

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ของกรมวิชาการเกษตร พ.ศ. ๒๕๖๘

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานอันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

๒. วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมวิชาการเกษตร สามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

๓. ขอบเขตการใช้

บุคลากรทุกคนในกรมวิชาการเกษตร รวมถึงผู้รับสัญญา และผู้เยี่ยมชมซึ่งแม้จะมีได้รับการว่าจ้างจากกรมวิชาการเกษตร แต่มีส่วนเกี่ยวข้องกับการทำงาน หรือสามารถเข้าถึงสารสนเทศของกรมวิชาการเกษตรและใช้กับทุกตำแหน่งพื้นที่ที่สามารถเข้าถึงสารสนเทศและเครือข่ายสารสนเทศของกรมวิชาการเกษตรได้ ซึ่งรวมถึงการเรียกใช้งานจากทางบ้าน หรือการเข้าถึงจากระยะไกล และการเชื่อมโยงจากองค์กรภายนอก และครอบคลุมการบริหารจัดการ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา การใช้งานระบบเครือข่ายอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์ การป้องกันระบบเครือข่ายและตรวจจับการบุกรุก การสำรองและกู้คืนข้อมูล การตรวจสอบ ตามนโยบาย รวมถึงการสร้าง ความตระหนักในเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๔. คำนิยาม

(๑) กรม หมายถึง กรมวิชาการเกษตร

(๒) ศูนย์ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๓) ผู้บริหารสูงสุด (Chief Executive Officer: CEO) หมายถึง อธิบดีกรมวิชาการเกษตร

(๔) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) หมายถึง รองอธิบดีกรมวิชาการเกษตร ที่กำกับดูแล ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่และความรับผิดชอบจัดทำและบริหารระบบฐานข้อมูลของกรม การพัฒนาระบบสารสนเทศและภูมิสารสนเทศเกษตร การพัฒนาระบบ รูปแบบ หลักเกณฑ์ และระเบียบวิธีทางสถิติเพื่อจัดทำข้อมูลวิชาการเกษตร การให้บริการองค์ความรู้ ข้อมูลวิชาการ และข้อมูลเตือนภัยด้านการเกษตร แก่เจ้าหน้าที่เกษตรกร เอกชน และหน่วยงานอื่นที่เกี่ยวข้อง การดำเนินการและบริหารงานตามมาตรฐานระบบความมั่นคงปลอดภัยด้านสารสนเทศของกรม การปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่อธิบดีมอบหมาย

(๕) ผู้บังคับบัญชา ...

- (๕) ผู้บังคับบัญชา หมายถึง ผู้บังคับบัญชาระดับสำนัก/กอง/ศูนย์
- (๖) ผู้ใช้งาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างตามสัญญาจ้างในกรม หรือผู้ที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศของกรม
- (๗) สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรม
- (๘) สินทรัพย์ หมายถึง ข้อมูลสารสนเทศ ระบบงานสารสนเทศ และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์แบบพกพา เครื่องพิมพ์ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง
- (๙) การเข้าถึง หรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย
- (๑๐) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง ความมั่นคงและปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม โดยอ้างไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non - Repudiation) และความน่าเชื่อถือ (Reliability)
- (๑๑) การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม
- (๑๒) มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย
- (๑๓) ขั้นตอนการปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- (๑๔) แนวทางปฏิบัติ หมายถึง แนวทางที่ควรปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์ หรือเป้าหมายได้ง่ายขึ้น
- (๑๕) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
- (๑๖) เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบาย ด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับ ความมั่นคงปลอดภัย
- (๑๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของกรมถูกบุกรุก หรือโจมตี และความมั่นคง ปลอดภัย ถูกคุกคาม

(๑๘) เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้สามารถเข้าใช้งานดูแลรักษาระบบเทคโนโลยีสารสนเทศของกรม ดังนี้

- ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์และระบบคอมพิวเตอร์

- ผู้พัฒนาระบบ (System Developer) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่รับผิดชอบให้หน้าที่ในการพัฒนาและดูแลรักษาระบบงานสารสนเทศของกรม

