บหลักฐานที่สามารถใช้ตรวจสอบได้ในภายหลัง สำหรับงานที่มีความเสี่ยง

ข้อ ๓๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Test, and Operational Facilities) ดังนี้

๓๘.๑ ให้พิจารณาการแยกเครื่องคอมพิวเตอร์ของระบบงานและมาตรการเพื่อใช้ในการแยกเครื่องคอมพิวเตอร์สำหรับการพัฒนา การทดสอบและการให้บริการออกจากกันตามความจำเป็นเพื่อป้องกันผลกระทบจากการทำงานที่มีต่อกัน

๓๘.๒ กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องคอมพิวเตอร์ที่ใช้สำหรับการพัฒนาไปสู่เครื่องที่ใช้สำหรับการให้บริการ

๓๘.๓ ให้มีการป้องกันการเข้าถึงโปรแกรมอรรถประโยชน์ เช่น ซอฟต์แวร์ทูลและยูทิลิตี้ เป็นต้น ที่ใช้สำหรับการพัฒนาระบบงานโดยไม่ได้รับอนุญาตในการเข้าถึงโปรแกรมฯ ดังกล่าวบนเครื่องคอมพิวเตอร์สำหรับการพัฒนา

๓๘.๔ กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกันสำหรับระบบงานที่ใช้ในการพัฒนาทดสอบและให้บริการจริง

ข้อ ๓๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดให้มีการตรวจสอบและติดตามการใช้ทรัพยากรของระบบและเครือข่ายคอมพิวเตอร์ ดังนี้

๓๙.๑ จัดทำแผนการตรวจสอบและติดตามทรัพยากรของระบบสารสนเทศ ดังนี้

๓๙.๑.๑ กำหนดประเภทของข้อมูลที่ใช้ในการตรวจสอบและติดตามการใช้ทรัพยากรของระบบ เช่น ร้อยละของการใช้ซีพียู ร้อยละของการใช้หน่วยความจำ ร้อยละของการใช้พื้นที่ฮาร์ดดิสก์ และร้อยละของปริมาณการใช้เครือข่าย เป็นต้น

๓๙.๑.๒ กำหนดค่าปริมาณการใช้ทรัพยากรสูงสุดบนระบบที่ยอมรับได้ ค่าต่าง ๆ เหล่านี้ใช้สำหรับเป็นจุดในการแจ้งเตือนว่าระบบสารสนเทศได้มีการใช้ทรัพยากรมาจนถึงค่าสูงสุดที่ยอมรับได้แล้วหรือไม่ เช่น กำหนดไว้ที่ร้อยละ ๘๐ ของการใช้ซีพียู เป็นต้น

๓๙.๑.๓ กำหนดความถี่ในการเข้าตรวจสอบปริมาณการใช้ทรัพยากรของระบบสารสนเทศ สำหรับระบบที่มีความสำคัญจากมากไปน้อย ให้กำหนดแผนการตรวจสอบและติดตามทรัพยากรของระบบด้วยความถี่ในการตรวจสอบจากสูงไปต่ำ เช่น ระบบที่มีความสำคัญมากควรมีความถี่ในการตรวจสอบสูงกว่าระบบที่มีความสำคัญปานกลางและน้อย เป็นต้น

๓๙.๒ ติดตามและตรวจสอบทรัพยากรของระบบตามแผนการตรวจสอบและติดตามทรัพยากรของระบบฯ ที่ได้กำหนดไว้เพื่อดูว่ายังมีทรัพยากรเพียงพอต่อการให้บริการหรือไม่

๓๙.๓ รายงานข้อมูลผลการติดตามการใช้ทรัพยากรของระบบสารสนเทศ เช่น สถิติปริมาณการใช้ซีพียู หน่วยความจำ ฮาร์ดดิสก์ และปริมาณเครือข่ายคอมพิวเตอร์ ให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

๓๙.๔ ประเมินความต้องการทรัพยากรของระบบสารสนเทศที่ต้องการเพิ่มเติมเพื่อนำไปใช้ในการวางแผนปรับปรุงประสิทธิภาพและขีดความสามารถของระบบต่อไป

## หมวด ๗
## การป้องกันชุดคำสั่งไม่พึงประสงค์
## (Protection Against Malicious Code)

ข้อ ๔๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ดังนี้

๔๐.๑ ห้ามการติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้แฟ้มข้อมูล (File) อื่นที่กองทัพบกไม่อนุญาตให้ใช้งาน

๔๐.๒ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๔๐.๓ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ให้กับระบบเทคโนโลยีสารสนเทศของกองทัพบก และอัพเดทซอฟต์แวร์ป้องกันชุดคำสั่งไม่พึงประสงค์เป็นประจำสม่ำเสมอ

๔๐.๔ ให้ผู้ดูแลระบบดำเนินการตรวจสอบชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ที่ให้บริการและอุปกรณ์เทคโนโลยีสารสนเทศอื่น ๆ ในบริเวณจุดทางเข้า - ออกเครือข่ายอย่างสม่ำเสมอเพื่อดักจับชุดคำสั่งไม่พึงประสงค์ที่จะเข้าสู่ระบบ

๔๐.๕ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับชุดคำสั่งไม่พึงประสงค์ได้แก่การรายงานการเกิดขึ้นของชุดคำสั่งไม่พึงประสงค์ การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่ตรวจพบ เป็นต้น

๔๐.๖ มีการติดตามข้อมูลข่าวสารเกี่ยวกับชุดคำสั่งไม่พึงประสงค์อย่างสม่ำเสมอ

๔๐.๗ ให้มีการสร้างความตระหนักเกี่ยวกับชุดคำสั่งไม่พึงประสงค์เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุชุดคำสั่งไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร รวมทั้งให้หน่วยมีการจัดการฝึกอบรมสร้างความตระหนักอย่างน้อยปีละ ๑ ครั้ง

## หมวด ๘
## การจัดการเข้าถึงข้อมูลสารสนเทศและโปรแกรมประยุกต์
## (Management of Access to Information and Applications)

ข้อ ๔๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการจัดการกับข้อมูลในแต่ละชั้นความลับ ดังนี้

๔๑.๑ กำหนดระดับชั้นความลับของข้อมูลซึ่งอย่างน้อยประกอบด้วย ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายใน และข้อมูลลับ

๔๑.๒ กำหนดแนวทางในการจัดหมวดหมู่ข้อมูลเป็นชั้นความลับที่เหมาะสม ซึ่งควรพิจารณาจัดหมวดหมู่จาก

๔๑.๒.๑ แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับก็จะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับก็จะเป็นประเภทเปิดเผยได้ เป็นต้น

๔๑.๒.๒ วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านระบบงบประมาณของหน่วย ดังนั้นข้อมูลนี้จะอยู่ในประเภทลับ เป็นต้น

๔๑.๒.๓ จำนวนบุคคลที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

๔๑.๒.๔ ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผยจะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการงบประมาณ ด้านการไม่ปฏิบัติตามกฎระเบียบข้อบังคับที่หน่วยกำหนดต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้นข้อมูลจะสามารถจัดอยู่ในประเภทใช้ภายในเท่านั้น หรือประเภทชั้นความลับ เป็นต้น

๔๑.๓ กำหนดขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับ ขั้นตอนฯ ควรประกอบด้วย การควบคุมการประมวลผล การควบคุมการเข้าถึง การจัดเก็บ การจัดการกับสื่อบันทึกข้อมูล การทำป้ายบ่งชี้ และการสื่อสารข้อมูลอย่างมั่นคงปลอดภัย

๔๑.๔ กำหนดให้มีการจำกัดการเข้าถึงข้อมูลสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๔๑.๕ กำหนดมาตรการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลสำคัญที่ยังคงค้างอยู่บนสื่อบันทึกข้อมูลนั้น โดยอาจปฏิบัติตามแนวทางดังนี้

| ประเภทสื่อบันทึกข้อมูล | วิธีทำลาย |
|---|---|
| กระดาษ | ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร |
| Flash Drive | - ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ<br>- ใช้วิธีการทุบหรือบดให้เสียหาย |
| แผ่น CD/DVD | ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร |
| เทป | ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย |
| ฮาร์ดดิสก์ | - ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ<br>- ใช้วิธีการทุบหรือบดให้เสียหาย |

๔๑.๖ กำหนดมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

๔๑.๗ กำหนดมาตรการป้องกันข้อมูลสำคัญที่มีการสั่งพิมพ์ออกมาทางเครื่องพิมพ์เพื่อป้องกันการเข้าถึงโดยผู้อื่น

๔๑.๘ จัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๔๑.๙ มาตรการในการนำวิธีการเข้ารหัสมาใช้กับข้อมูลชั้นความลับ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบกองทัพบก ว่าด้วยการรักษาความปลอดภัยกองทัพบก พ.ศ. ๒๕๖๓

ข้อ ๔๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดการสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System Documentation) ดังนี้

๔๒.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๔๒.๒ ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๔๒.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

ข้อ ๔๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดนโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures) ดังนี้

๔๓.๑ จัดทำนโยบายหรือแนวทางการใช้อย่างเหมาะสมสำหรับการใช้งานระบบหรืออุปกรณ์ที่ใช้ในการสื่อสารข้อมูลระหว่างกองทัพบก เช่น ห้ามใช้เพื่อก่อความรำคาญแก่ผู้อื่น ทำให้ผู้อื่นสูญเสียชื่อเสียง ปลอมเป็นบุคคลอื่น เป็นต้น

๔๓.๒ มีวิธีการทางเทคนิคป้องกันข้อมูลสำคัญจากการถูกเข้าถึง ถูกเปลี่ยนแปลงแก้ไข ถูกสวมรอยโดยผู้อื่น ถูกเปิดเผยความลับ โดยไม่ได้รับอนุญาต

๔๓.๓ จัดทำแนวทางสำหรับการจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารโต้ตอบ และแนวทางควรสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่หน่วยต้องปฏิบัติตาม

ข้อ ๔๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements) โดยมีแนวทางข้อตกลงสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายในกับหน่วยงานภายนอกดังต่อไปนี้

๔๔.๑ กำหนดนโยบายขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๔๔.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง วิธีการรับ เป็นต้น

๔๔.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๔๔.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบ

๔๔.๕ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

๔๔.๖ กำหนดสิทธิการเข้าถึงข้อมูล

๔๔.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๔๔.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ข้อ ๔๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดระบบสารสนเทศตามภารกิจที่ได้รับมอบที่มีการเชื่อมโยงถึงกัน พิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างหน่วยภายในกองทัพบก หรือหน่วยงานอื่นๆ ที่จะมาขอเชื่อมโยงกับกองทัพบก เป็นต้นดังนี้

๔๕.๑ กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

๔๕.๒ พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๔๕.๓ พิจารณาว่ามีกำลังพลใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

๔๕.๔ พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

๔๕.๕ ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลที่กำหนดชั้นความลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ข้อ ๔๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการหมดเวลาหรือหมดอายุการใช้งานระบบสารสนเทศ (Session Time-Out) ดังนี้

๔๖.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดการติดต่อและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๔๖.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดการติดต่อและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานที่มีข้อมูลสำคัญ ระบบงานที่กำหนดชั้นความลับ เป็นต้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔๖.๓ แนวทางปฏิบัติดังนี้

๔๖.๓.๑ เมื่อผู้ใช้งานไม่ได้ใช้งานหรือว่างเว้นจากการใช้งานในระยะเวลา ๕ นาที หรือตามที่ผู้รับผิดชอบกำหนด ให้มีการตัดการเชื่อมต่อการใช้งานออกจากระบบสารสนเทศโดยอัตโนมัติ

