038 (3)

สำเนาคู่ฉบับ

ประกาศสำนักงานจเรทหาร

เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของสำนักงานจเรทหาร

พ.ศ.๒๕๖๒

---

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อให้ระบบสารสนเทศของสำนักงานจเรทหารมีความปลอดภัยน่าเชื่อถือ ลดความเสี่ยงด้านปัญหาอาชญากรรมคอมพิวเตอร์จากการใช้งานเทคโนโลยีสารสนเทศ ลดความเสียหายต่าง ๆ ที่เกิดจากเหตุละเมิดความมั่นคงปลอดภัย และรักษาไว้ซึ่งความสามารถในการปฏิบัติภารกิจได้อย่างต่อเนื่อง รวมทั้งสอดคล้องกับกฎหมาย และสอดคล้องกับระเบียบที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศและด้านการประกอบธุรกรรมทางอิเล็กทรอนิกส์ กองบัญชาการกองทัพไทย และมิให้ผู้กระทำด้วยประการใด ๆ ทำให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดเข้าล่วงรู้ข้อมูล แก้ไขหรือทำลายข้อมูลในระบบสารสนเทศโดยมิชอบหรือมีการเผยแพร่ข้อมูลเท็จ ลามก อนาจาร ซึ่งก่อให้เกิดความเสียหาย สำนักงานจเรทหารจึงกำหนดแนวนโยบายและแนวปฏิบัติไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานจเรทหาร เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงานจเรทหาร พ.ศ.๒๕๖๒"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ นิยามศัพท์ที่ใช้ในนโยบายฉบับนี้ประกอบด้วย

๓.๑ ระบบสารสนเทศ หมายความว่า ระบบจัดการข้อมูลที่นำเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสารมาสร้างสารสนเทศ เพื่อนำมาวางแผน บริหาร พัฒนาและควบคุม

๓.๑.๑ ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยต้องกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓.๑.๒ ระบบเครือข่าย หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร ทั้งในระบบ Intranet (อินทราเน็ต : ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เพื่อติดต่อสื่อสารภายใน) และ ระบบ Internet (อินเตอร์เน็ต : ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานกับเครือข่ายอินเตอร์เน็ตทั่วโลก)

๓.๑.๓ สารสนเทศ หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟิก ให้ผู้ใช้สามารถเข้าใจได้ง่าย

/๓.๒ คอมพิวเตอร์...

๓.๒ คอมพิวเตอร์ หมายความว่า เครื่องมือ หรืออุปกรณ์อิเล็กทรอนิกส์ที่มีความสามารถรับข้อมูลเข้าประมวลผลตามโปรแกรม และแสดง บันทึก ส่งออกข้อมูล ซึ่งเป็นผลที่ได้จากการประมวลผลนั้น อาจมีลักษณะเป็นคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา ตลอดจนคอมพิวเตอร์อื่น ๆ รวมถึง แท็ปเลต และสมาร์ทโฟน

๓.๓ พื้นที่ใช้งานระบบสารสนเทศ หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ หรือพื้นที่เตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งพื้นที่โต๊ะทำงานที่มีคอมพิวเตอร์ส่วนบุคคลติดตั้งประจำโต๊ะทำงาน

๓.๔ ผู้บังคับบัญชา หมายความว่า ผู้ที่มีอำนาจและหน้าที่ในการบังคับบัญชาหนวย

๓.๕ ผู้ใช้งาน หมายความว่า ข้าราชการ พนักงานราชการ และลูกจ้างของสำนักงานจเรทหาร รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของสำนักงานจเรทหารที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๖ ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบงานสารสนเทศ

๓.๗ ผู้ดูแลเครือข่าย หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบให้เป็นผู้ดูแลเครือข่ายสารสนเทศ

๓.๘ สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นที่เกียวข้องกับระบบสารสนเทศ หรือเพื่อการเข้าถึงเข้าใช้สารสนเทศและสินทรัพย์สารสนเทศ

๓.๙ สินทรัพย์ หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ และรวมถึงสิ่งใดก็ตามที่มีคุณค่าในระบบสารสนเทศ เป็นต้น

๓.๑๐ การเข้าถึงการใช้งานสารสนเทศ หมายความว่า ความสามารถในการเข้าไปอันอาจทำให้สามารถอ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใด ๆ สำหรับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ สารสนเทศ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์ และวิธีการทางกายภาพ

๓.๑๑ การควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกียวกับการเข้าถึงโดยมิชอบเอาไว้

๓.๑๒ รหัสผ่าน หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมลและระบบเทคโนโลยีสารสนเทศ

/ ๒ บททั่วไป...