(๑๙) ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของกรมเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๒๐) ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของกรมที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์มาช่วยในการสร้างระบบสารสนเทศของกรม ที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้ การบริหาร การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบดังนี้ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ และข้อมูลสารสนเทศ

(๒๑) ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๒๒) ข้อมูลจราจรทางคอมพิวเตอร์ (Computer Traffic Data) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

(๒๓) ระบบคอมพิวเตอร์ (Computer System) หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๒๔) ระบบเครือข่าย (Network System) หมายถึง ระบบที่ใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของกรม

- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่าย อิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานของกรม เข้าด้วยกันเป็นเครือข่ายที่มี จุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และสารสนเทศภายในกรม

- ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของกรมเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

(๒๕) ห้องคอมพิวเตอร์แม่ข่าย (Server Room) หมายถึง ห้องที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายหรือคอมพิวเตอร์หลัก และอุปกรณ์เครือข่ายหลักที่ใช้งานในกรม

(๒๖) หน่วยงานภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึง และการใช้งานข้อมูล หรือสินทรัพย์ต่าง ๆ ของกรม โดยจะต้องได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(๒๗) จดหมายอิเล็กทรอนิกส์ (e-Mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์ และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้น จะถูกเก็บไว้ในตู้จดหมาย (Mail Box) ที่กำหนดไว้สำหรับผู้ใช้

(๒๘) สื่อบันทึกพกพา หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive, External Hard Disk เป็นต้น

(๒๙) ชื่อผู้ใช้ (Username) หมายถึง ชุดของตัวอักษร หรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

(๓๐) รหัสผ่าน (Password) หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

(๓๑) อุปกรณ์จัดหาเส้นทาง (Router) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทาง และค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

(๓๒) การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทัวไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

(๓๓) โปรแกรมไม่พึงประสงค์ หมายถึง โปรแกรมที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ทำให้ข้อข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๓๔) ระบบเครือข่ายไร้สาย (Wireless LAN) หมายถึง ระบบเครือข่ายสื่อสารข้อมูล โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ

(๓๕) MAC Address (Media Access Control Address) หมายถึง หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้มากับฮาร์ดแวร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหลายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๕ คู่ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

(๓๖) VPN (Virtual Private Network) หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับ - ส่งข้อมูลจริงจะทำได้โดยการเข้ารหัสเฉพาะแล้วรับ - ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

(๓๗) แผนผังระบบเครือข่าย (Network Diagram) หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของกรม

(๓๘) พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล

พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) หมายถึง พื้นที่ทำงานของเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

พื้นที่ติดตั้ง ...

พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) หมายถึง ห้องคอมพิวเตอร์แม่ข่าย (Server Room) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย

พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) หมายถึง ห้องคอมพิวเตอร์แม่ข่ายที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายที่จัดเก็บข้อมูลคอมพิวเตอร์

(๓๙) อุปกรณ์พกพา หมายถึง อุปกรณ์ที่ใช้ในการติดต่อสื่อสาร ประมวลผลข้อมูล และ/หรือ จัดเก็บข้อมูล โดยผู้ใช้งานสามารถนำพา และเคลื่อนย้ายได้โดยสะดวก ซึ่งรวมถึงอุปกรณ์พกพาที่เป็นทรัพย์สินของกรม และของผู้ใช้ ที่ได้ทำการลงทะเบียนและได้รับอนุญาตจากกรม ให้ใช้ในการเข้าถึงข้อมูล และระบบสารสนเทศของกรม ตัวอย่างอุปกรณ์พกพา เช่น คอมพิวเตอร์แบบพกพา, โทรศัพท์เคลื่อนที่, สมาร์ทโฟน, Tablet, PDA เป็นต้น

(๔๐) การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

(๔๑) ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมีขอบเขตใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