๔๖.๓.๒ ถ้ามีความพยายามเข้าสู่ระบบใหม่ ให้ยืนยันการใช้งานโดยใส่ชื่อผู้ใช้ (Username ) และรหัสผ่าน (Password) หรือวิธีการที่ปลอดภัยในการยืนยันตัวบุคคลในทุก ๆ ครั้ง

ข้อ ๔๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time) ดังนี้

๔๗.๑ กำหนดให้ระบบสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น

๔๗.๒ กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วย) ระบบงานที่กำหนดชั้นความลับ เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อเพื่อป้องกันบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึงข้อมูลได้โดยง่าย

๔๗.๓ แนวทางปฏิบัติดังนี้

๔๗.๓.๑ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพบก กำหนดให้ใช้งานได้ ๒ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หรือตามที่ผู้บังคับบัญชาเห็นสมควร

๔๗.๓.๒ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพบก กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น

๔๗.๓.๓ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของกองทัพบก ถ้ากระทำในช่วงนอกเวลาทำงานตามปกติ ต้องได้รับอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ ๔๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดคุณสมบัติของการล็อกอิน (Login) ที่มีความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ สำหรับเครื่องคอมพิวเตอร์ให้บริการหรืออุปกรณ์เครือข่ายคอมพิวเตอร์ที่หน่วยรับผิดชอบ ดังนี้

๔๘.๑ ไม่มีหรือไม่แสดงฟังก์ชั่น (Function) ให้การช่วยเหลือในระหว่างที่ทำการล็อกอิน (Login)

๔๘.๒ บันทึกความพยายามในการล็อกอินทั้งที่สำเร็จและไม่สำเร็จและแสดงประวัติการล็อกอิน ๓ ครั้งล่าสุด

๔๘.๓ ตัดการเชื่อมต่อหลังจากที่ทำการล็อกอินไม่สำเร็จเกินกว่า ๓ ครั้ง

๔๘.๔ เมื่อมีการใส่ข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความรวม ๆ เช่น “ข้อมูลการล็อกอิน ไม่ถูกต้อง”

๔๘.๕ ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของกองทัพบก การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงาน หากมีการตรวจพบ อาจมีการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม กองทัพบกมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”

๔๘.๖ ไม่แสดงรายละเอียดของระบบใด ๆ จนกว่าจะล็อกอินสำเร็จ

ข้อ ๔๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging) ของระบบงานภายในกองทัพบกดังนี้

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

๔๙.๑ ข้อมูลชื่อบัญชีผู้ใช้ระบบงาน

๔๙.๒ ข้อมูลวันเวลาที่เข้าถึงระบบงาน

๔๙.๓ ข้อมูลวันเวลาที่ออกจากระบบงาน

๔๙.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๔๙.๕ ข้อมูลชื่อเครื่องคอมพิวเตอร์ที่ใช้งาน

๔๙.๖ ข้อมูลการเข้าถึงระบบ (Log In) ทั้งที่สำเร็จและไม่สำเร็จ

๔๙.๗ ข้อมูลความพยายามในการเข้าถึงทรัพยากร เช่น ข้อมูลบัญชีผู้ใช้ฐานข้อมูลสำคัญของระบบงาน เป็นต้น ทั้งที่สำเร็จและไม่สำเร็จ

๔๙.๘ ข้อมูลการเปลี่ยนแปลงสิ่งแวดล้อมหรือการกำหนดค่า (Configuration) ของระบบงาน

๔๙.๙ ข้อมูลแสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบ เป็นต้น

๔๙.๑๐ ข้อมูลแสดงการใช้งานโปรแกรมประยุกต์ (Application Program)

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

๔๙.๑๒ ข้อมูลไอพีแอดเดรสที่เข้าถึง

๔๙.๑๓ ข้อมูลโพรโตคอลของเครือข่ายที่ใช้งาน

๔๙.๑๔ ข้อมูลการแจ้งเตือนเกี่ยวกับการเข้าถึงระบบจากการบุกรุก

๔๙.๑๕ ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

๔๙.๑๖ ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญ ๆ

๔๙.๑๗ ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

## หมวด ๙
## การบริหารจัดการการเข้าถึงระบบเครือข่ายสื่อสารข้อมูล
## (Management of Access to Data Communication Network)

ข้อ ๕๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดมาตรการทางเครือข่ายสื่อสารข้อมูล (Network Controls) เพื่อป้องกันข้อมูลในเครือข่าย ระบบงาน หรือบริการต่าง ๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๕๐.๑ กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

๕๐.๒ กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานและอุปกรณ์ที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๕๐.๓ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

๕๐.๔ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๕๐.๕ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๕๐.๖ มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๕๐.๗ มีการใช้ฮาร์ดแวร์หรือซอฟต์แวร์ สำหรับการบริหารจัดการเครือข่ายเพื่อระบุ เฝ้าตรวจ ติดตามสถานะ อุปกรณ์ในระบบสารสนเทศของกองทัพบก

ข้อ ๕๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการเข้าถึงระบบเครือข่ายดังนี้

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

๕๑.๒ ผู้ดูแลระบบ ควรดำเนินการแยกและติดตั้ง เครื่องคอมพิวเตอร์ให้บริการไว้ในวงเครือข่ายที่แยกต่างหากจากวงเครือข่ายของผู้ใช้งาน และใช้ Firewall หรืออุปกรณ์เครือข่ายอื่น ๆ เพื่อจำกัดให้เฉพาะกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้น จึงจะสามารถเชื่อมต่อเข้าไปยังเครื่องคอมพิวเตอร์ให้บริการนั้นได้ และสำหรับแนวทางปฏิบัติการใช้งานของไฟร์วอลล์ (Firewall) ของกองทัพบก มีดังนี้

๕๑.๒.๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

๕๑.๒.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๕๑.๒.๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๕๑.๒.๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login Account ก่อนการใช้งานทุกครั้ง

๕๑.๒.๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๕๑.๒.๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๕๑.๒.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๕๑.๒.๘ การกำหนดระเบียบในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางกองทัพบกอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากกองทัพบกก่อน

๕๑.๒.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

๕๑.๒.๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๕๑.๒.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๕๑.๒.๑๒ ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

๕๑.๒.๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

๕๑.๒.๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตหรือเชื่อมต่อเครือข่ายภายในโดยทันที

๕๑.๓ การเข้าสู่ระบบเครือข่ายภายในของกองทัพบก โดยผ่านทางอินเทอร์เน็ต จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๕๑.๔ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕๑.๕ ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕๑.๖ ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ เช่น ในการเชื่อมต่อเข้าสู่เครื่องคอมพิวเตอร์ให้บริการเพื่อบริหารจัดการระบบ ให้กำหนดเฉพาะชุดไอพีแอดเดรสของผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงเครื่องคอมพิวเตอร์ให้บริการนั้นได้

๕๑.๗ ผู้ดูแลระบบ ตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

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

๕๑.๙ ระบบเครือข่ายทั้งหมดของหน่วยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วย ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ เป็นต้น

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

๕๑.๑๐.๑ เป็นการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในของกองทัพบก ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๕๑.๑๐.๒ ให้ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกองทัพบก และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ทั้งที่เชื่อมต่อสู่เครือข่ายภายนอก และเครือข่ายภายในทุกเส้นทาง

๕๑.๑๐.๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากเครือข่ายภายนอกหรือเครือข่ายสาธารณะต่าง ๆ จะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๕๑.๑๐.๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๕๑.๑๐.๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๕๑.๑๐.๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

๕๑.๑๐.๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งานกิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๕๑.๑๐.๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๕๑.๑๐.๙ เครื่องคอมพิวเตอร์ที่ให้บริการที่มีการติดตั้ง Host-Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๕๑.๑๐.๑๐ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๕๑.๑๐.๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๕๑.๑๐.๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๕๑.๑๐.๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผนเผชิญเหตุที่เกิดขึ้น

๕๑.๑๐.๑๔ ผู้ดูแลระบบมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๕๑.๑๐.๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดระเบียบของกองทัพบก การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของกองทัพบก จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมายต่อไป หรือหากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ซึ่งได้มีการแก้ไขเพิ่มเติมอัตราโทษปรับหรือจำคุก ฐานส่งข้อมูลก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ หรือนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์อันเป็นเท็จ บิดเบือน ลามก ตัดต่อภาพผู้อื่นให้เสียชื่อเสียง อับอาย รวมถึงมาตรการบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดตามกฎหมาย สรุปประเด็นสำคัญดังนี้

- การฝากร้านใน Facebook Instagram ถือเป็นสแปม ปรับ ๒๐๐,๐๐๐ บาท

- ส่ง SMS มาโฆษณา โดยไม่รับความยินยอม ต้องมีทางเลือกให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ไม่เช่นนั้นถือเป็นสแปม ปรับ ๒๐๐,๐๐๐ บาท

- ส่ง E-Mail ขายของ ถือเป็นสแปม ปรับ ๒๐๐,๐๐๐ บาท

- กด Like ได้ไม่ผิด พ.ร.บ. ยกเว้นการกด Like เรื่องเกี่ยวกับสถาบันเสี่ยงเข้าข่ายความผิด มาตรา ๑๑๒ หรือมีความผิดร่วม

- กด Share ถือเป็นการเผยแพร่ หากข้อมูลที่ Share นั้นมีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตาม พ.ร.บ. โดยเฉพาะที่กระทบต่อบุคคลที่ ๓

- พบข้อมูลผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ของเรา แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเอง สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากแจ้งแล้วลบข้อมูลออก เจ้าของก็จะไม่มีความผิดตามกฎหมาย เช่น ความเห็นในเว็บไซต์ต่าง ๆ รวมไปถึง Facebook ที่ให้แสดงความคิดเห็น หากพบว่าการแสดงความเห็นผิดกฎหมาย เมื่อแจ้งไปที่หน่วยงานที่รับผิดชอบเพื่อลบได้ทันที เจ้าของระบบเว็บไซต์จะไม่มีความผิด

- ผู้ดูแลระบบ (Admin) ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ. เมื่อลบออกจากพื้นที่ที่ตนดูแล จะถือเป็นผู้พ้นผิด แต่หากไม่ยอมลบออกจะมีโทษจำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

- การ Post สิ่งลามกอนาจารที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้ จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท

- การ Post เกี่ยวกับเด็ก/เยาวชน ต้องปิดบังใบหน้า ยกเว้นเมื่อเป็นการเชิดชู ชื่นชมอย่างให้เกียรติ

- การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียเชื่อเสียง หรือถูกดูหมิ่นเกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย มีโทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๒๐๐,๐๐๐ บาท

- การ Post ด่าว่าผู้อื่น มีกฎหมายอาญาอยู่แล้ว ไม่มีข้อมูลจริง หรือถูกตัดต่อ ผู้ถูกกล่าวหาเอาผิดผู้ Post ได้ โทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๒๐๐,๐๐๐ บาท

- ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ

- ส่งรูปภาพแชร์ของผู้อื่น เช่น สวัสดี อวยพร ไม่ผิด ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์หรือหารายได้

๕๑.๑๑ การเข้าสู่ระบบงานเครือข่ายภายในหน่วย ผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

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

๕๑.๑๓ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕๑.๑๔ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อทำการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕๑.๑๕ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศของหน่วย และจะต้องจัดทำเป็นบัญชีไว้สำหรับระบุอุปกรณ์บนเครือข่ายได้