ข้อ ๔ บททั่วไป

๔.๑ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศมีขอบเขตความควบคุมสารสนเทศที่ใช้ภายในสำนักงานจเรทหาร มีวัตถุประสงค์เพื่อ

๔.๑.๑ รักษาระบบความปลอดภัยระบบสารสนเทศ ป้องกันการบุกรุกและความเสียหายที่มีต่อข้อมูลในระบบสารสนเทศ ป้องกันทรัพย์สินจากความเสียหายที่อาจเกิดขึ้นได้

๔.๑.๒ ระบบสารสนเทศมีความพร้อมใช้งานอยู่เสมอ

๔.๑.๓ การควบคุมการจัดระบบสารสนเทศ ถูกต้องตามลำดับขั้นตอนความลับ มีการเก็บสำรองข้อมูลและสามารถกู้คืนระบบได้เมื่อระบบมีปัญหา

๔.๒ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ได้จัดทำขึ้นเป็นลายลักษณ์อักษรโดยได้รับอนุมัติจากจเรทหาร แล้วเผยแพร่ให้ข้าราชการ พนักงานราชการ และลูกจ้างที่เกี่ยวข้องทราบและปฏิบัติ

๔.๓ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ต้องทบทวนปรับปรุงให้ทันสมัย

ข้อ ๕ ความรับผิดชอบของผู้บริหาร

๕.๑ ผลักดันให้ข้าราชการ พนักงานราชการ ลูกจ้างในสังกัด ตระหนักถึงความสำคัญในการรักษาความปลอดภัยของข้อมูลในระบบสารสนเทศและปฏิบัติตามกฎหมายที่เกี่ยวข้อง

๕.๒ ทบทวนนโยบาย และปรับปรุงให้ทันสมัยสอดคล้องกับนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของกองบัญชาการกองทัพไทย ซึ่งมีแนวนโยบายสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และมาตรฐานความมั่นคงปลอดภัยสารสนเทศ

๕.๓ ให้มีการจัดหมวดหมู่สารสนเทศและทรัพย์สินสารสนเทศในรูปแบบบัญชีควบคุมสามารถตรวจสอบได้ มีการรักษาความปลอดภัยที่เหมาะสม

๕.๔ กำหนดเจ้าหน้าที่ดูแลความมั่นคงปลอดภัยระบบสารสนเทศของกองงานรับผิดชอบการเก็บสำรองข้อมลอย่างต่อเนื่อง และควบคุมการเข้าถึงระบบเครือข่ายสารสนเทศของหน่วย

ข้อ ๖ การให้บริการระบบสารสนเทศของหน่วยงานด้านกรรมวิธีข้อมูล

๖.๑ หน่วยงานด้านกรรมวิธีข้อมูล มีหน้าที่ดูแล ควบคุม บริการด้านระบบสารสนเทศให้สามารถใช้งานได้อย่างต่อเนื่องตามสิทธิ์การใช้งาน

๖.๒ จัดเก็บและประสานหน่วยงานที่เกี่ยวข้องในการให้บริการชื่อผู้ใช้ (User Name) และ รหัสผ่าน (Password) สำหรับการเข้าใช้งานระบบสารสนเทศ ระบบไปรษณีย์อิเล็กทรอนิกส์ (Mil – Mail) อีเมล์ของกองบัญชาการกองทัพไทย

๖.๓ บริการเชื่อมต่อผ่านสายสัญญาณเข้าสู่ระบบเครือข่ายคอมพิวเตอร์

๖.๔ บริการเชื่อมต่อแบบไร้สายเข้าสู่ระบบเครือข่ายคอมพิวเตอร์

๖.๕ บริการเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบสารสนเทศภายในหน่วย

/๖.๖ บริการ...

