(สำเนา)

คำสั่งกองบัญชาการกองทัพไทย

(เฉพาะ)

ที่ ๓๒๒/๖๔

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท.

พ.ศ.๒๕๖๔

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. เป็นไปด้วยความเรียบร้อย เหมาะสม และเป็นไปในแนวทางเดียวกัน สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.๒๕๕๐ พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ.๒๕๕๓ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ.๒๕๖๒ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ.๒๕๖๒ และ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ รวมถึงกฎหมายอื่นๆ ที่เกี่ยวข้อง จึงให้ดำเนินการดังนี้

๑. ยกเลิกประกาศ บก.ทท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. พ.ศ๒๕๕๙ และให้ใช้ "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. พ.ศ.๒๕๖๔" ฉบับนี้แทน

๒. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. พ.ศ.๒๕๖๔ ประกอบด้วย ผนวก ก นิยาม ผนวก ข นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. และ ผนวก ค แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท.

๓. ให้ นขต.บก.ทท./นขต.ศบท. ข้าราชการ ลูกจ้าง ทหารกองประจำการ และพนักงานราชการ ของ บก.ทท. รวมถึงหน่วยงานหรือบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ บก.ทท. ยึดถือและปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด

๔. ให้ ศชบ.ทหาร มีหน้าที่ทบทวนและปรับปรุง ผนวก ค แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. โดยมอบให้ รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. สามารถอนุมัติแนวปฏิบัติฯ ดังกล่าวได้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๓๑ มีนาคม พ.ศ. ๒๕๖๔

(ลงชื่อ) พล.อ. เฉลิมพล ศรีสวัสดิ์

(เฉลิมพล ศรีสวัสดิ์)

ศชบ.ทหาร ผบ.ทสส.

/ การแจกจ่าย...

การแจกจ่าย : สน.ผบ.ทสส., สน.รอง ผบ.ทสส. (๑), (๒), (๓), (๔), สน.เสธ.ทหาร,
สน.รอง เสธ.ทหาร (๑), (๒), (๓), (๔)
: ส่วนราชการใน บก.ทท.

สำเนาถูกต้อง
พ.อ.

(อนุพงศ์ โปร่งจิตต์)
ผอ.กสบ.สบ.ทหาร
๗ เม.ย.๖๔

พ.จ.อ.หญิง สุชาดา พิมพ์/ทาน
พ.ต. ราเชน ตรวจ

ผนวก ก (นิยาม)

ประกอบคำสั่ง บก.ทท. (เฉพาะ) ที่ ๗๒๒ /๖๔ ลง ๓๑ มี.ค.๖๔

๑. ผู้ใช้งาน หมายความว่า ข้าราชการ ลูกจ้าง ทหารกองประจำการ และพนักงานราชการของ บก.ทท. รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ บก.ทท.

๒. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ บก.ทท.

๓. สินทรัพย์ (Asset) หมายความว่า ข้อมูลระบบสารสนเทศ ทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของ บก.ทท.

๔. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๕. การพิสูจน์และยืนยันตัวตน (Identification and Authentication) หมายความว่า กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล

๖. ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล หมายความว่า เครือข่ายทางอิเล็กทรอนิกส์ที่เชื่อมโยงข้อมูลระหว่างบุคคลใดๆ หรือหน่วยงานของรัฐเพื่อประโยชน์ในการพิสูจน์และยืนยันตัวตน และการทำธุรกรรมอื่นๆ ที่เกี่ยวเนื่องกับการพิสูจน์และยืนยันตัวตน

๗. ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หรือความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๘. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๙. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

๑๐. การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอก บก.ทท.

/๑๑. ภัยคุกคาม...

๑๑. ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๑๒. ไซเบอร์ (Cyber) หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

๑๓. รอง เสธ.ทหาร หมายถึง รอง เสธ.ทหาร ที่รับผิดชอบสายงานด้านไซเบอร์

๑๔. นโยบาย หมายถึง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. ฉบับนี้

ผนวก ข (นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท.)

ประกอบคำสั่ง บก.ทท. (เฉพาะ) ที่ ๓๖๒/๖๔ ลง ๓๑ มี.ค.๖๔

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. แบ่งออกเป็น ๓ ส่วน คือ นโยบายทั่วไป (General Policy) นโยบายเฉพาะ (Specific Policy) และนโยบายเฉพาะระบบ (System-Specific Policy) ดังนี้

ส่วนที่ ๑ นโยบายทั่วไป (General Policy) ประกอบด้วย

หมวดที่ ๑ โครงสร้างด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. ประกอบด้วย

๑.๑ ผบ.ทสส. ในฐานะผู้บริหารสูงสุดของ บก.ทท. (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายฉบับนี้

๑.๒ กำหนดให้ รอง เสธ.ทหาร ในฐานะผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. (Chief Information Security Officer : CISO) เป็นผู้ที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ บก.ทท. โดยให้มีหน้าที่ตามคำสั่งแต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท.

๑.๓ กำหนดให้ ผอ.ศชบ.ทหาร เป็นผู้ที่รับผิดชอบในระดับปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. โดยให้มีหน้าที่ตามที่กำหนดไว้ในภารกิจของ ศชบ.ทหาร รวมถึงมีหน้าที่จัดทำแนวปฏิบัติ ตรวจสอบ แจ้งเตือน และแก้ไขปัญหาเกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท.

หมวดที่ ๒ การดำเนินการเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. ประกอบด้วย

๒.๑ กำหนดให้มีการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. ให้สอดคล้องกับข้อกำหนดการบริหารราชการและกฎหมายที่เกี่ยวข้อง

๒.๒ กำหนดให้การปรับปรุงแก้ไขหรือเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. จะต้องขออนุมัติต่อ ผบ.ทสส. โดยสำเนาแจกจ่ายและประกาศเผยแพร่ทางเว็บไซต์ให้กำลังพลรวมไปถึงผู้ที่เกี่ยวข้องรับทราบและถือปฏิบัติ

๒.๓ กำหนดให้การปรับปรุงแก้ไขหรือเปลี่ยนแปลงแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. โดย ผบ.ทสส. มอบอำนาจให้ รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. พิจารณาและอนุมัติในนามของ ผบ.ทสส. ได้ ทั้งนี้ โดยไม่ขัดหรือแย้งกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท.

๒.๔ ให้ ศชบ.ทหาร ตรวจสอบ ทบทวน และประเมินนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. อย่างน้อย ๑ ครั้ง/ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๒.๕ ให้ ศชบ.ทหาร ดำเนินการในส่วนที่เกี่ยวข้องกับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ประกอบด้วย

/๒.๕.๑ รวบรวม...

๒.๕.๑ รวบรวม และจัดทำรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๔๖ และขออนุมัติ ผบ.ทสส. เพื่อแจ้งไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒.๕.๒ จัดทำแนวปฏิบัติเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงซึ่งมุ่งโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ ตามมาตรา ๑๒ วรรคหนึ่ง (๒) ที่กำหนดให้ ผบ.ทสส. เป็นกรรมการโดยตำแหน่ง ในคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และมีหน้าที่ตามมาตรา ๑๓ วรรคหนึ่ง (๒) ในการดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงดังกล่าว และขออนุมัติถึง ผบ.ทสส.

<u>หมวดที่ ๓</u> การรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. ประกอบด้วย

๓.๑ ศชบ.ทหาร จัดทำกรอบแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. (Cyber Security Framework : CSF) เพื่อใช้เป็นหลักในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ บก.ทท. โดยให้สอดคล้องกับ มาตรา ๑๓ วรรคสอง และ มาตรา ๔๔ แห่ง พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ รวมถึงกรอบแนวทางการบริหารความเสี่ยงด้านไซเบอร์ (Risk Management Framework : RMF) ทั้งนี้ ให้จัดทำเป็นแนวปฏิบัติและอย่างน้อยต้องประกอบด้วยเนื้อหา ดังนี้

๓.๑.๑ การแบ่งประเภทสินทรัพย์ (Asset Categorization)

๓.๑.๒ การกำหนดมาตรการควบคุม (Selecting Controls)

๓.๑.๓ การวางมาตรการควบคุม (Implementing Controls)

๓.๑.๔ การตรวจประเมินด้านความมั่นคงปลอดภัย (Security Assessment)

๓.๑.๕ การดำเนินการแก้ไข (Authorization)

๓.๑.๖ การเฝ้าระวังและติดตาม (Monitoring Controls)

๓.๒ การกำหนดมาตรการควบคุม (Selecting Controls) ตามข้อ ๓.๑.๒ อย่างน้อยต้องครอบคลุมเนื้อหาดังต่อไปนี้

๓.๒.๑ การควบคุมการเข้าถึง (Access Control : AC)

๓.๒.๑.๑ การควบคุมการเข้าถึง อย่างน้อยต้องครอบคลุมในเรื่อง การเข้าถึงระบบสารสนเทศ การเข้าถึงระบบเครือข่าย การเข้าถึงระบบปฏิบัติการ และการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๓.๒.๑.๒ สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการควบคุมการเข้าถึงระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๒ การสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training : AT) ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักในการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ บก.ทท.

/๓.๒.๓ การตรวจประเมิน...

๓.๒.๓ การตรวจประเมินมาตรฐาน (Audit and Accountability : AU)

๓.๒.๓.๑ ศชบ.ทหาร ในฐานะสายวิทยาการด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. เป็นหน่วยรับผิดชอบในการตรวจประเมินมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. และให้ดำเนินการตรวจประเมินมาตรฐานให้กับระบบสารสนเทศของ บก.ทท. อย่างน้อย ๑ ครั้ง/ปี โดยให้จัดทำเป็นแผนการตรวจประเมินมาตรฐานประจำปี ซึ่งจะต้องให้ความสำคัญต่อระบบสารสนเทศของ บก.ทท. ที่มีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" เป็นลำดับแรก หรือตามสั่งการของผู้บังคับบัญชา ทั้งนี้ ให้อำนาจ รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. สามารถอนุมัติแผนดังกล่าวได้

๓.๒.๓.๒ การตรวจประเมิน ตามข้อ ๓.๒.๓.๑ ต้องดำเนินการโดยผู้ตรวจสอบภายในระบบสารสนเทศ (Information System Auditor) ของ ศชบ.ทหาร ที่ได้มาตรฐานอย่างน้อยต้องผ่านการอบรมเกี่ยวกับ ISO/IEC 27001 หรือได้รับใบรับรองมาตรฐาน ISACA Certified Information Systems Auditor (CISA) หรือ IRCA ISO/IEC 27001 Lead Auditor หรือใบรับรองในลักษณะเดียวกัน ตามที่ ศชบ.ทหาร กำหนด

๓.๒.๓.๓ สตน.ทหาร ในฐานะหน่วยตรวจสอบภายในของ บก.ทท. (Internal Auditor) มีหน้าที่ตรวจสอบภายในด้านเทคโนโลยีสารสนเทศให้กับ นขต.บก.ทท. ตามที่กฎหมายกำหนด ทั้งนี้ ให้ดำเนินการร่วมกับ ศชบ.ทหาร เพื่อให้การตรวจสอบภายในด้านเทคโนโลยีสารสนเทศมีความเป็นมาตรฐานและเป็นไปในทิศทางเดียวกัน

๓.๒.๓.๔ ในกรณีที่ระบบสารสนเทศ ตามข้อ ๓.๒.๓.๑ อยู่บนเครือข่ายสารสนเทศเพื่อการควบคุมบังคับบัญชาของ บก.ทท. ให้ ศชบ.ทหาร ตรวจประเมินมาตรฐานตามนโยบายฉบับนี้ รวมถึง พ.ร.บ.กฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓ ด้วย

๓.๒.๓.๕ ศชบ.ทหาร รายงานผลการตรวจประเมินมาตรฐาน ตามข้อ ๓.๒.๓.๑ ถึง ผบ.ทสส. ในกรณีที่ตรวจพบว่าในหน่วยเดียวกันมีการละเมิดนโยบายฉบับนี้ซ้ำในประเด็นเดิมติดต่อกัน ให้ ศชบ.ทหาร ระบุข้อตรวจพบซ้ำดังกล่าวไว้ในรายงานผลการตรวจประเมินมาตรฐานด้วย

๓.๒.๓.๖ นขต.บก.ทท. จัดทำรายงานการประเมินตนเองทางไซเบอร์ นขต.บก.ทท. (Self Assessment Report : SAR) ตามแบบฟอร์มที่ ศชบ.ทหาร กำหนด อย่างน้อย ๑ ครั้ง/ปี พร้อมจัดส่งสำเนาให้ ศชบ.ทหาร เพื่อใช้ในการวิเคราะห์ ติดตามผล และปรับปรุงแก้ไขต่อไป

๓.๒.๔ การรับรองและประเมินความมั่นคงปลอดภัย (Security Assessment and Authorization : CA)

๓.๒.๔.๑ ศชบ.ทหาร เป็นหน่วยรับผิดชอบในการประเมินช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Testing) สำหรับระบบสารสนเทศของ บก.ทท. และให้ดำเนินการทดสอบเจาะระบบให้กับระบบสารสนเทศของ บก.ทท. อย่างน้อย ๑ ครั้ง/ปี โดยให้จัดทำเป็นแผนการทดสอบเจาะระบบประจำปีซึ่งจะต้องให้ความสำคัญต่อระบบสารสนเทศของ บก.ทท. ที่มีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" เป็นลำดับแรก หรือตามสั่งการของผู้บังคับบัญชา ทั้งนี้ ให้อำนาจ รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. สามารถอนุมัติแผนดังกล่าวได้

/๓.๒.๔.๒ ศชบ.ทหาร...

๓.๒.๔.๒ ศชบ.ทหาร รายงานผลการทดสอบเจาะระบบ ตามข้อ ๓.๒.๔.๑ ถึง ผบ.ทสส.

๓.๒.๔.๓ นขต.บก.ทท. อาจดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) หรือทดสอบเจาะระบบ (Penetration Testing) สำหรับระบบสารสนเทศของหน่วยได้ ทั้งนี้ ให้แจ้ง ศชบ.ทหาร ทราบก่อนเริ่มดำเนินการ เพื่อหารือแนวทางในการลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

๓.๒.๕ การจัดการด้านคอนฟิกเกอเรชัน (Configuration Management : CM) สส.ทหาร และ ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักร่วมกันในการจัดการด้านคอนฟิกเกอเรชัน ให้มีความมั่นคงปลอดภัย สำหรับระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๖ แผนเตรียมความพร้อมกรณีฉุกเฉิน (Contingency Planning : CP) สส.ทหาร จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อรับมือกับเหตุการณ์ที่อาจส่งผลกระทบต่อความต่อเนื่องในการปฏิบัติงานระบบสารสนเทศในภาพรวมของ บก.ทท. และ เป็นหน่วยรับผิดชอบหลักในการสำรองข้อมูลระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๗ การพิสูจน์และยืนยันตัวตน (Identification and Authentication : IA)

๓.๒.๗.๑ การพิสูจน์และยืนยันตัวตน อย่างน้อยต้องไม่ต่ำกว่าที่คณะกรรมการหรือคณะกรรมการ ตามมาตรา ๓๔/๔ วรรคสอง แห่ง พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ และที่แก้ไขเพิ่มเติม พ.ศ.๒๕๕๑ และ พ.ศ.๒๕๖๒ แล้วแต่กรณีประกาศกำหนด

๓.๒.๗.๒ สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการพิสูจน์และยืนยันตัวตนในภาพรวมของ บก.ทท.

๓.๒.๘ การรับมือเหตุการณ์ทางไซเบอร์ (Incident Response : IR) ศชบ.ทหาร จัดทำขั้นตอนปฏิบัติในการรับมือเหตุการณ์ทางไซเบอร์ บก.ทท. ซึ่งต้องเป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๑๓ วรรคหนึ่ง (๔) แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และเป็นหน่วยรับผิดชอบหลักในการรับมือเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๙ การบำรุงรักษา (Maintenance : MA)

๓.๒.๙.๑ สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการบำรุงรักษาระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๙.๒ ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักในการบำรุงรักษาระบบรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ บก.ทท.

๓.๒.๑๐ การป้องกันสื่อบันทึกข้อมูล (Media Protection : MP) สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการป้องกันสื่อบันทึกข้อมูลระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๑๑ การป้องกันทางกายภาพและสภาพแวดล้อม (Physical and Environmental Protection : PE) สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการป้องกันทางกายภาพและสภาพแวดล้อมระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๑๒ การวางแผน (Planning : PL) สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการวางแผนการให้บริการระบบสารสนเทศในภาพรวมของ บก.ทท.

/๓.๒.๑๓ การรักษา...

๓.๒.๑๓ การรักษาความปลอดภัยบุคคล (Personnel Security : PS)

๓.๒.๑๓.๑ สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการรักษาความปลอดภัยผู้ปฏิบัติงานด้านสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๑๓.๒ ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักในการรักษาความปลอดภัยผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ บก.ทท.

๓.๒.๑๔ การประเมินความเสี่ยง (Risk Assessment : RA)

๓.๒.๑๔.๑ นขต.บก.ทท. ประเมินความเสี่ยงด้านไซเบอร์ของหน่วยอย่างน้อย ๑ ครั้ง/ปี ตามแบบฟอร์มที่ ศชบ.ทหาร กำหนด

๓.๒.๑๔.๒ ศชบ.ทหาร ประเมินความเสี่ยงด้านไซเบอร์ในภาพรวมของ บก.ทท. อย่างน้อย ๑ ครั้ง/ปี และให้รายงานถึง ผบ.ทสส. รวมทั้งรวบรวมและสรุปรายงานผลการประเมินความเสี่ยงด้านไซเบอร์ของ นขต.บก.ทท. เสนอ รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. ทราบอย่างน้อย ๑ ครั้ง/ปี

๓.๒.๑๕ การจัดหาระบบและบริการ (Systems and Services Acquisition : SA)

๓.๒.๑๕.๑ สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการจัดหาระบบ และบริการระบบสารสนเทศในภาพรวมของ บก.ทท.

๓.๒.๑๕.๒ ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักในการจัดหาระบบสารสนเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ บก.ทท. และจัดการฝึกอบรมผู้พัฒนาระบบสารสนเทศของ นขต.บก.ทท. อย่างน้อย ๑ ครั้ง/ปี ให้สามารถพัฒนาระบบสารสนเทศซึ่งมีความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้น

๓.๒.๑๕.๓ นขต.บก.ทท. ที่มีการพัฒนาระบบสารสนเทศขึ้นใช้งานใน บก.ทท. จะต้องผ่านการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ของระบบดังกล่าวโดย ศชบ.ทหาร เสียก่อน จึงจะสามารถนำระบบดังกล่าวไปติดตั้งและใช้งานในสภาพแวดล้อมจริงได้

๓.๒.๑๖ การป้องกันระบบและการสื่อสาร (System and Communications Protection : SC)

๓.๒.๑๖.๑ สส.ทหาร เป็นหน่วยรับผิดชอบหลักเกี่ยวกับการป้องกันระบบและการสื่อสารในภาพรวมของ บก.ทท. ในหัวข้อต่อไปนี้

๓.๒.๑๖.๑ (๑) การตัดการเชื่อมต่อ (Network Disconnect and Isolation)

๓.๒.๑๖.๑ (๒) การเชื่อมต่อสู่เครือข่ายสาธารณะ (Public Access Protections)

๓.๒.๑๖.๑ (๓) การบริหารกุญแจ (Cryptographic Key Management and Protection)

๓.๒.๑๖.๒ ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักเกี่ยวกับการป้องกันระบบและการสื่อสารในภาพรวมของ บก.ทท. ในหัวข้อต่อไปนี้

/๓.๒.๑๖.๒ (๑) การปกป้อง...

๓.๒.๑๖.๒ (๑) การปกป้องเครือข่าย (Network Protection)

๓.๒.๑๖.๒ (๒) การปกป้องเครื่องแม่ข่าย (Server Protection)

๓.๒.๑๖.๒ (๓) การปกป้องผู้ใช้งาน (Endpoint Protection)

๓.๒.๑๗ ความถูกต้องครบถ้วนของระบบและสารสนเทศ (System and Information Integrity : SI)

๓.๒.๑๗.๑ สส.ทหาร เป็นหน่วยรับผิดชอบหลักเกี่ยวกับความถูกต้องครบถ้วนของระบบและสารสนเทศในภาพรวมของ บก.ทท. ในหัวข้อต่อไปนี้

๓.๒.๑๗.๑ (๑) การตรวจสอบข้อมูลก่อนนำเข้าระบบ (Information Input Validation)

๓.๒.๑๗.๑ (๒) ความถูกต้องครบถ้วนของซอฟต์แวร์ เฟิร์มแวร์ และข้อมูล (Software, Firmware, and Information Integrity)

๓.๒.๑๗.๒ ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักเกี่ยวกับความถูกต้องครบถ้วนของระบบและสารสนเทศในภาพรวมของ บก.ทท. ในหัวข้อต่อไปนี้

๓.๒.๑๗.๒ (๑) การป้องกันชุดคำสั่งที่ไม่ประสงค์ดี (Malicious Code Protection)

๓.๒.๑๗.๒ (๒) การเฝ้าระวังและตรวจจับ (Information System Monitoring)

๓.๒.๑๗.๒ (๓) การแจ้งเตือนและให้ข้อเสนอแนะ (Security Alerts, Advisories, and Directives)

๓.๒.๑๗.๒ (๔) การป้องกันสแปม (Spam Protection)

๓.๓ การวางมาตรการควบคุม (Implementing Controls) ตามข้อ ๓.๑.๓ มีวัตถุประสงค์เพื่อให้กับระบบสารสนเทศของ นขต.บก.ทท. ที่ได้มีการกำหนดมาตรการควบคุม (Selecting Controls) ไว้แล้ว สามารถดำเนินการวางมาตรการควบคุมได้อย่างมีประสิทธิภาพ ทั้งนี้ ให้เป็นไปตามที่แนวปฏิบัติใน ผนวก ค กำหนด

๓.๔ การตรวจประเมินด้านความมั่นคงปลอดภัย (Security Assessment) ตามข้อ ๓.๑.๔ มีวัตถุประสงค์เพื่อประเมินผลการดำเนินการวางมาตรการควบคุม (Implementing Controls) ว่าได้มีการดำเนินการอย่างถูกต้อง (Correctly) ตรงตามความมุ่งหมายของมาตรการควบคุม (Operating as Intended) รวมถึงได้ผลลัพธ์ตรงตามความต้องการ (Producing the Desired Outcome) ทั้งนี้ ให้เป็นไปตามที่แนวปฏิบัติใน ผนวก ค กำหนด

๓.๕ การดำเนินการแก้ไข (Authorization) ตามข้อ ๓.๑.๕ มีวัตถุประสงค์เพื่อให้เกิดการดำเนินการแก้ไขข้อตรวจพบภายหลังการตรวจประเมินด้านความมั่นคงปลอดภัย (Security Assessment) ดังนี้

๓.๕.๑ ภายหลัง ผบ.ทสส. รับทราบรายงานผลการตรวจประเมินมาตรฐาน ตามข้อ ๓.๒.๓.๕ หากพบว่ามีการละเมิดนโยบายฉบับนี้ ให้ หน.นขต.บก.ทท. กำกับดูแลให้หน่วยของตนมีการแก้ไขข้อตรวจพบดังกล่าวโดยเร็ว ทั้งนี้ ต้องไม่เกิน ๙๐ วัน นับตั้งแต่วันที่ หน.นขต.บก.ทท. รับทราบรายงานผลดังกล่าว พร้อมรายงานผลการปฏิบัติให้ ศชบ.ทหาร ทราบ รวมทั้งให้ ศชบ.ทหาร รายงานผลการแก้ไขดังกล่าวถึง ผบ.ทสส. ด้วย

/๓.๕.๒ ภายหลัง...

๓.๕.๒ ภายหลัง หน.นขต.บก.ทท. รับทราบรายงานผลการตรวจประเมินด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วย ตามข้อ ๓.๒.๓.๖ หากพบว่ามีการละเมิดนโยบายฉบับนี้ให้ หน.นขต.บก.ทท. กำกับดูแลให้หน่วยของตนมีการแก้ไขข้อตรวจพบดังกล่าวโดยเร็ว ทั้งนี้ ต้องไม่เกิน ๙๐ วัน นับตั้งแต่วันที่ หน.นขต.บก.ทท. รับทราบรายงานผลดังกล่าว

๓.๖ การเฝ้าระวังและติดตาม (Monitoring Controls) ตามข้อ ๓.๑.๖ มีวัตถุประสงค์เพื่อติดตามการดำเนินการตามข้อ ๓.๑.๑ - ๓.๑.๕ ให้มีประสิทธิภาพ ทั้งนี้ ให้เป็นไปตามที่แนวปฏิบัติใน ผนวก ค กำหนด

๓.๗ ศชบ.ทหาร จัดทำสถาปัตยกรรมด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. (RTARF Cybersecurity Enterprise Architecture) เพื่อใช้เป็นแนวทางในการพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ใน บก.ทท. ได้อย่างคุ้มค่า มีประสิทธิภาพ และสอดคล้องกับภารกิจของ บก.ทท. โดยให้จัดทำเป็นแนวปฏิบัติ และขออนุมัติถึง ผบ.ทสส. ทั้งนี้ อย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

๓.๗.๑ สถานะปัจจุบัน (Current State)

๓.๗.๒ สถานะอนาคต (Future State)

๓.๗.๓ การวิเคราะห์ความแตกต่าง (Gap Analysis)

๓.๗.๔ แผนที่แนวทางเพื่อให้สามารถบรรลุถึงสถานะอนาคต (Roadmap)

นอกจากนี้ เพื่อให้สถาปัตยกรรมด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. มีความสอดคล้องกับสถาปัตยกรรมด้านเทคโนโลยีสารสนเทศของ บก.ทท. (RTARF Information Technology Enterprise Architecture) จึงให้ สส.ทหาร และ ศชบ.ทหาร ร่วมกันรับผิดชอบในการบูรณาการสถาปัตยกรรมทั้งสองส่วนข้างต้น ให้สอดคล้องกับความต้องการของ บก.ทท. ตามวิสัยทัศน์ Digital HQ และ Smart HQ

ส่วนที่ ๒ นโยบายเฉพาะ (Specific Policy) ประกอบด้วย

<u>หมวดที่ ๑</u> นโยบายเฉพาะสำหรับผู้ใช้งาน (Acceptable Use Policy)

๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง และห้ามมิให้ใช้ร่วมกับผู้อื่น รวมทั้งห้ามมิให้เผยแพร่ หรือแจกจ่ายให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

๑.๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ อันเกิดจากบัญชีชื่อผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๑.๓ ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความมั่นคงปลอดภัย ตามที่กำหนดไว้ในนโยบายฉบับนี้

๑.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทันทีที่ได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๑.๕ ผู้ใช้งานต้องทำการพิสูจน์และยืนยันตัวตน (Identification and Authentication) ทุกครั้งก่อนที่จะใช้ระบบสารสนเทศของ บก.ทท. และหากการพิสูจน์และยืนยันตัวตนนั้นมีปัญหา หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบของหน่วยทราบทันที

/๑.๖ เมื่อผู้ใช้งาน...