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

๕๑.๑๗ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

## หมวด ๑๐
## การควบคุมการพัฒนาหรือจัดหาระบบงาน
## (Control of Application Development or Acquisition)

ข้อ ๕๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัยเพียงพอ ดังนี้

๕๒.๑ ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อยควรมี

๕๒.๑.๑ คุณสมบัติของการล็อกอินเข้าสู่ระบบงานที่มีความมั่นคงปลอดภัยของระบบสารสนเทศ ตามหมวด ๘

๕๒.๑.๒ การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับเข้าถึงระบบสารสนเทศตามหมวด ๔

๕๒.๑.๓ การเข้ารหัสข้อมูลสำคัญที่มีการรับ - ส่งข้อมูลระหว่างเครื่องผู้ใช้งานกับเครื่องคอมพิวเตอร์ให้บริการ

๕๒.๑.๔ การเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

๕๒.๑.๕ การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ หรือ ๓๐ นาที เป็นต้น

๕๒.๑.๖ การบันทึกบัญชีชื่อผู้ใช้งานที่ล็อกอินเข้าระบบ หมายเลข IP Address วันเวลาที่เข้าใช้ระบบ ความสำเร็จหรือไม่สำเร็จในการล็อกอินของผู้ใช้งาน

๕๒.๒ พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่ระบุไว้

๕๒.๓ พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

๕๒.๔ กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบ นำเสนอแผนดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบและรายงานผลการทดสอบให้ผู้บังคับบัญชาได้รับทราบ เพื่อให้คำแนะนำในการปรับปรุงต่าง ๆ ที่จำเป็น แผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

๕๒.๔.๑ แผนการทดสอบ UAT (User Acceptance Test)

๕๒.๔.๒ แผนการทดสอบ (System Integration Test)

๕๒.๔.๓ แผนการทดสอบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Test)

๕๒.๕ ไม่อนุญาตการนำข้อมูลสำคัญของกองทัพบกไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชาระดับสูงก่อน และหากเป็นไปได้ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

## หมวด ๑๑
## การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์ที่ให้บริการ (Server)
## (Management of Access to Service Server)

ข้อ ๕๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ (Control of Operational Software)

๕๓.๑ ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของหน่วยเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

๕๓.๒ ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วย

๕๓.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๕๓.๔ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๕๓.๕ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงาน เป็นต้น

๕๓.๖ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๕๓.๗ ทำการปรับปรุงไลบรารี่สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกับเทคโนโลยีทั้งหมดที่การติดตั้ง รวมทั้งเป็นปัจจุบัน

๕๓.๘ ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่น ๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

๕๓.๙ ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

๕๓.๑๐ ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่น ๆ

๕๓.๑๑ สำหรับซอฟต์แวร์ที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

๕๓.๑๒ ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

๕๓.๑๓ สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้

๕๓.๑๔ ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ (Patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๕๓.๑๕ ตรวจสอบและปิดพอร์ต (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

๕๓.๑๖ จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

๕๓.๑๗ จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้น จึงจะสามารถเชื่อมต่อเพื่อเข้าสู่ระบบงานที่ทำการติดตั้งนั้น

ข้อ ๕๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating System Changes) ดังนี้

๕๔.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๕๔.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้ง วางแผนด้าน งบประมาณที่จำเป็นต้องใช้ ในกรณีที่กองทัพบกต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

## หมวด ๑๒
## การจ้างงานหน่วยงานภายนอกให้บริการด้านเทคโนโลยีสารสนเทศ
## (Information Technology Service Delivery)

ข้อ ๕๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางการควบคุมการจ้างงานสำหรับการให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ดังนี้

๕๕.๑ จัดให้มีการควบคุมโครงการที่มีการจัดจ้างดำเนินการโดยหน่วยงานภายนอก

๕๕.๒ กำหนดให้มีการประเมินและจัดทำแผนการลด ความเสี่ยงสำหรับกรณีการเข้าถึงระบบงานหรือสารสนเทศโดยหน่วยงานภายนอก โดยปฏิบัติตามแนวทางการประเมินตามหมวด ๒๑ การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศ

๕๕.๓ กำหนดให้มีการอ้างอิงข้อปฏิบัติที่เกี่ยวข้องในระเบียบของกองทัพบกฉบับนี้ไว้ในสัญญาจ้างเพื่อให้ผู้รับจ้างปฏิบัติตามอย่างเคร่งครัด

๕๕.๔ กำหนดให้มีการทำสัญญาการไม่เปิดเผยข้อมูลสำคัญที่ได้รับจากกองทัพบกให้แก่ผู้อื่น

๕๕.๕ สำหรับบริการต่าง ๆ ที่เป็นงานให้บริการตามวงรอบระยะเวลาที่กำหนดไว้ หรือตามคำร้องขอจากหน่วยงานผู้ว่าจ้าง เช่น บริการบำรุงรักษาฮาร์ดแวร์ บริการแก้ไขปัญหาฮาร์ดแวร์ บริการแก้ไขปัญหาระบบงาน บริการจ้างในลักษณะ Help Desk ให้กำหนดรายละเอียดการบริการหรือตามที่กองทัพบกกำหนด ลงไว้ในสัญญาจ้างดังนี้

๕๕.๕.๑ รายละเอียดของบริการ

๕๕.๕.๒ ระดับการให้บริการ (Service Level Agreement)

๕๕.๕.๓ ผู้รับผิดชอบในการเฝ้าระวังหรือติดตามการให้บริการ

๕๕.๕.๔ วิธีการติดตามการให้บริการ

๕๕.๕.๕ วงรอบระยะที่ชัดเจนของการทบทวนการปฏิบัติงาน เช่น ทุก ๆ ๓ เดือน เป็นต้น

๕๕.๕.๖ รูปแบบของรายงานที่ต้องการและความถี่ในการจัดส่งรายงาน

๕๕.๖ กำหนดให้มีการติดตามการให้บริการตามข้อ ๕๕.๕ อย่างสม่ำเสมอและบันทึกผลการติดตามนั้นไว้ด้วย

๕๕.๗ ทบทวนการให้บริการตามข้อ ๕๕.๕ จากผลการปฏิบัติงานในช่วงเวลาที่ผ่านมาหรือผลที่ได้บันทึกไว้ ร้องขอให้ผู้ให้บริการปรับปรุงการให้บริการเพิ่มเติมตามที่ต้องการ และ/หรือ แก้ไขสัญญาจ้างตามความเหมาะสมและจำเป็น

๕๕.๘ กรณีการจ้างพัฒนาซอฟต์แวร์หรือระบบงานโดยหน่วยงานภายนอก (Outsourced Software Development) ให้ปฏิบัติตามแนวทางดังนี้

๕๕.๘.๑ กำหนดให้มีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของซอฟต์แวร์หรือระบบงานที่จะทำการพัฒนาขึ้นมาอย่างเป็นลายลักษณ์อักษร

๕๕.๘.๒ ควรพิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนาซอฟต์แวร์ที่มีการจัดจ้างดำเนินการจากผู้รับจ้างภายนอก

๕๕.๘.๓ ควรพิจารณากำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้รับจ้างภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้รับจ้างภายนอกนั้น

๕๕.๘.๔ ให้มีการตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์ในซอฟต์แวร์ต่าง ๆ ที่ถูกพัฒนาขึ้นก่อนดำเนินการติดตั้งหรือทดสอบการใช้งานจริง

**หมวด ๑๓**

**การตรวจสอบการใช้งานระบบ**

**(Monitoring System Use)**

ข้อ ๕๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่ใช้งานเพื่อกำหนดแนวทางในการเฝ้าระวังและดูแลระบบเหล่านั้น และกำหนดให้มีการเฝ้าระวังและดูแลระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่หน่วยต้องปฏิบัติตามอย่างสม่ำเสมอ โดยการตรวจสอบดังต่อไปนี้

๕๖.๑ ชื่อบัญชีผู้ใช้งาน

๕๖.๒ กิจกรรมการใช้งานและประเภทของกิจกรรม

๕๖.๓ วัน/เวลาที่เข้าถึง

๕๖.๔ แฟ้มข้อมูลหรือข้อมูลที่ถูกเข้าถึง

๕๖.๕ โปรแกรมทั่วไปและอรรถประโยชน์ต่าง ๆ (Utilities) ที่ถูกเรียกใช้งาน

๕๖.๖ การใช้บัญชีผู้ใช้งานในระดับสูง เช่น Supervisor, Root, Administrator เป็นต้น

๕๖.๗ การเปิด - ปิดการทำงานของระบบ

๕๖.๘ การถอดถอนหรือติดตั้งอุปกรณ์สำหรับนำเข้าและส่งออกข้อมูล (I/O) เช่น ฮาร์ดดิสก์ เป็นต้น

๕๖.๙ การใช้คำสั่งของผู้ใช้งานที่ได้รับการปฏิเสธโดยระบบ เช่น พยายามใช้คำสั่งทั้งที่ไม่มีสิทธิ การพยายามเข้าถึงระบบอย่างไม่ถูกต้อง เป็นต้น

๕๖.๑๐ ความพยายามในการเข้าถึงข้อมูลหรือทรัพยากรของระบบที่ได้รับการปฏิเสธโดยระบบ

๕๖.๑๑ การแจ้งเตือนจากไฟร์วอลล์หรือระบบป้องกันการบุกรุก

๕๖.๑๒ การแจ้งเตือนจากอุปกรณ์แจ้งเตือน (Console) ของผู้ดูแลระบบ

๕๖.๑๓ การแจ้งเตือนเมื่อระบบทำงานผิดปกติ เช่น ฮาร์ดดิสก์เต็ม เป็นต้น

๕๖.๑๔ การแจ้งเตือนจากโปรแกรมบริหารจัดการเครือข่าย

๕๖.๑๕ การแจ้งเตือนการทำงานของระบบล้มเหลวหรือหยุดชะงัก

๕๖.๑๖ ความพยายามในการเปลี่ยนแปลงค่าการติดตั้งระบบ (Configuration) ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

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

ข้อ ๕๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้งานทั่วไป

๕๗.๑ เครื่องคอมพิวเตอร์ที่หน่วยอนุญาตให้ผู้ใช้ ใช้งานเป็นสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบก ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของกองทัพบกเท่านั้น

๕๗.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วย ต้องเป็นโปรแกรมที่กองทัพบกได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๕๗.๓ ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

๕๗.๔ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช่ของกองทัพบกเชื่อมต่อเข้ากับระบบและเครือข่ายคอมพิวเตอร์ของกองทัพบก

๕๗.๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกองทัพบกเท่านั้น

๕๗.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๕๗.๗ ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่อง

๕๗.๘ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๕๗.๙ ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๕๗.๑๐ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวบุคคลที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงานโดยไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอย่างเหมาะสม และต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภายในกองทัพบกอย่างเคร่งครัด ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ข้อ ๕๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้รหัสผ่าน ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารที่หน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

ข้อ ๕๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการป้องกันจากโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ (Malware) ดังนี้

๕๙.๑ ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่น ๆ เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของกองทัพบก

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

๕๙.๓ ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น ๆ เกิดความเสียหาย ถูกทำลาย แก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๖๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการสำรองข้อมูลและการกู้คืนดังนี้

๖๐.๑ ผู้ใช้งานคอมพิวเตอร์ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๖๐.๒ ผู้ใช้งานคอมพิวเตอร์มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖๐.๓ ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงานเพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