๖.๖ บริการเว็บไซต์สำนักงานจเรทหารบน Internet , Intranet

๖.๗ บริการโปรแกรมประยุกต์บนระบบปฏิบัติการ Windows

๖.๘ บริการสืบค้นข้อมลบนระบบเครือข่าย Internet , Intranet

๖.๙ บริการอื่น ๆ ที่ได้รับมอบหมาย

ข้อ ๗ ระบบความมั่นคงปลอดภัยของระบบสารสนเทศทางกายภาพและสิ่งแวดล้อม

๗.๑ วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงอาคารสถานที่และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งเป็นทรัพย์สินมีค่าและจำเป็นต้องรักษาความลับ มีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วย

๗.๒ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๗.๒.๑ ภายในหน่วยงาน การจำแนกและกำหนดพื้นที่ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยจัดทำเป็นเอกสาร เพื่อการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายที่อาจเกิดขึ้นได้

๗.๒.๒ ควรกำหนดและแบ่งแยกพื้นที่การใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน แบ่งได้เป็นพื้นที่ทั่วไป พื้นที่ทำงานของผู้ดูแลระบบ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ พื้นที่ใช้งานเครือข่ายไร้สาย เป็นต้น

ข้อ ๘ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๘.๑ กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๘.๑.๑ การควบคมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๘.๑.๒ ผู้ดูแลระบบ กำหนดสิทธิ์ในการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานและหน้าที่ของเจ้าหน้าที่ รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๘.๑.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๘.๑.๔ ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

/๘.๒ การควบคุม...

๘.๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๘.๒.๑ เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นจะนำไปสู่ความเสี่ยง

๘.๒.๒ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๘.๒.๓ จัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัย รวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์

๘.๒.๔ การจัดวางสายสัญญาณและสายไฟฟ้าควรมีการเก็บสายให้เรียบร้อย เช่น ชื่อผู้รับผิดชอบอุปกรณ์แต่ละชนิด

๘.๒.๕ ติดประกาศการบำรุงรักษาอุปกรณ์ เช่น ชื่อผู้รับผิดชอบอุปกรณ์แต่ละชนิด

๘.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน บัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

๘.๓.๑ กำหนดให้มีการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิ์ในการใช้งานตามความจำเป็น และมีการยกเลิกสิทธิ์การใช้งานเมื่อเปลี่ยนตำแหน่งหรือลาออก

๘.๓.๒ กำหนดสิทธิ์การเข้าใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ระบบไปรษณีย์อิเล็กทรอนิกส์ (Mil-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) โดยจัดทำเป็นลายลักษณ์อักษรและมีการทบทวนสิทธิ์อยู่เสมอ

๘.๓.๓ ผู้ดูแลระบบ จัดทำเอกสาร บริหารจัดการบัญชีรายชื่อผู้ใช้งาน (Account) และรหัสผ่านของเจ้าหน้าที่ โดยพิจารณาจากหน้าที่ที่ปฏิบัติงาน มีการควบคุมอย่างเข้มงวด กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา และมีการเปลี่ยนแปลงรหัสผ่านเมื่อหมดความจำเป็น

๘.๓.๔ กรณีต้องให้สิทธิพิเศษกับผู้ใช้งาน หมายถึงผู้ใช้งานที่มีสิทธิสูงสุด ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุม

๘.๔ การบริหารจัดการการเข้าถึงระบบเครือข่าย

๘.๔.๑ ผู้ดูแลระบบออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีการกำหนดกลุ่มผู้ใช้ และกลุ่มของระบบสารสนเทศเพื่อป้องกันการบุกรุกเค้อย่างเป็นระบบ

๘.๔.๒ ผู้ดูแลระบบมีวิธีจำกัดการใช้งานเพื่อควบคุมให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาต มีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

/๘.๔.๓ จัดทำ...