(๔๒) ไซเบอร์ (Cyber) หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

๕. องค์ประกอบของแนวปฏิบัติ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และการสื่อสารของกรมแต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรม เพื่อที่จะทำให้กรมมีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงานทรัพย์สิน บุคลากรของกรมวิชาการเกษตร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย ประกอบด้วย ๙ ส่วน ดังนี้

ส่วนที่ ๑ ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

ส่วนที่ ๒ แนวปฏิบัติในการกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบในการรักษาความมั่นคงปลอดภัย สารสนเทศ (The Responsible authority)

๒.๑ ระดับนโยบาย

๒.๒ ระดับปฏิบัติ

ส่วนที่ ๓ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

๓.๑ การเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control)

๓.๒ การควบคุม...

๓.๒ การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๓.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓.๔ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๓.๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๓.๖ นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

๓.๗ นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

๓.๘ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓.๙ ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of Use Access Right)

๓.๑๐ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์สื่อสารเคลื่อนที่ (Personal Computer and Mobile Computing)

๓.๑๒ การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)

๓.๑๓ การใช้งานระบบอินเทอร์เน็ต (Internet)

๓.๑๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

ส่วนที่ ๔ นโยบายความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๔.๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room)

๔.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

๔.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๔.๔ การนำทรัพย์สินของกรมออกนอกกรม (Removal of Property)

๔.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกกรม (Security of Equipment Off – Premises)

๔.๖ การกำจัดอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment)

๔.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

ส่วนที่ ๕ นโยบายจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance Policy)

๕.๑ การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย

๕.๒ การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล

๕.๓ มาตรการในการเข้ารหัสข้อมูล

๕.๔ การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

๕.๕ การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและการสนับสนุน

๕.๖ การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

ส่วนที่ ๖ นโยบาย ...

ส่วนที่ ๖ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ (Backup and Recovery)

ส่วนที่ ๗ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment)

ส่วนที่ ๘ นโยบายการรับมือภัยคุกคามทางไซเบอร์

๘.๑ การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

๘.๒ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

๘.๓ การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, eradication, and recovery)

๘.๔ การดำเนินงานที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

ส่วนที่ ๙ นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ส่วนที่ ๑

ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

วัตถุประสงค์

เพื่อให้การจัดประเภทข้อมูล ความสำคัญ และการจัดแบ่งลำดับชั้นความลับของข้อมูลสำหรับการบริหารจัดการ การควบคุมการเข้าถึงข้อมูลตามสิทธิที่ได้รับอย่างถูกต้อง เหมาะสม และปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบ/ผู้ที่เกี่ยวข้อง

แนวปฏิบัติ

กรม มีการกำหนดประเภทและลำดับความสำคัญของข้อมูล ดังนี้

๑. การจัดแบ่งประเภทของข้อมูล แบ่งออกเป็น ๒ ประเภท คือ

๑.๑ ข้อมูลสารสนเทศด้านการปฏิบัติงานและการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

๑.๒ ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลด้านการเกษตร ข้อมูลเตือนภัยด้านการเกษตร ข้อมูลด้านนำเข้า - ส่งออก สินค้าเกษตร ข้อมูลเพื่อการติดต่อประสานงาน เป็นต้น

๒. การจัดแบ่งลำดับความสำคัญของข้อมูลแต่ละประเภท แบ่งออกเป็น ๓ ระดับ

๒.๑ ข้อมูลที่มีระดับความสำคัญมากที่สุด

๒.๒ ข้อมูลที่มีระดับความสำคัญปานกลาง

๒.๓ ข้อมูลที่มีระดับความสำคัญน้อย

๓. การจัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภท แบ่งออกเป็น ๓ ระดับ คือ

๓.๑ ลับ หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

๓.๒ ลับมาก หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

๓.๓ ลับที่สุด หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐร้ายแรงที่สุด

๔. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๔.๔ มีมาตรการ ...