## หมวด ๑๕
## การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
## (Use of Notebook Computer)

ข้อ ๖๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติการใช้งานทั่วไป ดังนี้

๖๑.๑ เครื่องคอมพิวเตอร์แบบพกพาที่กองทัพบกอนุญาตให้ผู้ใช้ใช้งานเป็นสิ่งอุปกรณ์หรือทรัพย์สินของกองทัพบก ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของกองทัพบกเท่านั้น

๖๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของกองทัพบกต้องเป็นโปรแกรมที่กองทัพบกได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๖๑.๓ ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๖๑.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๖๑.๕ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

๖๑.๖ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา ปลายดินสอ เป็นต้น กดสัมผัสหน้าจอแสดงผลให้เป็นรอยขีดข่วนหรือทำให้จอแสดงผลของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๖๑.๗ ไม่วางของที่มีน้ำหนักมากทับบนหน้าจอแสดงผลและแป้นพิมพ์

๖๑.๘ การเช็ดทำความสะอาดหน้าจอแสดงผลควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอแสดงผลมีรอยขีดข่วนได้

๖๑.๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๖๑.๑๐ การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ ๖๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดความปลอดภัยทางด้านกายภาพ ดังนี้

๖๒.๑ ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรเก็บเครื่องไว้ในสถานที่ที่มีอุปกรณ์ป้องกันขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

๖๒.๒ ผู้ใช้ไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้นฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ ๖๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ ดังนี้

๖๓.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๖๓.๒ ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

๖๓.๓ ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาหน้าจอแสดงผล (Screen Saver) โดยตั้งเวลาในกรณีไม่ได้ใช้งานในห้วงระยะเวลาขณะหนึ่ง เช่น ตั้งไว้ ๑๕ นาที เป็นต้น ให้ทำการปิดกั้นการใช้งาน (Lock) สำหรับหน้าจอแสดงผล หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๖๓.๔ ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอแสดงผลเป็นเวลานาน

๖๓.๕ ห้ามบันทึกชื่อผู้ใช้งานและรหัสผ่านไว้บนสถานที่ที่พบเห็นได้ง่าย เช่น บันทึกไว้บนอุปกรณ์คอมพิวเตอร์ บันทึกไว้บนโต๊ะทำงาน เป็นต้น

ข้อ ๖๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้รหัสผ่าน ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

ข้อ ๖๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดการสำรองข้อมูลและการกู้คืน ดังนี้

๖๕.๑ ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

๖๕.๒ ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๖๕.๓ แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

๖๕.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก ให้ปฏิบัติตามแนวทางการทำลายสื่อบันทึกข้อมูลในหมวด ๘ การจัดการเข้าถึงข้อมูลสารสนเทศและโปรแกรมประยุกต์

๖๕.๕ ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงานเพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการของหน่วยผู้ใช้งานและหน่วยงาน

## หมวด ๑๖
## การใช้งานอินเทอร์เน็ต
## (Use of the Internet)

ข้อ ๖๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตดังนี้

๖๖.๑ ให้ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS/IDS เป็นต้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้น แต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

๖๖.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาก่อนทำการเชื่อมต่ออินเทอร์เน็ตเพื่อใช้งานโปรแกรมเข้าชมเว็บไซต์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการที่โปรแกรมเข้าชมเว็บไซต์ติดตั้งอยู่ก่อนการใช้งาน

๖๖.๓ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกองทัพบกและเครือข่ายอินเทอร์เน็ตภายในหน่วยงานเพื่อกระทำการต่อไปนี้

๖๖.๓.๑ หาประโยชน์ในเชิงธุรกิจส่วนตัว

๖๖.๓.๒ เพื่อความบันเทิง ได้แก่ การเล่นเกม ดูภาพยนตร์ฟังเพลง ในเวลาราชการ

๖๖.๓.๓ กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงของหน่วยงาน เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อหน่วยงาน หรือข้อมูลสำคัญที่เป็นความลับของหน่วยงาน

๖๖.๔ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกองทัพบกและเครือข่ายอินเทอร์เน็ตภายในหน่วยงานเพื่อการกระทำผิดกฎหมาย ต่อไปนี้

๖๖.๔.๑ นำเข้าหรือเผยแพร่ ข้อมูลหรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์

๖๖.๔.๒ แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์

๖๖.๔.๓ กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นพนันออนไลน์ การนำเข้า หรือเผยแพร่สื่อลามก อนาจาร

๖๖.๔.๔ กระทำการที่ส่งผลร้าย กระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย เป็นต้น

๖๖.๔.๕ กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิ์ของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของผู้อื่น ทั้งที่เป็นข้อมูลจริง หรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่ทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๖๖.๔.๕ กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะอันเป็นเท็จเพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิดความเสียหายต่าง ๆ

๖๖.๕ ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกองทัพบก โดยผ่านความเห็นชอบจากผู้บังคับบัญชา

๖๖.๖ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับทางราชการและที่เกี่ยวข้องกับกองทัพบก โดยไม่ได้รับอนุญาตอย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต เช่น เอกสารที่กำหนดชั้นความลับ ร่างหนังสือประกาศหรือคำสั่งต่าง ๆ เอกสารการบรรยายสรุปที่เกี่ยวข้องกับความมั่นคงฯ เอกสารที่เป็นสื่ออิเล็กทรอนิกส์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงฯ เป็นต้น

๖๖.๗ ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๖๖.๘ การใช้งานกระดานสนทนา (Web Board) ของหน่วย ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลส่วนบุคคล และเป็นความลับของทางราชการ โดยไม่ได้รับอนุญาต รวมทั้งต้องไม่บันทึกข้อมูลที่เป็นการใส่ร้ายให้ร้ายบุคคลอื่น และการบันทึกข้อมูลที่ผิดกฎหมายต่าง ๆ

๖๖.๙ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

๖๖.๑๐ การใช้งานระบบเครือข่ายอินเทอร์เน็ตไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๖๖.๑๑ หลังจากใช้งานอินเทอร์เน็ตเสร็จเรียบร้อยแล้ว ให้ทำการออกจากระบบ (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๖๖.๑๒ ผู้ใช้งานต้องปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และ/หรือกฎหมาย ระเบียบ วิธีปฏิบัติทางคอมพิวเตอร์อื่น ๆ ที่เกี่ยวข้องอย่างเคร่งครัดอย่างเคร่งครัด

ข้อ ๖๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดมาตรการป้องกันและรักษาความปลอดภัยจากการเชื่อมต่ออินเทอร์เน็ตความเร็วสูงดังนี้

๖๗.๑ การขอเปิดใช้บริการเชื่อมต่ออินเตอร์เน็ตความเร็วสูง ผ่านโทรศัพท์เลขหมายเอกชน หน่วยผู้ขอใช้จะต้องเสนอขออนุมัติกองทัพบกผ่านกรมการทหารสื่อสาร (สส.) เพื่อพิจารณาความเหมาะสมและความจำเป็นในการใช้งานต่อไป

๖๗.๒ การเชื่อมต่ออินเตอร์เน็ตความเร็วสูง จะต้องไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ของทางราชการที่เชื่อมต่อกับเครือข่ายภายในกองทัพบก (Intranet) หรือเครื่องคอมพิวเตอร์ส่วนตัวที่มีข้อมูลข่าวสารของกองทัพบก ที่เป็นชั้นความลับ และ/หรือข้อมูลที่อาจส่งผลกระทบด้านความมั่นคงของประเทศโดยเด็ดขาด

ข้อ ๖๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ กรณีที่มีการให้บริการเข้าถึงระบบอินเทอร์เน็ตจากภายในหน่วยงาน โดยการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

## หมวด ๑๗
## การใช้งานจดหมายอิเล็กทรอนิกส์
## (Use of Electronic Mail)

ข้อ ๖๙ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail : @rta.mi.th) ของหน่วยงานภายในกองทัพบกต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยยื่นคำขอกับเจ้าหน้าที่หน่วยงานที่รับผิดชอบระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ของ ทบ. (โดย สส.)

ข้อ ๗๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์ดังนี้

๗๐.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกองทัพบกให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอเช่น การเปลี่ยนตำแหน่ง เปลี่ยนต้นสังกัด การลาออกจากราชการ การเกษียณอายุ เป็นต้น

๗๐.๒ ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกองทัพบก

๗๐.๓ การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

๗๐.๔ รหัสผ่านของจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

๗๐.๕ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของกองทัพบก หรือ จดหมายอิเล็กทรอนิกส์ (E-mail) ของภาครัฐเพื่อใช้ในการติดต่องานราชการ

๗๐.๖ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๗๐.๗ ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้เช่น ไม่เกิน ๓ ครั้ง

๗๐.๘ ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน เป็นต้น

๗๐.๙ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกองทัพบกหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกองทัพบก

๗๐.๑๐ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๗๐.๑๑ ผู้ใช้ควรทำการตรวจสอบเอกสารที่แนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบแฟ้มข้อมูลโดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดแฟ้มข้อมูลที่เป็น Executable File เช่น .exe, .com เป็นต้น

๗๐.๑๒ ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๗๐.๑๓ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๗๐.๑๔ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๗๐.๑๕ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะ ดังนี้

๗๐.๑๕.๑ เป็นจดหมายขยะ (Spam Mail)

๗๐.๑๕.๒ เป็นจดหมายลูกโซ่ (Chain Letter)

๗๐.๑๕.๓ เป็นการละเมิดต่อกฎหมาย หรือสิทธิ ของบุคคลอื่น

๗๐.๑๕.๕ มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๗๐.๑๖ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับที่ส่งไป

๗๐.๑๗ ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ (E-Mail) ตามความจำเป็นอย่างสม่ำเสมอ

๗๐.๑๘ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงานทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

๗๐.๑๙ ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตนเพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๗๑ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ - ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ข้อ ๗๒ ผู้ใช้งานต้องยึดถือและปฏิบัติ เรื่องหลักเกณฑ์และวิธีการปฏิบัติในการรับ - ส่งและเก็บรักษาข่าวสารและหนังสือราชการโดยจดหมายอิเล็กทรอนิกส์ ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ.๒๕๖๔ อย่างเคร่งครัด

## หมวด ๑๘
## การใช้งานทรัพย์สินทางปัญญา
## (Use of Intellectual Property)

ข้อ ๗๓ ทรัพย์สินทางปัญญา หมายถึง ผลงานอันเกิดจากความคิดสร้างสรรค์ของมนุษย์โดยทั่ว ๆ ไป โดยทรัพย์สินทางปัญญาแบ่งเป็น ๒ กลุ่มหลักคือ ทรัพย์สินอุตสาหกรรมและลิขสิทธิ์

ข้อ ๗๔ ทรัพย์สินอุตสาหกรรม คือทรัพย์สินที่จับต้องไม่ได้ที่เกี่ยวข้องกับอุตสาหกรรม ความคิดหรืองานสร้างสรรค์ หรือผลิตภัณฑ์ที่ใช้ในทางอุตสาหกรรม โดยทรัพย์สินอุตสาหกรรม ได้แก่

๗๔.๑ สิทธิบัตร (Patent)

๗๔.๒ เครื่องหมายการค้า (Trademark)

๗๔.๓ สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

๗๔.๔ ความลับทางการค้า (Trade Secrets)

๗๔.๕ แบบผังภูมิวงจรรวม (Layout - Designs Of Integrated Circuit)