๘.๔.๓ จัดทำแผนผังระบบเครือข่าย ขอบเขตที่ตั้งอุปกรณ์และการปรับปรุงให้เป็นปัจจุบันเสมอ

๘.๔.๔ การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ด้านกรรมวิธีข้อมูลเท่านั้น

๘.๕ การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย (Server)

๘.๕.๑ กำหนดผู้รับผิดชอบดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการแก้ไขหรือเปลี่ยนแปลงค่าของโปรแกรมระบบ

๘.๕.๒ ดำเนินการติดตั้งปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ

๘.๕.๓ การติดตั้งและเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย (Server) ดำเนินการโดยเจ้าหน้าที่ด้านกรรมวิธีข้อมลเท่านั้น

๘.๖ การใช้งานเครื่องคอมพิวเตอร์สำนักงาน

๘.๖.๑ เพื่อให้ผู้ใช้งานทราบหน้าที่และความรับผิดชอบในการใช้งานคอมพิวเตอร์ของหน่วยงาน โดยทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลให้มีความลับ ความถูกต้อง พร้อมใช้งานเสมอ

๘.๖.๒ ผู้ใช้งานเครื่องคอมพิวเตอร์หน่วยงานเพื่องานของหน่วย ไม่อนุญาตให้ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

๘.๖.๓ การเคลื่อนย้าย ส่งซ่อมเครื่องคอมพิวเตอร์ ผู้ใช้งานต้องแจ้งให้หน้าที่ด้านกรรมวิธีข้อมูลทราบ

๘.๖.๔ การตรวจสอบไวรัส ทุกครั้งที่มีการใช้งานเครื่องคอมพิวเตอร์

๘.๖.๕ ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์หน่วยงาน

๘.๖.๖ ผู้ใช้งานประจำเครื่องคอมพิวเตอร์ของหน่วยปฏิบัติ ดังนี้

๘.๖.๖.๑ ไม่นำอาหาร เครื่องดื่ม ใกล้บริเวณเครื่องคอมพิวเตอร์

๘.๖.๖.๒ ไม่วางสื่อแม่เหล็กใกล้หน้าจอเครื่องคอมพิวเตอร์

๘.๖.๖.๓ กำหนดรหัสผ่านในการเข้าใช้งาน

๘.๖.๖.๔ กำหนดให้ล็อกหน้าจอเครื่องคอมพิวเตอร์ หลังจากไม่ได้ใช้งานเป็นเวลา ๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

๘.๖.๖.๕ ติดตั้งโปรแกรมป้องกันไวรัส และตรวจสอบหาไวรัสจากสื่อต่าง ๆ ก่อนนำมาใช้งานในเครื่องคอมพิวเตอร์

๘.๖.๖.๖ รับผิดชอบสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึก เช่น DVD, CD, External hard disk

/๘.๖.๖.๗ เก็บรักษา...

๘.๖.๖.๗ เก็บรักษาสื่อสำรองไว้ในสถานที่ที่เหมาะสม

๘.๖.๖.๘ ไม่ดัดแปลงและแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และทำนุบำรุงรักษาสภาพเครื่องคอมพิวเตอร์ให้มีสภาพคงเดิม

๘.๖.๖.๙ ห้ามนำโปรแกรมที่ไม่มีลิขสิทธิ์มาใช้งานกับเครื่องคอมพิวเตอร์

๘.๗ การใช้งานระบบอินเตอร์เน็ต (Use of the Internet)

๘.๗.๑ เพื่อให้ผู้ใช้งานทราบกฎเกณฑ์ แนวทางปฏิบัติการใช้งานอินเตอร์เน็ตอย่างปลอดภัย และป้องกันไม่ให้ละเมิด พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ โดยส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของสำนักงานจเรทหารถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๘.๗.๒ แนวทางการปฏิบัติ

๘.๗.๒.๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย Proxy, Firewall และ IPS-IDS (Intrusion Prevention System) ที่สำนักงานจเรทหารได้จัดสรรไว้เท่านั้น

๘.๗.๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาต้องติดตั้งโปรแกรมป้องกันไวรัสก่อนเชื่อมต่อเว็บเบราเซอร์ (Web Browser) รวมทั้งการรับ-ส่งข้อมูลผ่านระบบอินเตอร์เน็ตต้องตรวจสอบไวรัส (Virus Scanning) ก่อนการรับ-ส่งข้อมูลทุกครั้ง