๔.๔ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรม เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมให้ทำการสำรอง และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน เป็นต้น

ส่วนที่ ๒

แนวปฏิบัติในการกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Role and responsibility)

วัตถุประสงค์

๑. เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ของกรม ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของกรม ทั้งระดับนโยบาย และระดับปฏิบัติ ได้แก่ ผู้บริหาร ผู้ดูแลระบบ และผู้ใช้งาน ได้รับรู้เข้าใจ บทบาท หน้าที่ ความรับผิดชอบ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษา ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ผู้รับผิดชอบ

ทุกหน่วยงานใน กวก.

แนวปฏิบัติ

การกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยทาง ไซเบอร์และสารสนเทศ มีแนวทางปฏิบัติ คือ ต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบ อย่างชัดเจนเป็นลายลักษณ์อักษร โดยกำหนดหน้าที่ ความรับผิดชอบของผู้ที่เกี่ยวข้องกับ การรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดังนี้

๑. ระดับนโยบาย

รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูล สารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และ สารสนเทศ ผู้รับผิดชอบ ได้แก่

๑.๑ ผู้บริหารระดับสูงสุด (CEO) เป็นผู้ลงนามอนุมัติแนวนโยบาย และแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของกรม และเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่ กรม หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติใน การรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) เป็นผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทาง ไซเบอร์ และสารสนเทศของกรม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ของกรม

๑.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑.๓.๑ กำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในส่วนเทคโนโลยีสารสนเทศรับผิดชอบการดูแลระบบสารสนเทศที่กรมใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ

๑.๓.๒ ควบคุมตรวจสอบการปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติ เพื่อให้คงไว้ซึ่งการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๑.๓.๓ รายงานการติดตามและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ และสารสนเทศ รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นและส่งผลกระทบต่อกรมต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO)

๑.๓.๔ จัดให้มีช่องทางการติดต่อสื่อสารสำหรับใช้รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๒. ระดับปฏิบัติ

๒.๑ ผู้อำนวยการกลุ่ม/ฝ่าย ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑.๑ เป็นผู้รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ และดูแลให้มีการติดตามตรวจสอบในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ พร้อมทั้งรายงานแนวโน้มความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นและส่งผลกระทบต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑.๒ ศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง ควบคุม ดูแล การใช้ระบบสารสนเทศต่าง ๆ ให้เป็นไปตามแผน ป้องกัน แก้ไขและสำรองฉุกเฉิน ให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงในส่วนที่สำคัญ และรายงานผลการทดสอบและการปฏิบัติตามแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๒.๑.๓ ผู้ดูแลระบบระดับ Administrator ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมาย ให้ปฏิบัติหน้าที่เป็นผู้รับผิดชอบ

๒.๑.๑ ดูแลรักษาและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๒.๑.๒ ตรวจสอบและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติหรือมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ ไม่คาดคิด ให้รีบดำเนินการแก้ไขในทันทีเพื่อป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้น ในกรณีที่เกิดสิ่งผิดปกติดังกล่าวเกิดขึ้นจากการละเมิดหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และพิจารณาระงับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศในทันที

๒.๑.๓ ติดตั้งเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบการเข้ารหัสสารสนเทศ ระบบป้องกันและตรวจจับการบุกรุก ระบบป้องกันและกำจัดซอฟต์แวร์ประสงค์ร้าย รวมทั้งอุปกรณ์และระบบอื่นใดที่จำเป็นเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างมั่นคง

๒.๑.๔ ตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และติดตั้งปรับปรุงการแก้ไขข้อบกพร่อง (Patch) ของระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงและทันสมัยอยู่เสมอ

๒.๑.๕ เปลี่ยนรหัสผ่าน ...