๑.๖ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ จะต้องตั้งค่าให้เครื่องคอมพิวเตอร์ทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง ตามที่กำหนดไว้ในนโยบายฉบับนี้

๑.๗ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของ บก.ทท. ที่ได้รับมอบไว้ให้ใช้งาน

๑.๘ ทรัพย์สินและระบบสารสนเทศต่างๆ ที่ บก.ทท. จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของ บก.ทท. เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่ บก.ทท. มิได้กำหนด หรือทำให้เกิดความเสียหายต่อ บก.ทท.

๑.๙ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่ บก.ทท. มอบไว้ให้ใช้งาน และผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

๑.๑๐ ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของ บก.ทท. ถือเป็นทรัพย์สินของ บก.ทท. ห้ามมิให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๑.๑๑ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บ รักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามสมควร โดย บก.ทท. จะเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลดังกล่าว โดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ บก.ทท. ต้องทำการตรวจสอบข้อมูลซึ่งคาดว่าข้อมูลนั้นเกี่ยวข้องกับ บก.ทท. หรือข้อมูลนั้นอยู่ในทรัพย์สินสารสนเทศของ บก.ทท. ซึ่งชุดตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของ ศชบ.ทหาร สามารถทำการรวบรวม บันทึก และตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวดที่ ๒ นโยบายเฉพาะสำหรับผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Operation Policy)

๒.๑ ในกรณีที่ ศชบ.ทหาร ตรวจพบเหตุการณ์ที่คาดว่าจะเป็นภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบสารสนเทศของ บก.ทท. ให้ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท. และนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. ดำเนินการร่วมกับส่วนรับมือเหตุการณ์ทางไซเบอร์ของ ศชบ.ทหาร เพื่อแก้ไขปัญหาดังกล่าว

๒.๒ ในกรณีที่ ศชบ.ทหาร ตรวจพบเหตุการณ์ที่คาดว่าจะเป็นภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบสารสนเทศของ บก.ทท. ให้ชุดตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของ ศชบ.ทหาร มีอำนาจเข้าดำเนินการเก็บรวบรวมพยานหลักฐานใน นขต.บก.ทท. ได้ทันที ทั้งนี้ ให้แจ้งหัวหน้าหน่วยดังกล่าวก่อนเข้าดำเนินการเก็บพยานหลักฐานด้วย

๒.๓ ชุดตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของ ศชบ.ทหาร ต้องเก็บรวบรวมพยานหลักฐานทางดิจิทัลใน นขต.บก.ทท. เท่าที่จำเป็น และต้องเก็บรักษาพยานหลักฐานดังกล่าวไว้เป็นความลับ ในกรณีที่เกิดการรั่วไหลของข้อมูลให้ ศชบ.ทหาร รายงานเหตุการณ์ให้ รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. ทราบโดยเร็ว

๒.๔ ศชบ.ทหาร จัดให้มีสถานที่และมาตรการในการเก็บพยานหลักฐานทางดิจิทัลให้เป็นมาตรฐาน สามารถใช้เป็นพยานหลักฐานได้เป็นอย่างดี เพื่อป้องกันมิให้ผู้ที่ไม่เกี่ยวข้องสามารถล่วงรู้ข้อมูลดังกล่าวได้

/๒.๕ ขว.ทหาร...

๒.๕ ขว.ทหาร จัดทำทำเนียบกำลังรบด้านไซเบอร์ เพื่อให้ทราบถึงขีดความสามารถด้านไซเบอร์ของประเทศต่างๆ

๒.๖ ศชบ.ทหาร พัฒนาระบบฐานข้อมูลภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence Database) ที่อาจส่งผลกระทบต่อระบบสารสนเทศของ บก.ทท. ซึ่งจะนำไปสู่การป้องกัน เฝ้าระวัง ตรวจจับ และรับมือกับภัยคุกคามดังกล่าว ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

๒.๗ ศชบ.ทหาร จัดให้มีสถานที่ในการพัฒนาบุคลากรด้านไซเบอร์ของ บก.ทท. เพื่อให้มีขีดความสามารถที่เพียงพอในการป้องกันภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม ตามนโยบายฉบับนี้

๒.๘ หน.นขต.บก.ทท. แต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง และนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ รวมไปถึงการดำเนินการเพื่อปรับปรุงคำสั่งแต่งตั้งให้เป็นปัจจุบันอยู่เสมอ พร้อมทั้งส่งสำเนาให้ ศชบ.ทหาร ทราบ เพื่อใช้ในการติดต่อประสานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกันต่อไป

๒.๙ นขต.บก.ทท. อาจพิจารณาจัดทำนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยได้ ทั้งนี้ โดยไม่ขัดหรือแย้งกับนโยบายฉบับนี้

๒.๑๐ นขต.บก.ทท. จะต้องมีระบบหรือโปรแกรมรักษาความมั่นคงปลอดภัยไซเบอร์ติดตั้งบนเครื่องคอมพิวเตอร์ ทั้งเครื่องแม่ข่ายและเครื่องลูกข่ายของหน่วย ตามที่ ศชบ.ทหาร กำหนด ในกรณีที่ไม่มีระบบหรือโปรแกรมรักษาความมั่นคงปลอดภัยไซเบอร์ติดตั้ง และส่งผลกระทบต่อระบบสารสนเทศของ บก.ทท. ให้ สส.ทหาร ดำเนินการระงับการเชื่อมต่อของเครื่องคอมพิวเตอร์ดังกล่าวจากเครือข่าย บก.ทท. โดยเร็ว

ส่วนที่ ๓ นโยบายเฉพาะระบบ (System-Specific Policy) ประกอบด้วย

<u>หมวดที่ ๑</u> นโยบายระบบสารสนเทศเพื่อการควบคุมบังคับบัญชา (Command and Control System Policies) ประกอบด้วย

๑.๑ เนื่องจากระบบสารสนเทศเพื่อการควบคุมบังคับบัญชาถือว่าเป็นระบบที่มีความสำคัญสูงสุดของ บก.ทท. และมีผลกระทบโดยตรงต่อความมั่นคงของประเทศ จึงให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ตามนโยบายฉบับนี้ รวมไปถึง พ.ร.ฎ.ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓

๑.๒ การดำเนินการตามข้อ ๑.๑ ให้พิจารณาถึงระดับความเสี่ยงด้านไซเบอร์เป็นสำคัญ

๑.๓ เพื่อให้ ศบท. มีการรักษาความปลอดภัยไซเบอร์สอดคล้องกับนโยบายฉบับนี้ จึงกำหนดให้หน่วยงานใน ศบท. มีบทบาทหน้าที่ และความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ดังต่อไปนี้

๑.๓.๑ ฝสส.ศบท. รับผิดชอบในฐานะผู้ดูแลบัญชีผู้ใช้ (Account Manager) ผู้ดูแลระบบ (System Administrator) และผู้ดูแลข้อมูลจราจรคอมพิวเตอร์ (Log Controller) ในภาพรวมของ ศบท.

๑.๓.๒ ศรช.ศบท. รับผิดชอบในฐานะนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ ศบท.

/๑.๓.๓ ฝ่ายต่างๆ...

๑.๓.๓ ฝ่ายต่างๆ ใน ศบท. ซึ่งมีการจัดหาและติดตั้งใช้งานระบบสารสนเทศบน ศบท. ทั้งที่มีการเชื่อมต่อ และมิได้เชื่อมต่อกับระบบระบบสารสนเทศเพื่อการควบคุมบังคับบัญชา (Command and Control System) มีความรับผิดชอบในฐานะนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ในฝ่ายของตนเอง

หมวดที่ ๒ นโยบายระบบสารสนเทศเพื่อการบริหารงานทั่วไป (Management Information System Policies)

๒.๑ ศชบ.ทหาร และ สส.ทหาร จัดทำข้อตกลงในการปฏิบัติงานร่วมกัน (Operational Level Agreement : OLA) ดังนี้

๒.๑.๑ ศชบ.ทหาร กำหนดความต้องการด้านการให้บริการทางสารสนเทศ บก.ทท. จาก สส.ทหาร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้

๒.๑.๑.๑ การบริหารคอนฟิเกอเรชัน (Configuration Management)

๒.๑.๑.๒ การบริหารโปรแกรมปิดช่องโหว่ (Patch Management)

๒.๑.๑.๓ แผนกู้คืนระบบ (Disaster Recovery Plan)

๒.๑.๑.๔ แผนเผชิญเหตุด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๒.๑.๑.๕ บัญชีสินทรัพย์และผังเครือข่าย (Asset Inventory and Network Diagram)

๒.๑.๑.๖ การควบคุมการเข้าถึง (Access Control)

๒.๑.๑.๗ การจราจรทางคอมพิวเตอร์ (Log Management)

๒.๑.๑.๘ การเข้าถึงจากระยะไกล (Remote Access)

๒.๑.๑.๙ การบริหารแบนด์วิธ (Bandwidth Management)

๒.๑.๑.๑๐ การบริหารผู้ใช้ (User Account Management)

๒.๑.๑.๑๑ การพิสูจน์และยืนยันตัวตน (Identification and Authentication)

๒.๑.๒ สส.ทหาร กำหนดความต้องการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. จาก ศชบ.ทหาร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้

๒.๑.๒.๑ สถาปัตยกรรมด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity EA)

๒.๑.๒.๒ การประเมินความเสี่ยงด้านไซเบอร์ (Risk Assessment)

๒.๑.๒.๓ การประเมินช่องโหว่ (Vulnerability Assessment)

๒.๑.๒.๔ การทดสอบเจาะระบบ (Penetration Testing)

๒.๑.๒.๕ การเฝ้าระวังและตรวจจับทางไซเบอร์ (Network Security Monitoring)

๒.๑.๒.๖ การรับมือเหตุการณ์ทางไซเบอร์ (Incident Response)

๒.๑.๒.๗ การตรวจประเมินมาตรฐาน (Auditing)

๒.๑.๒.๘ ข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence)

๒.๑.๒.๙ การฝึกการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Exercise)

๒.๑.๒.๑๐ การอบรมเพิ่มพูนความรู้ทางไซเบอร์ (Cybersecurity Awareness)

๒.๒ ศชบ.ทหาร และ สส.ทหาร รายงานผลการจัดทำข้อตกลงตามข้อ ๒.๑ ให้ รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. อนุมัติภายใน ๙๐ วัน นับตั้งแต่ ศชบ.ทหาร และ สส.ทหาร รับทราบนโยบายฉบับนี้

/บทเฉพาะกาล...

บทเฉพาะกาล

เนื่องจากนโยบายฉบับนี้ได้รับการอนุมัติจาก ผบ.ทสส. และเริ่มมีผลบังคับใช้ในปีงบประมาณ พ.ศ.๒๕๖๔ ทำให้ นขต.บก.ทท. มีความจำเป็นต้องใช้เวลาในการปรับแนวทางการปฏิบัติงานเพื่อให้เกิดความสอดคล้องกับนโยบาย จึงให้ดำเนินการ ดังนี้

๑. ศชบ.ทหาร ตรวจประเมินมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. ตามแผนการตรวจประเมินมาตรฐาน ประจำปีงบประมาณ พ.ศ.๒๕๖๔ ในลักษณะของการตรวจแนะนำ เพื่อให้ นขต.บก.ทท. ซึ่งเป็นหน่วยรับตรวจ มีความเข้าใจเกี่ยวกับการปฏิบัติตามนโยบายฉบับนี้เพิ่มมากขึ้น ทั้งนี้ ให้รายงานผลการตรวจประเมินมาตรฐาน ประจำปีงบประมาณ พ.ศ.๒๕๖๔ ถึง ผบ.ทสส. ด้วย

๒. การดำเนินการของ ศชบ.ทหาร ที่เกี่ยวข้องกับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ประกอบด้วย การจัดทำแนวปฏิบัติเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงซึ่งมุ่งโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ ตามมาตรา ๑๒ วรรคหนึ่ง (๒) การจัดทำแผนการรับมือเหตุการณ์ทางไซเบอร์ บก.ทท. ซึ่งต้องสอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) การจัดทำกรอบแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. (RTARF Cybersecurity Framework) เพื่อใช้เป็นหลักในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของ บก.ทท. ให้สอดคล้องกับ มาตรา ๑๓ วรรคสอง และ มาตรา ๔๔ รวมถึงการจัดทำรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๔๖ ให้ดำเนินการภายหลังจากที่กฎหมายลำดับรอง ตาม พ.ร.บ. ดังกล่าวมีผลบังคับใช้

ผนวก ค (แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท.)

ประกอบคำสั่ง บก.ทท. (เฉพาะ) ที่ ๒๒๒/๖๔ ลง ๒๗ มี.ค.๖๔

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. ฉบับนี้ จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อกำหนดรายละเอียดและอธิบายการปฏิบัติเพิ่มเติมจาก ผนวก ข นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. ซึ่งจะทำให้ นขต.บก.ทท./นขต.ศบท. ข้าราชการ ลูกจ้าง ทหารกองประจำการ และพนักงานราชการของ บก.ทท. รวมถึงหน่วยงานภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ บก.ทท. สามารถนำไปปฏิบัติได้อย่างถูกต้องและสอดคล้องกับนโยบายดังกล่าว ทั้งนี้ เพื่อให้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. มีความเป็นมาตรฐาน และสอดคล้องกับกฎหมายที่เกี่ยวข้อง จึงจัดทำแนวปฏิบัติฉบับนี้ตาม พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ และ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ รวมถึงหลักการจาก NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, NIST SP 800-60 Vol. 1 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories ของสหรัฐฯ

ทั้งนี้ กำหนดให้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. แบ่งออกได้เป็น ๒ ส่วน คือ แนวปฏิบัติทั่วไป (General Guideline) และแนวปฏิบัติเฉพาะ (Specific Guideline)

ส่วนที่ ๑ แนวปฏิบัติทั่วไป (General Guideline) ประกอบด้วย

๑.๑ การแบ่งประเภทสินทรัพย์ (Asset Categorization)

ให้ผู้ดูแลระบบของ นขต.บก.ทท. มีหน้าที่ในการแบ่งประเภทสินทรัพย์สารสนเทศตามแนวปฏิบัติดังต่อไปนี้

๑.๑.๑ ประเภทและวัตถุประสงค์ของความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Categories and Objectives)

๑.๑.๑.๑ ประเภทของความมั่นคงปลอดภัยไซเบอร์ แบ่งได้เป็น ๓ ระดับ ตามผลกระทบที่อาจเกิดขึ้นกับข้อมูลสารสนเทศ ได้แก่ ระดับพื้นฐาน (Low) ระดับปานกลาง (Moderate) และระดับเคร่งครัด (High)

๑.๑.๑.๒ วัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) แบ่งได้เป็น ๓ ประเภท ได้แก่

๑.๑.๑.๒ (๑) การรักษาความลับ (Confidentiality)

๑.๑.๑.๒ (๒) การรักษาความถูกต้องครบถ้วน (Integrity)

๑.๑.๑.๒ (๓) การรักษาสภาพพร้อมใช้งาน (Availability)

/๑.๑.๒ การประเมิน...

๑.๑.๒ การประเมินระดับผลกระทบ (Impact Assessment)

๑.๑.๒.๑ ผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ แบ่งได้เป็น ๓ ระดับ ได้แก่ ระดับต่ำ (Low) ระดับปานกลาง (Moderate) และระดับสูง (High)

๑.๑.๒.๒ ให้มีวิธีการประเมินระดับผลกระทบขั้นต้น ตามวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยใช้วิธีคำนวณดังนี้

ระดับผลกระทบขั้นต้น = ระดับผลกระทบด้านการรักษาความลับ
+ ระดับผลกระทบด้านการรักษาความถูกต้องครบถ้วน
+ ระดับผลกระทบด้านการรักษาสภาพพร้อมใช้งาน

๑.๑.๓ การแบ่งประเภทสินทรัพย์ตามระดับผลกระทบและประเภทของความมั่นคงปลอดภัย (Assignment of Impact Levels and Security Categorization)

ให้มีการแบ่งประเภทสินทรัพย์ตามระดับผลกระทบและประเภทของความมั่นคงปลอดภัยไซเบอร์ใน บก.ทท. ดังต่อไปนี้

๑.๑.๓.๑ ขั้นที่ ๑ : ระบุประเภทของข้อมูลสารสนเทศ (Identify Information Types) ดังนี้

๑.๑.๓.๑ (๑) ข้อมูลด้านกำลังพล
๑.๑.๓.๑ (๒) ข้อมูลด้านการข่าว
๑.๑.๓.๑ (๓) ข้อมูลด้านยุทธการ
๑.๑.๓.๑ (๔) ข้อมูลด้านส่งกำลังบำรุง
๑.๑.๓.๑ (๕) ข้อมูลด้านกิจการพลเรือน
๑.๑.๓.๑ (๖) ข้อมูลด้านการศึกษา
๑.๑.๓.๑ (๗) ข้อมูลด้านการแพทย์
๑.๑.๓.๑ (๘) ข้อมูลด้านงบประมาณและการเงิน
๑.๑.๓.๑ (๙) ข้อมูลด้านกฎหมาย
๑.๑.๓.๑ (๑๐) ข้อมูลด้านธุรการ
๑.๑.๓.๑ (๑๑) ข้อมูลด้านเทคโนโลยีสารสนเทศและไซเบอร์

๑.๑.๓.๒ ขั้นที่ ๒ : กำหนดระดับผลกระทบ

ในขั้นตอนนี้ ให้เลือกระดับผลกระทบขั้นต้น ตามตารางที่กำหนดให้ต่อไปนี้

ระดับผลกระทบ "ต่ำ"	ระดับผลกระทบ "ปานกลาง"	ระดับผลกระทบ "สูง"
ข้อมูลด้านการศึกษา ข้อมูลด้านธุรการ	ข้อมูลด้านส่งกำลังบำรุง ข้อมูลด้านกิจการพลเรือน ข้อมูลด้านงบประมาณและการเงิน ข้อมูลด้านกฎหมาย ข้อมูลด้านเทคโนโลยีสารสนเทศและไซเบอร์	ข้อมูลด้านกำลังพล ข้อมูลด้านการข่าว ข้อมูลด้านยุทธการ ข้อมูลด้านการแพทย์

ในกรณีที่ นขต.บก.ทท. พบว่า ไม่สามารถระบุประเภทของข้อมูลตามขั้นตอนที่ ๑ ได้ ให้หน่วยพิจารณาระดับผลกระทบ โดยใช้วิธีการคำนวณตามข้อ ๑.๑.๒.๒

/ยกตัวอย่าง...

ยกตัวอย่าง เช่น ระดับผลกระทบของข้อมูล ก = {ระดับผลกระทบด้านการรักษาความลับของข้อมูล ก} + {ระดับผลกระทบด้านการรักษาความถูกต้องครบถ้วนของข้อมูล ก} + {ระดับผลกระทบด้านการรักษาสภาพพร้อมใช้งานของข้อมูล ก}

๑.๑.๓.๓ ขั้นที่ ๓ : ทบทวนและปรับระดับผลกระทบ

ในกรณีที่ นขต.บก.ทท. มีความเห็นว่า ระดับผลกระทบขั้นต้นที่กำหนดให้ในตารางข้อ ๑.๑.๓.๒ ไม่สอดคล้องกับความเป็นจริง หน่วยอาจพิจารณาปรับเพิ่มหรือลดระดับผลกระทบของข้อมูลได้ ทั้งนี้ ให้บันทึกเหตุผลของการดำเนินการดังกล่าวเป็นลายลักษณ์อักษร และลงนามรับรองโดยผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูงของหน่วยไว้ด้วย

ในกรณีที่พบว่ามีข้อมูลส่วนบุคคลอยู่ร่วมกับข้อมูลตามข้อ ๑.๑.๓.๒ หน่วยจะต้องปรับระดับผลกระทบให้เหมาะสม ตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ กำหนดด้วย

นอกจากนี้ ให้พิจารณาปรับระดับผลกระทบ โดยคำนึงถึงลำดับชั้นความลับของข้อมูลสารสนเทศ ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ ดังนี้

๑.๑.๓.๓ (๑) ลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุดต่อ บก.ทท.

๑.๑.๓.๓ (๒) ลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงต่อ บก.ทท.

๑.๑.๓.๓ (๓) ลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อ บก.ทท.

ยกตัวอย่าง เช่น หน่วยงาน ก มีระบบงานในลักษณะ e-Learning เพื่อให้กำลังพลของหน่วยสามารถเข้ามาเรียนรู้ในเรื่องต่างๆ ซึ่งจะมีระดับผลกระทบของข้อมูลนี้เป็น "ระดับต่ำ" อย่างไรก็ตาม หากพบว่าในระบบ e-Learning ดังกล่าว มีเนื้อหาที่เป็นชั้นความลับ "ลับมาก" หน่วยงาน ก อาจพิจารณาปรับระดับผลกระทบของข้อมูลนี้ได้ ดังนี้

{ระดับผลกระทบด้านการรักษาความลับของข้อมูล = ปานกลาง} + {ระดับผลกระทบด้านการรักษาความถูกต้องครบถ้วนของข้อมูล = ต่ำ} + {ระดับผลกระทบด้านการรักษาสภาพพร้อมใช้งานของข้อมูล = ต่ำ}

ทำให้สามารถสรุปได้ว่า ระดับผลกระทบของข้อมูลในระบบ e-Learning นี้ = "ปานกลาง"

๑.๑.๓.๔ ขั้นที่ ๔ : กำหนดประเภทของความมั่นคงปลอดภัย

กำหนดประเภทของความมั่นคงปลอดภัยให้สอดคล้องกับระดับผลกระทบของข้อมูล ดังนี้

๑.๑.๓.๔ (๑) ระดับผลกระทบ "ต่ำ" ประเภทของความมั่นคงปลอดภัย "ระดับพื้นฐาน"

๑.๑.๓.๔ (๒) ระดับผลกระทบ "ปานกลาง" ประเภทของความมั่นคงปลอดภัย "ระดับปานกลาง"

๑.๑.๓.๔ (๓) ระดับผลกระทบ "สูง" ประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"

/๑.๑.๔ การบันทึก...

๑.๑.๔ การบันทึกผล (Data Classification Document)

ให้ทำการบันทึกผลการแบ่งประเภทสินทรัพย์สารสนเทศ ตามข้อ ๑.๑.๒ - ๑.๑.๓ ลงในแบบฟอร์มตามที่ ศชบ.ทหาร กำหนด

๑.๒ การกำหนดมาตรการควบคุม (Selecting Controls)

ให้นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. กำหนดมาตรการควบคุม (Controls) ตามประเภทของความมั่นคงปลอดภัย (Security Categorization) ที่ได้มีการกำหนดให้กับข้อมูลสารสนเทศของหน่วยในข้อ ๑.๑.๓.๔ ดังนี้

ประเภทของความมั่นคงปลอดภัย "ระดับพื้นฐาน"	ประเภทของความมั่นคงปลอดภัย "ระดับปานกลาง"	ประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"
AC-1, AC-2 (1-4), AC-3 (1-4), AC-4	AC-1, AC-2 (1-6), AC-3 (1-7), AC-4, AC-5 (1)	AC-1, AC-2 (1-11), AC-3 (1-9), AC-4, AC-5 (1-4)
AT-1, AT-2, AT-3	AT-1, AT-2, AT-3	AT-1, AT-2, AT-3
AU-1, AU-2, AU-3	AU-1, AU-2, AU-3	AU-1, AU-2, AU-3
CA-1, CA-2	CA-1, CA-2	CA-1, CA-2
CM-1, CM-2, CM-3 (1-2), CM-4 (1-2), CM-5, CM-6 (1)	CM-1, CM-2, CM-3 (1-2), CM-4 (1-2), CM-5, CM-6 (1)	CM-1, CM-2, CM-3 (1-4), CM-4 (1-3), CM-5, CM-6 (1-2)
CP-1 (1-3), CP-2, CP-3, CP-4	CP-1 (1-3), CP-2, CP-3, CP-4	CP-1 (1-4), CP-2, CP-3, CP-4
IA-1, IA-2 (1-2)	IA-1, IA-2 (1-3)	IA-1, IA-2 (1-4)
IR-1, IR-2, IR-3, IR-4, IR-5, IR-6	IR-1, IR-2, IR-3, IR-4, IR-5, IR-6	IR-1, IR-2, IR-3, IR-4, IR-5, IR-6
MA-1 (1-2)	MA-1 (1-2), MA-2	MA-1 (1-3), MA-2, MA-3
MP-1, MP-2, MP-3, MP-4, MP-5, MP-6	MP-1, MP-2, MP-3, MP-4, MP-5, MP-6	MP-1, MP-2, MP-3, MP-4, MP-5, MP-6
PE-1, PE-2 (1-4)	PE-1, PE-2 (1-6), PE-7 (1), PE-8, PE-9, PE-10	PE-1, PE-2 (1-7), PE-3, PE-4, PE-5, PE-6, PE-7 (1-3), PE-8, PE-9, PE-10, PE-11, PE-12, PE-13
PL-1, PL-2	PL-1, PL-2	PL-1, PL-2
PS-1, PS-2	PS-1, PS-2	PS-1, PS-2
RA-1, RA-2	RA-1, RA-2	RA-1, RA-2
SA-1 (1-2), SA-2, SA-3 (1, 4)	SA-1 (1-5), SA-2, SA-3 (1, 4)	SA-1 (1-10), SA-2, SA-3 (1-4), SA-4
SC-1, SC-2, SC-3, SC-4, SC-5, SC-6	SC-1, SC-2, SC-3, SC-4, SC-5, SC-6	SC-1, SC-2, SC-3, SC-4, SC-5, SC-6
SI-1, SI-2, SI-3, SI-4, SI-5, SI-6	SI-1, SI-2, SI-3, SI-4, SI-5, SI-6	SI-1, SI-2, SI-3, SI-4, SI-5, SI-6

ทั้งนี้ ให้บันทึกผลการกำหนดมาตรการควบคุมข้างต้น ตามแบบฟอร์มที่ ศชบ.ทหาร กำหนด

๑.๒.๑ การควบคุมการเข้าถึง (Access Control : AC)

๑.๒.๑.๑ การควบคุมการเข้าถึงสารสนเทศ (AC-1 Access Control Policy and Procedures) นขต.บก.ทท. ดำเนินการควบคุมการเข้าถึงสารสนเทศตามนโยบายฉบับนี้ ให้สอดคล้องกับประเภทของความมั่นคงปลอดภัย (Security Categorization) ที่ได้มีการกำหนดให้กับข้อมูลสารสนเทศของหน่วย

๑.๒.๑.๒ การจัดการบัญชีผู้ใช้ (AC-2 Account Management)

๑.๒.๑.๒ (๑) นขต.บก.ทท. ระบุประเภทของบัญชีผู้ใช้งานระบบสารสนเทศของหน่วยอย่างน้อยต้องประกอบด้วย

/๑.๒.๑.๒ (๑.๑) ผู้ดูแล...