๘.๗.๒.๓ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเตอร์เน็ตเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว ไม่เข้าเว็บไซต์ที่ไม่เหมาะสม มีเนื้อหาขัดต่อศีลธรรม ชาติ ศาสนา พระมหากษัตริย์ หรือเป็นภัยต่อสังคม

๘.๗.๒.๔ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่ไม่เหมาะสม ละเมิดสิทธิ์ของผู้อื่น หรืออาจก่อให้เกิดความเสียหายต่อสำนักงานจเรทหาร

๘.๗.๒.๕ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานจเรทหาร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต

๘.๗.๒.๖ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร การก่อการร้าย ข้อมูลที่เป็นเท็จ หรือนำเข้าข้อมูล ภาพของผู้อื่นที่เกิดจากการสร้างขึ้น ตัด ต่อ เติม หรือดัดแปลง อันจะทำให้เสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง เสียความอับอาย รวมทั้งภาพลามกอนาจารเผยแพร่ผ่านระบบอินเตอร์เน็ต

๘.๗.๒.๗ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเตอร์เน็ต ซึ่งรวมถึง Patch หรือ File ต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

/๘.๗.๒.๘ ในการ...

๘.๗.๒.๘ ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุให้ร้าย อันจะทำให้เกิดความเสื่อมเสียต่อสำนักงานจเรทหาร รวมถึงการทำลายความสัมพันธ์กับหน่วยงานอื่น ๆ

๘.๗.๒.๙ หลังจากใช้งานระบบอินเตอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๘.๘ การพัฒนาและการบริหารจัดการเว็บไซต์ (Web Site Development and Management) เพื่อให้ผู้ดูแลและบริหารจัดการเว็บไซต์ (Web Master) ได้ทราบถึงกฎเกณฑ์ แนวทางปฏิบัติในการพัฒนาและการบริหารจัดการเว็บไซต์อย่างปลอดภัย และป้องกันไม่ให้เกิดการละเมิด พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และการคุกคามจากผู้ไม่ประสงค์ดี รบกวนจนไม่สามารถทำงานตามปกติได้ ผู้ดูแลและบริหารจัดการเว็บไซต์ต้องปฏิบัติ ดังนี้

๘.๘.๑ หมั่นตรวจสอบระบบที่ใช้ซอฟต์แวร์สำเร็จรูป (Content Management System) ซึ่งพัฒนาจากผู้พัฒนาภายนอก (Third Party) ได้แก่ Mambo, Joomla, WordPress PhP-nuke หรือ Drupal โดยตรวจสอบข้อมูลจากเว็บไซต์ (Web Site) ของผู้พัฒนาเสมอ เพื่อเป็นข้อมูลในการตัดสินใจปรับปรุง (Update) ซอฟต์แวร์แพคเกจนั้น

๘.๘.๒ ปรับปรุง หรือ Patch เครื่องมือที่ใช้ในการพัฒนาเว็บไซต์ โดยเฉพาะการใช้ซอฟต์แวร์สำเร็จรูปในการพัฒนา รวมถึงปรับเปลี่ยนการใช้งานไม่ให้เป็นแบบ Default (Hardening) ในโฟลเดอร์ (Folder) หลักที่เกี่ยวข้อง คือ โฟลเดอร์ admin และไฟล์ชื่อ login.html และ login.php รวมถึงการตั้งค่ารหัสผ่านให้เป็นชื่อที่ยากต่อการคาดเดา เนื่องจากเป็นส่วนที่ผู้ดูแลเว็บไซต์ (Web Master) ใช้งานเพียงผู้เดียว

๘.๘.๓ ตรวจสอบผู้ให้บริการเครือข่ายระบบอินเตอร์เน็ต และผู้ให้บริการ Web Hosting ที่มีความน่าเชื่อถือและตระหนักถึงความปลอดภัยของระบบ

๘.๘.๔ ตรวจสอบการรับและแสดงผลข้อมูลหน้าเว็บไซต์ (Web Page) และทุกครั้งที่รับ-ส่งข้อมูลบนเว็บไซต์ เพื่อป้องกันการส่งค่าที่เป็นอันตรายต่อการบุกรุกเว็บไซต์