ข้อ ๗๕ ลิขสิทธิ์ คืองานสร้างสรรค์อันเกิดจากความรู้ ความสามารถ ความพยายาม โดยถูกถ่ายทอดออกมา (Express) ในลักษณะใดลักษณะหนึ่ง ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ "ลิขสิทธิ์ หมายความว่า สิทธิแต่ผู้เดียวที่จะทำการใด ๆ ตามพระราชบัญญัตินี้เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น" ดังนั้น ลิขสิทธิ์จัดเป็นทรัพย์สินทางปัญญาประเภทเดียว ที่ได้รับความคุ้มครองอัตโนมัติโดยไม่ต้องจดทะเบียน ซึ่งจะคุ้มครองทันทีทุกประเทศภายใต้อนุสัญญากรุงเบิร์น (Berne Convention) เมื่องานนั้นได้ถูกสร้างสรรค์ขึ้น ดังนั้น โปรแกรมคอมพิวเตอร์ จัดเป็นลิขสิทธิ์ประเภทงานวรรณกรรม ซึ่งคุ้มครองอัตโนมัติทั่วโลกเมื่อมีการสร้างสรรค์

ข้อ ๗๖ ลิขสิทธิ์ซอฟต์แวร์ หมายถึงซอฟต์แวร์ที่มีผู้อื่นสร้างสรรค์ขึ้น หากจำเป็นจะใช้งานต้องได้รับการอนุญาตจากผู้สร้างโดยใบอนุญาต (License) ซึ่งเป็นสัญญาระหว่างผู้สร้างกับผู้ใช้ซอฟต์แวร์ ใบอนุญาตเป็นการให้สิทธิผู้ใช้ในการใช้ซอฟต์แวร์ได้โดยไม่ถือเป็นการละเมิดลิขสิทธิ์

ข้อ ๗๗ ผู้ใช้งานระบบสารสนเทศของกองทัพบกควรจะต้องปฏิบัติตามเงื่อนไขการใช้งาน และไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น ดังนี้

๗๗.๑ ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของซอฟต์แวร์หรือทรัพย์สินทางปัญญาอื่น ๆ ที่กองทัพบก หรือผู้ใช้งานมีใช้งานหรือครอบครอง

๗๗.๒ ห้ามทำซ้ำ เปลี่ยนแปลง หรือแก้ไขทรัพย์สินทางปัญญาไปสู่รูปแบบอื่นที่เป็นการละเมิดเงื่อนไขหรือข้อตกลงการใช้งาน

๗๗.๓ ห้ามสำเนาทั้งหมดหรือบางส่วนของหนังสือ บทความ เพลง ภาพยนตร์ รายงาน หรือเอกสารอื่น ๆ ที่เป็นการละเมิดเงื่อนไขของเจ้าของทรัพย์สินทางปัญญา

ข้อ ๗๘ สิ่งต่อไปนี้ไม่ถือว่าเป็นงานอันมีลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ ได้แก่

๗๘.๑ ข่าวประจำวัน และข้อเท็จจริงต่าง ๆ ที่มีลักษณะเป็นเพียงข่าวสารอันมิใช่งานในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ

๗๘.๒ รัฐธรรมนูญ และกฎหมาย

๗๘.๓ ระเบียบ ข้อบังคับ ประกาศ คำสั่ง คำชี้แจง และหนังสือโต้ตอบของกระทรวง ทบวง กรม หรือหน่วยงานอื่นใดของรัฐหรือของท้องถิ่น

๗๘.๔ คำพิพากษา คำสั่ง คำวินิจฉัย และรายงานของทางราชการ

๗๘.๕ คำแปลและการรวบรวมสิ่งต่าง ๆ ตาม (๗๘.๑) ถึง (๗๘.๔) ที่กระทรวง ทบวง กรม หรือหน่วยงานอื่นใดของรัฐหรือของท้องถิ่นจัดทำขึ้น

ข้อ ๗๙ ให้หน่วยงานในกองทัพบกที่ดำเนินการพัฒนาและใช้งานด้านระบบสารสนเทศ ปฏิบัติตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ อย่างเคร่งครัด

## หมวด ๑๙
## การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
## (Wireless LAN Access Control)

ข้อ ๘๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ดังนี้

๘๐.๑ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๘๐.๒ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) โดยเฉพาะระบบงานที่เป็นชั้นความลับดังกล่าวด้วย

๘๐.๓ ผู้ดูแลระบบต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) หรือที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าโดยไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

๘๐.๔ ผู้ดูแลระบบเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และหรือบัญชีผู้ใช้งาน โดยอนุญาตเฉพาะผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายตามที่กำหนดไว้เท่านั้น

๘๐.๕ ผู้ดูแลระบบต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๘๐.๖ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๘๐.๗ ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๘๐.๘ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานต่อหัวหน้าหน่วยงานทราบทันที

๘๐.๙ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในหน่วยงาน

๘๐.๑๐ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๘๐.๑๑ ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

ข้อ ๘๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในกองทัพบกจะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

ข้อ ๘๒ ผู้ใช้งานต้องระบุอุปกรณ์ที่จะเข้าใช้งานในเครือข่ายไร้สายของกองทัพบก นอกจากการลงทะเบียนการใช้งานแล้ว จะต้องแจ้งค่า MAC Address ของเครื่อง หรืออุปกรณ์ที่จะเข้ามาใช้งาน เพื่อให้ผู้รับผิดชอบเครือข่ายไร้สายของกองทัพบก บันทึกเป็นหลักฐานการเข้าใช้งานต่อไป

## หมวด ๒๐
## ระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน
## (Backup System and Contingency Plan)

ข้อ ๘๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางปฏิบัติในการคัดเลือกและจัดทำระบบสำรองและกู้คืนระบบ ดังนี้

๘๓.๑ กำหนดระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้

๘๓.๒ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๘๓.๓ กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้อง เป็นต้น

๘๓.๔ กำหนดความถี่ในการสำรองข้อมูลของระบบงาน เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรมีความถี่ในการสำรองข้อมูลมากขึ้น เป็นต้น

๘๓.๕ ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๘๓.๖ ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

๘๓.๗ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่

๘๓.๘ แนวทางปฏิบัติสำหรับการสำรองข้อมูลดังนี้

๘๓.๘.๑ ผู้ดูแลระบบต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามแนวทางการสำรองข้อมูลของกองทัพบก

๘๓.๘.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๘๓.๘.๓ การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำราองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๘๓.๘.๔ ให้ผู้ดูแลระบบมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบและ/หรือผู้ดูแลเครือข่ายไม่สามารถปฏิบัติงานได้

๘๓.๘.๕ ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้รับผิดชอบระบบสารสนเทศของหน่วยทราบ

๘๓.๘.๖ ให้ผู้ดูแลระบบและผู้ดูแลเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสมพร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือการสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๘๓.๘.๗ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๘๓.๘.๘ แนวทางที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

๘๓.๘.๙ สำหรับความถี่ในการสำรองข้อมูลมีดังนี้

| รายการ | ข้อมูลที่ต้องสำรอง | ความถี่ในการสำรอง |
|---|---|---|
| ระบบ E-mail | ค่าติดตั้งของระบบ (Configure) | ช่วงก่อนและหลังการเปลี่ยนค่า |
| | ข้อมูลในส่วน Mailbox | ๑ ครั้งต่อเดือน |
| Web Server | ค่าติดตั้งของระบบ (Configure) | ช่วงก่อนและหลังการเปลี่ยนค่า |
| | ข้อมูลต่าง ๆ 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 อื่น ๆ | ค่าติดตั้งของระบบ (Configure) | ช่วงก่อนและหลังการเปลี่ยนค่า |
| | ข้อมูลที่มีความสำคัญของระบบงานที่ถูกเก็บในอุปกรณ์ต่าง ๆ เหล่านั้น | ๑ ครั้งต่อเดือน |

๘๓.๘.๑๐ ผู้ดูแลระบบและผู้ดูแลเครือข่ายสารสนเทศ รับผิดชอบความถูกต้องและความสมบูรณ์ของข้อมูล ตามความถี่ในข้อ ๘๓.๘.๙

๘๓.๙ แนวทางปฏิบัติสำหรับการกู้คืนระบบดังนี้

๘๓.๙.๑ ในกรณีพบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบ และ/หรือผู้ดูแลเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้รับผิดชอบระบบสารสนเทศของหน่วย หรือผู้ที่ได้รับมอบหมายทราบ

๘๓.๙.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๘๓.๙.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันที พร้องทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

ข้อ ๘๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบกต้องกำหนดแนวทางเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินดังนี้

๘๔.๑ กำหนดระบบงานที่มีความสำคัญทั้งหมดของกองทัพบก และจัดทำเป็นบัญชีรายชื่อของระบบงาน ดังกล่าวรวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

๘๔.๒ ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงที่พบ โดยให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๘๔.๓ กำหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบงาน และข้อมูลในฐานข้อมูล เป็นต้น รวมถึงกำหนดความถี่ในการสำรองข้อมูล วิธีการสำรองข้อมูล เช่น แบบ Full Backup หรือแบบ Incremental Backup เป็นต้น สำหรับระบบงานที่มีความสำคัญเหล่านั้น

๘๔.๔ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน (Contingency Plan) เพื่อรับมือกับภัยพิบัติ ที่อาจเกิดขึ้นได้ ทั้งวิธีการทางอิเล็กทรอนิกส์ และทางกายภาพ อีกทั้งให้กำหนดห้วงในการทดสอบแผนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง โดยแผนฯ ต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

๘๔.๔.๑ การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๘๔.๔.๒ การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๘๔.๔.๓ การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

๘๔.๔.๔ การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

๘๔.๔.๕ การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ เช่น เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น

๘๔.๔.๖ การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๘๔.๕ ให้ทำการปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยมุ่งเน้นไปที่ระบบที่มีความสำคัญสูง

๘๔.๖ ให้ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่าง สม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

๘๔.๗ ให้ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้นั้นว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่อย่างน้อยปีละ ๑ ครั้ง ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และ บันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

๘๔.๘ ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินรวมทั้งเมื่อมีการปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

## หมวด ๒๑
## การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศ
## (Inspection and Assessment of Information System Security Risks)

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ และเพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ข้อ ๘๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยของข้อมูล ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่ตนเองรับผิดชอบอย่างสม่ำเสมอดังนี้

๘๕.๑ ตรวจสอบและประเมินด้านการบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศ

๘๕.๒ ตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม

๘๕.๓ ตรวจสอบและประเมินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลและการปฏิบัติการไซเบอร์

๘๕.๔ ตรวจสอบและประเมินการควบคุมการเข้าถึง

๘๕.๕ ตรวจสอบและประเมินด้านการพัฒนาระบบสารสนเทศ เช่น ด้านการจัดซื้อจัดจ้างพัฒนาระบบฯ รวมทั้งด้านการดูแลและการปรนนิบัติบำรุงระบบสารสนเทศ เป็นต้น

๘๕.๖ ตรวจสอบและประเมินด้านความพร้อมการรับมือกับเหตุการณ์เฉพาะหน้า

๘๕.๗ ตรวจสอบความสอดคล้องกับระเบียบฉบับนี้

๘๕.๘ ตรวจสอบและประเมินตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

ข้อ ๘๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก ต้องจัดให้มีการประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ ซึ่งประกอบด้วยทรัพย์สิน ๖ หมวด ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ระบบงาน และเครือข่าย ที่หน่วยรับผิดชอบอย่างน้อยปีละ ๑ ครั้ง โดยปฏิบัติตามแนวทางการประเมินดังนี้