๑.๒.๑.๒ (๑.๑) ผู้ดูแลบัญชีผู้ใช้ (Account Manager)

๑.๒.๑.๒ (๑.๒) ผู้ดูแลระบบ (System Administrator)

๑.๒.๑.๒ (๑.๓) ผู้ดูแลข้อมูลจราจรคอมพิวเตอร์ (Log Controller)

๑.๒.๑.๒ (๑.๔) ผู้ใช้งาน (User)

๑.๒.๑.๒ (๒) กำหนดหน้าที่ ความรับผิดชอบ สิทธิ์หรือระดับชั้นในการเข้าถึง เวลาที่เข้าถึงได้ รวมทั้งช่องทางการเข้าถึง อย่างน้อยดังนี้

หัวข้อ	ผู้ดูแลบัญชีผู้ใช้	ผู้ดูแลระบบ	ผู้ดูแลข้อมูลจราจรคอมพิวเตอร์	ผู้ใช้งาน
สิทธิ์หรือระดับชั้นในการเข้าถึง	สามารถเข้าถึงระบบสารสนเทศในส่วนที่เกี่ยวข้องกับ การสร้าง (Create) เปิดใช้งาน (Enable) แก้ไข (Modifies) ยกเลิก (Disable) และลบ (Delete) บัญชีผู้ใช้งานระบบสารสนเทศของหน่วย	สามารถเข้าถึงระบบสารสนเทศในส่วนที่เกี่ยวข้องกับการตั้งค่า และดูแลระบบสารสนเทศของหน่วย	สามารถเข้าถึงระบบสารสนเทศในส่วนที่เกี่ยวข้องกับ การตรวจสอบ ติดตาม ปกป้อง ข้อมูลจราจรคอมพิวเตอร์ในระบบสารสนเทศของหน่วย	สามารถเข้าถึงระบบสารสนเทศในส่วนที่เกี่ยวข้องกับงานตามหน้าที่ ความรับผิดชอบ หรืองานที่ได้รับมอบหมาย
เวลาที่เข้าถึงได้	๒๔ ชม.			วัน - เวลาราชการ หรือเมื่อมีความจำเป็นตามภารกิจ
ช่องทางการเข้าถึง	- ระบบสารสนเทศตามภารกิจของผู้ดูแลบัญชีผู้ใช้ - ระบบสารสนเทศตามภารกิจของผู้ดูแลระบบ - ระบบสารสนเทศตามภารกิจของผู้ดูแลข้อมูลจราจรคอมพิวเตอร์			- ระบบสารสนเทศของหน่วย - ระบบสารสนเทศของ บก.ทท.

๑.๒.๑.๒ (๓) การลงทะเบียนและการอนุมัติบัญชีผู้ใช้งาน (User Registration) ให้มีขั้นตอนการปฏิบัติ ดังนี้

๑.๒.๑.๒ (๓.๑) ผู้ใช้งาน นขต.บก.ทท. ต้องใช้งานระบบสารสนเทศของหน่วย ตามบทบาท หน้าที่ ความรับผิดชอบ วัตถุประสงค์ของระบบ รวมไปถึงภารกิจหรือเจตนารมณ์ผู้บังคับบัญชาเท่านั้น

๑.๒.๑.๒ (๓.๒) ผู้ดูแลระบบ นขต.บก.ทท. จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิ์และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๑.๒.๑.๒ (๓.๓) ผู้ดูแลระบบ นขต.บก.ทท. ต้องระบุชื่อบัญชีให้ผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

๑.๒.๑.๒ (๓.๔) ผู้ดูแลระบบ นขต.บก.ทท. ต้องตรวจสอบและมอบหมายสิทธิ์ ในการเข้าถึงระบบให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน อย่างน้อยตามที่กำหนดในข้อ ๑.๒.๑.๒ (๒)

/๑.๒.๑.๒ (๓.๕) ผู้ดูแล...

๑.๒.๑.๒ (๓.๕) ผู้ดูแลระบบ นขต.บก.ทท. ขออนุมัติบัญชีผู้ใช้งาน เป็นลายลักษณ์อักษรต่อผู้อนุมัติบัญชีผู้ใช้งาน ดังนี้

ระบบสารสนเทศ	เจ้าของระบบ	ผู้ดูแลระบบ	ผู้อนุมัติสิทธิ์	ผู้อนุมัติบัญชี
บก.ทท.				
- บริการระบบเครือข่าย MIS/C[๔]I	บก.ทท.	สส.ทหาร	จก.สส.ทหาร	จก.สส.ทหาร
- บริการเครื่องแม่ข่าย บก.ทท.	บก.ทท.	สส.ทหาร	จก.สส.ทหาร	จก.สส.ทหาร
- เว็บไซต์ บก.ทท. (rtarf.mi.th)	บก.ทท.	สส.ทหาร	จก.สส.ทหาร	จก.สส.ทหาร
- ระบบงานต่างๆ เช่น ระบบตรวจสอบประวัติฯ	หน่วยที่รับผิดชอบ	สส.ทหาร/หน่วยที่รับผิดชอบ	หน.หน่วยที่รับผิดชอบ	จก.สส.ทหาร
- ระบบรักษาความปลอดภัยไซเบอร์ บก.ทท.	บก.ทท.	ศชบ.ทหาร	ผอ.ศชบ.ทหาร	ผอ.ศชบ.ทหาร
นขต.บก.ทท.				
- ระบบเครือข่ายภายใน	นขต.บก.ทท.	CIO หน่วย	CIO หน่วย	CIO หน่วย
- เครื่องแม่ข่ายภายใน	นขต.บก.ทท.	CIO หน่วย	กองที่รับผิดชอบ	CIO หน่วย
- ฐานข้อมูลภายใน	นขต.บก.ทท.	CIO หน่วย	กองที่รับผิดชอบ	CIO หน่วย
- เว็บไซต์ของหน่วย	นขต.บก.ทท.	CIO หน่วย	CIO หน่วย	CIO หน่วย
- ระบบงานภายใน	กองที่รับผิดชอบ	CIO หน่วย	กองที่รับผิดชอบ	CIO หน่วย

๑.๒.๑.๒ (๓.๖) ผู้ดูแลระบบ นขต.บก.ทท. จัดทำและแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์ และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศ ซึ่งต้องครอบคลุมถึงนโยบายฉบับนี้ รวมทั้งกำหนดให้ผู้ใช้งานลงนามรับทราบในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๑.๒.๑.๒ (๓.๗) ผู้ดูแลระบบ นขต.บก.ทท. บันทึกและจัดเก็บข้อมูลการขออนุมัติ

๑.๒.๑.๒ (๔) การยกเลิกเพิกถอนบัญชีผู้ใช้งาน (User Revocation) ให้มีขั้นตอนการปฏิบัติ ดังนี้

๑.๒.๑.๒ (๔.๑) ผู้ดูแลระบบ นขต.บก.ทท. ดำเนินการยกเลิก (Disable) หรือลบ (Delete) บัญชีผู้ใช้งานระบบสารสนเทศของหน่วย เมื่อลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง โดยมีการบันทึกหรืออนุมัติเป็นลายลักษณ์อักษร

๑.๒.๑.๒ (๔.๒) ผู้ใช้งาน นขต.บก.ทท. แจ้งเตือนให้ผู้ดูแลบัญชีผู้ใช้ (Account Manager) ทราบ เมื่อหมดความจำเป็นในการใช้งานบัญชีผู้ใช้ หรือเมื่อผู้ใช้มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ หรือเมื่อมีการเปลี่ยนแปลงขั้นตอนการปฏิบัติงานเกิดขึ้น

๑.๒.๑.๒ (๕) ให้ ผู้ดูแลระบบ นขต.บก.ทท. และนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. ติดตามการใช้งานบัญชีผู้ใช้งานระบบสารสนเทศของหน่วยอย่างต่อเนื่อง

๑.๒.๑.๒ (๖) การทบทวนสิทธิ์บัญชีผู้ใช้งาน (Review of User Access Rights) ให้มีขั้นตอนการปฏิบัติ ดังนี้

/๑.๒.๑.๒ (๖.๑) ผู้ดูแล...

๑.๒.๑.๒ (๖.๑) ผู้ดูแลระบบ นขต.บก.ทท. ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานอย่างน้อย ๑ ครั้ง/ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง

๑.๒.๑.๒ (๖.๒) ผู้ดูแลระบบ นขต.บก.ทท. ทบทวนสิทธิ์สำหรับบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privilege User) โดยต้องทบทวนด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๑.๒.๑.๒ (๖.๓) ผู้ดูแลระบบ นขต.บก.ทท. บันทึกผลการทบทวนสิทธิ์เป็นลายลักษณ์อักษร เพื่อใช้ในการตรวจสอบในภายหลังต่อไป

๑.๒.๑.๒ (๗) ผู้ดูแลระบบ นขต.บก.ทท. ใช้ระบบสารสนเทศเพื่อติดตามการใช้งานของบัญชีผู้ใช้งานระบบสารสนเทศของหน่วย ยกตัวอย่างเช่น หากพบว่าบัญชีผู้ใช้งานไม่มีความเคลื่อนไหวเป็นระยะเวลา ๓ เดือน ให้ระบบทำการแจ้งเตือนไปยังผู้ดูแลบัญชีผู้ใช้ (Account Manager) เพื่อพิจารณายกเลิก (Disable) หรือลบ (Delete) บัญชีผู้ใช้งานดังกล่าวต่อไป เป็นต้น

๑.๒.๑.๒ (๘) ผู้ดูแลระบบ นขต.บก.ทท. ทำการตั้งค่าวันหมดอายุสำหรับบัญชีผู้ใช้งานระบบสารสนเทศของหน่วย ประเภทบัญชีชั่วคราว (Temporary Account) หรือประเภทฉุกเฉิน (Emergency Account) อย่างอัตโนมัติ

๑.๒.๑.๒ (๙) ผู้ดูแลระบบ นขต.บก.ทท. ทำการยกเลิก (Disable) หรือลบ (Delete) บัญชีผู้ใช้งานระบบสารสนเทศของหน่วย ที่พบว่าไม่มีความเคลื่อนไหวตามระยะเวลาที่หน่วยกำหนด หรือเกินกว่า ๖ เดือน ขึ้นกับว่าระยะเวลาใดน้อยกว่ากัน

๑.๒.๑.๒ (๑๐) ผู้ดูแลระบบ นขต.บก.ทท. ทำการตั้งค่าให้ระบบมีการแจ้งเตือนไปยังผู้ดูแลข้อมูลจราจรคอมพิวเตอร์ (Log Controller) ในกรณีที่มีการสร้าง (Create) เปิดใช้งาน (Enable) แก้ไข (Modify) ยกเลิก (Disable) หรือลบ (Delete) บัญชีผู้ใช้งานระบบสารสนเทศของหน่วย

๑.๒.๑.๒ (๑๑) ผู้ดูแลระบบ นขต.บก.ทท. ทำการตั้งค่าให้บัญชีผู้ใช้ต้องออกจากระบบอย่างอัตโนมัติ หากบัญชีผู้ใช้ดังกล่าวเข้าสู่ระบบแล้วมิได้มีกิจกรรมใดๆ ตามระยะเวลาที่กำหนด (Inactivity Logout)

๑.๒.๑.๓ การควบคุมการเข้าถึงเครือข่าย (AC-3 Network Access Control)

๑.๒.๑.๓ (๑) สส.ทหาร ต้องกำหนดระบบสารสนเทศที่สำคัญ อย่างน้อยประกอบด้วย ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่าย ระบบเครือข่ายไร้สาย อินเทอร์เน็ต หรืออินทราเน็ต ซึ่งต้องมีการใช้งานผ่านบริการเครือข่ายของ บก.ทท. และต้องมีการควบคุมการเข้าถึง โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๑.๒.๑.๓ (๒) ผู้ใช้งานต้องเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑.๒.๑.๓ (๓) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก (User Authentication for External Connection) มีข้อปฏิบัติดังนี้

/๑.๒.๑.๓ (๓.๑) ผู้ใช้งาน...

๑.๒.๑.๓ (๓.๑) ผู้ใช้งานต้องยืนยันตัวบุคคล (Authentication) ก่อนเข้าใช้งานเครือข่ายสารสนเทศของ บก.ทท. จากภายนอก ด้วยวิธีการตามที่ สส.ทหาร กำหนด อย่างน้อยประกอบด้วยขั้นตอนดังต่อไปนี้

๑.๒.๑.๓ (๓.๑.๑) ลงทะเบียนสำหรับผู้ใช้งานที่อยู่ภายนอก

๑.๒.๑.๓ (๓.๑.๒) รับทราบขั้นตอนการเข้าใช้งานเครือข่ายสารสนเทศของ บก.ทท. จากภายนอก

๑.๒.๑.๓ (๓.๑.๓) ยืนยันตัวบุคคลก่อนเข้าใช้งาน

๑.๒.๑.๓ (๓.๒) สส.ทหาร ต้องกำหนดให้มีมาตรการทางเทคนิคในการควบคุมการเข้าใช้งานเครือข่ายสารสนเทศของ บก.ทท. จากภายนอก อย่างน้อยประกอบด้วย

๑.๒.๑.๓ (๓.๒.๑) ต้องมีการใช้งานโปรโตคอลที่มีการเข้ารหัสข้อมูลอย่างมั่นคงปลอดภัย ทั้งนี้ต้องไม่น้อยกว่า TLS 1.2 หรือ AES หรือดีกว่า

๑.๒.๑.๓ (๓.๒.๒) ต้องมีการยืนยันตัวบุคคลผู้ใช้งานเพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้รหัสผ่าน หรือการใช้สมาร์ทการ์ด หรือการใช้ User Token ที่ใช้เทคโนโลยี PKI

๑.๒.๑.๓ (๓.๒.๓) ต้องมีการบันทึกข้อมูลการเข้าใช้เครือข่ายสารสนเทศของ บก.ทท. จากภายนอก และส่งให้ ศชบ.ทหาร เพื่อดำเนินการเฝ้าระวังและตรวจจับเหตุการณ์ที่ไม่พึงประสงค์

๑.๒.๑.๓ (๓.๓) ศชบ.ทหาร ต้องเฝ้าระวังและตรวจจับเหตุการณ์ที่ไม่พึงประสงค์ในการเข้าใช้งานเครือข่ายสารสนเทศของ บก.ทท. จากภายนอก พร้อมแจ้งเตือนให้ สส.ทหาร ทราบอย่างต่อเนื่อง

๑.๒.๑.๓ (๔) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network) ให้ สส.ทหาร กำหนดหมายเลขไอพี (IP Address) ให้กับอุปกรณ์ใดๆ ที่เชื่อมต่ออยู่กับระบบเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายนั้นได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้หมายเลขไอพีในการระบุถึงอุปกรณ์เครือข่ายได้ ให้ใช้หมายเลขอุปกรณ์ (MAC Address) ในการระบุถึงอุปกรณ์เครือข่ายแทน

๑.๒.๑.๓ (๕) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ให้ สส.ทหาร ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

๑.๒.๑.๓ (๕.๑) ป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านทางเครือข่าย

๑.๒.๑.๓ (๕.๒) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่ง ระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๑.๒.๑.๓ (๕.๓) ตรวจสอบพอร์ตที่ไม่มีการใช้งานอย่างสม่ำเสมอ

/๑.๒.๑.๓ (๖) การแบ่งแยก...

๑.๒.๑.๓ (๖) การแบ่งแยกเครือข่าย (Segregation in Network) ให้ สส.ทหาร ทำการแบ่งแยกเครือข่าย สำหรับกลุ่มผู้ใช้งานอย่างน้อยดังนี้

๑.๒.๑.๓ (๖.๑) กลุ่มของระบบสารสนเทศที่สามารถเข้าถึงได้จากภายนอก และกลุ่มของระบบสารสนเทศที่สามารถเข้าถึงได้เฉพาะจากภายใน

๑.๒.๑.๓ (๗) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้มีการควบคุมการเชื่อมต่อทางเครือข่าย ดังนี้

๑.๒.๑.๓ (๗.๑) ให้ สส.ทหาร ควบคุมการเข้าถึงหรือใช้งานเครือข่าย MIS, C^{4}I ของ บก.ทท. ประกอบด้วย

๑.๒.๑.๓ (๗.๑.๑) ลงทะเบียนผู้ใช้งานตามข้อ ๑.๒.๑.๒ (๓)

๑.๒.๑.๓ (๗.๑.๒) ลงทะเบียนเครื่องคอมพิวเตอร์กับ สส.ทหาร

๑.๒.๑.๓ (๗.๑.๓) ผู้ดูแลระบบของ นขต.บก.ทท. ต้องปรับปรุงเครื่องคอมพิวเตอร์ ให้เป็นไปตามคอนฟิกเกอเรชันพื้นฐานซึ่งมีความมั่นคงปลอดภัย (Secure Baseline Configuration) ตามข้อ ๑.๒.๕.๑ (๑)

๑.๒.๑.๓ (๗.๑.๔) ผู้ดูแลระบบของ นขต.บก.ทท. เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย MIS หรือ C^{4}I โดยให้มีการยืนยันตัวบุคคลเพื่อเข้าใช้งานเครือข่าย ตามข้อ ๑.๒.๗

๑.๒.๑.๓ (๗.๒) ให้ผู้ดูแลระบบของ นขต.บก.ทท. ควบคุมการเข้าถึงหรือใช้งานเครือข่ายของหน่วย ประกอบด้วย

๑.๒.๑.๓ (๗.๒.๑) ลงทะเบียนผู้ใช้งานตามข้อ ๑.๒.๑.๒ (๓)

๑.๒.๑.๓ (๗.๒.๒) ลงทะเบียนเครื่องคอมพิวเตอร์กับผู้ดูแลระบบ นขต.บก.ทท.

๑.๒.๑.๓ (๗.๒.๓) ผู้ดูแลระบบ นขต.บก.ทท. ปรับปรุงเครื่องคอมพิวเตอร์ ให้เป็นไปตาม Security Baseline ตามข้อ ๑.๒.๕.๑ (๑)

๑.๒.๑.๓ (๗.๒.๔) ผู้ดูแลระบบของ นขต.บก.ทท. เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายของหน่วย โดยให้มีการยืนยันตัวบุคคลเพื่อเข้าใช้งานเครือข่าย ตามข้อ ๑.๒.๗

๑.๒.๑.๓ (๗.๓) การควบคุมการเข้าถึงหรือใช้งานเครือข่าย ให้ สส.ทหาร และ นขต.บก.ทท. ต้องติดตั้งและใช้งานเครื่องแม่ข่ายช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารการเข้าถึงหรือใช้งานเครือข่ายของหน่วย

/๑.๒.๑.๓ (๘) การควบคุม...

๑.๒.๑.๓ (๘) การควบคุมการจัดเส้นทางเครือข่าย (Network Routing Control) ให้มีการควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๑.๒.๑.๓ (๘.๑) สส.ทหาร ควบคุมไม่ให้ทำการเปิดเผยการใช้หมายเลขไอพี (IP Address Plan)

๑.๒.๑.๓ (๘.๒) สส.ทหาร กำหนดให้ทำการแปลงหมายเลขไอพีเพื่อแยกเครือข่ายย่อย

๑.๒.๑.๓ (๘.๓) สส.ทหาร กำหนดตารางการใช้เส้นทางบนระบบเครือข่าย (Network Routing Table) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณข้อมูล (Layer 3 Switch) เพื่อบังคับผู้ใช้งานให้สามารถใช้เส้นทางเครือข่ายเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่ายที่ได้รับอนุญาตเท่านั้น

๑.๒.๑.๓ (๘.๔) ศชบ.ทหาร กำหนดให้มีการใช้อุปกรณ์ไฟร์วอลล์เพื่อควบคุมเส้นทางบนระบบเครือข่ายให้มีความมั่นคงปลอดภัย

๑.๒.๑.๓ (๘.๕) สส.ทหาร จำกัดการใช้เส้นทางบนระบบเครือข่ายจากอุปกรณ์คอมพิวเตอร์ที่ใช้งานไปยังเครื่องแม่ข่ายที่ให้บริการต่างๆ โดยการเชื่อมต่อเข้าสู่เครื่องแม่ข่ายที่ให้บริการเพื่อบริหารจัดการระบบให้กำหนดเฉพาะชุดหมายเลขไอพีของผู้ดูแลระบบสารสนเทศเท่านั้นที่สามารถเข้าถึงเครื่องแม่ข่ายให้บริการนั้นได้

๑.๒.๑.๓ (๙) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๓ (๙.๑) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ บก.ทท. จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการอนุมัติจาก จก.สส.ทหาร หรือผู้ที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษร

๑.๒.๑.๓ (๙.๒) ผู้ดูแลระบบ นขต.บก.ทท. ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งาน ในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๑.๒.๑.๓ (๙.๓) ผู้ดูแลระบบ นขต.บก.ทท. ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๑.๒.๑.๓ (๙.๔) ผู้ดูแลระบบ นขต.บก.ทท. ต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Wireless Access Point) ให้เหมาะสม เพื่อเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน รวมถึงเพื่อป้องกันไม่ให้ผู้ไม่หวังดีสามารถเข้าถึงและควบคุมอุปกรณ์ได้

/๑.๒.๑.๓ (๙.๕) ผู้ดูแล...

๑.๒.๑.๓ (๙.๕) ผู้ดูแลระบบ นขต.บก.ทท. และนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. ต้องร่วมกันตั้งค่าอุปกรณ์กระจายสัญญาณ (Wireless Access Point) ให้มีความมั่นคงปลอดภัยอย่างน้อยประกอบด้วย ดังนี้

๑.๒.๑.๓ (๙.๕.๑) เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าตั้งต้น (Default) มาจากผู้ผลิตทันที

๑.๒.๑.๓ (๙.๕.๒) อัพเดตเฟิร์มแวร์ของอุปกรณ์กระจายสัญญาณ

๑.๒.๑.๓ (๙.๕.๓) เปลี่ยนชื่อผู้ใช้และรหัสผ่านที่ถูกกำหนดเป็นค่าตั้งต้น (Default) มาจากผู้ผลิตทันที

๑.๒.๑.๓ (๙.๕.๔) ตั้งค่าอุปกรณ์กระจายสัญญาณให้ใช้งานโปรโตคอล WPA2 เป็นอย่างน้อย

๑.๒.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ (AC-4 Operating System Access Control)

๑.๒.๑.๔ (๑) การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการ จะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๔ (๑.๑) การเข้าใช้งาน (Secure Log-on Procedures) ผู้ใช้งานต้องตั้งค่าให้ระบบปฏิบัติการมีการยืนยันตัวตนก่อนเข้าใช้งาน

๑.๒.๑.๔ (๑.๒) การเข้าถึงและการควบคุมโดยวิธีการยืนยันตัวตน ให้ สส.ทหาร และ นขต.บก.ทท. ต้องติดตั้งและใช้งานเครื่องแม่ข่ายช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารการเข้าถึงเครื่องคอมพิวเตอร์ของหน่วย และกำหนดให้มีการยืนยันตัวตนให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๑.๒.๑.๔ (๒) พิสูจน์และยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๔ (๒.๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งานและรหัสผ่านสำหรับเข้าใช้งานระบบปฏิบัติการ

๑.๒.๑.๔ (๒.๒) ผู้ดูแลระบบ นขต.บก.ทท. ต้องกำกับดูแลให้มีการลงทะเบียนผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ในหน่วย รวมถึงการความคุมการเข้าถึง โดยให้สอดคล้องกับนโยบายฉบับนี้

๑.๒.๑.๔ (๓) การบริหารจัดการรหัสผ่าน (Password Management System) โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๔ (๓.๑) ผู้ดูแลระบบ นขต.บก.ทท. ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๑.๒.๑.๔ (๓.๒) ผู้ดูแลระบบ นขต.บก.ทท. ต้องกำหนดให้ผู้ใช้งานลงนามในเอกสารเพื่อแสดงสิทธิ์ และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของหน่วย

/๑.๒.๑.๔ (๓.๓) การมอบ...

๑.๒.๑.๔ (๓.๓) การมอบบัญชีผู้ใช้งานให้กับผู้ใช้งานครั้งแรก ให้กำหนดรหัสผ่านชั่วคราวจากการสุ่มให้กับผู้ใช้งาน เมื่อผู้ใช้งานได้รับรหัสผ่านแล้วระบบต้องสามารถให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านนั้นเป็นรหัสผ่านของตนเอง และสามารถทำงานเชิงโต้ตอบโดยแจ้งเตือนผู้ใช้กรณีตั้งรหัสผ่านไม่เป็นไปตามที่นโยบายฉบับนี้กำหนด

๑.๒.๑.๔ (๓.๔) การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างมั่นคงปลอดภัย

๑.๒.๑.๔ (๓.๕) ผู้ใช้งานต้องตอบยืนยันการได้รับรหัสผ่าน

๑.๒.๑.๔ (๓.๖) ผู้ดูแลระบบ นขต.บก.ทท. ต้องจัดทำระบบที่ทำให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านด้วยตนเองได้

๑.๒.๑.๔ (๓.๗) ผู้ดูแลระบบ นขต.บก.ทท. ต้องดำเนินการเข้ารหัสข้อมูลรหัสผ่าน ที่เก็บไว้ในระบบสารสนเทศของหน่วยอย่างเหมาะสม

๑.๒.๑.๔ (๓.๘) ผู้ดูแลระบบ นขต.บก.ทท. ต้องกำหนดให้ผู้ใช้งานสามารถใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง กรณีผู้ใช้งานพิมพ์รหัสผิดเกิน ๓ ครั้ง ระบบต้องระงับการใช้งานและผู้ใช้งานต้องทำเรื่องขอรหัสผ่านใหม่จากผู้ดูแลระบบของหน่วย

๑.๒.๑.๔ (๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๔ (๔.๑) ผู้ดูแลระบบ นขต.บก.ทท. ต้องจำกัดสิทธิ์การเข้าถึงและกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ ในเครื่องคอมพิวเตอร์ที่อยู่ภายในหน่วยของตน

๑.๒.๑.๔ (๔.๒) ผู้ดูแลระบบ นขต.บก.ทท. ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๑.๒.๑.๔ (๔.๓) ในกรณีที่มีความจำเป็น ผู้ใช้งานต้องขออนุญาตใช้งานโปรแกรมอรรถประโยชน์ไปยังผู้ดูแลระบบของหน่วย

๑.๒.๑.๔ (๕) การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out) โดยกำหนดหลักเกณฑ์การหมดเวลาใช้งานระบบปฏิบัติการเมื่อว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ผู้ดูแลระบบ ผู้พัฒนาระบบ หรือผู้ใช้งาน ทำการตั้งค่าเพื่อให้ยุติการใช้งานระบบปฏิบัติการนั้น ดังนี้

ประเภทของความมั่นคงปลอดภัย "ระดับพื้นฐาน"	ประเภทของความมั่นคงปลอดภัย "ระดับปานกลาง"	ประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"
ไม่เกิน ๓๐ นาที	ไม่เกิน ๒๐ นาที	ไม่เกิน ๑๐ นาที

๑.๒.๑.๔ (๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) โดยกำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบปฏิบัติการ ให้ผู้ดูแลระบบ ผู้พัฒนาระบบ หรือผู้ใช้งาน ทำการตั้งค่าเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนด ดังนี้

ประเภทของความมั่นคงปลอดภัย "ระดับพื้นฐาน"	ประเภทของความมั่นคงปลอดภัย "ระดับปานกลาง"	ประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"
ไม่เกิน ๒๔ ชั่วโมง	ไม่เกิน ๑๒ ชั่วโมง	ไม่เกิน ๖ ชั่วโมง

/๑.๒.๑.๕ การควบคุม...