๒.๒.๕ เปลี่ยนรหัสผ่านสำหรับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ ทุก ๓ เดือน หรือเมื่อมีความจำเป็น

๒.๒.๖ ดำเนินการการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) พร้อมทั้งทำการทดสอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศที่กำหนดไว้

๒.๒.๗ ดูแลรักษาและตรวจสอบช่องทางการสื่อสาร (Communication port) ของระบบเทคโนโลยี และปิดช่องทางการสื่อสาร (Communication port) ที่ไม่มีความจำเป็นต้องใช้งานในพื้นที่ เพื่อป้องกันการถูกเจาะเข้าระบบจากบุคคลภายนอก (Hacker) ที่ไม่ได้รับอนุญาต

๒.๒.๘ ดูแลรักษาและปรับปรุงบัญชีรายชื่อผู้ใช้งานของระบบเทคโนโลยีสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอโดยให้ยกเลิกสิทธิ์ของผู้ใช้งานทันทีที่พ้นสภาพจากการเป็นผู้ใช้งาน

๒.๒.๙ จัดทำรายงานการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ และนำเสนอต่อผู้อำนวยการกลุ่ม/ฝ่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบหรือเพื่อพิจารณาสั่งการเกี่ยวกับการแก้ไข การปรับปรุงประสิทธิภาพและการให้บริการต่อไป

๒.๒.๑๐ ปฏิบัติงานอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของกรมตามที่ได้รับมอบหมาย

๒.๓ ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอกกรม ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรม รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๓

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของกรม

๒. เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศ มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกภัยคุกคามต่าง ๆ

๓. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับกรมได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๑. การเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control)

๑.๑ จัดทำบัญชีทรัพย์สิน หรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบ หรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

๑.๓ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งาน ของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ โดยต้องกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

๑.๓.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- บอกรายข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๑.๓.๒ กำหนดเกณฑ์ ...

๑.๓.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๓.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาต เป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓.๔ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศ ของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๔ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๑.๔.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และ คำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและการบัญชี เป็นต้น

- ข้อมูลสารสนเทศด้านการเกษตรที่ให้บริการ

๑.๔.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด

- ข้อมูลที่มีระดับความสำคัญปานกลาง

- ข้อมูลที่มีระดับความสำคัญน้อย

๑.๔.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิด ความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิด ความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิด ความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผย หรือเผยแพร่ทั่วไปได้

๑.๔.๔ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย

๑.๔.๕ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ผู้ที่เกี่ยวข้องที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดได้นั้น จะต้องรับสิทธิจากศูนย์ โดยมีการกำหนดบัญชีผู้เกี่ยวข้องตามระดับการเข้าถึงให้สามารถเข้าใช้งาน มีการแยก ประเภทความรับผิดชอบ และมีการพิสูจน์ตัวตน สิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูล ที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

- ระบบเครือข่ายภายใน (Intranet)

- ระบบเครือข่าย ...

- ระบบเครือข่ายอินเทอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)

๑.๕ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๓ ส่วน คือ

๑.๕.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ โดยผู้ดูแลระบบรับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑.๕.๒ มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย โดยผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๑.๕.๓ จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภารกิจดังนี้

๑.๕.๓.๑ Executive คือ กลุ่มผู้บริหาร อธิบดี รองอธิบดี และผู้อำนวยการสำนัก/กอง/ศูนย์

๑.๕.๓.๒ Administrator คือ กลุ่มของผู้ดูแลระบบศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑.๕.๓.๓ Officer คือ กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของกรม ได้แก่ ข้าราชการ พนักงานราชการ และพนักงานจ้างเหมา

๑.๕.๓.๔ Consultant คือ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับกรม

๑.๕.๓.๕ Guest คือ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

๒. การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุมอย่างน้อย ดังนี้

๒.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๒.๑.๑ ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ที่ได้รับ จะต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒ ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา ๑๕ นาที ต้องทำการยุติการใช้งานทันที

๒.๑.๓ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับดังนี้

- กำหนดสิทธิให้กับผู้ใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลแต่ละระดับชั้น

- กำหนดให้มีการรับ - ส่งข้อมูลที่มีการเข้ารหัสอย่างน้อย SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ

- การนำอุปกรณ์คอมพิวเตอร์ หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

๒.๑.๔ การเข้าถึง ...