๘๖.๑ กำหนดให้มีการจัดทำบัญชีทรัพย์สินสารสนเทศ

๘๖.๒ ระบุและประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ

๘๖.๓ จัดลำดับความเสี่ยงจากสูงมาต่ำ

๘๖.๔ จัดทำแผนการลดความเสี่ยงโดยคำนึงถึงการจัดการกับความเสี่ยงสูงก่อน

๘๖.๕ กำหนดให้มีการปฏิบัติตามแผนการลดความเสี่ยงที่กำหนดไว้และติดตามจนกระทั่งแล้วเสร็จ

๘๖.๖ กำหนดความรับผิดชอบในการตรวจสอบและประเมินความเสี่ยง

๘๖.๖.๑ กรณีการตรวจสอบภายในหน่วยงานของกองทัพบก (Internal Auditor)

๘๖.๖.๑.๑ ให้ผู้รับผิดชอบระบบสารสนเทศภายในกองทัพบก แต่งตั้งหน่วยงาน คณะกรรมการหรือคณะทำงาน สำหรับการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของกองทัพบก

๘๖.๖.๑.๒ วงรอบการตรวจสอบปีละ ๑ ครั้ง

๘๖.๖.๑.๓ ภายหลังการตรวจสอบ ให้รายงานผลการตรวจสอบให้หน่วยที่ได้รับการตรวจสอบ และผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

๗๖.๖.๒ กรณีผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๘๖.๖.๒.๑ ให้ผู้รับผิดชอบระบบสารสนเทศภายในกองทัพบกพิจารณาจัดทำโครงการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของกองทัพบก

๘๖.๖.๒.๒ โดยให้มีการจัดจ้างดำเนินการในวงรอบ ๑ ปีงบประมาณ

๘๖.๖.๒.๓ ภายหลังการตรวจสอบ ให้รายงานผลการตรวจสอบให้หน่วยที่ได้รับการตรวจสอบ และผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

## หมวด ๒๒
## การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
## (Security Incident Management)

ข้อ ๘๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกองทัพบก เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่ตรวจพบให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๘๗.๑ ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด ได้แก่ ระดับสูง ระดับกลาง หรือระดับต่ำ

๘๗.๒ แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

๘๗.๓ วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็น กรณีการบุกรุก การโจมตีระบบหรือระบบได้รับความเสียหาย กรณีที่ไม่สามารถวิเคราะห์และแก้ไขโดยหน่วยงานเองได้ ให้ประสานงานขอความช่วยเหลือจากผู้ที่มีความรู้และความเชี่ยวชาญ เช่น ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ แห่งชาติ (Thailand Computer Emergency Response Team : Thai CERT) หรือหน่วยงานภายนอกอื่น ๆ เป็นต้น

๘๗.๔ กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

๘๗.๕ จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลางขึ้นไป และแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงานดังนี้

๘๗.๕.๑ รายละเอียดเหตุการณ์

๘๗.๕.๒ วันเวลาที่เกิดขึ้น

๘๗.๕.๓ ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง

๘๗.๕.๔ สถานะของเหตุการณ์ในแต่ละช่วงเวลา

๘๗.๕.๕ ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา

๘๗.๕.๖ สาเหตุและวิธีการแก้ไข

๘๗.๕.๗ ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

**หมวด ๒๓**

**การบริหารความต่อเนื่องในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ**

**(Continuity Management in Information System Security)**

ข้อ ๘๘ เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของกองทัพหน่วยภายในกองทัพบก อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของกองทัพและหน่วยภายในกองทัพบก

ข้อ ๘๙ แนวทางปฏิบัติ

๘๙.๑ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของหน่วยที่จัดทำขึ้น

๘๙.๒ ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นอย่างน้อย ปีละ ๑ ครั้ง

๘๙.๓ ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๘๙.๔ ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรองอย่างน้อยปีละ ๑ ครั้ง

**หมวด ๒๔**

**การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ**

**(Security of Information Systems)**

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีแนวทางปฏิบัติเพิ่มเติมดังนี้

ข้อ ๙๐ ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมายหรือขัดต่อศีลธรรมอันดี เป็นต้น

ข้อ ๙๑ ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่นทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้

ข้อ ๙๒ ห้ามเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่นเพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก

ข้อ ๙๓ ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นจ้าของข้อมูลนั้น ๆ

ข้อ ๙๔ ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของหน่วยงานให้เกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น

ข้อ ๙๕ ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของหน่วยงานและของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์

ข้อ ๙๖ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง

ข้อ ๙๗ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

## หมวด ๒๕
## การประชุมผ่านสื่ออิเล็กทรอนิกส์
## (Electronic Meeting)

ข้อ ๙๘ อิเล็กทรอนิกส์ หมายถึง การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้าคลื่นแม่เหล็กไฟฟ้าหรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็กหรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น

ข้อ ๙๙ การประชุมผ่านสื่ออิเล็กทรอนิกส์ หมายถึง การประชุมที่กฎหมายบัญญัติให้ต้องมีการประชุมที่ได้กระทำผ่านสื่ออิเล็กทรอนิกส์ โดยผู้ร่วมประชุมมิได้อยู่ในสถานที่เดียวกันและสามารถประชุมปรึกษาหารือและแสดงความคิดเห็นระหว่างกันได้ผ่านสื่ออิเล็กทรอนิกส์

ข้อ ๑๐๐ ระบบควบคุมการประชุม หมายถึง ระบบเครือข่ายคอมพิวเตอร์ และ/หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เชื่อมโยงกันเป็นเครือข่าย และมีการสื่อสารข้อมูลกันโดยใช้เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือการโทรคมนาคม เพื่อให้ผู้ร่วมประชุมสามารถเข้าถึงและใช้งานสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ไม่ว่าจะเป็นการประชุมด้วยเสียงหรือทั้งเสียงและภาพ

ข้อ ๑๐๑ ผู้ให้บริการ หมายถึง ผู้ให้บริการระบบควบคุมการประชุม

ข้อ ๑๐๒ ผู้ควบคุมระบบ หมายถึง ผู้ทำหน้าที่ดูแลและบริหารจัดการระบบควบคุมการประชุม

ข้อ ๑๐๓ ผู้ร่วมประชุม หมายถึง ประธานกรรมการ รองประธานกรรมการ กรรมการอนุกรรมการ เลขานุการ และผู้ช่วยเลขานุการของคณะกรรมการ คณะอนุกรรมการ หรือคณะบุคคลอื่นตามที่กฎหมายกำหนด และให้หมายความรวมถึงผู้ซึ่งต้องชี้แจงแสดงความคิดเห็นต่อคณะกรรมการคณะอนุกรรมการ หรือคณะบุคคลนั้นด้วย

ข้อ ๑๐๔ การประชุมผ่านสื่ออิเล็กทรอนิกส์ ให้ยึดถือและปฏิบัติตาม “พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓” และ “ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓” อย่างเคร่งครัด

## หมวด ๒๖
## การปฏิบัติราชการทางอิเล็กทรอนิกส์
## (Working by Electronic)

พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ เป็นกฎหมายกลางที่มีวัตถุประสงค์หลัก ในการขจัดปัญหาและอุปสรรคทางข้อกฎหมายและกฎระเบียบต่าง ๆ เพื่อให้ประชาชนสามารถยื่นคำขอหรือติดต่อใด ๆ กับหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐ รวมทั้งการติดต่อราชการระหว่างหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐด้วยกัน สามารถทำโดยวิธีการทางอิเล็กทรอนิกส์ได้โดยชอบด้วยกฎหมาย ดังนี้

ข้อ ๑๐๕ พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ ได้ประกาศในราชกิจจานุเบกษา เมื่อ ๑๒ พ.ค. ๒๕๖๒ มีผลบังคับใช้ ตั้งแต่วันที่ ๑๐ มิ.ย. ๒๕๖๕ เป็นต้นมา กำหนดให้ทุกส่วนราชการต้องส่งเสริมให้การทำงานและการให้บริการของภาครัฐสามารถใช้วิธีการทางอิเล็กทรอนิกส์ได้ เพื่อเป็นการอำนวยความสะดวกแก่ประชาชน

ข้อ ๑๐๖ งานที่ต้องให้บริการทางอิเล็กทรอนิกส์ประกอบด้วย การสืบค้นข้อมูล การพิสูจน์และยืนยันตัวตน การจัดทำแบบคำขอและยื่นคำขอ การตรวจสอบและพิจารณาคำขอ การอนุมัติและอนุญาต การชำระค่าธรรมเนียม การออกใบอนุญาตและเอกสารอื่นพร้อมทั้งลงนาม การจัดส่งใบอนุญาตและเอกสารอื่น การติดตามสถานะและแจ้งเตือน และ การแสดงใบอนุญาต

ข้อ ๑๐๗ แนวทางวิธีการทางอิเล็กทรอนิกส์ตามพระราชบัญญัติฯ แบ่งเป็น ๓ ระดับ คือ

๑๐๗.๑ ระดับเริ่มต้น (Initial) หมายถึง หน่วยงานที่มีข้อจำกัดด้านบุคลากร เทคโนโลยีหรืองบประมาณ ให้จัดทำบริการอย่างง่ายโดยอาศัยช่องทางอีเมล์ (E-Mail) หรือ Social Media เน้นการอำนวยความสะดวกเบื้องต้น

๑๐๗.๒ ระดับมาตรฐาน (Standard) หมายถึง หน่วยงานที่มีความพร้อมทั้งบุคลากร เทคโนโลยีและงบประมาณระดับมาตรฐาน ให้จัดทำบริการรูปแบบ Web Application หรือ Mobile Application เน้นให้บริการได้ครบถ้วน ซึ่งอาจใช้บริการ Backend แพลตฟอร์มดิจิทัลกลางก็ได้

๑๐๗.๓ ระดับสูง (Advance) หมายถึง หน่วยงานที่มีความพร้อมทั้งบุคลากร เทคโนโลยีและงบประมาณระดับสูง ให้นำเทคโนโลยีที่ทันสมัยมาใช้ เช่น AI หรือ Machine Learning รองรับการประมวลผลที่ซับซ้อนและมีจำนวนมาก รวมทั้งมีความพร้อมในการเชื่อมโยงข้อมูลกับหน่วยงานอื่น ๆ