๑.๒.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (AC-5 Application and Information Access Control)

๑.๒.๑.๕ (๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๕ (๑.๑) ผู้ใช้งาน รวมถึงเจ้าหน้าที่หรือบุคคลจากภายนอกที่เข้ามาใช้งาน หรือเข้าถึงสารสนเทศ ฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน ต้องปฏิบัติในส่วนของการควบคุมการเข้าถึงให้สอดคล้องตามนโยบายฉบับนี้

๑.๒.๑.๕ (๑.๒) ผู้ดูแลระบบ นขต.บก.ทท. ต้องมีการควบคุมพนักงานจากภายนอก (Outsource) ที่มีการจ้างเหมาดำเนินการเกี่ยวกับระบบสารสนเทศของหน่วยอย่างน้อยดังนี้

๑.๒.๑.๕ (๑.๒.๑) กำหนดให้มีเจ้าหน้าที่ผู้ควบคุมงานเพื่อคอยกำกับดูแลการดำเนินงานต่างๆ ของพนักงานจากภายนอก

๑.๒.๑.๕ (๑.๒.๒) แจ้งให้พนักงานจากภายนอกที่มีการจ้างเหมาดำเนินการเกี่ยวกับระบบสารสนเทศของหน่วย รับทราบและปฏิบัติเกี่ยวกับการปฏิบัติในส่วนของการควบคุมการเข้าถึงให้สอดคล้องตามนโยบายฉบับนี้

๑.๒.๑.๕ (๑.๒.๓) กำกับดูแลพนักงานจากภายนอกที่มีการจ้างเหมาดำเนินการเกี่ยวกับระบบสารสนเทศของหน่วยอย่างต่อเนื่อง

๑.๒.๑.๕ (๑.๒.๔) กำหนดให้พนักงานจากภายนอกลงนามในสัญญารักษาความลับ (Non-Disclosure Agreement)

๑.๒.๑.๕ (๑.๓) ผู้ใช้งานที่ต้องการเข้าถึงโปรแกรมประยุกต์ผ่านทางระบบเครือข่ายสาธารณะ ให้ใช้ช่องทางระบบเครือข่ายส่วนบุคคลเสมือน (VPN) และต้องมีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัยตามที่ สส.ทหาร กำหนด

๑.๒.๑.๕ (๑.๔) ผู้ดูแลระบบ นขต.บก.ทท. และ สส.ทหาร ต้องบันทึกข้อมูลพฤติกรรมการใช้งานข้อมูลโดยการจัดเก็บ Audit Log เป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้งานเพื่อใช้ในการตรวจสอบในภายหลัง ทั้งนี้ต้องไม่น้อยกว่าที่กำหนดไว้ใน พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.๒๕๕๐ และ พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐

๑.๒.๑.๕ (๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง (Sensitive System Isolation) โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๕ (๒.๑) กำหนดให้ระบบสารสนเทศเพื่อการควบคุมบังคับบัญชา บก.ทท. (Command and Control Information System : C^4I) เป็นระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงซึ่งอย่างน้อยจะต้องดำเนินการตามมาตรการดังต่อไปนี้

๑.๒.๑.๕ (๒.๑.๑) แยกระบบออกจากระบบอื่นๆ โดยไม่อนุญาตให้มีการเชื่อมต่อระบบเข้าสู่อินเทอร์เน็ต รวมไปถึงการกำหนดให้สามารถใช้งานเฉพาะกลุ่มเท่านั้น และต้องกำหนดช่องทางและวิธีการในการเข้าถึงโดยจัดให้มีเครื่องแม่ข่ายควบคุมแยกต่างหาก การติดต่อกับเครื่องแม่ข่ายต้องผ่าน Firewall เพื่อจำกัดการเข้าถึงเฉพาะการใช้เครือข่ายภายในเท่านั้น

/๑.๒.๑.๕ (๒.๑.๒) ควบคุม...

๑.๒.๑.๕ (๒.๑.๒) ควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ โดยกำหนดให้มีศูนย์ข้อมูลระบบสนับสนุน ระบบสภาพแวดล้อม ระบบสำรอง ระบบตรวจสอบสภาพพร้อมใช้งานอย่างเพียงพอ

๑.๒.๑.๕ (๒.๒) กำหนดให้ระบบสารสนเทศของ บก.ทท. ซึ่งมีผลการประเมินประเภทของความมั่นคงปลอดภัยอยู่ในระดับ "สูง" อย่างน้อยให้มีการแยกระบบออกจากระบบอื่นๆ โดยกำหนดให้สามารถใช้งานเฉพาะกลุ่มเท่านั้น และต้องกำหนดช่องทางและวิธีการในการเข้าถึงเพื่อจำกัดการเข้าถึงเฉพาะการใช้เครือข่ายภายในเท่านั้น

๑.๒.๑.๕ (๓) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Mobile Computing and Communications) โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑.๕ (๓.๑) ผู้ใช้งานต้องดูแลอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่โดยการปรับปรุงระบบปฏิบัติการ รวมถึงซอฟต์แวร์ที่ติดตั้งให้ทันสมัยอยู่เสมอ

๑.๒.๑.๕ (๓.๒) ผู้ใช้งานต้องติดตั้งโปรแกรมสำหรับป้องกันภัยคุกคามทางไซเบอร์ บนอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ตามที่ ศซบ.ทหาร กำหนด

๑.๒.๑.๕ (๓.๓) ผู้ดูแลระบบ หรือผู้ใช้งาน ต้องทำการเข้ารหัสสื่อบันทึกข้อมูลบนอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันกรณีอุปกรณ์ดังกล่าวสูญหายและส่งผลให้ข้อมูลสำคัญรั่วไหล

๑.๒.๑.๕ (๔) การปฏิบัติงานจากภายนอก (Teleworking) โดยมีแนวปฏิบัติดังนี้

๑.๒.๑.๕ (๔.๑) กำหนดการเข้าถึงโปรแกรมประยุกต์และสารสนเทศของ บก.ทท. ได้ ๒ ช่องทาง คือ

๑.๒.๑.๕ (๔.๑.๑) การเข้าถึงผ่านโปรแกรมประยุกต์และสารสนเทศที่เปิดให้ใช้งานจากภายนอกได้โดยตรง ได้แก่ จดหมายอิเล็กทรอนิกส์และระบบเว็บไซต์

๑.๒.๑.๕ (๔.๑.๒) การเข้าถึงผ่านโปรแกรมประยุกต์และสารสนเทศผ่านระบบ VPN

๑.๒.๑.๕ (๔.๒) ในกรณีที่ผู้ใช้งานเป็นพนักงานจากภายนอก หรือบุคคลภายนอก ต้องได้รับการอนุมัติจาก สส.ทหาร ก่อนเข้าใช้งาน

๑.๒.๑.๕ (๔.๓) อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อเข้ากับโปรแกรมประยุกต์และระบบสารสนเทศผ่านช่องทางการปฏิบัติงานจากภายนอก ต้องได้รับการติดตั้งโปรแกรมสำหรับป้องกันภัยคุกคามทางไซเบอร์ที่ได้รับการปรับปรุงอยู่เสมอ

๑.๒.๒ การสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training : AT)

๑.๒.๒.๑ หลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (AT-1 Security Awareness and Training Course)

/๑.๒.๒.๑ (๑) ศซบ.ทหาร...

๑.๒.๒.๑ (๑) ศชบ.ทหาร กำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศในภาพรวมของ บก.ทท. ทั้งในระดับผู้บริหาร และผู้ปฏิบัติงาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๑.๒.๒.๑ (๒) สปท. พิจารณาความเหมาะสมของหลักสูตรใน บก.ทท. โดยให้มีการเพิ่มเนื้อหาในเรื่องการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศเข้าไว้ในหลักสูตรด้วย

๑.๒.๒.๒ การฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศภายในหน่วย (AT-2 Internal Security Awareness Training) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท. จัดให้มีการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ ภายในหน่วยของตน อย่างน้อย ๑ ครั้ง/ปี

๑.๒.๒.๓ การฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศสำหรับกำลังพลใหม่ (AT-3 Role-Based Security Awareness Training)

๑.๒.๒.๓ (๑) ในกรณีที่กำลังพลของหน่วยมีการเปลี่ยนตำแหน่งหน้าที่ในการปฏิบัติงานและตำแหน่งหน้าที่ดังกล่าวมีการปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศของ บก.ทท. หน่วยต้องจัดให้มีการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศให้กับกำลังพลดังกล่าวด้วย

๑.๒.๒.๓ (๒) กพ.ทหาร เพิ่มหัวข้อการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งของการฝึกอบรมสำหรับกำลังพลใหม่ที่จะเข้ารับราชการใน บก.ทท.

๑.๒.๓ การตรวจประเมินมาตรฐาน (Audit and Accountability : AU)

๑.๒.๓.๑ แผนการตรวจประเมินมาตรฐาน (AU-1 Cybersecurity Auditing Plan)

๑.๒.๓.๑ (๑) หน.นขต.บก.ทท. ในฐานะผู้บริหารสูงสุดของหน่วยเป็นผู้รับผิดชอบต่อความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติของกำลังพลในหน่วยของตนตามนโยบายฉบับนี้ ทั้งนี้ หน.นขต.บก.ทท. ต้องมอบหมายให้ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูงของหน่วย หรือนายทหารสัญญาบัตรตั้งแต่ พ.อ.(พ) หรือ น.อ.(พ) ขึ้นไป ทำหน้าที่เป็นหัวหน้าชุดรับการตรวจประเมิน ตามข้อ ๑.๒.๓.๑ (๒)

๑.๒.๓.๑ (๒) ศชบ.ทหาร จัดทำแผนการตรวจประเมินมาตรฐานประจำปี โดยพิจารณาจากระดับความสำคัญของระบบสารสนเทศของ บก.ทท. ซึ่งมีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" เป็นลำดับแรก หรือตามสั่งการของผู้บังคับบัญชา และขออนุมัติแผนดังกล่าวถึง รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท.

๑.๒.๓.๑ (๓) ศชบ.ทหาร จัดการอบรมเกี่ยวกับการตรวจประเมินมาตรฐานอย่างน้อยตามมาตรฐาน ISO/IEC 27001 หรือ ISO 19011 ให้กับกำลังพลของ ศชบ.ทหาร ซึ่งจะต้องทำหน้าที่เป็นชุดตรวจประเมินมาตรฐาน อย่างน้อย ๑ ครั้ง/ปี ทั้งนี้ อาจกำหนดให้มีชุดตรวจประเมินมาตรฐานจากภายนอกเข้ามาตรวจประเมินมาตรฐานชุดตรวจประเมินดังกล่าวด้วย

/๑.๒.๓.๒ กระบวนการ...

๑.๒.๓.๒ กระบวนการตรวจประเมินมาตรฐาน (AU-2 Cybersecurity Auditing Process)

๑.๒.๓.๒ (๑) ชุดตรวจประเมินจาก ศชบ.ทหาร เข้าดำเนินการตรวจประเมินมาตรฐาน นขต.บก.ทท. ตามขั้นตอนดังต่อไปนี้เป็นอย่างน้อย

๑.๒.๓.๒ (๑.๑) ประชุมเปิดการตรวจประเมินมาตรฐาน

๑.๒.๓.๒ (๑.๒) ดำเนินการตรวจประเมินมาตรฐาน

๑.๒.๓.๒ (๑.๓) ประชุมยืนยันผลการตรวจประเมินมาตรฐาน

๑.๒.๓.๒ (๑.๔) ประชุมปิดการตรวจประเมินมาตรฐาน

๑.๒.๓.๒ (๒) ในกรณีที่ชุดตรวจประเมินจาก ศชบ.ทหาร ไม่ได้รับความร่วมมือจากชุดรับการตรวจประเมินตามข้อ ๑.๒.๓.๑ (๑) ให้ ผอ.ศชบ.ทหาร รายงานปัญหาดังกล่าวถึง รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. โดยเร็ว

๑.๒.๓.๒ (๓) ภายหลังเสร็จสิ้นการตรวจประเมินมาตรฐานให้ ศชบ.ทหาร รายงานผลการตรวจประเมินตามข้อ ๑.๒.๓.๑ (๒) ถึง ผบ.ทสส.

๑.๒.๓.๓ การแก้ไขข้อตรวจพบ (AU-3 Corrections and Corrective Actions)

๑.๒.๓.๓ (๑) ภายหลังจาก นขต.บก.ทท. ได้รับทราบรายงานผลการตรวจประเมินมาตรฐานตามข้อ ๑.๒.๓.๒ (๓) หน่วยจะต้องดำเนินการแก้ไขข้อตรวจพบที่เกิดขึ้นโดยเร็ว ดังนี้

๑.๒.๓.๓ (๑.๑) ข้อตรวจพบหลัก (Major Non-Conformity) ภายใน ๙๐ วัน

๑.๒.๓.๓ (๑.๒) ข้อตรวจพบรอง (Minor Non-Conformity) ภายใน ๑๒๐ วัน

๑.๒.๓.๓ (๒) เมื่อ นขต.บก.ทท. ดำเนินการแก้ไขข้อตรวจพบตามข้อ ๑.๒.๓.๓ (๑) แล้วเสร็จ ให้แจ้ง ศชบ.ทหาร เป็นลายลักษณ์อักษร เพื่อเข้าดำเนินการตรวจติดตามผลการแก้ไข และออกรายงานผลการแก้ไขให้หน่วย รวมทั้งสรุปผลการตรวจติดตามกล่าวถึง รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท. เพื่อทราบต่อไป

๑.๒.๔ การรับรองและประเมินความมั่นคงปลอดภัย (Security Assessment and Authorization : CA)

๑.๒.๔.๑ การทดสอบเจาะระบบ (CA-1 Penetration Testing) ศชบ.ทหาร จัดทำแผนการทดสอบเจาะระบบประจำปี โดยพิจารณาจากระดับความสำคัญของระบบสารสนเทศของ บก.ทท. ซึ่งมีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" เป็นลำดับแรกหรือตามสั่งการของผู้บังคับบัญชา ดังนี้

๑.๒.๔.๑ (๑) กำหนดรายชื่อของ นขต.บก.ทท. จากระดับความสำคัญของระบบสารสนเทศ ซึ่งมีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"

๑.๒.๔.๑ (๒) ตรวจสอบระดับความเสี่ยงด้านไซเบอร์ของ นขต.บก.ทท. จากรายงานการประเมินความเสี่ยงด้านไซเบอร์ของหน่วย

๑.๒.๔.๑ (๓) ตรวจสอบนโยบายของผู้บังคับบัญชาระดับสูงเกี่ยวกับงานสำคัญเร่งด่วนที่มีผลกระทบสูงต่อ บก.ทท. และมีความเกี่ยวข้องกับระบบสารสนเทศของ บก.ทท.

๑.๒.๔.๑ (๔) จัดทำแผนการทดสอบเจาะระบบประจำปี โดยหารือร่วมกับหน่วยเกี่ยวกับขอบเขต และห้วงเวลาที่จะเข้าดำเนินการ

/๑.๒.๔.๑ (๕) ขออนุมัติ...

๑.๒.๔.๑ (๕) ขออนุมัติแผนการทดสอบเจาะระบบประจำปีตามข้อ ๑.๒.๔.๑ (๔) ถึง รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท.

๑.๒.๔.๑ (๖) จัดทำข้อตกลงการให้บริการทดสอบเจาะระบบ (Rule of Engagement : ROE)

๑.๒.๔.๑ (๗) ชุดทดสอบเจาะระบบของ ศชบ.ทหาร เข้าดำเนินการทดสอบเจาะระบบ ซึ่งจะต้องดำเนินการตามข้อตกลงการให้บริการทดสอบเจาะระบบในข้อ ๑.๒.๔.๑ (๖) โดยเคร่งครัด

๑.๒.๔.๑ (๘) จัดทำรายงานผลการทดสอบเจาะระบบถึง ผบ.ทสส. ซึ่งจะต้องมีข้อเสนอแนะเพื่อให้หน่วยสามารถปรับปรุงแก้ไขช่องโหว่ หรือความไม่มั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศของหน่วยต่อไปด้วย

๑.๒.๔.๑ (๙) นขต.บก.ทท. รายงานผลการแก้ไขตามรายงานและข้อเสนอแนะในข้อ ๑.๒.๔.๑ (๘) ภายหลังดำเนินการแก้ไขแล้วเสร็จ

๑.๒.๔.๒ การประเมินตนเองด้านความมั่นคงปลอดภัยไซเบอร์ (CA-2 Cybersecurity Self Assessment) นขต.บก.ทท. ดำเนินการประเมินผลการดำเนินการตามมาตรการควบคุมที่ได้ระบุไว้ในแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วย ดังนี้

๑.๒.๔.๒ (๑) ศชบ.ทหาร จัดทำแบบฟอร์มสำหรับรายงานการประเมินตนเองทางไซเบอร์ นขต.บก.ทท. (Self Assessment Report : SAR) เพื่อใช้ในการตรวจประเมินความมีประสิทธิภาพในการดำเนินการตามมาตรการควบคุมตามที่หน่วยกำหนด พร้อมทั้งให้บรรจุแบบฟอร์มดังกล่าวในคู่มือการรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. รวมไปถึงดำเนินการจัดการฝึกอบรมการใช้งานแบบฟอร์มดังกล่าวด้วย

๑.๒.๔.๒ (๒) นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. จัดทำแผนการประเมินตนเองด้านความมั่นคงปลอดภัยไซเบอร์ (Security Assessment Plan) ซึ่งอย่างน้อยต้องประกอบด้วย รายการมาตรการควบคุม (Security Control Baseline) แผนการวางมาตรการควบคุม (Implementation Plan) ชื่อผู้ทำหน้าที่ประเมิน ห้วงเวลาการประเมิน และแบบฟอร์มตามข้อ ๑.๒.๔.๒ (๑)

๑.๒.๔.๒ (๓) นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. ขออนุมัติแผนการประเมินตนเองด้านความมั่นคงปลอดภัยไซเบอร์ ตามข้อ ๑.๒.๔.๒ (๑) ถึงผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท.

๑.๒.๔.๒ (๔) นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. ดำเนินการตรวจประเมินตามแผนการประเมินในข้อ ๑.๒.๔.๒ (๒)

๑.๒.๔.๒ (๕) นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. รายงานผลการตรวจประเมินถึง หน.นขต.บก.ทท. เพื่อรับทราบผล หรือข้อตรวจพบเกี่ยวกับการละเมิดนโยบายฉบับนี้ ในกรณีที่พบการละเมิดให้ นขต.บก.ทท. กำกับดูแลให้มีการแก้ไขข้อตรวจพบดังกล่าวโดยเร็ว ทั้งนี้ ต้องไม่เกิน ๙๐ วัน นับตั้งแต่วันที่ หน.นขต.บก.ทท. รับทราบรายงานผลดังกล่าว

๑.๒.๕ การจัดการด้านคอนฟิกเกอเรชัน (Configuration Management : CM)

๑.๒.๕.๑ คอนฟิกเกอเรชันพื้นฐานซึ่งมีความมั่นคงปลอดภัย (CM-1 Secure Baseline Configuration)

/๑.๒.๕.๑ (๑) ศชบ.ทหาร...

๑.๒.๕.๑ (๑) ศชบ.ทหาร จัดทำ ทบทวน ปรับปรุง และแจกจ่ายคอนฟิกเกอเรชันพื้นฐานซึ่งมีความมั่นคงปลอดภัย สำหรับระบบสารสนเทศของ บก.ทท. ดังนี้

๑.๒.๕.๑ (๑.๑) ระบบปฏิบัติการบนเครื่องแม่ข่าย (Server Operating System)

๑.๒.๕.๑ (๑.๒) ระบบปฏิบัติการบนเครื่องลูกข่าย (Client Operating System)

๑.๒.๕.๑ (๑.๓) อุปกรณ์เครือข่าย (Network Device)

๑.๒.๕.๑ (๑.๔) อุปกรณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Device)

๑.๒.๕.๑ (๒) สส.ทหาร ดำเนินการควบคุมการจัดทำคุณลักษณะเฉพาะสิ่งอุปกรณ์ชั่วคราวสายสื่อสารของ นขต.บก.ทท. ให้มีการระบุข้อความซึ่งมีผลบังคับให้ผู้ขายหรือผู้รับจ้างตามสัญญาซื้อขายกับ บก.ทท. จะต้องดำเนินการปรับปรุงให้ระบบสารสนเทศซึ่งจะดำเนินการติดตั้งใน บก.ทท. จะต้องมีการตั้งค่าตามคอนฟิกเกอเรชันพื้นฐานในข้อ ๑.๒.๕.๑ (๑.๑) ๑.๒.๕.๑ (๑.๒) ๑.๒.๕.๑ (๑.๓)

๑.๒.๕.๑ (๓) ศชบ.ทหาร ดำเนินการควบคุมการจัดทำคุณลักษณะเฉพาะสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ของ นขต.บก.ทท. ให้มีการระบุข้อความซึ่งมีผลบังคับให้ผู้ขายหรือผู้รับจ้างตามสัญญาซื้อขายกับ บก.ทท. จะต้องดำเนินการปรับปรุงให้ระบบสารสนเทศที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะดำเนินการติดตั้งใน บก.ทท. จะต้องมีการตั้งค่าตามคอนฟิกเกอเรชันพื้นฐานในข้อ ๑.๒.๕.๑ (๑.๔)

๑.๒.๕.๑ (๔) ผู้ดูแลระบบ นขต.บก.ทท. ดำเนินการควบคุมการติดตั้งระบบสารสนเทศของหน่วย ตามคอนฟิกเกอเรชันพื้นฐานในข้อ ๑.๒.๕.๑ (๑)

๑.๒.๕.๑ (๕) ผู้ดูแลระบบ นขต.บก.ทท. ดำเนินการควบคุมการติดตั้งโปรแกรมป้องกันไวรัสตามที่ ศชบ.ทหาร กำหนด ทั้งบนเครื่องแม่ข่ายและเครื่องลูกข่าย

๑.๒.๕.๑ (๖) ผู้ดูแลระบบ นขต.บก.ทท. ส่งรายงานสรุปผลการดำเนินการตามข้อ ๒.๒.๕.๑ (๔) ให้ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูงของหน่วย เพื่อทราบและควบคุมการดำเนินการให้เป็นไปตามแนวปฏิบัติข้อนี้ อย่างน้อย ๑ ครั้ง/ปี

๑.๒.๕.๒ การควบคุมการเปลี่ยนแปลงคอนฟิกเกอเรชัน (CM-2 Configuration Change Control)

๑.๒.๕.๒ (๑) สส.ทหาร ควบคุมการเปลี่ยนแปลงคอนฟิกเกอเรชันภายหลังการติดตั้งบนระบบสารสนเทศของ บก.ทท. ดังนี้

๑.๒.๕.๒ (๑.๑) ตรวจสอบและติดตามการตั้งค่าคอนฟิกเกอเรชันบนเครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์เครือข่าย อยู่เสมอ

๑.๒.๕.๒ (๑.๒) ไม่อนุญาตให้ระบบสารสนเทศซึ่งมีการตั้งค่าคอนฟิกเกอเรชันที่ไม่ปลอดภัยเชื่อมต่อเข้ากับเครือข่ายของ บก.ทท.

๑.๒.๕.๒ (๑.๓) รายงานลักษณะการเปลี่ยนแปลงคอนฟิกเกอเรชันภายหลังการติดตั้งบนระบบสารสนเทศของ บก.ทท. ให้ ศชบ.ทหาร ทราบอย่างสม่ำเสมอ อย่างน้อย ๑ ครั้ง/เดือน ซึ่งต้องครอบคลุมในหัวข้อต่อไปนี้เป็นอย่างน้อย

๑.๒.๕.๒ (๑.๓.๑) เวอร์ชันของระบบปฏิบัติการบนเครื่องแม่ข่าย

/๑.๒.๕.๒ (๑.๓.๒) เวอร์ชันของ...