๘.๘.๕ ต้องไม่นำไฟล์หน้าเว็บไซต์ และ Script ของผู้อื่นมาดัดแปลงหน้าเว็บไซต์ของส่วนราชการ เนื่องจากอาจฝังชุดคำสั่งที่เป็นอันตราย หรือภัยคุกคามต่อข้อมูลเครื่องคอมพิวเตอร์และเครือข่าย

๘.๘.๖ ทุกหน้าเว็บไซต์ที่พัฒนาขึ้น ต้องแบ่งแยกประเภทและชนิดของข้อมูลที่รับ-ส่ง ให้ชัดเจน เพื่อให้ง่ายต่อการพัฒนาฟังก์ชั่นสำหรับตรวจสอบ หากดำเนินการรับค่าหรือกรอกข้อมูล ผู้พัฒนาเว็บไซต์ต้องตรวจสอบว่าข้อมูลที่ได้รับจากผู้ใช้งานในแต่ละส่วนตรงตามรูปแบบและข้อกำหนดของแต่ละประเภทก่อนนำไปประมวลผล และไม่ปล่อยให้ข้อมูลที่ส่งเข้ามาประมวลผลโดยไม่ผ่านการตรวจสอบ

๘.๘.๗ ตรวจสอบประเภทหรือนามสกุลของไฟล์ (File Extension) ในส่วนที่ผ่านกระบวนการอัพโหลด (Upload) เพื่อป้องกันการอัพโหลดไฟล์สคริปต์อันตราย หรือไฟล์ที่จะก่อให้เกิดปัญหาบนเครื่องคอมพิวเตอร์แม่ข่าย (Web Server) ของเว็บไซต์ และผู้ดูแลเว็บไซต์ต้องกำหนดขอบเขตและประเภทของไฟล์ที่อนุญาตให้สามารถอัพโหลดได้

/๘.๘.๘ ต้องไม่...

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

๘.๘.๙ จัดการสิทธิไฟล์ต้นฉบับของเว็บไซต์ด้วยสิทธิผู้ใช้งานของตนเอง ไม่ใช่ผ่านหน้าเว็บไซต์อัพโหลดใด ๆ เพราะจะทำให้สิทธิของไฟล์ต่าง ๆ ที่อยู่บนระบบเป็นของเครื่องคอมพิวเตอร์แม่ข่าย

๘.๘.๑๐ ต้องลบไฟล์ หรือโฟลเดอร์ หรือโฟลเดอร์ย่อยต่าง ๆ ที่ไม่จำเป็นต่อการใช้งานและที่แปลกปลอมเข้ามาในเว็บไซต์

๘.๘.๑๑ สำรองข้อมูลของเว็บไซต์และไฟล์ต้นฉบับไว้ที่แหล่งบันทึกข้อมูลอื่นนอกเหนือจากบนเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้บริการอยู่ หากเว็บไซต์ถูกเปลี่ยนแปลงหรือแก้ไขข้อมูลจะได้สามารถกู้คืนข้อมูลได้อย่างรวดเร็วและสมบูรณ์

๘.๙ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๘.๙.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ ในรูปแบบและลักษณะตามที่กองบัญชาการกองทัพไทยกำหนดไว้เท่านั้น

๘.๙.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับสำนักงานจเรทหารผู้ใช้งานต้องแจ้งศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร โดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

๘.๑๐ การบำรุงรักษาอุปกรณ์

๘.๑๐.๑ กำหนดให้มีการบำรุงรักษาอุปกรณ์ทุก ๓ เดือน

๘.๑๐.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาที่กรมการสื่อสารทหารแนะนำ

๘.๑๐.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ สำหรับให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

ประกาศ ณ วันที่ ๑ กุมภาพันธ์ พ.ศ.๒๕๖๒

พลโท

(ธรรมนูญ เชี่ยวการปราบ)

จเรทหาร

สำนักงานจเรทหาร

น.ต.หญิง.....ร.น. ร่าง ๑๑ ก.พ.๖๒

ร.ท.หญิง.....ร.น. พิมพ์/ทาน ๑๑ ก.พ.๖๒

พ.อ.หญิง.....ตรวจ ๑๑ ก.พ.๖๒

พล.ต.....ตรวจ ๑๒ ก.พ.๖๒