ข้อ ๑๐๘ คำแนะนำการใช้เครื่องมือตามความพร้อมของหน่วยงานทั้งในระดับเริ่มต้น ระดับมาตรฐาน ระดับสูง เพื่อให้หน่วยงานทราบถึงภาพรวมการใช้เครื่องมือสำหรับวิธีการทางอิเล็กทรอนิกส์ในกระบวนการปฏิบัติงานทุกขั้นตอนดังนี้

| เครื่องมือ / กระบวนการ | ระดับเริ่มต้น | ระดับมาตรฐาน | ระดับสูง |
|---|---|---|---|
| การสืบค้นข้อมูล | อีเมล์/สื่อสังคมออนไลน์/ เว็บบอร์ด | เว็บไซต์ หรือ Aplicaion | เว็บไซต์ หรือ Chatbot Application |
| การพิสูจน์และยืนยันตัวตน | Identity ที่มีความน่าเชื่อถือระดับที่ ๑ หรือมากกว่า (IAL1) | Identity ที่มีความน่าเชื่อถือระดับที่ ๑ หรือมากกว่า (IAL1) | Identity ที่มีความน่าเชื่อถือระดับที่ ๒ หรือมากกว่า (IAL2) |
| การจัดทำแบบคำขอและยื่นคำขอ | - PDF From<br>- Google From<br>- MS From | แบบฟอร์มอิเล็กทรอนิกส์ (E-From) | แบบฟอร์มอิเล็กทรอนิกส์ (E-From) ที่เชื่อมโยงข้อมูลแบบอัตโนมัติ |
| การตรวจสอบและพิจารณาคำขอ | พิมพ์เป็นกระดาษดำเนินการผ่านระบบสารบรรณ | ผ่านระบบที่เชื่อมต่อกับ Application ของหน่วยงาน | เพิ่มเติมการเชื่อมโยงข้อมูลกับหน่วยงานสำหรับตรวจสอบและพิจารณาคำขอ |
| การอนุมัติและอนุญาต | อนุมัติและอนุญาตใบคำขอและเอกสารที่พิมพ์เป็นกระดาษ | ผ่านระบบที่เชื่อมต่อกับ Application ของหน่วยงาน | เพิ่มเติมการใช้ลายมือชื่ออิเล็กทรอนิกส์ |
| การชำระค่าธรรมเนียม | เปิดบัญชีของหน่วยงาน | Application ของหน่วยงาน | Application ของหน่วยงาน |
| การออกใบอนุญาตและเอกสารอื่นพร้อมทั้งลงนาม | แปลงใบอนุญาต/เอกสารกระดาษเป็นอิเล็กทรอนิกส์ | จัดทำเป็นไฟล์อิเล็กทรอนิกส์ลงนามแบบ e-Signature | จัดทำตามแบบมาตรฐาน ขมธอ.11-2560 หรือ ขมธอ. 24-2563 |
| การจัดส่งใบอนุญาตและเอกสารอื่น | จัดส่งผ่านช่องทางที่ผู้ยื่นคำขอใช้ | จัดส่งผ่านทาง Application ของหน่วยงาน | จัดส่งผ่านทาง Application ของหน่วยงาน |
| การติดตามสถานะและแจ้งเตือน | แจ้งเตือนผ่านทางช่องทางที่ผู้ยื่นคำขอใช้ | แจ้งเตือนผ่าน Application ของหน่วยงาน | แจ้งเตือนผ่าน Application ของหน่วยงาน |
| การแสดงใบอนุญาต | ภาพถ่ายอิเล็กทรอนิกส์จากอุปกรณ์อิเล็กทรอนิกส์ | ภาพถ่ายจากเว็บไซต์หรือ Application ของหน่วยงาน | ภาพถ่ายจากแพลตฟอร์มดิจิทัลกลาง |

แนวทางปฏิบัติของหน่วยงานในกองทัพบกเพื่อดำเนินการตาม พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ ให้ดำเนินการดังนี้

ข้อ ๑๐๙ ใช้การรับ - ส่งอีเมล์ที่ใช้สำหรับช่องติดต่อทางอิเล็กทรอนิกส์ โดยกองทัพบกกำหนดให้ใช้โดเมน ชื่อหน่วย_servicecenter@rta.mi.th หรือ rta_servicecenter@rta.mi.th ใช้สำหรับกรมสารบรรณทหารบก

ข้อ ๑๑๐ ต้องแปลงไฟล์เอกสารเป็น PDF ที่ถูกต้องและได้มาตรฐาน เช่น มาตรฐาน PDF/A ซึ่งเป็นมาตรฐาน ISO และตัวอักษร A ย่อมาจาก "Archiving" ซึ่ง PDF/A กำหนดกฎสำหรับการเก็บรักษาเอกสารอิเล็กทรอนิกส์ในระยะยาว/สามารถอ่านได้ในอนาคตและตรวจสอบความถูกต้องได้ หรือใช้มาตรฐาน ISO 32000-2 เป็นต้น

ข้อ ๑๑๑ ต้องยึดถือและปฏิบัติตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ. ๒๕๖๔ โดยเฉพาะภาคผนวก ๖ หลักเกณฑ์และวิธีการปฏิบัติในการรับส่งและเก็บรักษาข้อมูลข่าวสารและหนังสือราชการด้วยระบบสารบรรณอิเล็กทรอนิกส์ และภาคผนวก ๗ หลักเกณฑ์และวิธีการปฏิบัติในการรับส่งและเก็บรักษาข้อมูลข่าวสารและหนังสือราชการโดยไปรษณีย์อิเล็กทรอนิกส์

ข้อ ๑๑๒ การตรวจเอกสาร ไฟล์บัตรประจำตัวประชาชน ไฟล์ทะเบียนบ้าน ไฟล์ใบขับขี่ หรืออื่น ๆ ผ่านระบบ (เว็บไซต์ Linkage Center - http://linkagemgmt.bora.dopa.go.th) หากทำไม่ได้ ใช้การส่งผ่านอีเมล์ไปให้ตรวจสอบ

ข้อ ๑๑๓ การตรวจเอกสารแบบอิเล็กทรอนิกส์ สำหรับเอกสารที่หน่วยงานของรัฐออกได้มีการรับรองโดยใช้ใบรับรองอิเล็กทรอนิกส์ที่ออกโดย Certificate Authority (CA) ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (National Root Certification Authority of Thailand : NRCA)

ข้อ ๑๑๔ การฝากไฟล์เอกสารบนระบบ Cloud เช่น Google Drive หรือ Dropbox กรณีไฟล์ที่ส่งมอบมีขนาดใหญ่ ต้องเป็นไปตามมาฐานด้านการรักษาความมั่นคงปลอดภัยระบบคลาวด์ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาต (สกมช.)

ข้อ ๑๑๕ ให้มีการใช้วีดีโอคอล บน Application Line หรือ Facebook เพื่อยืนยันตัวตนผู้ยื่นคำขอ

ข้อ ๑๑๖ ข้อมูลเปิดของหน่วยงานต้องประกาศให้ทราบบนเว็บไซต์ศูนย์กลางข้อมูลเปิดภาครัฐ www.data.go.th

ข้อ ๑๑๗ ต้องออกระเบียบการส่งต่อเรื่องภายในหน่วยว่าจะใช้อะไร เป็นช่องทางการติดต่อสื่อสารทางอิเล็กทรอนิกส์

ข้อ ๑๑๘ รวบรวมข้อมูลใบอนุญาตหรือเอกสารหลักฐานอื่นใดที่มีกฎหมายกำหนดให้ผู้รับใบอนุญาตมีหน้าที่ต้องแสดงไว้ในที่เปิดเผยที่หน่วยเป็นผู้ออก แล้วนำข้อมูลที่รวบรวมได้มาบันทึกเป็นฐานข้อมูลใบอนุญาตไว้ในรูปแบบอิเล็กทรอนิกส์ โดยใช้โปรแกรม เช่น Microsoft Excel, Google Sheets, Apple Numbers หรือแอปพลิเคชันอื่นใดก็ได้ (ถ้ามี) โดยการบันทึกในรูปแบบอิเล็กทรอนิกส์นั้นจะต้องมีข้อมูลให้ครบถ้วนตามที่ระบุไว้บนใบอนุญาตที่เป็นกระดาษ รวมทั้งระบุสถานะของใบอนุญาตแต่ละใบว่ายังมีผลใช้บังคับอยู่ ถูกพักใช้ หรือถูกเพิกถอนด้วย

ข้อ ๑๑๙ ให้หน่วยงานเปิดเผยไฟล์ข้อมูลใบอนุญาตด้วยวิธีการดังต่อไปนี้

๑๑๙.๑ เปิดเผยในเว็บไซต์ของหน่วย หรือ ในกรณีที่หน่วยงานไม่มีเว็บไซต์เป็นของตนเอง ให้หน่วยนำไฟล์ฐานข้อมูลไปสำรองเก็บไว้บน Cloud Storage เช่น Google Drive, OneDrive พร้อมทั้งตั้งสถานะให้ประชาชน หรือหน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐเข้าดูข้อมูลได้ และคัดลอก URL ช่องทางเข้าถึงมาจัดทำเป็นประกาศของหน่วยให้ประชาชน หรือหน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐทราบทางช่องทางประชาสัมพันธ์ของหน่วย

๑๑๙.๒ เปิดเผยไฟล์ฐานข้อมูลใบอนุญาตผ่านศูนย์กลางข้อมูลเปิดภาครัฐ www.data.go.th โดยหน่วยสามารถลงทะเบียนที่เว็บไซต์ https://data.go.th/pages/digital-id-e-mail และเข้าใช้งาน www.data.go.th ในฐานะเจ้าหน้าที่หน่วยงานรัฐ เพื่อบันทึกไฟล์ข้อมูลฯ ดังกล่าวไว้ในระบบ ในการนี้ให้บันทึกไฟล์ข้อมูลฯ ทุกสิ้นเดือนที่มีการปรับปรุงข้อมูล

ข้อ ๑๒๐ ทั้งนี้ ไฟล์ที่หน่วยจะส่งให้เปิดเผยตามข้อ ๑๑๙.๒ ให้ตั้งสิทธิเข้าถึงไฟล์เป็นแบบอ่านอย่างเดียว (Read-Only) เพื่อป้องกันมิให้บุคคลอื่นสามารถแก้ไขข้อมูลโดยมิได้รับอนุญาต

**หมวด ๒๗**

**การคุ้มครองข้อมูลส่วนบุคคล**

**(Personal Data Protection)**

ข้อ ๑๒๑ ข้อมูลส่วนบุคคล คือ ข้อมูลที่เกี่ยวข้องกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อมก็ตาม ตัวอย่างของข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล เบอร์โทรศัพท์ อีเมลส่วนตัว ที่อยู่ปัจจุบัน เลขบัตรประชาชน เลขหนังสือเดินทาง เลขใบอนุญาตขับขี่ ประวัติการทำงาน ข้อมูลการศึกษา ข้อมูลด้านการเงิน ข้อมูลสุขภาพ ทะเบียนรถยนต์ โฉนดที่ดิน ทะเบียนบ้าน วันเดือนปีเกิด เชื้อชาติ น้ำหนักส่วนสูง รูปถ่าย ข้อมูลบนอินเทอร์เน็ตที่ระบุตัวตนได้ เช่น Username - Password, Cookies IP Address, GPS Location เป็นต้น

ข้อ ๑๒๒ ข้อมูลที่มีความละเอียดอ่อนเป็นพิเศษ (Sensitive Personal Data) ที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องระมัดระวังในการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล เพราะเป็นข้อมูลที่มีความละเอียดอ่อนและอาจส่งผลกระทบที่ร้ายแรงต่อเจ้าของข้อมูลได้มากกว่าข้อมูลส่วนบุคคลแบบปกติ ทั้งในแง่ของการทำงาน สังคม และชีวิตความเป็นอยู่ โดยเฉพาะอาจนำไปสู่การเลือกปฏิบัติได้ ซึ่งเมื่อกระทำผิดจะทำให้มีบทลงโทษที่รุนแรงขึ้นด้วย ตัวอย่างเช่น เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อ พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลด้านสุขภาพ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ เป็นต้น

ข้อ ๑๒๓ แนวทางปฏิบัติของหน่วยในกองทัพบก เพื่อดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act : PDPA) ดังนี้

๑๒๓.๑ ตั้งคณะทำงานภายในองค์กร ได้แก่ ฝ่ายกำหนดนโยบายองค์กร ฝ่ายกฎหมาย ฝ่ายเทคโนโลยีสารสนเทศและฝ่ายบุคคล เพื่อร่วมกันกำหนดและศึกษาทำความเข้าใจบริบทของกฎหมาย เตรียมความพร้อมปรับเปลี่ยนให้องค์กรรองรับต่อ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