๑.๒.๕.๒ (๑.๓.๒) เวอร์ชันของระบบปฏิบัติการบนเครื่องลูกข่าย

๑.๒.๕.๒ (๑.๓.๓) เวอร์ชันของเฟิร์มแวร์บนอุปกรณ์เครือข่าย

๑.๒.๕.๒ (๒) ผู้ดูแลระบบ นขต.บก.ทท. ควบคุมการเปลี่ยนแปลงคอนฟิกเกอเรชันภายหลังการติดตั้งบนระบบสารสนเทศหน่วย ดังนี้

๑.๒.๕.๒ (๒.๑) ตรวจสอบและติดตามการตั้งค่าคอนฟิกเกอเรชันบนเครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์เครือข่ายอยู่เสมอ

๑.๒.๕.๒ (๒.๒) ปรับปรุงเวอร์ชันของระบบปฏิบัติการ รวมถึงเฟิร์มแวร์บนอุปกรณ์เครือข่าย ให้ทันสมัยอยู่เสมอ

๑.๒.๕.๒ (๒.๓) ปรับปรุงโปรแกรมป้องกันไวรัสบนเครื่องแม่ข่ายและเครื่องลูกข่าย ให้ทันสมัยอยู่เสมอ

๑.๒.๕.๒ (๓) ในกรณีที่ผู้ดูแลระบบ นขต.บก.ทท. มีความจำเป็นต้องเปลี่ยนแปลงคอนฟิกเกอเรชันซึ่งมีลักษณะแตกต่างออกไปจากคอนฟิกเกอร์เรชันที่มีความมั่นคงปลอดภัย ให้จัดทำหลักฐานการเปลี่ยนแปลงพร้อมเหตุผลประกอบ

๑.๒.๕.๓ ฟังก์ชันการทำงานที่จำเป็น (CM-3 Least Functionality)

๑.๒.๕.๓ (๑) ศชบ.ทหาร จัดทำและแจกจ่ายรายการฟังก์ชันการทำงานที่ไม่จำเป็นต้องเปิดใช้งานบนระบบสารสนเทศให้กับ นขต.บก.ทท. เพื่อเป็นการควบคุมการใช้งานพอร์ต (Port) โปรโตคอล (Protocol) รวมถึงบริการ (Service) บนระบบสารสนเทศของ บก.ทท. ให้มีความมั่นคงปลอดภัยอย่างน้อยดังนี้

๑.๒.๕.๓ (๑.๑) พอร์ต โปรโตคอล หรือบริการ ที่ไม่มีความมั่นคงปลอดภัยเพียงพอ และไม่อนุญาตให้ใช้งาน เช่น Telnet, SMBv1 เป็นต้น

๑.๒.๕.๓ (๑.๒) พอร์ต โปรโตคอล หรือบริการ ที่อนุญาตให้ใช้งานได้เฉพาะกลุ่ม เช่น SFTP, SSH จะอนุญาตให้เฉพาะกลุ่มผู้ดูแลระบบ หรือกลุ่มความมั่นคงปลอดภัยไซเบอร์ เท่านั้น

๑.๒.๕.๓ (๒) ศชบ.ทหาร จัดทำและแจกจ่ายรายการฮาร์ดแวร์ หรือซอฟต์แวร์ที่ไม่มีความมั่นคงปลอดภัยเพียงพอ (Unauthorized Hardware and Software/Blacklisting) เพื่อให้ นขต.บก.ทท. ใช้เป็นข้อพิจารณาในการจัดซื้อ หรือติดตั้งใช้งาน

๑.๒.๕.๓ (๓) ในกรณีที่ นขต.บก.ทท. มีความจำเป็นต้องใช้งานพอร์ต โปรโตคอล หรือบริการ ที่ไม่มีความมั่นคงปลอดภัยเพียงพอ ให้แจ้งไปยัง ศชบ.ทหาร เพื่อพิจารณาแนวทางแก้ไขที่เหมาะสม

๑.๒.๕.๓ (๔) ในกรณีที่ นขต.บก.ทท. มีความต้องการใช้งานพอร์ต โปรโตคอล หรือบริการ ที่มีลักษณะแตกต่างจากการใช้งานทั่วไปให้แจ้งไปยัง ศชบ.ทหาร เพื่อให้ตรวจสอบความเสี่ยงด้านความไม่มั่นคงปลอดภัย หรือช่องโหว่ของพอร์ต โปรโตคอล หรือบริการดังกล่าวก่อนที่จะเริ่มติดตั้งและใช้งาน

๑.๒.๕.๔ รายการสินทรัพย์ (CM-4 Information System Component Inventory)

๑.๒.๕.๔ (๑) ผู้ดูแลระบบ นขต.บก.ทท. จัดทำบัญชีสินทรัพย์สารสนเทศของหน่วย โดยต้องครอบคลุมทั้งฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์เครือข่าย และระบบฐานข้อมูลที่อยู่ในความรับผิดชอบของหน่วยทั้งหมด

/๑.๒.๕.๔ (๒) ในกรณี...

๑.๒.๕.๔ (๒) ในกรณีที่มีการติดตั้งใหม่ ถอนการติดตั้ง หรือเปลี่ยนแปลงการตั้งค่าสินทรัพย์สารสนเทศของหน่วย ให้ผู้ดูแลระบบ นขต.บก.ทท. ปรับปรุงบัญชีสินทรัพย์สารสนเทศให้มีความทันสมัยอยู่เสมอ

๑.๒.๕.๔ (๓) ผู้ดูแลระบบ นขต.บก.ทท. จัดหาและติดตั้งระบบบริหารสินทรัพย์สารสนเทศ (Information Asset Management System) เพื่อติดตาม ควบคุม บริหาร สินทรัพย์สารสนเทศของหน่วยได้อย่างอัตโนมัติ

๑.๒.๕.๕ ข้อห้ามการใช้งานซอฟต์แวร์ (CM-5 Software Usage Restrictions)

๑.๒.๕.๕ (๑) ห้ามมิให้มีการใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ในระบบสารสนเทศของ บก.ทท.

๑.๒.๕.๕ (๒) ห้ามมิให้มีการใช้งานซอฟต์แวร์ประเภท Peer-to-Peer เพื่อป้องกันมิให้มีการใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ รวมถึงการใช้งานเพื่อเข้าถึงข้อมูลที่ไม่เหมาะสมอื่นๆ

๑.๒.๕.๕ (๓) สส.ทหาร ควบคุมและป้องกันมิให้ นขต.บก.ทท. เข้าถึงและใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ในระบบสารสนเทศของ บก.ทท.

๑.๒.๕.๖ ซอฟต์แวร์ที่ติดตั้งโดยผู้ใช้ (CM-6 User-Installed Software)

๑.๒.๕.๖ (๑) ห้ามมิให้มีการติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ในระบบสารสนเทศของ บก.ทท.

๑.๒.๕.๖ (๒) ห้ามมิให้มีการติดตั้งซอฟต์แวร์ที่ไม่มีความมั่นคงปลอดภัยเพียงพอ (Unauthorized Hardware and Software/Blacklisting) ตามรายการที่ ศชบ.ทหาร กำหนด บนระบบสารสนเทศของ บก.ทท.

๑.๒.๖ แผนเผชิญเหตุ (Contingency Planning : CP)

๑.๒.๖.๑ การสำรองข้อมูลและระบบคอมพิวเตอร์ (CP-1 Information System Backup)

๑.๒.๖.๑ (๑) การคัดเลือกระบบสารสนเทศของ บก.ทท. สำหรับการสำรองข้อมูลให้เป็นไปตาม ๒.๑ การแบ่งประเภทสินทรัพย์

๑.๒.๖.๑ (๒) การจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยมีแนวปฏิบัติ ดังนี้

๑.๒.๖.๑ (๒.๑) กำหนดระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) และระยะเวลาสูงสุดที่จะกู้ข้อมูลได้ (Recovery Time Objective : RTO) สำหรับระบบสารสนเทศตามข้อ ๑.๒.๖.๑ (๑) อย่างน้อยดังนี้

ประเภทของความมั่นคงปลอดภัย "ระดับพื้นฐาน"	ประเภทของความมั่นคงปลอดภัย "ระดับปานกลาง"	ประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"
RPO = ๓๖ ชั่วโมง RTO = ๗๒ ชั่วโมง	RPO = ๑๒ ชั่วโมง RTO = ๒๔ ชั่วโมง	RPO = ๔ ชั่วโมง RTO = ๘ ชั่วโมง

๑.๒.๖.๑ (๒.๒) ผู้ดูแลระบบ นขต.บก.ทท. และ สส.ทหาร จัดทำขั้นตอนปฏิบัติ และดำเนินการสำรองข้อมูลสำหรับระบบสารสนเทศแต่ละระบบ อย่างน้อยต้องประกอบด้วยซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกเกอเรชัน (Configuration) และข้อมูลในระบบ

/๑.๒.๖.๑ (๒.๓) ผู้ดูแล...

๑.๒.๖.๑ (๒.๓) ผู้ดูแลระบบ นขต.บก.ทท. และ สส.ทหาร จัดทำบันทึกการสำรองข้อมูล (Operator Logs) ประกอบด้วยรายละเอียดการสำรองข้อมูล โดยมี วันเวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูล ที่บันทึก สำเร็จ/ไม่สำเร็จ

๑.๒.๖.๑ (๒.๔) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่ที่ใช้จัดเก็บข้อมูล

๑.๒.๖.๑ (๓) ผู้ดูแลระบบ นขต.บก.ทท. และ สส.ทหาร ตรวจสอบความพร้อมใช้งานและถูกต้องครบถ้วนของข้อมูลสำรอง ขั้นตอนการสำรองข้อมูล และขั้นตอนการกู้คืนข้อมูลอยู่เสมอ

๑.๒.๖.๑ (๔) การเข้ารหัสข้อมูลสำรอง (Encrypted backup) ผู้ดูแลระบบ นขต.บก.ทท.และ สส.ทหาร ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๑.๒.๖.๒ แผนเตรียมความพร้อมกรณีฉุกเฉิน (CP-2 Continuity Plan) เพื่อรับมือกับเหตุการณ์ที่อาจส่งผลกระทบต่อความต่อเนื่องในการปฏิบัติการด้านระบบสารสนเทศของ บก.ทท. โดยแผนเตรียมความพร้อมดังกล่าวจะต้องประกอบด้วยแผนย่อยไม่น้อยกว่า แผนบริหารความต่อเนื่อง (Business Continuity Plan) แผนการติดต่อสื่อสารและประชาสัมพันธ์ (Crisis Communication Plan) แผนการอพยพเคลื่อนย้าย (Occupant Emergency Plan) แผนกู้คืนระบบ (Disaster Recovery Plan) แผนรับมือเหตุการณ์ทางไซเบอร์ (Cyber Incident Response Plan) และแผนฟื้นฟู (Recovery Plan) โดยมีรายละเอียดดังนี้

๑.๒.๖.๒ (๑) สส.ทหาร จัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan) อย่างน้อยต้องประกอบด้วย ดังนี้

๑.๒.๖.๒ (๑.๑) แต่งตั้งคณะกรรมการบริหารความต่อเนื่อง ซึ่งต้องมีองค์ประกอบไม่น้อยกว่า ดังนี้

๑.๒.๖.๒ (๑.๑.๑) คณะกรรมการบริหารความต่อเนื่อง (BCP Committee)

๑.๒.๖.๒ (๑.๑.๒) คณะทำงานผู้ประสานงาน (BCP Coordinator)

๑.๒.๖.๒ (๑.๑.๓) คณะทำงานสื่อสารและประชาสัมพันธ์ (BCP Communication Team)

๑.๒.๖.๒ (๑.๑.๔) คณะทำงานรักษาความปลอดภัยสถานที่ (BCP Physical Security Team)

๑.๒.๖.๒ (๑.๑.๕) คณะทำงานเทคโนโลยีสารสนเทศ (BCP IT Team)

๑.๒.๖.๒ (๑.๑.๖) คณะทำงานความมั่นคงปลอดภัยไซเบอร์ (BCP Cybersecurity Team)

๑.๒.๖.๒ (๑.๑.๗) คณะทำงานกำลังพลและส่งกำลัง (BCP Personnel and Logistic Team)

/๑.๒.๖.๒ (๑.๒) กำหนด...

๑.๒.๖.๒ (๑.๒) กำหนดประเภทเหตุการณ์วิกฤติหรือเหตุการณ์ฉุกเฉิน

๑.๒.๖.๒ (๑.๓) ประเมินความเสี่ยงของเหตุการณ์วิกฤติ และความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของ บก.ทท. พร้อมกำหนดระดับความเสี่ยงที่ยอมรับได้ให้ชัดเจน

๑.๒.๖.๒ (๑.๔) กำหนดขั้นตอนและดำเนินการตามแผนบริหารความต่อเนื่อง

๑.๒.๖.๒ (๒) คณะกรรมการบริหารความต่อเนื่อง ดำเนินการร่วมกับ กร.ทหาร จัดทำแผนการติดต่อสื่อสารและประชาสัมพันธ์ (Crisis Communication Plan) เพื่อใช้ในการติดต่อสื่อสารและประชาสัมพันธ์กับหน่วยงานทั้งภายในและภายนอก บก.ทท. ในห้วงที่เกิดเหตุการณ์วิกฤติ อย่างน้อยต้องประกอบด้วย ดังนี้

๑.๒.๖.๒ (๒.๑) กำหนดขั้นตอนในการสื่อสาร และการประชาสัมพันธ์ในห้วงที่เกิดเหตุการณ์วิกฤติ

๑.๒.๖.๒ (๒.๑.๑) จัดทำผังรายชื่อการแจ้งเหตุฉุกเฉิน (Call Tree)

๑.๒.๖.๒ (๒.๑.๒) กำหนดช่องทางการสื่อสารทั้งช่องทางหลักและสำรอง

๑.๒.๖.๒ (๒.๒) เมื่อคณะกรรมการบริหารความต่อเนื่อง ประกาศใช้แผนบริหารความต่อเนื่อง ให้คณะทำงานสื่อสารและประชาสัมพันธ์ (BCP Communication Team) แจ้งข่าวสารดังกล่าวตามผังรายชื่อการแจ้งเหตุฉุกเฉินที่กำหนด

๑.๒.๖.๒ (๒.๓) ประชาสัมพันธ์สถานการณ์ทั้งภายในและภายนอก บก.ทท. โดยข้อมูลที่ใช้ในการประชาสัมพันธ์ กร.ทหาร จะต้องนำเสนอเพื่อขอความเห็นจากคณะกรรมการบริหารความต่อเนื่อง ตามข้อ ๑.๒.๖.๒ (๑.๑) เสียก่อน และควรมีการเผยแพร่ข้อมูลตามความจำเป็น และดำเนินการอย่างต่อเนื่องเพื่อให้กำลังพลที่เกี่ยวข้องเข้าใจสถานการณ์ที่เกิดขึ้น

๑.๒.๖.๒ (๒.๔) คณะกรรมการบริหารความต่อเนื่อง ดำเนินการร่วมกับ ขว.ทหาร จัดทำแผนการอพยพเคลื่อนย้าย (Occupant Emergency Plan) เพื่อใช้ในการอพยพกำลังพลและสิ่งของที่เกี่ยวข้องไปยังศูนย์ข้อมูลสำรอง บก.ทท. อย่างน้อยต้องประกอบด้วย ดังนี้

๑.๒.๖.๒ (๒.๔.๑) ขั้นตอนในการอพยพกำลังพลและสิ่งของที่เกี่ยวข้องไปยังศูนย์ข้อมูลสำรอง บก.ทท.

๑.๒.๖.๒ (๒.๔.๒) รับผิดชอบในการตรวจสอบผู้ที่ได้รับบาดเจ็บ และให้การช่วยเหลือ

๑.๒.๖.๒ (๓) คณะกรรมการบริหารความต่อเนื่อง จัดทำแผนกู้คืนระบบ (Disaster Recovery Plan) เพื่อกู้คืนระบบสารสนเทศที่สำคัญของ บก.ทท. ณ ศูนย์ข้อมูลสำรอง บก.ทท. อย่างน้อยต้องประกอบด้วย ดังนี้

/๑.๒.๖.๒ (๓.๑) ขั้นตอน..

๑.๒.๖.๒ (๓.๑) ขั้นตอนในการกู้คืนระบบสารสนเทศที่สำคัญของ บก.ทท. ณ ศูนย์ข้อมูลสำรอง บก.ทท.

๑.๒.๖.๒ (๓.๒) จัดเตรียมอุปกรณ์ ซอฟต์แวร์ เครือข่ายการสื่อสาร และอุปกรณ์สนับสนุนต่างๆ ณ ศูนย์ข้อมูลสำรอง บก.ทท.

๑.๒.๖.๒ (๔) คณะกรรมการบริหารความต่อเนื่อง ดำเนินการร่วมกับ ศชบ.ทหาร จัดทำแผนรับมือเหตุการณ์ทางไซเบอร์ (Cyber Incident Response Plan) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่อาจมีผลกระทบต่อระบบสารสนเทศที่สำคัญของ บก.ทท. ณ ศูนย์ข้อมูลสำรอง บก.ทท. อย่างน้อยต้องประกอบด้วย ดังนี้

๑.๒.๖.๒ (๔.๑) ขั้นตอนในการรับมือกับภัยคุกคามทางไซเบอร์ที่อาจมีผลกระทบต่อระบบสารสนเทศที่สำคัญของ บก.ทท. ณ ศูนย์ข้อมูลสำรอง บก.ทท.

๑.๒.๖.๒ (๔.๒) จัดเตรียมระบบเฝ้าระวังและตรวจจับเหตุการณ์ทางไซเบอร์ และระบบรับมือต่อเหตุการณ์ทางไซเบอร์ รวมถึงกำลังพลผู้ปฏิบัติงานที่เกี่ยวข้อง

๑.๒.๖.๒ (๕) คณะกรรมการบริหารความต่อเนื่อง จัดทำแผนฟื้นฟู (Recovery Plan) เพื่อฟื้นฟูระบบสารสนเทศ ณ ศูนย์ข้อมูลหลัก บก.ทท. ภายหลังเหตุการณ์วิกฤติผ่านไปแล้ว อย่างน้อยต้องประกอบด้วย ดังนี้

๑.๒.๖.๒ (๕.๑) ขั้นตอนในการฟื้นฟูระบบสารสนเทศ ณ ศูนย์ข้อมูลหลัก บก.ทท.

๑.๒.๖.๒ (๕.๒) ตรวจสอบความเสียหาย ความปลอดภัย และความพร้อมใช้งานของศูนย์ข้อมูลหลัก บก.ทท. รวมถึงบริเวณใกล้เคียง

๑.๒.๖.๒ (๕.๓) จัดเตรียมอุปกรณ์ ซอฟต์แวร์ เครือข่ายการสื่อสาร และอุปกรณ์สนับสนุนต่างๆ ณ ศูนย์ข้อมูลหลัก บก.ทท.

๑.๒.๖.๓ การทดสอบแผนเตรียมความพร้อมกรณีฉุกเฉิน (CP-3 Continuity Plan Testing) สส.ทหาร ทบทวนและทดสอบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อย ๑ ครั้ง/ปี ตามระดับความเสี่ยงที่ยอมรับได้ หรือเมื่อมีเหตุการณ์ที่สำคัญ

๑.๒.๖.๔ การฝึกอบรมแผนเตรียมความพร้อมกรณีฉุกเฉิน (CP-4 Continuity Training) สส.ทหาร จัดการฝึกอบรมแผนเตรียมความพร้อมกรณีฉุกเฉิน ให้กับกำลังพลที่เกี่ยวข้อง อย่างน้อย ๑ ครั้ง/ปี

๑.๒.๗ การพิสูจน์และยืนยันตัวตน (Identification and Authentication : IA)

๑.๒.๗.๑ การบริหารจัดการรหัสผ่าน (IA-1 User Password Management)

๑.๒.๗.๑ (๑) มีการเปลี่ยนรหัสผ่านให้มีความมั่นคงปลอดภัย

๑.๒.๗.๑ (๒) การใช้งานบัญชีผู้ใช้งานและรหัสผ่านต้องแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๑.๒.๗.๑ (๓) การตั้งรหัสผ่านชั่วคราวต้องยากต่อการเดา และต้องมีความแตกต่างกัน และอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติเพื่อยืนยันรหัสผ่านใหม่

/๑.๒.๗.๑ (๔) ต้องส่งมอบ...

๑.๒.๗.๑ (๔) ต้องส่งมอบบัญชีผู้ใช้งาน รหัสผ่านชั่วคราว ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่น ถ้าใช้พลนำสารส่งต้องใส่ของปิดผนึกให้เรียบร้อย หรือส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่านให้กับผู้ใช้งานโดยตรง เมื่อผู้ใช้งานต้องทำการลงชื่อเข้าใช้งานระบบงานครั้งแรกให้ทำการเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๑.๒.๗.๑ (๕) การเปลี่ยนรหัสผ่านต้องมีการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๑.๒.๗.๑ (๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privilege Account) ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากผู้อนุมัติสิทธิ์และผู้อนุมัติบัญชีผู้ใช้ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับว่าเข้าได้ถึงระดับไดได้บ้าง และต้องกำหนดให้รหัสบัญชีผู้ใช้งานที่มีสิทธิ์สูงต่างจากรหัสผ่านของบัญชีผู้ใช้งานทั่วไป

๑.๒.๗.๑ (๗) ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน ให้แสดงเป็นเครื่องหมายดอกจัน (*) บนหน้าจอ

๑.๒.๗.๑ (๘) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๑.๒.๗.๒ หน้าที่ความรับผิดชอบของผู้ใช้งาน (IA-2 User Responsibilities)

๑.๒.๗.๒ (๑) การใช้งานรหัสผ่าน (Password Use)

๑.๒.๗.๒ (๑.๑) การกำหนดรหัสผ่าน

๑.๒.๗.๒ (๑.๑.๑) ผู้ใช้งานต้องกำหนดรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น อย่างน้อยต้องกำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เน้นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๑.๒.๗.๒ (๑.๑.๒) ผู้ใช้งานต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม

๑.๒.๗.๒ (๑.๑.๓) ผู้ใช้งานต้องหลีกเลี่ยงการกำหนดรหัสผ่านที่ง่ายต่อการคาดเดา เช่น กลุ่มอักขระที่เรียงกัน (123, abcd) หรือ กลุ่มของตัวอักขระที่เหมือนกัน (111, aaa)

๑.๒.๗.๒ (๑.๒) การใช้งานรหัสผ่าน

๑.๒.๗.๒ (๑.๒.๑) ผู้ใช้งานต้องไม่ใช้รหัสผ่านส่วนบุคคลร่วมกับบุคคลอื่น

๑.๒.๗.๒ (๑.๒.๒) ผู้ใช้งานต้องเก็บรักษารหัสผ่านไว้เป็นความลับ

๑.๒.๗.๒ (๑.๓) การเปลี่ยนรหัสผ่าน

๑.๒.๗.๒ (๑.๓.๑) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีในครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

๑.๒.๗.๒ (๑.๓.๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้ หรือตามรอบระยะเวลาที่กำหนด

๑.๒.๗.๒ (๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ (Unattended User Equipment)

/๑.๒.๗.๒ (๒.๑) หน่วยต้องสร้าง...

๑.๒.๗.๒ (๒.๑) หน่วยต้องสร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๑.๒.๗.๒ (๒.๒) ผู้ใช้งานต้องล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน

๑.๒.๗.๒ (๒.๓) ผู้ใช้งานต้องตั้งค่าล็อกหน้าจอเครื่องคอมพิวเตอร์อย่างน้อยหลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเข้าใช้งานได้

๑.๒.๗.๒ (๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

๑.๒.๗.๒ (๓.๑) ผู้ใช้งานต้องไม่ทิ้งหรือปล่อยสินทรัพย์สารสนเทศของ บก.ทท. ให้อยู่ในสถานที่ที่ไม่ปลอดภัย หรืออยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๑.๒.๗.๒ (๓.๒) ผู้ใช้งานต้องออกจากระบบ (Logout) โดยทันทีเมื่อเสร็จสิ้นการใช้งาน เพื่อป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ หรือระบบสารสนเทศโดยไม่ได้รับอนุญาต

๑.๒.๗.๒ (๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ รวมถึงวิธีปฏิบัติเพิ่มเติม ดังนี้

๑.๒.๗.๒ (๔.๑) ข้อมูลอิเล็กทรอนิกส์ "ลับที่สุด" ให้มีการเข้ารหัสไฟล์ (File Encryption) รวมถึงการเข้ารหัสสื่อบันทึกข้อมูล (Media Encryption) และการเข้ารหัสการรับส่งข้อมูลผ่านช่องทางการสื่อสาร (Communication Encryption) ทุกครั้ง

๑.๒.๗.๒ (๔.๒) ข้อมูลอิเล็กทรอนิกส์ "ลับมาก" ให้มีการเข้ารหัสสื่อบันทึกข้อมูล (Media Encryption) และการเข้ารหัสการรับส่งข้อมูลผ่านช่องทางการสื่อสาร (Communication Encryption) ทุกครั้ง

๑.๒.๗.๒ (๔.๓) ข้อมูลอิเล็กทรอนิกส์ "ลับ" ให้มีการเข้ารหัสการรับส่งข้อมูลผ่านช่องทางการสื่อสาร (Communication Encryption) ทุกครั้ง

๑.๒.๘ การรับมือเหตุการณ์ทางไซเบอร์ (Incident Response : IR)

๑.๒.๘.๑ แผนรับมือเหตุการณ์ทางไซเบอร์ (IR-1 Incident Response Plan)

๑.๒.๘.๑ (๑) ให้มีการจัดทำแผนรับมือเหตุการณ์ทางไซเบอร์ บก.ทท. ซึ่งอย่างน้อยต้องประกอบด้วย

๑.๒.๘.๑ (๑.๑) วัตถุประสงค์

๑.๒.๘.๑ (๑.๒) ขอบเขต

๑.๒.๘.๑ (๑.๓) นิยามของเหตุการณ์ทางไซเบอร์ (Event and Incident)

๑.๒.๘.๑ (๑.๔) โครงสร้าง หน้าที่ ความรับผิดชอบของส่วนรับมือเหตุการณ์ทางไซเบอร์

๑.๒.๘.๑ (๑.๕) ประเภทของเหตุการณ์ทางไซเบอร์ (Incident Type)

๑.๒.๘.๑ (๑.๖) ระดับความรุนแรงของเหตุการณ์ทางไซเบอร์ (Incident Severity Level)

๑.๒.๘.๑ (๑.๗) ขั้นตอนปฏิบัติ

๑.๒.๘.๑ (๑.๘) แผนการติดต่อสื่อสาร

/๑.๒.๘.๑ (๒) เมื่อได้รับ...

๑.๒.๘.๑ (๒) เมื่อได้รับการประสานให้ นขต.บก.ทท. แจ้งรายชื่อผู้ทำหน้าที่นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยให้ ศชบ.ทหาร ทราบโดยเร็ว เพื่อให้สามารถแก้ไขปัญหาจากเหตุการณ์ทางไซเบอร์ร่วมกับเจ้าหน้าที่ของส่วนรับมือเหตุการณ์ทางไซเบอร์ ศชบ.ทหาร ได้อย่างมีประสิทธิภาพ

๑.๒.๘.๒ การฝึกรับมือเหตุการณ์ทางไซเบอร์ (IR-2 Incident Response Training) ให้มีการฝึกกำลังพลที่ปฏิบัติหน้าที่เกี่ยวกับการรับมือเหตุการณ์ทางไซเบอร์ของ บก.ทท. เพื่อให้กำลังพลดังกล่าวมีความรู้ความเข้าใจ เกี่ยวกับหน้าที่และความรับผิดชอบตามที่กำหนดไว้ในแผนอย่างน้อยปีละ ๑ ครั้ง

๑.๒.๘.๓ การทดสอบแผนรับมือเหตุการณ์ทางไซเบอร์ (IR-3 Incident Response Testing) ให้มีการทดสอบแผนรับมือเหตุการณ์ทางไซเบอร์ บก.ทท. เพื่อให้ทราบถึงความเหมาะสมของแผนดังกล่าว รวมถึงเกิดการบูรณาการแผนดังกล่าวเข้ากับแผนอื่นที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๑.๒.๘.๔ การรับมือเหตุการณ์ทางไซเบอร์ (IR-4 Incident Handling) ให้มีการพัฒนาขีดความสามารถด้านการรับมือเหตุการณ์ทางไซเบอร์ของ บก.ทท. ซึ่งอย่างน้อยต้องประกอบด้วย

๑.๒.๘.๔ (๑) พัฒนาระบบสารสนเทศเพื่อรับมือเหตุการณ์ทางไซเบอร์ของ บก.ทท.

๑.๒.๘.๔ (๒) จัดทำขั้นตอนปฏิบัติ หรือระเบียบปฏิบัติประจำ เพื่อรับมือเหตุการณ์ทางไซเบอร์ของ บก.ทท.

๑.๒.๘.๔ (๓) จัดทำขั้นตอนปฏิบัติด้านการรับมือเหตุการณ์ทางไซเบอร์เบื้องต้นให้กับ นขต.บก.ทท.

๑.๒.๘.๔ (๔) จัดให้มีช่องทางการติดต่อสื่อสารระหว่างส่วนรับมือเหตุการณ์ทางไซเบอร์ ศชบ.ทหาร กับ นขต.บก.ทท. เพื่อใช้ในการแก้ไขปัญหาร่วมกัน รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามไซเบอร์ด้วย

๑.๒.๘.๕ การติดตามเหตุการณ์ทางไซเบอร์ (IR-5 Incident Monitoring) ให้มีการบันทึกและติดตามเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นใน บก.ทท. ประกอบด้วย ลักษณะของเหตุการณ์ (Incident Overview) สถานภาพของเหตุการณ์ (Incident Status) สิ่งที่ตรวจพบ (Observable) การปฏิบัติเพื่อรับมือเหตุการณ์ (Incident Task) และบทเรียนที่ได้รับ (Lesson Learned) เพื่อใช้ในการปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. ต่อไป

๑.๒.๘.๖ การรายงานเหตุการณ์ทางไซเบอร์ (IR-6 Incident Reporting)

๑.๒.๘.๖ (๑) ให้มีการรายงานเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นใน บก.ทท. ให้ ผบ.ทสส. ทราบ อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๑.๒.๘.๖ (๒) ในกรณีที่ นขต.บก.ทท. ตรวจพบเหตุการณ์ทางไซเบอร์ภายในหน่วยของตน ให้นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยรายงานเหตุการณ์ดังกล่าวให้ ศชบ.ทหาร ทราบโดยเร็ว

๑.๒.๙ การบำรุงรักษา (Maintenance : MA)

๑.๒.๙.๑ มาตรการควบคุมการบำรุงรักษา (MA-1 Controlled Maintenance)

๑.๒.๙.๑ (๑) ให้มีการวางแผน ดำเนินการ บันทึก และทบทวนแนวทางการบำรุงรักษาระบบสารสนเทศ และระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ของ บก.ทท. อย่างเป็นลายลักษณ์อักษร อย่างน้อยจะต้องมีการระบุเกี่ยวกับบริษัทเจ้าของผลิตภัณฑ์ (Manufacturer or Vendor) รุ่น (Model) เวอร์ชัน (Version) ซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ

/๑.๒.๙.๑ (๒) ให้มี...

๑.๒.๙.๑ (๒) ให้มีขั้นตอน รวมถึงการดำเนินการขออนุมัติ การบำรุงรักษาระบบสารสนเทศ และระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ของ บก.ทท. อย่างเป็นลายลักษณ์อักษร ซึ่งจะต้องครอบคลุมทั้งการดำเนินการในที่ตั้ง (On Site) การดำเนินการนอกที่ตั้ง (Off Site) และการดำเนินการจากภายนอก (Remote Site)

๑.๒.๙.๑ (๓) ในกรณีที่จะต้องนำอุปกรณ์สารสนเทศไปบำรุงรักษานอกที่ตั้ง ให้หน่วยเจ้าของอุปกรณ์ดำเนินการตรวจสอบ และทำลายข้อมูลสำคัญบนสื่อบันทึกข้อมูล ตามหลักเกณฑ์ที่กำหนดไว้ในแนวปฏิบัตินี้

๑.๒.๙.๒ เครื่องมือในการบำรุงรักษา (MA-2 Maintenance Tools) ให้มีการควบคุมเครื่องมือในการบำรุงรักษาระบบสารสนเทศ และระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ของ บก.ทท. อย่างเหมาะสม ประกอบด้วย

๑.๒.๙.๒ (๑) ให้มีการพิจารณา และการอนุมัติ เครื่องมือในการบำรุงรักษาก่อนนำเข้ามาใช้ในหน่วยงาน

๑.๒.๙.๒ (๒) ให้มีการมอบหมายความรับผิดชอบให้กับผู้ใช้งานเครื่องมือในการบำรุงรักษา ตามหน้าที่และความรับผิดชอบอย่างเป็นลายลักษณ์อักษร

๑.๒.๙.๒ (๓) ให้มีการตั้งค่าเครื่องมือในการบำรุงรักษา เพื่อป้องกันมิให้ผู้ที่มิได้รับอนุญาตสามารถใช้งานเครื่องมือดังกล่าวได้ ประกอบด้วย

๑.๒.๙.๒ (๓.๑) การป้องกันทางกายภาพ

๑.๒.๙.๒ (๓.๒) หรือการป้องกันการเข้าถึง (Access Control)

๑.๒.๙.๒ (๓.๓) หรือการกำหนดสิทธิ์เท่าที่จำเป็น (Least Privilege)

๑.๒.๙.๓ เจ้าหน้าที่บำรุงรักษา (MA-3 Maintenance Personnel)

๑.๒.๙.๓ (๑) ให้มีขั้นตอนการอนุมัติ กำหนดหน้าที่ และความรับผิดชอบ ให้กำลังพลของหน่วยทำหน้าที่เจ้าหน้าที่บำรุงรักษาระบบสารสนเทศ และระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. หรือ นขต.บก.ทท.

๑.๒.๙.๓ (๒) ในกรณีที่มีเจ้าหน้าที่จากภายนอกเข้ามาบำรุงรักษาระบบสารสนเทศและระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. หรือ นขต.บก.ทท. หน่วยเจ้าของระบบจะต้องจัดให้มีเจ้าหน้าที่ของหน่วยเข้ามาควบคุม กำกับดูแล เจ้าหน้าที่บำรุงรักษาดังกล่าวให้ปฏิบัติตามนโยบายและแนวปฏิบัติฉบับนี้ รวมทั้งจะต้องมีการบันทึกข้อมูลเกี่ยวกับการปฏิบัติดังกล่าวไว้ด้วย

๑.๒.๑๐ การป้องกันสื่อบันทึกข้อมูล (Media Protection : MP)

๑.๒.๑๐.๑ การเข้าถึงสื่อบันทึกข้อมูล (MP-1 Media Access) ให้มีการป้องกันการเข้าถึงสื่อบันทึกข้อมูล ซึ่งมีการบันทึกข้อมูลสารสนเทศของหน่วย ดังนี้

(๑) การป้องกันทางกายภาพ

(๒) หรือ การไม่ทิ้งสื่อบันทึกข้อมูลไว้โดยไม่มีผู้ดูแล

(๓) หรือ การเข้ารหัสสื่อบันทึกข้อมูล

/๑.๒.๑๐.๒ การกำหนด...

๑.๒.๑๐.๒ การกำหนดสัญลักษณ์บนสื่อบันทึกข้อมูลดิจิทัล (MP-2 Digital Media Marking) ในกรณีที่มีการบันทึกข้อมูลที่มีชั้นความลับบนสื่อบันทึกข้อมูลดิจิทัล ประกอบด้วย แผ่นดิสก์ (Diskettes) เทปแม่เหล็ก (Magnetic Tapes) ฮาร์ดดิสก์ภายนอก (External or Removal Hard Disk Drives - Solid State, Magnetic) แฟลชไดรฟ์ (Flash Drives) คอมแพ็คดิสก์ (Compact Discs) เป็นต้น ให้มีการกำหนดสัญลักษณ์บนสื่อบันทึกข้อมูล หรือใช้วัสดุปิดทับซึ่งมีการกำหนดสัญลักษณ์ ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ดังนี้

สื่อบันทึกข้อมูลดิจิทัลที่มีการบันทึกข้อมูลชั้นความลับ "ลับ"	สื่อบันทึกข้อมูลดิจิทัลที่มีการบันทึกข้อมูลชั้นความลับ "ลับมาก"	สื่อบันทึกข้อมูลดิจิทัลที่มีการบันทึกข้อมูลชั้นความลับ "ลับที่สุด"
ลับ	ลับมาก	ลับที่สุด

๑.๒.๑๐.๓ พื้นที่จัดเก็บสื่อบันทึกข้อมูลดิจิทัล (MP-3 Digital Media Storage) ในกรณีที่มีการบันทึกข้อมูลที่มีชั้นความลับบนสื่อบันทึกข้อมูลดิจิทัล ประกอบด้วย แผ่นดิสก์ (Diskettes) เทปแม่เหล็ก (Magnetic Tapes) ฮาร์ดดิสก์ภายนอก (External or Removal Hard Disk Drives - Solid State, Magnetic) แฟลชไดรฟ์ (Flash Drives) คอมแพ็คดิสก์ (Compact Discs) เป็นต้น ให้มีการจัดเก็บสื่อบันทึกข้อมูลดังกล่าวไว้ในพื้นที่ซึ่งมีความมั่นคงปลอดภัย ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ รวมถึงแนวปฏิบัติเกี่ยวกับการควบคุมการเข้าพื้นที่ด้วย

๑.๒.๑๐.๔ การเคลื่อนย้ายสื่อบันทึกข้อมูลดิจิทัล (MP-4 Digital Media Transport) ให้มีการป้องกันหรือควบคุมในระหว่างการเคลื่อนย้ายสื่อบันทึกข้อมูลดิจิทัล ประกอบด้วย แผ่นดิสก์ (Diskettes) เทปแม่เหล็ก (Magnetic Tapes) ฮาร์ดดิสก์ภายนอก (External or Removal Hard Disk Drives -Solid State, Magnetic) แฟลชไดรฟ์ (Flash Drives) คอมแพ็คดิสก์ (Compact Discs) เป็นต้น ที่มีการบันทึกข้อมูลที่มีชั้นความลับ โดยให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๑.๒.๑๐.๕ การทำลายข้อมูลบนสื่อบันทึกข้อมูล (MP-5 Media Sanitization) ให้เป็นไปตามประเภทของความมั่นคงปลอดภัย ดังนี้

๑.๒.๑๐.๕ (๑) กำหนดให้มีวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูล ดังนี้

๑.๒.๑๐.๕ (๑.๑) การลบข้อมูล (Clear) หมายถึง วิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูล ด้วยการใช้ซอฟต์แวร์หรือฮาร์ดแวร์ ทำการเขียนทับพื้นที่บนสื่อบันทึกข้อมูล (User-Addressable Storage Space) ด้วยข้อมูลที่ไม่มีนัยยะสำคัญ เพื่อมิให้ผู้อื่นสามารถใช้วิธีการทั่วไปในการกู้คืนข้อมูลกลับมาได้ (Simple Non-Invasive Data Recovery Techniques)

๑.๒.๑๐.๕ (๑.๒) การล้างข้อมูล (Purge) หมายถึง วิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลด้วยการใช้เทคนิคทางตรรกะ (Logical) หรือกายภาพ (Physical) เพื่อมิให้ผู้อื่นสามารถใช้วิธีการในห้องปฏิบัติการในการกู้คืนข้อมูลกลับมาได้ (State of the Art Laboratory Techniques)

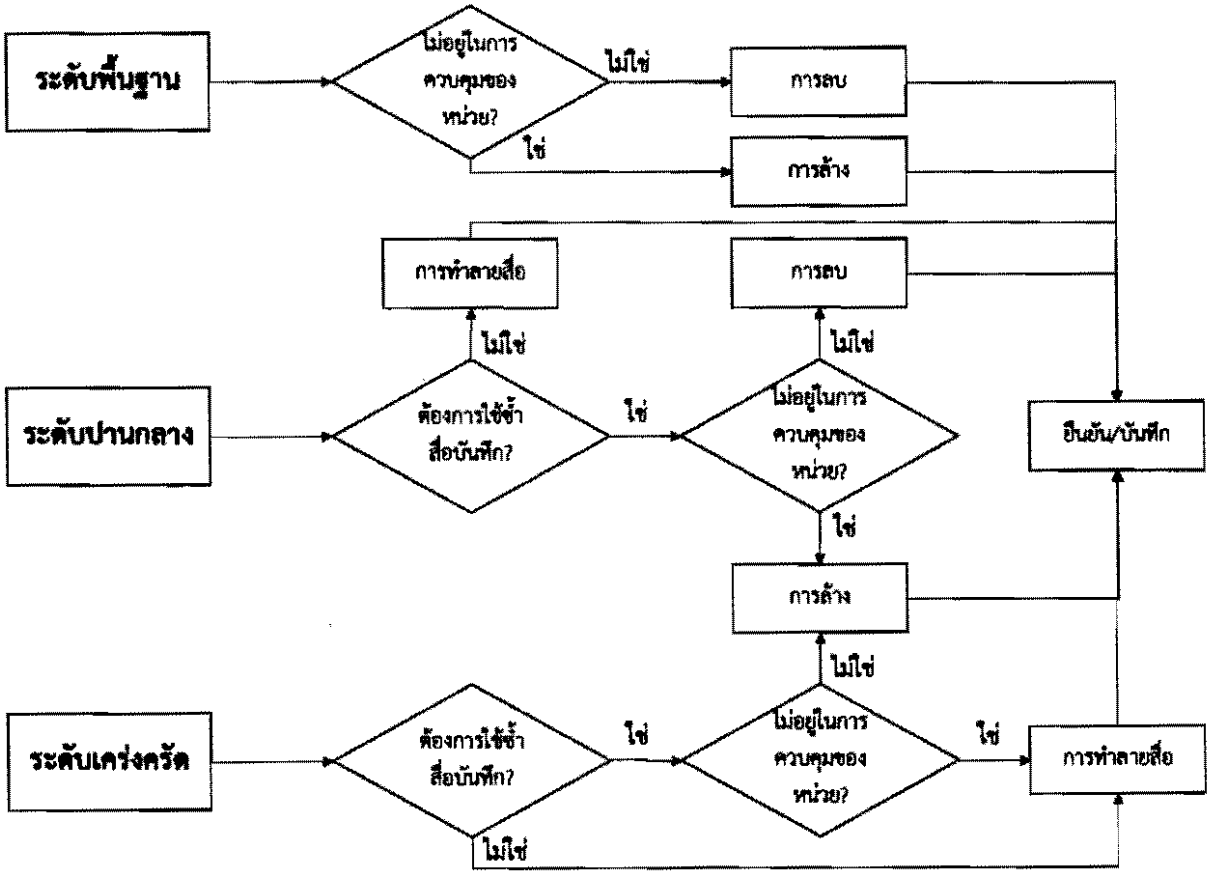
๑.๒.๑๐.๕ (๑.๓) การทำลายสื่อบันทึกข้อมูล (Destroy) หมายถึง วิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูล ด้วยการใช้เทคนิคทางตรรกะ (Logical) หรือกายภาพ (Physical) เพื่อมิให้ผู้อื่นสามารถใช้วิธีการในห้องปฏิบัติการในการกู้คืนข้อมูล รวมถึงไม่สามารถใช้งานสื่อบันทึกข้อมูลดังกล่าวได้ด้วย

/๑.๒.๑๐.๕ (๒) ให้ใช้...

๑.๒.๑๐.๕ (๒) ให้ใช้วิธีการทำลายข้อมูลตามประเภทของความมั่นคงปลอดภัย ดังนี้

ประเภทของความมั่นคงปลอดภัย "ระดับพื้นฐาน"	ประเภทของความมั่นคงปลอดภัย "ระดับปานกลาง"	ประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"
การลบ หรือล้าง	การลบ หรือล้าง หรือทำลาย	การล้าง หรือทำลาย

๑.๒.๑๐.๕ (๓) กำหนดเงื่อนไขในการทำลายข้อมูลบนสื่อบันทึกข้อมูล ดังนี้



/๑.๒.๑๐.๕ (๔) กำหนดให้...

๑.๒.๑๐.๕ (๔) กำหนดให้สื่อแต่ละประเภท มีวิธีการทำลายข้อมูล ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการลบ	วิธีการล้าง	วิธีการทำลาย
อุปกรณ์เครือข่าย Router, Switch	- Full Manufacturer's Reset	- ทำได้เฉพาะบางรุ่น ให้สอบถามจากบริษัท - ในกรณีที่ไม่สามารถทำได้ ให้ใช้วิธีทำลาย	- ฉีก หรือบด - แยกส่วน - เผา
โทรศัพท์มือถือ แท็บเล็ต	- Factory Reset (Erase All Content and Settings)	- Factory Reset (Erase All Content and Settings)	- ฉีก หรือบด - แยกส่วน - เผา
อุปกรณ์สำนักงาน Printer, Multifunction, Fax	- Full Manufacturer's Reset	- ทำได้เฉพาะบางรุ่น ให้สอบถามจากบริษัท - ในกรณีที่สามารถถอดสื่อบันทึกข้อมูลออกได้ ให้ทำตามประเภทของสื่อบันทึก - ในกรณีที่ไม่สามารถทำได้ ให้ใช้วิธีทำลาย	- ฉีก หรือบด - แยกส่วน - เผา
แผ่นดิสก์	- เขียนข้อมูลทับโดยใช้ซอฟต์แวร์ - หรือบน Windows ให้ Format จำนวนไม่น้อยกว่า ๓ ครั้ง ด้วยคำสั่ง Format X: /P:3 *replace X with the target drive letter	- Degauss	- ฉีก หรือบด - เผา
แผ่นซีดี/ดีวีดี/บลูเรย์	- กรณีที่สามารถทำการ format ได้ ให้ทำการ format จำนวน ๑ รอบ	-	- ฉีก หรือบด - เผา
ฮาร์ดดิสก์ (Magnetic Disk Drive)	- เขียนข้อมูลทับโดยใช้ซอฟต์แวร์ - หรือบน Windows ให้ Format จำนวนไม่น้อยกว่า ๓ ครั้ง ด้วยคำสั่ง Format X:/P:3 *replace X with the target drive letter - หรือบน Linux ให้ Disk Wiping ด้วยคำสั่ง dd if=/dev/zero of=/dev/sdX bs=1M *replace X with the target drive letter	- Degauss	- ฉีก หรือบด - เผา
ฮาร์ดดิสก์ SSD (Solid State Drive)	- เขียนข้อมูลทับโดยใช้ซอฟต์แวร์อย่างน้อย ๑ ครั้ง	- กรณีเป็น ATA SSD และอุปกรณ์รองรับให้ใช้คำสั่งประเภท Block Erase หรือ Sanitize Crypto Scramble - กรณีเป็น SCSI SSD และอุปกรณ์รองรับให้ใช้คำสั่ง Block Erase หรือ Cryptographic Erase	- ฉีก หรือบด - เผา

/ประเภทสื่อ...

ประเภทสื่อบันทึกข้อมูล	วิธีการลบ	วิธีการล้าง	วิธีการทำลาย
เทปแม่เหล็ก	- เขียนข้อมูลทับโดยใช้ซอฟต์แวร์ จำนวนไม่น้อยกว่า ๑ ครั้ง	- Degauss	- ฉีก หรือบด - เผา
แฟลชไดรฟ์	- เขียนข้อมูลทับโดยใช้ซอฟต์แวร์ - หรือบน Windows ให้ Format จำนวนไม่น้อยกว่า ๒ ครั้ง ด้วยคำสั่ง Format X: /P:2 *replace X with the target drive letter	-	- ฉีก หรือบด - เผา
เมโมรีการ์ด SD, SDHC, MMC, Compact Flash Memory	- เขียนข้อมูลทับโดยใช้ซอฟต์แวร์ - หรือบน Windows ให้ Format จำนวนไม่น้อยกว่า ๒ ครั้ง ด้วยคำสั่ง Format X: /P:2 *replace X with the target drive letter	-	- ฉีก หรือบด - เผา

๑.๒.๑๐.๖ การใช้สื่อบันทึกข้อมูลดิจิทัล (MP-6 Digital Media Use) ให้มีการใช้งานสื่อบันทึกข้อมูลดิจิทัล ประกอบด้วย แผ่นดิสก์ (Diskettes) เทปแม่เหล็ก (Magnetic Tapes) ฮาร์ดดิสก์ภายนอก (External or Removal Hard Disk Drives - Solid State, Magnetic) แฟล็ชไดรฟ์ (Flash Drives) คอมแพ็คดิสก์ (Compact Discs) เป็นต้น อย่างมั่นคงปลอดภัยดังนี้

๑.๒.๑๐.๖ (๑) ห้ามมิให้ใช้สื่อบันทึกข้อมูลดิจิทัลที่ไม่ทราบแหล่งที่มา

๑.๒.๑๐.๖ (๒) ห้ามมิให้ใช้สื่อบันทึกข้อมูลดิจิทัลกับเครื่องคอมพิวเตอร์ หรือโน้ตบุ๊กซึ่งมีการเชื่อมต่อกับเครือข่ายสารสนเทศของ บก.ทท. ซึ่งมิได้มีการติดตั้งโปรแกรมป้องกันมัลแวร์ ตามที่ ศชบ.ทหาร กำหนด

๑.๒.๑๐.๖ (๓) หลังจากเชื่อมต่อสื่อบันทึกข้อมูลดิจิทัลกับเครื่องคอมพิวเตอร์หรือโน้ตบุ๊ก ให้ทำการสแกนด้วยโปรแกรมป้องกันมัลแวร์ทุกครั้ง หรือทำการตั้งค่าโปรแกรมป้องกันมัลแวร์ให้ทำการสแกนสื่อบันทึกข้อมูลดิจิทัลทันทีที่มีการเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือโน้ตบุ๊ก

๑.๒.๑๑ การป้องกันทางกายภาพและสภาพแวดล้อม (Physical and Environmental Protection : PE)

๑.๒.๑๑.๑ สิทธิ์ในการเข้าพื้นที่ (PE-1 Physical Access Authorizations) ให้มีการจัดทำบัญชีของบุคคลที่อนุญาตให้เข้าปฏิบัติงานในพื้นที่ที่มีการรักษาความปลอดภัย พื้นที่ควบคุม หรือพื้นที่หวงห้าม โดยต้องจัดทำเป็นลายลักษณ์อักษร รวมทั้งต้องได้รับการอนุมัติ และปรับปรุงให้มีความทันสมัยอยู่เสมอ

๑.๒.๑๑.๒ การควบคุมการเข้าพื้นที่ (PE-2 Physical Access Control) ให้มีการควบคุมการเข้าพื้นที่ตามสิทธิ์ที่ได้รับของแต่ละบุคคล โดยจะต้องให้มีความสอดคล้องกับระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ดังนี้

/๑.๒.๑๑.๒ (๑) แผนการ...

๑.๒.๑๑.๒ (๑) แผนการรักษาความปลอดภัยเกี่ยวกับสถานที่จะต้องครอบคลุมถึงพื้นที่ติดตั้งและใช้งานระบบสารสนเทศของหน่วยด้วย

๑.๒.๑๑.๒ (๒) มาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ จะต้องพิจารณาถึงการกำหนดพื้นที่ที่มีการรักษาความปลอดภัย การป้องกันการเข้าถึงทางกายภาพ ระบบแสงสว่าง ระบบสัญญาณเตือน ระบบตรวจสอบและพิสูจน์ตัวตน ทั้งนี้ให้เหมาะสมกับประเภทความมั่นคงปลอดภัยของระบบสารสนเทศนั้น

๑.๒.๑๑.๒ (๓) การสำรวจและตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่จะต้องครอบคลุมถึงพื้นที่ติดตั้งและใช้งานระบบสารสนเทศของหน่วยด้วย

๑.๒.๑๑.๒ (๔) ก่อนอนุญาตให้เข้าพื้นที่ต้องมีการพิสูจน์ตัวตนเสียก่อน

๑.๒.๑๑.๒ (๕) เมื่อได้รับการอนุญาตให้เข้าพื้นที่แล้วจะต้องมีการติดตามการปฏิบัติงานของบุคคลดังกล่าว ทั้งนี้ให้ใช้วิธีการเฝ้าติดตามทางอิเล็กทรอนิกส์ หรือการเฝ้าติดตามโดยใช้บุคคลตามระดับความสำคัญของพื้นที่ และมาตรการรักษาความปลอดภัยพื้นที่ของหน่วย

๑.๒.๑๑.๒ (๖) บันทึกการเข้าออกของบุคคล รวมถึงขณะปฏิบัติงานในพื้นที่ที่มีการรักษาความปลอดภัย พื้นที่ควบคุม หรือพื้นที่หวงห้าม

๑.๒.๑๑.๒ (๗) ให้มีการเปลี่ยนกุญแจ (Physical Key) รหัสที่ใช้กับกุญแจ (Physical Combination Key) หรือรหัสผ่าน (Password for Physical Access Device) ในการเข้าพื้นที่ที่มีการรักษาความปลอดภัย พื้นที่ควบคุม หรือพื้นที่หวงห้าม อย่างน้อย ๑ ครั้ง/ปี หรือเมื่อพบเหตุการณ์ที่คาดว่าอุปกรณ์ดังกล่าวถูกเข้าควบคุมโดยผู้ที่ไม่ประสงค์ดี

๑.๒.๑๑.๓ การควบคุมสื่อที่ใช้ในการรับส่งข้อมูล (PE-3 Access Control for Transmission Media) ให้มีการควบคุมสื่อที่ใช้ในการรับส่งข้อมูลสารสนเทศในพื้นที่ที่มีการรักษาความปลอดภัย พื้นที่ควบคุม หรือพื้นที่หวงห้าม เพื่อลดผลกระทบจากความเสี่ยงตามธรรมชาติ เช่น สัตว์กัดแทะ สภาพอากาศ หรือความเสี่ยงที่เกิดจากมนุษย์ เช่น อุบัติเหตุ การดักฟัง การทำให้เสียหาย ดังนี้

๑.๒.๑๑.๓ (๑) ห่อหุ้มสายสัญญาณด้วยวัสดุป้องกัน

๑.๒.๑๑.๓ (๒) ปิดล็อคตู้เก็บสายสัญญาณ หรืออุปกรณ์เครือข่าย หรืออุปกรณ์สื่อสาร

๑.๒.๑๑.๓ (๓) ตัดการเชื่อมต่อ หรือปิดการทำงานของช่องเชื่อมต่อที่มิได้ใช้งาน

๑.๒.๑๑.๔ การติดตามการเข้าถึงทางกายภาพ (PE-4 Monitoring Physical Access)

๑.๒.๑๑.๔ (๑) ให้มีการติดตามการเข้าถึงทางกายภาพสำหรับระบบสารสนเทศ อุปกรณ์ประมวลผล สื่อบันทึกข้อมูล ระบบฐานข้อมูล อุปกรณ์เครือข่าย และศูนย์ข้อมูล

๑.๒.๑๑.๔ (๒) ให้มีการตรวจสอบบันทึกการเข้าออกของบุคคลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง/ปี หรือตามมาตรการรักษาความปลอดภัยของหน่วย

๑.๒.๑๑.๔ (๓) ในกรณีที่ นขต.บก.ทท. ตรวจพบเหตุการณ์ผิดปกติ ให้ประสานการปฏิบัติร่วมกับ ศชบ.ทหาร เพื่อร่วมกันตรวจสอบและแก้ไขเหตุการณ์ดังกล่าวต่อไป

/๑.๒.๑๑.๕ การบันทึก...