๑๒๓.๒ จับคู่ข้อมูล (Data Map) เพื่อตรวจสอบกระบวนการที่ใช้เก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีในองค์กร ตามกระบวนการไหลของข้อมูล (Data Flow) เพื่อให้ทราบถึงแหล่งและประเภทข้อมูล

๑๒๓.๓ แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO) เพื่อดำเนินการให้คำแนะนำ ตรวจสอบ ประสานงานให้ความร่วมมือพร้อมรักษาความลับของข้อมูลส่วนบุคคล

๑๒๓.๔ ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact) โดยกำหนดขอบเขตวัตถุประสงค์ ความจำเป็น ของข้อมูลส่วนบุคคล เพื่อนำมาจัดการความเสี่ยงและกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล

๑๒๓.๕ ระบุ บันทึกแหล่งที่มาของข้อมูลส่วนบุคคลที่หน่วยงานจัดเก็บ เพื่อกำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อสิทธิและเสรีภาพของบุคคล

๑๒๓.๖ ระบุ กำหนดฐานการประมวลผลของข้อมูลส่วนบุคคลแบบทั่วไป และแบบละเอียดอ่อน

๑๒๓.๗ กำหนดหลักเกณฑ์และวิธีการขอความยินยอมสอดคล้องกับสิทธิของเจ้าของข้อมูล รวมถึงการใช้สิทธิถอนความยินยอม ขอการเข้าถึงและสิทธิในการปรับปรุงข้อมูลให้เป็นปัจจุบัน

๑๒๓.๘ จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร พร้อมทั้งกำหนดหลักการต่าง ๆ เช่น การรวบรวม การใช้หรือการรักษาข้อมูลส่วนบุคคล เป็นต้น

๑๒๓.๙ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยต้องสอดคล้องกับมาตรฐานสากล เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย

๑๒๓.๑๐ กำกับ ดูแล ตรวจสอบและประเมินความเสี่ยง

๑๒๓.๑๑ ทบทวน ปรับปรุงกระบวนการและมาตรการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๑๒๓.๑๒ สร้างความตระหนักรู้ และฝึกอบรมให้ความรู้ให้กับผู้ที่เกี่ยวข้องเป็นประจำ

๑๒๓.๑๓ กำหนดมาตรการที่เหมาะสมด้านการรั่วไหลของข้อมูล (Data Breaches) การออกแบบและพัฒนาระบบโดยคำนึงถึงความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล (Security and Privacy by Design) รวมทั้งพัฒนาระบบเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น การใช้นามแฝง หรือการเข้ารหัสข้อมูล (Encoding)

๑๒๓.๑๔ กำหนดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลทางด้านกายภาพ (Physical Security)

๑๒๓.๑๕ กำหนดหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน

๑๒๓.๑๖ กำหนดมาตรการหรือแนวปฏิบัติที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เพียงพอ (Cross-Border Data Transfer)

ข้อ ๑๒๔ หน่วยงานในกองทัพบกจะต้องปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) โดยให้บริหารจัดการ ๓ ปัจจัย ดังนี้

๑๒๔.๑ ปัจจัยด้านบุคคล (People) ต้องดูแลและควบคุมบุคคลให้ปฏิบัติตาม PDPA โดยอาจทำได้หลายวิธี เช่น การให้ความรู้ การอบรม การให้คำแนะนำ รวมถึงการใช้หนังสือหรือเอกสารทางอิเล็กทรอนิกส์เพื่อขอความยินยอมของบุคคลนั้น ๆ

๑๑๓.๒ ปัจจัยด้านกระบวนการจัดการ (Process) ต้องตรวจสอบการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในปัจจุบันเพื่อระบุถึงที่มาของข้อมูล ประเภทของข้อมูล จัดกลุ่มข้อมูล ระบุถึงความเสี่ยงของข้อมูล และปรับเปลี่ยนวิธีการเมื่อพบว่าวิธีการนั้นมีความเสี่ยงต่อการละเมิดสิทธิข้อมูลส่วนบุคคล

๑๑๓.๓ ปัจจัยด้านเทคโนโลยี (Technology) ต้องใช้เครื่องมือที่ทันสมัยเพื่อมารองรับในการดำเนินงาน ให้การจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นไปตามพรบ. คุ้มครองข้อมูลส่วนบุคคล เช่น ระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention) ระบบแจ้งเตือน หรือระบบการเก็บข้อมูล เป็นต้น

## หมวด ๒๘
## การสร้างความตระหนักรู้ในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ
## (Raising Awareness of Information System Security)

ข้อ ๑๒๕ วัตถุประสงค์

๑๒๕.๑ เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของกองทัพบก

๑๒๕.๒ เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๑๒๕.๓ เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

ข้อ ๑๒๖ โดยหน่วยที่เกี่ยวข้องของกองทัพบกมีแนวทางปฏิบัติดังนี้

๑๒๖.๑ จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๑๒๖.๒ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๑๒๖.๓ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๑๒๖.๔ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๑๒๖.๕ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผลและสำรวจความต้องการของผู้ใช้งาน

๑๒๖.๖ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๑๒๖.๗ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

๑๒๖.๘ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกองทัพบก และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

## หมวด ๒๙
## หน้าที่และความรับผิดชอบ
## (Duties and Responsibilities)

ข้อ ๑๒๗ ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัติตามระเบียบนี้โดยเฉพาะในกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามระเบียบกองทัพบกว่าด้วยการรักษาความปลอดภัยสารสนเทศของกองทัพบก ฉบับนี้ ให้ผู้บังคับบัญชาสูงสุดในพื้นที่แต่งตั้งเจ้าหน้าที่รับผิดชอบการรักษาความปลอดภัยระบบสารสนเทศของหน่วย โดยเป็นผู้รับผิดชอบตามระเบียบฉบับนี้ ทั้งด้านการวบควบคุม กำกับดูแล การใช้งาน การบริหารความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยมีแนวทางปฏิบัติดังนี้

๑๒๗.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือและหน่วยที่เกี่ยวข้องทราบ

๑๒๗.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๑๒๗.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๑๒๗.๔ ให้พิจารณาสั่งการลงโทษทางวินัยตามแบบธรรมเนียมทหารหรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้จะโดยเจตนาหรือไม่เจตนา และการละเมิดนั้นจะเกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๑๒๘ ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการดังนี้

๑๒๘.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่าง ๆ ประมวลลับหรือรหัสผ่านที่จำเป็นในการใช้ เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนหรือเกิดเสียหายอย่างใดหรือไม่

๑๒๘.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันที ในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่ เห็นสมควร

ข้อ ๑๒๙ ความรับผิดชอบของผู้ใช้งานต่อระเบียบฉบับนี้มีดังนี้

๑๒๙.๑ ปฏิบัติตามระเบียบฯ อย่างเคร่งครัด และต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๑๒๙.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของกองทัพบก

๑๒๙.๓ ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ของกองทัพบก

๑๒๙.๔ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังผู้บังคับบัญชาและผู้รับผิดชอบระบบสารสนเทศโดยเร็วที่สุด

ข้อ ๑๓๐ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของของผู้บังคับบัญชาสามารถแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติหากจำเป็นให้รายงานหน่วยเหนือได้ตามความเหมาะสม

ข้อ ๑๓๑ ให้ส่วนราชการที่มีศูนย์สารสนเทศหรือศูนย์กรรมวิธีข้อมูลอัตโนมัติอยู่ในสังกัดสามารถออกระเบียบปลีกย่อยได้โดยไม่ขัดต่อระเบียบนี้

## หมวด ๓๐
## หน่วยโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของ ทบ.
## (Critical Information Infrastructure : CII)
## เรื่อง การจัดทำประมวลแนวทางปฏิบัติ

ในฐานะที่กองทัพบกหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ด้านความมั่นคงของประเทศ โดยกำหนดให้ กรมยุทธการทหารบก กรมการทหารสื่อสาร และศูนย์ไซเบอร์กองทัพบก เป็นหน่วยหน่วยงานรับผิดชอบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของกองทัพบก และต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลและเป็นไปตาม “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔” สรุปได้ดังนี้

ข้อ ๑๓๒ การจัดทำประมวลแนวทางปฏิบัติมีองค์ประกอบ ๓ ส่วน ดังนี้

๑๓๒.๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๓๒.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๓๒.๓ แผนการรับมือภัยคุกคามทางไซเบอร์

**ส่วนที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

**แนวปฏิบัติ**

ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบดังนี้

๑.๑ กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

๑.๒ บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (๑.๑)

๑.๓ การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด

**ส่วนที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

**แนวปฏิบัติ**

เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุม เรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหาร ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๒.๑.๑ การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยง จากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการ ปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒.๑.๒ การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหา แนวทางในการจัดการความเสี่ยงที่เหมาะสม

๒.๑.๓ การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมิน ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่าง ต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI) ด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคง ปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๒.๓ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ยอมรับได้ที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ ของหน่วยงานที่ได้รับมอบหมาย ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มี การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

## ส่วนที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์

**แนวปฏิบัติ**

๓.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดดังต่อไปนี้

๓.๑.๑ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคน และรายละเอียดการติดต่อ

๓.๑.๒ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจน ภาระหน้าที่ในการรายงานภายใต้กฎหมายและข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ

๓.๑.๓ เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

๓.๑.๔ ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๑.๕ การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

๓.๑.๖ ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

๓.๑.๗ ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

๓.๑.๘ ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

๓.๑.๙ กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๓.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๓.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

**เรื่อง กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**


ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ โดยต้องดำเนินการและจัดทำตามกรอบมาตรฐานซึ่งประกอบไปด้วย ๖ หัวข้อหลัก (ดังรูป) ดังนี้

**ข้อ ๑ Identify :** การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล ได้แก่

๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

**ข้อ ๒ Protect** : มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้นได้แก่

๒.๑ การควบคุมการเข้าถึง (Access Control)

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

**ข้อ ๓ Detect :** มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ได้แก่ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

**ข้อ ๔ Respond :** มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ ได้แก่

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

**ข้อ ๕ Recover** : มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ โดยต้องดำเนินการตามกรอบมาตรฐานการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery

**ข้อ ๖ Govern** : มาตรการการกำกับดูแล ได้แก่ การวางนโยบายควบคุม (Govern) พิจารณาความเสี่ยงขององค์กร, ผลกระทบหากเกิดภัยไซเบอร์ และเป้าหมายของการรักษาความปลอดภัยไซเบอร์ของหน่วย

## หมวด ๓๑
## เอกสารอ้างอิง
## (Reference)


๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐

๒. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๓. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๔. พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๕. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

๖. ระเบียบกองทัพบกว่าด้วยความรับผิดชอบในสิ่งอุปกรณ์ พ.ศ. ๒๕๕๕

๗. พระราชบัญญัติการกกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับที่ ๒)

๘. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๙. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑๐. ระเบียบกองทัพบกว่าด้วยการรักษาความปลอดภัยกองทัพบก พ.ศ. ๒๕๖๓

๑๑. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๕๓๖๓

๑๒. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓

๑๓. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ ฉบับที่ ๔ พ.ศ. ๒๕๖๔

๑๔. พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

๑๕. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๑๖. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๑๗. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๗ เดือน พฤษภาคม พ.ศ. ๒๕๖๗

พลเอก

( เจริญชัย หินเธาว์ )

ผู้บัญชาการทหารบก