๑.๒.๑๑.๕ การบันทึกผู้มาตรวจเยี่ยม (PE-5 Visitor Access Records) กรณีมีผู้มาตรวจเยี่ยมในพื้นที่ที่มีการรักษาความปลอดภัย พื้นที่ควบคุม หรือพื้นที่หวงห้าม ให้มีการบันทึกรายละเอียดขั้นต้นของบุคคลดังกล่าว อย่างน้อยประกอบด้วย ชื่อ นามสกุล เวลาที่เข้าเยี่ยมชม และเวลาที่ออก เพื่อใช้ในการตรวจสอบกรณีพบเหตุการณ์ผิดปกติในภายหลัง

๑.๒.๑๑.๖ การป้องกันอุปกรณ์ไฟฟ้าและสายไฟฟ้า (PE-6 Power Equipment and Cabling) ให้มีการป้องกันอุปกรณ์ไฟฟ้าและสายไฟฟ้าเพื่อลดผลกระทบจากความเสี่ยงตามธรรมชาติ เช่น สัตว์กัดแทะ สภาพอากาศ หรือความเสี่ยงที่เกิดจากมนุษย์ เช่น อุบัติเหตุ การทำให้เสียหาย ดังนี้

๑.๒.๑๑.๖ (๑) ต้องมีการปิดล็อคห้อง หรือควบคุมการเข้าถึงเครื่องกำเนิดไฟฟ้า หรือส่วนควบคุมเครื่องกำเนิดไฟฟ้า มิให้บุคคลที่ไม่เกี่ยวข้องสามารถเข้าถึงได้

๑.๒.๑๑.๖ (๒) อุปกรณ์ไฟฟ้าและสายไฟฟ้าที่อยู่นอกอาคาร จะต้องมีการห่อหุ้มด้วยวัสดุที่มีความทนทาน หรือบรรจุไว้ในสิ่งห่อหุ้มที่แข็งแรงทนทาน หรือการล็อคอุปกรณ์ดังกล่าวด้วยกุญแจที่แข็งแรงทนทาน

๑.๒.๑๑.๗ แหล่งจ่ายไฟฉุกเฉิน (PE-7 Emergency Power) ให้มีการจัดหาแหล่งจ่ายไฟฉุกเฉินสำหรับระบบสารสนเทศซึ่งมีความสำคัญซึ่งมีความจำเป็นต้องสามารถทำงานได้อย่างต่อเนื่อง ทั้งนี้ ให้คำนึงถึงผลกระทบต่อภารกิจหลักของ บก.ทท. รวมถึงชีวิตของกำลังพล เป็นลำดับแรก ดังนี้

๑.๒.๑๑.๗ (๑) ให้มีการเชื่อมต่อแหล่งจ่ายไฟชั่วคราว ซึ่งมาจากแหล่งจ่ายไฟอื่น (Alternate Power Supply) ซึ่งหากแหล่งจ่ายไฟหลักไม่สามารถจ่ายไฟได้ จะไม่ได้รับผลกระทบจากแหล่งจ่ายไฟหลักนั้น ทั้งนี้ ระยะเวลาการจ่ายไฟฟ้าของแหล่งจ่ายไฟชั่วคราว จะต้องเพียงพอที่จะทำให้สามารถปิดระบบดังกล่าวได้ หรือเพียงพอต่อการสลับไปใช้แหล่งจ่ายไฟฉุกเฉินได้ ในกรณีที่เป็นระบบสารสนเทศที่มีความสำคัญ

๑.๒.๑๑.๗ (๒) ให้มีการเชื่อมต่อแหล่งจ่ายไฟฉุกเฉิน ซึ่งมาจากแหล่งจ่ายไฟอื่น (Alternate Power Supply) ซึ่งหากแหล่งจ่ายไฟหลักไม่สามารถจ่ายไฟได้ จะไม่ได้รับผลกระทบจากแหล่งจ่ายไฟหลักนั้น

๑.๒.๑๑.๗ (๓) หรือให้มีการเชื่อมต่อแหล่งจ่ายไฟฉุกเฉิน ซึ่งมาจากแหล่งจ่ายไฟของหน่วย (Self-Contained) ได้แก่ เครื่องกำเนิดไฟฟ้าของหน่วย หรือเครื่องกำเนินไฟฟ้าของ บก.ทท. ซึ่งหากแหล่งจ่ายไฟหลักไม่สามารถจ่ายไฟได้จะไม่ได้รับผลกระทบจากแหล่งจ่ายไฟหลักนั้น

๑.๒.๑๑.๘ ระบบส่องสว่างฉุกเฉิน (PE-8 Emergency Lighting) ให้มีการจัดหาและติดตั้งระบบส่องสว่างฉุกเฉินสำหรับระบบสารสนเทศซึ่งมีความสำคัญซึ่งมีความจำเป็นต้องสามารถทำงานได้อย่างต่อเนื่อง ทั้งนี้ ให้คำนึงถึงผลกระทบต่อภารกิจหลักของ บก.ทท. รวมถึงชีวิตของกำลังพลเป็นลำดับแรก อย่างน้อยต้องครอบคลุมพื้นที่ ดังนี้

๑.๒.๑๑.๘ (๑) ศูนย์ข้อมูล

๑.๒.๑๑.๘ (๒) ห้องปฏิบัติการ หรือห้องควบคุมบังคับบัญชา

๑.๒.๑๑.๘ (๓) ทางออกฉุกเฉิน

/๑.๒.๑๑.๙ ระบบ...

๑.๒.๑๑.๙ ระบบป้องกันอัคคีภัย (PE-9 Fire Protection) ให้มีการจัดหาและติดตั้งระบบป้องกันอัคคีภัยสำหรับระบบสารสนเทศซึ่งมีความสำคัญซึ่งมีความจำเป็นต้องสามารถทำงานได้อย่างต่อเนื่อง ทั้งนี้ ให้คำนึงถึงผลกระทบต่อภารกิจหลักของ บก.ทท. รวมถึงชีวิตของกำลังพลเป็นลำดับแรก อย่างน้อยต้องครอบคลุมพื้นที่ ดังนี้

๑.๒.๑๑.๙ (๑) ศูนย์ข้อมูล

๑.๒.๑๑.๙ (๒) ห้องปฏิบัติการ หรือห้องควบคุมบังคับบัญชา

๑.๒.๑๑.๙ (๓) ทางออกฉุกเฉิน

๑.๒.๑๑.๑๐ ระบบควบคุมอุณหภูมิและความชื้น (PE-10 Temperature and Humidity Controls) ให้มีการจัดหาและติดตั้งระบบควบคุมอุณหภูมิและความชื้นสำหรับศูนย์ข้อมูล หรือพื้นที่ซึ่งมีการติดตั้งเครื่องแม่ข่ายบนระบบสารสนเทศ ซึ่งมีความสำคัญซึ่งมีความจำเป็นต้องสามารถทำงานได้อย่างต่อเนื่อง ทั้งนี้ ให้มีการติดตามสถานะของอุณหภูมิและความชื้น ดังนี้

ประเภทของความมั่นคงปลอดภัย "ระดับพื้นฐาน"	ประเภทของความมั่นคงปลอดภัย "ระดับปานกลาง"	ประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด"
-	อุณหภูมิ = ๑๘ - ๒๗ องศาเซลเซียส ความชื้น = ๔๐ - ๖๐ เปอร์เซ็นต์	อุณหภูมิ = ๒๐ - ๒๔ องศาเซลเซียส ความชื้น = ๔๕ - ๕๕ เปอร์เซ็นต์

หากพบว่าสถานะของอุณหภูมิและความชื้นไม่เป็นไปตามตารางข้างต้น ให้ดำเนินการแก้ไขโดยเร็ว

๑.๒.๑๑.๑๑ ระบบป้องกันน้ำรั่วซึม (PE-11 Water Damage Protection) ให้มีการจัดหาและติดตั้งระบบป้องกันน้ำรั่วซึมสำหรับศูนย์ข้อมูล หรือพื้นที่ซึ่งมีการติดตั้งเครื่องแม่ข่ายบนระบบสารสนเทศซึ่งมีความสำคัญซึ่งมีความจำเป็นต้องสามารถทำงานได้อย่างต่อเนื่อง ดังนี้

๑.๒.๑๑.๑๑ (๑) ติดตั้งอุปกรณ์ตรวจจับและแจ้งเตือนน้ำรั่วซึม

๑.๒.๑๑.๑๑ (๒) ติดตั้งอุปกรณ์ตัดไฟฟ้า (Master Shutoff or Isolation Valves)

๑.๒.๑๑.๑๒ การนำอุปกรณ์เข้า - ออก (PE-12 Delivery and Removal) ให้มีการอนุมัติ ติดตาม ควบคุม การนำอุปกรณ์สารสนเทศของหน่วยเข้า - ออก จากพื้นที่ รวมทั้งจะต้องมีการบันทึกการนำอุปกรณ์เข้า - ออก จากพื้นที่ด้วยทุกครั้ง

๑.๒.๑๑.๑๓ พื้นที่ปฏิบัติงานสำรอง (PE-13 Alternate Work Site) ให้มีการเตรียมการวางมาตรการควบคุมตามแผนเตรียมความพร้อมกรณีฉุกเฉินของ บก.ทท. ณ พื้นที่ปฏิบัติงานสำรอง

๑.๒.๑๒ การวางแผน (Planning : PL)

๑.๒.๑๒.๑ แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (PL-1 Cyber Security Plan)

๑.๒.๑๒.๑ (๑) นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วย เพื่อทำให้ระบบสารสนเทศของหน่วยมีความมั่นคงปลอดภัยไซเบอร์อย่างเป็นรูปธรรม ทั้งนี้ ให้จัดทำแผนตามรูปแบบที่ ศซบ.ทหาร กำหนด และขออนุมัติต่อ หน.นขต.บก.ทท. เป็นลายลักษณ์อักษรให้แล้วเสร็จภายใน ๙๐ วัน นับตั้งแต่นโยบายฉบับนี้มีผลบังคับใช้ พร้อมทั้งส่งสำเนาของแผนดังกล่าวให้ ศซบ.ทหาร ทราบโดยเร็ว โดยแผนดังกล่าวอย่างน้อยจะต้องมีลักษณะดังนี้

/๑.๒.๑๒.๑ (๑.๑) สอดคล้อง...

๑.๒.๑๒.๑ (๑.๑) สอดคล้องกับสถาปัตยกรรมองค์กร (ถ้ามี)

๑.๒.๑๒.๑ (๑.๒) สอดคล้องกับนโยบายฉบับนี้

๑.๒.๑๒.๑ (๑.๓) กำหนดผู้รับผิดชอบที่ชัดเจน

๑.๒.๑๒.๑ (๑.๔) กำหนดห้วงเวลาในการดำเนินการ

๑.๒.๑๒.๑ (๑.๕) กำหนดวิธีการในการรายงานผล

๑.๒.๑๒.๑ (๑.๖) กำหนดขอบเขตของระบบสารสนเทศ

๑.๒.๑๒.๑ (๑.๗) กำหนดประเภทของความมั่นคงปลอดภัย

๑.๒.๑๒.๑ (๑.๘) ระบุประเภทของภัยคุกคามทางไซเบอร์

๑.๒.๑๒.๑ (๑.๙) ระบุมาตรการควบคุมที่จะต้องดำเนินการ

๑.๒.๑๒.๑ (๒) นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. ทบทวน และปรับปรุง แผนรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วย อย่างน้อย ๑ ครั้ง/ปี

๑.๒.๑๒.๒ การกำหนดมาตรการควบคุม (PL-2 Baseline Selection)

๑.๒.๑๒.๒ (๑) นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. กำหนดมาตรการควบคุมที่จะต้องดำเนินการ ตามตารางข้อ ๑.๒

๑.๒.๑๒.๒ (๒) ศชบ.ทหาร กำหนดรูปแบบ (Template) ในการระบุมาตรการควบคุมของ นขต.บก.ทท. เพื่อให้ นขต.บก.ทท. สามารถดำเนินการตามมาตรการควบคุมได้อย่างเหมาะสม

๑.๒.๑๓ การรักษาความปลอดภัยบุคคล (Personnel Security : PS)

๑.๒.๑๓.๑ การตรวจสอบประวัติบุคคล (PS-1 Personnel Screening) ให้ นขต.บก.ทท. ตรวจสอบประวัติของกำลังพลที่จะปฏิบัติงานกับระบบสารสนเทศของหน่วย ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ รวมถึงระเบียบอื่นที่เกี่ยวข้อง

๑.๒.๑๓.๒ การเปลี่ยนตำแหน่ง หรือพ้นจากการปฏิบัติงาน (PS-2 Personnel Termination and Transfer) ภายหลังจากกำลังพลมีการเปลี่ยนตำแหน่งหรือพ้นจากการปฏิบัติงานกับระบบสารสนเทศของ นขต.บก.ทท. ให้ดำเนินการยกเลิกสิทธิ์การเข้าถึงระบบดังกล่าวโดยทันที

๑.๒.๑๔ การประเมินความเสี่ยง (Risk Assessment : RA)

๑.๒.๑๔.๑ การประเมินความเสี่ยงด้านไซเบอร์ (RA-1 Cybersecurity Risk Assessment)

๑.๒.๑๔.๑ (๑) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท. รายงานผลการประเมินความเสี่ยงด้านไซเบอร์ของหน่วยให้หัวหน้าหน่วยทราบ เป็นลายลักษณ์อักษร เพื่อพิจารณาอนุมัติแนวทางการบริหารความเสี่ยงด้านไซเบอร์ ตามระดับความเสี่ยงที่ยอมรับได้ต่อไป รวมทั้งจะต้องส่งสำเนารายงานผลการประเมินความเสี่ยงดังกล่าวให้ ศชบ.ทหาร ทุกไตรมาสที่ ๒ ของปีงบประมาณ ก่อน มี.ค. ของทุกปี

/๑.๒.๑๔.๑ (๒) ศชบ.ทหาร...

๑.๒.๑๔.๑ (๒) ศชบ.ทหาร รายงานผลการประเมินความเสี่ยงด้านไซเบอร์ บก.ทท. ถึง ผบ.ทสส. ในฐานะผู้รับผิดชอบสูงสุดต่อความเสี่ยงด้านไซเบอร์ของ บก.ทท. เพื่อพิจารณาอนุมัติแนวทางการบริหารความเสี่ยงด้านไซเบอร์ ตามระดับความเสี่ยงที่ยอมรับได้ต่อไป

๑.๒.๑๔.๑ (๓) ศชบ.ทหาร จัดทำแบบฟอร์มสำหรับ นขต.บก.ทท. เพื่อใช้ในการประเมินความเสี่ยงด้านไซเบอร์ของ นขต.บก.ทท. โดยให้บรรจุแบบฟอร์มดังกล่าวไว้ในคู่มือการรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. พร้อมทั้งจัดให้มีการฝึกอบรมเพื่อให้สามารถใช้งานแบบฟอร์มดังกล่าวได้อย่างถูกต้อง

๑.๒.๑๔.๒ การบริหารความเสี่ยงด้านไซเบอร์ (RA-2 Cybersecurity Risk Management)

๑.๒.๑๔.๒ (๑) ภายหลังจากผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท. รายงานผลการประเมินความเสี่ยงด้านไซเบอร์ของหน่วยให้หัวหน้าหน่วยทราบเป็นลายลักษณ์อักษร ให้ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท. จัดทำแผนการบริหารความเสี่ยงด้านไซเบอร์ ตามแบบฟอร์มที่ ศชบ.ทหาร กำหนด ขออนุมัติต่อหัวหน้าหน่วยเพื่อดำเนินการให้สอดคล้องกับรายงานผลการประเมินความเสี่ยงด้านไซเบอร์ของหน่วย โดยจะต้องมีการบันทึกผลการปฏิบัติเป็นลายลักษณ์อักษร

๑.๒.๑๔.๒ (๒) ศชบ.ทหาร จัดทำแบบฟอร์มสำหรับ นขต.บก.ทท. เพื่อใช้ในการจัดทำแผนการบริหารความเสี่ยงด้านไซเบอร์ของหน่วย โดยให้บรรจุแบบฟอร์มดังกล่าวไว้ในคู่มือการรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. พร้อมทั้งจัดให้มีการฝึกอบรมเพื่อให้สามารถใช้งานแบบฟอร์มดังกล่าวได้อย่างถูกต้อง

๑.๒.๑๕ การจัดหาระบบและบริการ (Systems and Services Acquisition : SA)

๑.๒.๑๕.๑ กระบวนการจัดหา (SA-1 Acquisition Process)

๑.๒.๑๕.๑ (๑) สส.ทหาร เป็นหน่วยรับผิดชอบหลักในการจัดหาระบบและบริการระบบสารสนเทศของ บก.ทท. โดยการพิจารณาคุณลักษณะเฉพาะสิ่งอุปกรณ์ชั่วคราวสายสื่อสารให้กับ นขต.บก.ทท. ซึ่งจะต้องคำนึงถึงคุณภาพ ประสิทธิภาพ ความคุ้มค่า และความถูกต้องของลิขสิทธิ์

๑.๒.๑๕.๑ (๒) ศชบ.ทหาร เป็นหน่วยรับผิดชอบหลักในการจัดหาระบบและบริการระบบสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. โดยการพิจารณาคุณลักษณะเฉพาะสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ให้กับ นขต.บก.ทท. ซึ่งจะต้องคำนึงถึงความมั่นคงปลอดภัยไซเบอร์ของสิ่งอุปกรณ์ดังกล่าว

๑.๒.๑๕.๑ (๓) ในห้วงของการจัดทำรายการความต้องการสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ให้นายทหารรักษาความมั่งคงปลอดภัยไซเบอร์ นขต.บก.ทท. ทบทวนรายละเอียดของสิ่งอุปกรณ์หรือระบบสารสนเทศของหน่วย ในประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมส่งผลการทบทวนให้ สส.ทหาร หรือ ศชบ.ทหาร ซึ่งมีหน้าที่พิจารณาความเหมาะสมของรายการความต้องการดังกล่าว โดยมีรูปแบบตามตัวอย่าง ดังนี้

/สิ่งอุปกรณ์...

สิ่งอุปกรณ์	ตัวอย่างรายละเอียด	ตัวอย่างประเด็นฯ	ข้อเสนอแนะ
เครื่องคอมพิวเตอร์ เครื่องแม่ข่าย หรือโน้ตบุ๊ก	Windows 10	CVE-2019-1384 CVE-2019-0721 CVE-2019-0719 CVE-2019-1365	Windows 10 มีความเหมาะสม ทั้งนี้ควรติดตั้งระบบปฏิบัติการ พร้อมอัพเดตด้านความปลอดภัย ให้เป็นเวอร์ชันล่าสุด
อุปกรณ์เครือข่าย	Cisco SG200-26 L2 Switch	End of Sale End-of-Support Date: 31-MAY-2023	ควรเลือกเป็นรุ่นที่ใหม่กว่า และมีระยะสนับสนุนที่ยาวนานกว่า
ซอฟต์แวร์	Microsoft Office 2016	Supported by Microsoft until 2025	ควรเลือกเป็นรุ่นที่ใหม่กว่า และมีระยะสนับสนุนที่ยาวนานกว่า เช่น Microsoft Office 2019
โทรศัพท์มือถือ	Samsung Galaxy A7 ver.2018	Android 8.0	ควรเลือกเป็นรุ่นที่ใหม่กว่า เช่น Samsung Galaxy A30s ซึ่งใช้ระบบปฏิบัติการ Android 9.0 ที่มีความปลอดภัยมากกว่า
เว็บไซต์ หรือเว็บแอพลิเคชัน	Joomla! 2.5.28 AppServ 8.4.0	End of Support	ควรเลือกเป็นรุ่นที่ใหม่กว่า เช่น Joomla! 3.9.13, AppServ 9.3.0 ที่มีความปลอดภัยมากกว่า

๑.๒.๑๕.๑ (๔) ในห้วงของการจัดทำรายการความต้องการสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ให้ นขต.บก.ทท. พิจารณาบรรจุรายการผลิตภัณฑ์ซึ่งมีลิขสิทธิ์ถูกต้องตามกฎหมาย ให้ครอบคลุมทั้งฮาร์ดแวร์ และซอฟต์แวร์ ซึ่งจะต้องใช้งานจริงเพื่อลดปัญหาที่เกิดจากการติดตั้งใช้งานผลิตภัณฑ์ละเมิดลิขสิทธิ์ภายหลังการจัดหาแล้วเสร็จ

๑.๒.๑๕.๑ (๕) สส.ทหาร และ ศชบ.ทหาร ซึ่งมีหน้าที่พิจารณาความเหมาะสมของรายการความต้องการสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ให้ นขต.บก.ทท. พิจารณาถึงประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ในหัวข้อต่อไปนี้เป็นอย่างน้อย

๑.๒.๑๕.๑ (๕.๑) เวอร์ชันของระบบปฏิบัติการ ซอฟต์แวร์หรือเฟิร์มแวร์

๑.๒.๑๕.๑ (๕.๒) ระยะเวลายุติการสนับสนุนผลิตภัณฑ์

๑.๒.๑๕.๑ (๕.๓) ช่องโหว่ของผลิตภัณฑ์

๑.๒.๑๕.๑ (๕.๔) การควบคุมการเข้าถึง (Access Control)

๑.๒.๑๕.๑ (๕.๕) การเข้ารหัส (Encryption)

๑.๒.๑๕.๑ (๕.๖) ความเข้ากันได้กับระบบที่มีอยู่เดิม (Interoperability)

/๑.๒.๑๕.๑ (๖) ในขั้นตอน...

๑.๒.๑๕.๑ (๖) ในขั้นตอนของการทำสัญญาซื้อขาย ให้ นขต.บก.ทท. ที่เป็นหน่วยรับผิดชอบในการร่างสัญญา รวมถึงการร่างข้อกำหนดความต้องการทั่วไปในการซื้อสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) จะต้องมีการกำหนดให้ผู้ขาย หรือผู้รับจ้างดำเนินการต่อไปนี้เป็นอย่างน้อย

๑.๒.๑๕.๑ (๖.๑) ภายหลังการติดตั้ง จะต้องดำเนินการปรับปรุงรุ่นของระบบปฏิบัติการ (Operating System) หรือเฟิร์มแวร์ (Firmware) หรือซอฟต์แวร์ (Software) หรือชุดคำสั่งด้านความปลอดภัย (Security Patch) ให้เป็นเวอร์ชันล่าสุดตามมาตรฐานที่ทางผู้ผลิตกำหนด

๑.๒.๑๕.๑ (๖.๒) ภายหลังการติดตั้งจะต้องดำเนินการตั้งค่าการใช้งานสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ให้มีความมั่นคงปลอดภัย โดยให้เป็นไปตามนโยบายฉบับนี้

๑.๒.๑๕.๑ (๖.๓) จัดให้มีการอบรมการใช้งานสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) อย่างมั่นคงปลอดภัย

๑.๒.๑๕.๑ (๖.๔) กรณีเป็นการจัดหาระบบสารสนเทศซึ่งมีลักษณะเป็น Web Application หรือ Mobile Application จะต้องกำหนดให้มีการทดสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐาน OWASP Top 10 เวอร์ชันปัจจุบัน

๑.๒.๑๕.๑ (๗) นขต.บก.ทท. จะต้องกำกับดูแลให้ผู้ขาย หรือผู้รับจ้างดำเนินการตามสัญญาซื้อขายสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์)

๑.๒.๑๕.๑ (๘) นขต.บก.ทท. จะต้องจัดให้มีนายทหารรักษาความปลอดภัยไซเบอร์ นขต.บก.ทท. เข้าร่วมในขั้นตอนของการตรวจรับสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) เพื่อให้ความเห็นเกี่ยวกับการปฏิบัติของผู้ขาย หรือผู้รับจ้างที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๒.๑๕.๑ (๙) นขต.บก.ทท. จะต้องจัดให้นายทหารรักษาความปลอดภัยไซเบอร์ นขต.บก.ทท. หรือผู้ดูแลระบบ หรือผู้ใช้สิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) เข้าร่วมการอบรมการใช้งานสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ให้มีความมั่นคงปลอดภัยตามที่ระบุไว้ในสัญญาซื้อขาย

๑.๒.๑๕.๑ (๑๐) ในกรณีที่มีการเปลี่ยนแปลงผู้ทำหน้าที่นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. ให้ นขต.บก.ทท. จัดให้มีการถ่ายทอดความรู้เกี่ยวกับการใช้งานสิ่งอุปกรณ์ชั่วคราวสายสื่อสาร หรือสายสื่อสาร (ความมั่นคงปลอดภัยไซเบอร์) ให้มีความมั่นคงปลอดภัยด้วย

๑.๒.๑๕.๒ บริการระบบสารสนเทศจากหน่วยงานภายนอก (SA-2 External Information System Services)

๑.๒.๑๕.๒ (๑) นขต.บก.ทท. ซึ่งมีการใช้บริการระบบสารสนเทศจากหน่วยงานภายนอก จะต้องแจ้งให้หน่วยงานดังกล่าวทราบและปฏิบัติตามนโยบายฉบับนี้ พร้อมบันทึกหลักฐานเป็นลายลักษณ์อักษร

/๑.๒.๑๕.๒ (๒) นขต.บก.ทท. ...

๑.๒.๑๕.๒ (๒) นขต.บก.ทท. จะต้องจัดให้มีผู้รับผิดชอบในการทำงานร่วมกับบริการระบบสารสนเทศจากหน่วยงานภายนอก โดยจะต้องกำหนดบทบาท หน้าที่ ความรับผิดชอบให้ชัดเจน

๑.๒.๑๕.๒ (๓) ผู้รับผิดชอบตามข้อ ๒.๒.๑๕.๒ (๒) จะต้องติดตามการปฏิบัติงานของหน่วยงานดังกล่าวอย่างสม่ำเสมอ พร้อมบันทึกหลักฐานการติดตามเป็นลายลักษณ์อักษร

๑.๒.๑๕.๓ การประเมินความปลอดภัยของระบบก่อนเริ่มใช้งาน (SA-3 Developer Security Testing and Evaluation)

๑.๒.๑๕.๓ (๑) นขต.บก.ทท. ที่มีการพัฒนาระบบสารสนเทศขึ้นใช้งานใน บก.ทท. จะต้องมีการประเมินความปลอดภัยของระบบก่อนเริ่มใช้งาน โดย ศชบ.ทหาร และดำเนินการแก้ไขระบบดังกล่าวให้มีความมั่นคงปลอดภัยเพียงพอตามที่ ศชบ.ทหาร กำหนด

๑.๒.๑๕.๓ (๒) ระบบสารสนเทศตามข้อ ๒.๒.๑๕.๓ (๑) ซึ่งมีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" จะไม่สามารถเริ่มใช้งานระบบได้ หากไม่สามารถแก้ไขช่องโหว่ในระดับร้ายแรงได้ทั้งหมด ตามมาตรฐานดังต่อไปนี้

๑.๒.๑๕.๓ (๒.๑) กรณีเป็น Web Application จะต้องได้รับการประเมินโดยมาตรฐาน OWASP Top 10 : 2017 (for Web Application) หรือใหม่กว่า

๑.๒.๑๕.๓ (๒.๑) กรณีเป็น Mobile Application จะต้องได้รับการประเมินโดยมาตรฐาน OWASP Top 10 : 2016 (for Mobile) หรือใหม่กว่า

๑.๒.๑๕.๓ (๓) ในกรณีที่เป็นระบบสารสนเทศที่ได้มีการติดตั้งและใช้งานก่อนที่จะมีนโยบายฉบับนี้ และ ศชบ.ทหาร ตรวจพบว่าระบบสารสนเทศดังกล่าวมีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" แต่มิได้มีความมั่นคงปลอดภัยเพียงพอ หน่วยเจ้าของระบบดังกล่าวจะต้องดำเนินการแก้ไขให้แล้วเสร็จโดยเร็ว ทั้งนี้จะต้องไม่เกิน ๓๐ วัน นับตั้งแต่วันที่ได้รับแจ้งจาก ศชบ.ทหาร ให้ดำเนินการแก้ไข

๑.๒.๑๕.๓ (๔) ระบบสารสนเทศตามข้อ ๒.๒.๑๕.๓ (๒) - (๓) ซึ่งมีการเก็บข้อมูลที่มีชั้นความลับ "ลับมาก" ขึ้นไป หรือ มีการเก็บข้อมูลผู้ใช้งาน อันได้แก่ หมายเลขประจำตัวประชาชน หมายเลขประจำตัวข้าราชการ ยศ - ชื่อ - สกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล หรือข้อมูลอื่นใดที่สามารถระบุตัวบุคคลได้ หน่วยเจ้าของระบบดังกล่าวจะต้องดำเนินการให้มีการเข้ารหัสข้อมูลดังกล่าวอย่างเพียงพอ อย่างน้อยดังต่อไปนี้

๑.๒.๑๕.๓ (๔.๑) ข้อมูลที่มีการเก็บไว้บนเครื่องแม่ข่ายจะต้องมีการเข้ารหัสด้วย 128-bit Advanced Encryption Standard (AES) หรือ Hash Function ประเภท bcrypt เป็นอย่างน้อย

๑.๒.๑๕.๓ (๔.๒) การรับส่งข้อมูลระหว่างเครื่องแม่ข่ายและเครื่องปลายทาง จะต้องมีการเข้ารหัสด้วย Transport Layer Security (TLS) ตั้งแต่เวอร์ชัน ๑.๒ ขึ้นไป

๑.๒.๑๕.๔ การฝึกอบรมผู้พัฒนาระบบ (SA-4 Developer Security Architecture and Design) ให้ ศชบ.ทหาร จัดการฝึกอบรมเกี่ยวกับแนวทางการพัฒนาระบบสารสนเทศอย่างปลอดภัยให้กับผู้พัฒนาระบบของ บก.ทท. โดยคำนึงถึงระดับความเสี่ยงด้านไซเบอร์ที่มีต่อ บก.ทท.

/๑.๒.๑๖ การป้องกัน...

๑.๒.๑๖ การป้องกันระบบและการสื่อสาร (System and Communications Protection : SC)

๑.๒.๑๖.๑ การตัดการเชื่อมต่อ (SC-1 Network Disconnect and Isolation) ให้ สส.ทหาร รับผิดชอบเรื่องการตัดการเชื่อมต่อ โดยรับผิดชอบอุปกรณ์ดังต่อไปนี้

๑.๒.๑๖.๑ (๑) Core Switch

๑.๒.๑๖.๑ (๒) DMZ Switch

๑.๒.๑๖.๑ (๓) L3 Switch

๑.๒.๑๖.๒ การเชื่อมต่อสู่เครือข่ายสาธารณะ (SC-2 Public Access Protections) ให้ สส.ทหาร รับผิดชอบเรื่องการเชื่อมต่อสู่เครือข่ายสาธารณะ โดยรับผิดชอบอุปกรณ์ดังต่อไปนี้

๑.๒.๑๖.๒ (๑) Internet Switch

๑.๒.๑๖.๒ (๒) Internet Access Management

๑.๒.๑๖.๒ (๓) DDoS Protection

๑.๒.๑๖.๓ การบริหารกุญแจ (SC-3 Cryptographic Key Management and Protection) ให้ สส.ทหาร รับผิดชอบเรื่องการบริหารกุญแจ โดยรับผิดชอบอุปกรณ์ดังต่อไปนี้

๑.๒.๑๖.๓ (๑) Public Key Infrastructure (PKI)

๑.๒.๑๖.๓ (๒) Key Management System

๑.๒.๑๖.๔ การปกป้องเครือข่าย (SC-4 Network Protection) ให้ ศชบ.ทหาร รับผิดชอบเรื่องการปกป้องเครือข่าย โดยรับผิดชอบอุปกรณ์ดังต่อไปนี้

๑.๒.๑๖.๔ (๑) Firewall

๑.๒.๑๖.๔ (๒) IDS

๑.๒.๑๖.๔ (๓) IPS

๑.๒.๑๖.๕ การปกป้องเครื่องแม่ข่าย (SC-5 Server Protection) ให้ ศชบ.ทหาร รับผิดชอบเรื่องการปกป้องเครื่องแม่ข่าย โดยรับผิดชอบอุปกรณ์ดังต่อไปนี้

๑.๒.๑๖.๕ (๑) Web Application Firewall

๑.๒.๑๖.๕ (๒) Antivirus Gateway

๑.๒.๑๖.๖ การปกป้องผู้ใช้งาน (SC-6 Endpoint Protection) ให้ ศชบ.ทหาร รับผิดชอบเรื่องการปกป้องผู้ใช้งาน โดยรับผิดชอบอุปกรณ์ดังต่อไปนี้

๑.๒.๑๖.๖ (๑) Antivirus Endpoint Security

๑.๒.๑๖.๖ (๒) Host-based IDS (TPS)

๑.๒.๑๗ ความถูกต้องครบถ้วนของระบบและสารสนเทศ (System and Information Integrity : SI)

๑.๒.๑๗.๑ การตรวจสอบข้อมูลก่อนนำเข้าระบบ (SI-1 Information Input Validation) ให้ สส.ทหาร รับผิดชอบในเรื่องการตรวจสอบข้อมูลก่อนนำเข้าระบบ โดยดำเนินการ บูรณาการ ด้านการพัฒนาระบบสารสนเทศของ บก.ทท. เพื่อให้มีการตรวจสอบข้อมูลของผู้ใช้งานก่อนที่จะนำเข้าสู่ระบบสารสนเทศและประมวลผล อย่างน้อยประกอบด้วย

/๑.๒.๑๗.๑ (๑) ในขั้นตอน...

๑.๒.๑๗.๑ (๑) ในขั้นตอนการออกแบบ ให้ผู้พัฒนาระบบตั้งสมมติฐานไว้เสมอว่าผู้ใช้งานจะมีการนำเข้าข้อมูลที่ไม่ประสงค์ดี (Malicious Data Input)

๑.๒.๑๗.๑ (๒) พัฒนาระบบโดยอาศัยหลักการรวมศูนย์ (Centralized Approach)

๑.๒.๑๗.๑ (๓) หลีกเลี่ยงการเชื่อถือข้อมูลที่ตรวจสอบการนำเข้าจากฝั่งผู้ใช้งาน (Client-side Validation)

๑.๒.๑๗.๑ (๔) ระมัดระวังการอนุญาตให้ผู้ใช้สามารถกำหนดชื่อไฟล์ (File Name) หรือตำแหน่งที่อยู่ (Address) โดยมิได้มีการควบคุมรูปแบบ (Format) หรือตรวจสอบสิทธิ์อย่างเหมาะสม

๑.๒.๑๗.๑ (๕) กำหนดรูปแบบของข้อมูลที่อนุญาตให้นำเข้า (Valid Types, Patterns, and Ranges Constrains) และไม่อนุญาตให้นำเข้า (Reject) พร้อมทั้งพัฒนาระบบให้มีการจัดการข้อมูลดังกล่าว (Sanitize) อย่างมั่นคงปลอดภัย

๑.๒.๑๗.๑ (๖) พัฒนาระบบโดยให้มีการเข้ารหัสคุกกี้ซึ่งอาจมีข้อมูลสำคัญของผู้ใช้ (Sensitive Cookie State)

๑.๒.๑๗.๑ (๗) ต้องมีการตรวจสอบยืนยันข้อมูลที่นำเข้าจากฝั่งผู้ใช้งานเสมอ

๑.๒.๑๗.๒ ความถูกต้องครบถ้วนของซอฟต์แวร์ เฟิร์มแวร์ และข้อมูล (SI-2 Software, Firmware, and Information Integrity) สส.ทหาร รับผิดชอบในเรื่องความถูกต้องครบถ้วนของซอฟต์แวร์ เฟิร์มแวร์ และข้อมูล โดยดำเนินการ บูรณาการ และให้บริการ อย่างน้อยประกอบด้วย

๑.๒.๑๗.๒ (๑) การตรวจสอบความถูกต้องครบถ้วน (Integrity Checks) ของระบบปฏิบัติการ (Operating System) ซอฟต์แวร์ (Software) เฟิร์มแวร์ (Firmware) หรือไบออส (BIOS)

๑.๒.๑๗.๒ (๒) การจัดทำรายการซอฟต์แวร์ที่อนุญาต (White Listing) และไม่อนุญาต (Black Listing) ให้ติดตั้งในระบบสารสนเทศของ บก.ทท.

๑.๒.๑๗.๒ (๓) จัดให้มีระบบบริหารความถูกต้องครบถ้วนของซอฟต์แวร์และเฟิร์มแวร์ จากส่วนกลาง (Centralized Integrity System)

๑.๒.๑๗.๒ (๔) จัดให้มีการปกป้องความถูกต้องครบถ้วนของซอฟต์แวร์และเฟิร์มแวร์ โดยการเข้ารหัสอย่างเหมาะสม (Cryptographic Protection)

๑.๒.๑๗.๓ การป้องกันชุดคำสั่งที่ไม่ประสงค์ดี (SI-3 Malicious Code Protection) ศชบ.ทหาร รับผิดชอบในเรื่องการป้องกันชุดคำสั่งที่ไม่ประสงค์ดี โดยดำเนินการ และบูรณาการ อย่างน้อยประกอบด้วย

๑.๒.๑๗.๓ (๑) จัดให้มีโปรแกรมป้องกันมัลแวร์ (Antivirus/Malware Protection) และโปรแกรมตรวจจับมัลแวร์ (Host-based Threat Protection System) เพื่อปกป้องเครื่องคอมพิวเตอร์ของ บก.ทท.

๑.๒.๑๗.๓ (๒) จัดให้มีระบบป้องกันมัลแวร์จากส่วนกลาง สำหรับระบบสารสนเทศของ บก.ทท. (Centralized Malware Protection System)

/๑.๒.๑๗.๓ (๓) จัดให้มี...

๑.๒.๑๗.๓ (๓) จัดให้มีการอบรมผู้ใช้งานที่เกี่ยวข้องกับการติดตั้งและใช้งานโปรแกรมป้องกันมัลแวร์ (Antivirus/Malware Protection) และโปรแกรมตรวจจับมัลแวร์ (Host-based Threat Protection System)

๑.๒.๑๗.๔ การเฝ้าระวังและตรวจจับ (SI-4 Information System Monitoring) ให้ ศชบ.ทหาร รับผิดชอบในเรื่องการเฝ้าระวังและตรวจจับเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท. โดยดำเนินการ และบูรณาการ อย่างน้อยประกอบด้วย

๑.๒.๑๗.๔ (๑) จัดให้มีระบบเฝ้าระวังและตรวจจับเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท.

๑.๒.๑๗.๔ (๒) จัดให้มีเจ้าหน้าที่เฝ้าระวังและตรวจจับเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท. ตลอด ๒๔ ชั่วโมง

๑.๒.๑๗.๔ (๓) จัดให้มีกระบวนการเฝ้าระวังและตรวจจับเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท. พร้อมทั้งรายงานผลการปฏิบัติให้ ผบ.ทสส. ทราบ อย่างน้อยสัปดาห์ละ ๑ ครั้ง โดยจะต้องระบุถึงความเสี่ยงด้านไซเบอร์ที่สำคัญ รวมถึงผลการปฏิบัติเพื่อรับมือและแก้ไขปัญหาดังกล่าว

๑.๒.๑๗.๕ การแจ้งเตือนและให้ข้อเสนอแนะ (SI-5 Security Alerts, Advisories, and Directives) ศชบ.ทหาร รับผิดชอบในเรื่องการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท. และให้ข้อเสนอแนะเพื่อแก้ไขเหตุการณ์ดังกล่าว โดยดำเนินการ และบูรณาการ อย่างน้อยประกอบด้วย

๑.๒.๑๗.๕ (๑) จัดให้มีระบบรับมือและแก้ไขปัญหาจากเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท.

๑.๒.๑๗.๕ (๒) จัดให้มีเจ้าหน้าที่รับมือและแก้ไขปัญหาจากเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท. ตลอด ๒๔ ชั่วโมง

๑.๒.๑๗.๕ (๓) จัดให้มีกระบวนการรับมือและแก้ไขปัญหาจากเหตุการณ์ทางไซเบอร์ที่มีต่อระบบสารสนเทศของ บก.ทท. ซึ่งจะต้องมีขีดความสามารถในการแจ้งเตือน นขต.บก.ทท. เกี่ยวกับภัยคุกคามทางไซเบอร์ และให้ข้อเสนอแนะเพื่อแก้ไขเหตุการณ์ดังกล่าว

๑.๒.๑๗.๖ การป้องกันสแปม (SI-6 Spam Protection) ศชบ.ทหาร รับผิดชอบในเรื่องการป้องกันสแปมของ บก.ทท. อย่างน้อยประกอบด้วย

๑.๒.๑๗.๖ (๑) จัดให้มีระบบป้องกันสแปมของ บก.ทท. ทั้งในส่วนการจราจรทางคอมพิวเตอร์ขาเข้าและขาออก เพื่อติดตาม ระงับ ยับยั้ง การจราจรทางคอมพิวเตอร์ที่มีลักษณะเป็นสแปม

๑.๒.๑๗.๖ (๒) ปรับปรุงระบบป้องกันสแปมตามข้อ ๑.๒.๑๗.๖ (๑) อย่างสม่ำเสมอ

๑.๓ การวางมาตรการควบคุม (Implementing Controls) ประกอบด้วย ขั้นตอนในการดำเนินการทั้งสิ้น ๓ ขั้นตอน ได้แก่ ขั้นเตรียมการ (Prepare) ขั้นดำเนินการ (Implement) และขั้นรายงานผล (Report) โดยมีรายละเอียดดังนี้

/๑.๓.๑ ขั้นเตรียมการ...

๑.๓.๑ ขั้นเตรียมการ (Prepare) ให้ นขต.บก.ทท. รวบรวมข้อมูลที่จำเป็น และมีความเป็นปัจจุบัน ดังนี้

๑.๓.๑.๑ คำสั่งแต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท. และนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท.

๑.๓.๑.๒ รายงานผลการประเมินความเสี่ยงด้านไซเบอร์ของ นขต.บก.ทท. (Risk Assessment)

๑.๓.๑.๓ รายงานผลการดำเนินการเพื่อบริหารความเสี่ยงด้านไซเบอร์ของ นขต.บก.ทท. (Risk Mitigation)

๑.๓.๑.๔ รายงานผลการจัดประเภทของความมั่นคงปลอดภัย (Security Categorization) ของ นขต.บก.ทท.

๑.๓.๑.๕ รายงานผลการกำหนดมาตรการควบคุม (Control Selecting) ของ นขต.บก.ทท.

๑.๓.๒ ขั้นดำเนินการ (Implement) ให้ นขต.บก.ทท. ดำเนินการดังนี้

๑.๓.๒.๑ จัดทำแผนการวางมาตรการควบคุม (Information System Security Plan)

๑.๓.๒.๒ ขออนุมัติแผนการวางมาตรการควบคุมตามข้อ ๑.๓.๒.๑ ถึง หน.นขต.บก.ทท.

๑.๓.๒.๓ ดำเนินการตามแผนในข้อ ๑.๓.๒.๒

๑.๓.๓ ขั้นรายงานผล (Report) ให้ นขต.บก.ทท. ดำเนินการดังนี้

๑.๓.๓.๑ รายงานผลการดำเนินการถึง หน.นขต.บก.ทท.

๑.๓.๓.๒ สำเนารายงานผลการดำเนินการตามข้อ ๑.๓.๓.๑ ให้ ศชบ.ทหาร ทราบ อย่างน้อย ๑ ครั้ง/ปี ไม่เกิน ก.ย. ของทุกปี

๑.๓.๔ ศชบ.ทหาร จัดทำขั้นตอนโดยละเอียดสำหรับข้อ ๑.๓.๑ - ๑.๓.๓ พร้อมทั้งบรรจุไว้ในคู่มือการรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. รวมทั้งจะต้องจัดให้มีการฝึกอบรมสำหรับนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. เพื่อให้มีความรู้ความเข้าใจเกี่ยวกับขั้นตอนการปฏิบัติดังกล่าวด้วย

๑.๔ การตรวจประเมินด้านความมั่นคงปลอดภัย (Security Assessment) ประกอบด้วย

๑.๔.๑ การประเมินตนเองทางไซเบอร์ นขต.บก.ทท. (Self-Assessment Report : SAR) ดังนี้

๑.๔.๑.๑ นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. จัดทำแผนการประเมินตนเองทางไซเบอร์ของหน่วยเสนอ หน.นขต.บก.ทท. (ผ่านผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท.) เพื่ออนุมัติ ทั้งนี้ ให้เป็นไปตามแบบฟอร์มที่ ศชบ.ทหาร กำหนด

๑.๔.๑.๒ นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. รายงานผลการประเมินตนเองทางไซเบอร์ของหน่วยเสนอ หน.นขต.บก.ทท. (ผ่านผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท.) พร้อมข้อเสนอแนะเพื่อดำเนินการแก้ไข

๑.๔.๒ การตรวจประเมินมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ บก.ทท. (Cybersecurity Auditing) ศชบ.ทหาร ดำเนินการดังนี้

๑.๔.๒.๑ จัดทำแผนการตรวจประเมินมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. โดยจัดทำเป็นแผนประจำปี ซึ่งพิจารณาจากระดับความสำคัญของระบบสารสนเทศของ บก.ทท. ที่มีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" เป็นลำดับแรก หรือตามสั่งการของผู้บังคับบัญชา พร้อมขออนุมัติแผนดังกล่าวถึง รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท.

/๑.๔.๒.๒ รายงาน...

๑.๔.๒.๒ รายงานผลการตรวจประเมินด้านความมั่นคงปลอดภัยไซเบอร์ของ บก.ทท. เสนอ ผบ.ทสส. (ผ่าน รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท.) พร้อมข้อเสนอแนะเพื่อดำเนินการแก้ไข

๑.๔.๓ การประเมินช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ บก.ทท. (Penetration Testing) ศชบ.ทหาร ดำเนินการดังนี้

๑.๕.๓.๑ ประเมินช่องโหว่ให้กับระบบสารสนเทศของ บก.ทท. โดยพิจารณาจากระดับความสำคัญของระบบสารสนเทศของ บก.ทท. ซึ่งมีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" เป็นลำดับแรก หรือตามสั่งการของผู้บังคับบัญชา

๑.๕.๓.๒ จัดทำแผนการทดสอบเจาะระบบของ บก.ทท. โดยจัดทำเป็นแผนประจำปี ซึ่งพิจารณาจากระดับความสำคัญของระบบสารสนเทศของ บก.ทท. ที่มีประเภทของความมั่นคงปลอดภัย "ระดับเคร่งครัด" เป็นลำดับแรก หรือตามสั่งการของผู้บังคับบัญชา พร้อมขออนุมัติแผนดังกล่าวถึง รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท.

๑.๔.๓.๓ รายงานผลการทดสอบเจาะระบบของ บก.ทท. เสนอ ผบ.ทสส. (ผ่าน รอง เสธ.ทหาร/ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง บก.ทท.) พร้อมข้อเสนอแนะเพื่อดำเนินการแก้ไข

๑.๕ การดำเนินการแก้ไข (Authorization) นขต.บก.ทท. ดำเนินการดังนี้

๑.๕.๑ ภายหลังรับทราบรายงานผลการประเมินตนเองทางไซเบอร์ของหน่วย ให้นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. จัดทำแผนการแก้ไขข้อตรวจพบ (ถ้ามี) ตามแบบฟอร์มที่ ศชบ.ทหาร กำหนด เสนอ หน.นขต.บก.ทท. (ผ่านผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท.) เพื่ออนุมัติและดำเนินการแก้ไข ภายในระยะที่กำหนดต่อไป

๑.๕.๒ ภายหลังรับทราบสำเนาหนังสือที่ ผบ.ทสส. รับทราบรายงานผลการตรวจประเมินมาตรฐานและการทดสอบเจาะระบบของ บก.ทท. ให้นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. จัดทำแผนการแก้ไขข้อตรวจพบ (ถ้ามี) ตามแบบฟอร์มที่ ศชบ.ทหาร กำหนด เสนอ หน.นขต.บก.ทท. (ผ่านผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท.) เพื่ออนุมัติและดำเนินการแก้ไข ภายในระยะที่กำหนดต่อไป

๑.๖ การเฝ้าระวังและติดตาม (Monitoring Controls) ศชบ.ทหาร ดำเนินการดังนี้

๑.๖.๑ ทบทวนแนวทางการดำเนินการด้านไซเบอร์ของ บก.ทท. ดังต่อไปนี้ อย่างน้อย ๑ ครั้ง/ปี ประกอบไปด้วย

๑.๖.๑.๑ แผนการตรวจประเมินมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

๑.๖.๑.๒ แผนการทดสอบเจาะระบบ

๑.๖.๑.๓ คู่มือการรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท.

๑.๖.๒ ทบทวนแนวทางการดำเนินการด้านไซเบอร์ของ บก.ทท. ดังต่อไปนี้ อย่างน้อยทุก ๒ ปี

๑.๖.๒.๑ ข้อตกลงในการปฏิบัติงานร่วมกัน (Operational Level Agreement : OLA) ระหว่าง ศชบ.ทหาร และ สส.ทหาร

/๑.๖.๒.๒ แนวปฏิบัติ...

๑.๖.๒.๒ แนวปฏิบัติในการแบ่งประเภทสินทรัพย์ (Asset Categorization)

๑.๖.๒.๓ แนวปฏิบัติในการกำหนดมาตรการควบคุม (Selecting Controls)

๑.๖.๓ ทบทวนสถาปัตยกรรมด้านความมั่นคงปลอดภัยไซเบอร์ บก.ทท. (Cybersecurity Enterprise Architecture) อย่างน้อยทุก ๓ ปี

ส่วนที่ ๒ แนวปฏิบัติเฉพาะ (Specific Guideline) ประกอบด้วย

๒.๑ การปกป้องผู้ใช้งานของ บก.ทท. จากภัยคุกคามทางไซเบอร์

๒.๑.๑ นขต.บก.ทท. ติดตั้งโปรแกรมป้องกันไวรัส หรือโปรแกรมเพื่อปกป้องเครื่องผู้ใช้ของ นขต.บก.ทท. (Endpoint Security) ทั้งในส่วนเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ และโน้ตบุ๊ก ก่อนที่จะดำเนินการเชื่อมต่อเข้ากับระบบสารสนเทศเพื่อการจัดการ และระบบสารสนเทศเพื่อการควบคุมบังคับบัญชา ของ บก.ทท. พร้อมทั้งรายงานสถานภาพการติดตั้งโปรแกรมดังกล่าวให้ ศชบ.ทหาร ทราบ อย่างน้อยเดือนละ ๑ ครั้ง

๒.๑.๒ ในกรณีที่ตรวจพบอุปกรณ์ที่มิได้มีการติดตั้งโปรแกรมป้องกันไวรัส ตามที่ ศชบ.ทหาร กำหนด ให้ สส.ทหาร ดำเนินการตัดการเชื่อมต่ออุปกรณ์ดังกล่าวออกจากเครือข่ายภายใน ๓ วันทำการ นับตั้งแต่ได้รับการประสานจาก ศชบ.ทหาร

๒.๑.๓ ศชบ.ทหาร จัดหาโปรแกรมป้องกันไวรัส หรือโปรแกรมเพื่อปกป้องเครื่องผู้ใช้ของ นขต.บก.ทท. (Endpoint Security) ในภาพรวมของ บก.ทท. และจัดให้มีการอบรมเพื่อให้นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. สามารถติดตั้งใช้งานโปรแกรมดังกล่าวได้อย่างมีประสิทธิภาพ

๒.๒ การดำเนินการเพื่อรับมือเหตุการณ์ที่คาดว่าจะเป็นภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบสารสนเทศของ บก.ทท.

๒.๒.๑ ศชบ.ทหาร จัดทำแนวทางการรับมือเหตุการณ์ด้านไซเบอร์ร่วมกันระหว่าง นขต.บก.ทท. และ ศชบ.ทหาร พร้อมทั้งแจ้งให้ นขต.บก.ทท. ทราบ ในการประชุมคณะกรรมการความมั่นคงปลอดภัยไซเบอร์ บก.ทท. หรือเทียบเท่า อย่างน้อย ๑ ครั้ง/ปี

๒.๒.๒ นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. เป็นผู้รับผิดชอบหลักในการรับมือเหตุการณ์ด้านไซเบอร์ที่มีต่อ นขต.บก.ทท. ทั้งนี้ หากไม่สามารถรับมือเหตุการณ์ดังกล่าวได้จะต้องแจ้งให้ ศชบ.ทหาร (ผ่าน ศรช.ศบท.) โดยเร็ว

๒.๓ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล ให้ ศชบ.ทหาร ดำเนินการดังนี้

๒.๓.๑ เก็บรวบรวมพยานหลักฐานทางดิจิทัลของ นขต.บก.ทท. เท่าที่จำเป็น โดยจะต้องแจ้งให้ นขต.บก.ทท. ทราบ ผ่าน นายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท. หรือผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง นขต.บก.ทท. ก่อนที่จะนำพยานหลักฐานทางดิจิทัลของ นขต.บก.ทท. ออกมาได้

๒.๓.๒ เก็บรักษาพยานหลักฐานทางดิจิทัลของ นขต.บก.ทท. ไว้เป็นความลับ ดังนี้

๒.๓.๒.๑ เก็บพยานหลักฐานที่ได้รับจาก นขต.บก.ทท. โดยให้มีการปกปิดอย่างเหมาะสม และมีการบันทึกการดำเนินการเก็บพยานหลักฐานในทุกขั้นตอน

/๒.๓.๒.๒ ส่งต่อพยาน...

๒.๓.๒.๒ ส่งต่อพยานหลักฐานโดยคำนึงถึงหลักการของห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)

๒.๓.๒.๓ เก็บพยานหลักฐานไว้ในพื้นที่ซึ่ง ศชบ.ทหาร กำหนด ซึ่งจะต้องได้รับการปกป้องทั้งในเชิงกายภาพ และการเฝ้าระวังการปนเปื้อนอย่างต่อเนื่อง

๒.๓.๓ สถานที่และมาตรการในการเก็บและตรวจพิสูจน์พยานหลักฐานทางดิจิทัล จะต้องได้รับการรับรองความมีมาตรฐานสากล ได้แก่ มาตรฐาน ISO/IEC 17025 : 2017 หรือเทียบเท่า