๒.๑.๔ การเข้าถึงระบบสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใด ๆ จะต้องได้รับสิทธิ์และได้รับอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิ์ที่ให้กับหน่วยงานนั้น ๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใด ๆ ที่มีผลต่อระบบจะต้องเป็นผู้รับผิดชอบ

๒.๑.๕ ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน

๒.๑.๖ ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

๒.๑.๗ ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบ สารสนเทศของผู้ให้บริการภายนอก (Outsource)

๒.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

๒.๒.๑ การแยกระบบสารสนเทศที่มีความสำคัญสูง และจำเป็นต้องได้รับการดูแลเป็นพิเศษ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบสารสนเทศอื่น ๆ ให้ทำงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) โดยไม่ใช้ปะปนกับระบบสารสนเทศอื่น เพื่อป้องกันความผิดพลาดอันอาจเกิดจากระบบสารสนเทศอื่นซึ่งทำงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่ายเดียวกัน ซึ่งจำเป็นต้องติดตั้งอยู่ในห้องคอมพิวเตอร์แม่ข่าย (Server Room) ที่มีมีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

๒.๒.๒ มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่าย ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า – ออกห้องคอมพิวเตอร์แม่ข่าย และอื่น ๆ เพื่อป้องกันการรบกวนการทำงานของระบบสารสนเทศของกรมงานหยุดชะงัก

๒.๒.๓ ควบคุมการเข้าใช้งานระบบสารสนเทศจากเครือข่ายภายใน และเครือข่ายภายนอก โดยการกำหนดสิทธิ์การเข้าใช้งานโดยทำการกำหนดค่าที่ Firewall

๒.๒.๔ มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานภายนอก (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๒.๒.๔.๑ อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกหน่วยงานต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ

๒.๒.๔.๒ การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเปิดสิทธิ์ให้ปฏิบัติงานจากภายนอกได้

๒.๒.๔.๓ ผู้ปฏิบัติงานจากภายนอกต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบสารสนเทศขององค์กร

๒.๒.๕ ควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนด

๒.๒.๖ วางแผนการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายการสำรองระบบสารสนเทศ

๒.๓ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

๒.๓.๑ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

๒.๓.๒ ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพ สำหรับระบบสื่อสารข้อมูล ระหว่างสถานที่ที่จะปฏิบัติงานจากระยะไกล และระบบงานต่าง ๆ ภายในกรม ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานตามแนวปฏิบัติการควบคุมการเข้าถึง

๒.๓.๓ ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัว หรือบุคคลอื่นเข้าถึงระบบเทคโนโลยีสารสนเทศของกรม

๒.๓.๔ การขออนุมัติ หรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงระบบเครือข่าย โดยต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียด ดังนี้

๒.๓.๔.๑ เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน

๒.๓.๔.๒ รายละเอียดและลักษณะของระบบงาน

๒.๓.๔.๓ ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

๒.๓.๔.๔ รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

๒.๓.๔.๕ ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน

๒.๓.๕ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่าง ๆ ภายในหน่วยงาน

๒.๓.๖ การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓.๗ ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับ ชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

๒.๓.๘ การเข้าสู่ระบบระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๒.๓.๙ ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๒.๓.๑๐ ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓.๑๑ ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๓.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยผู้ดูแลระบบกำหนดให้ผู้ใช้งาน

๓.๑.๑ ผู้ใช้งานจะต้องทำการกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของกรม

๓.๑.๒ ผู้ใช้งานจะต้องทำการตั้งค่าให้ระบบปฏิบัติการทำการป้องกันด้วยรหัสผ่านทุกครั้งที่เปิดใช้งาน

๓.๑.๓ ผู้ใช้งานจะต้องทำการตั้งค่าการใช้โปรแกรมถนอมหน้าจอ เมื่อไม่มีการใช้งานให้ทำการล็อกหน้าจอด้วยรหัสผ่าน

๓.๑.๔ ผู้ใช้งานต้องทำการลงบันทึกออก (Log out) ทุกครั้งเมื่อไม่ได้ใช้งานเป็นเวลานาน

๓.๑.๕ กำหนดให้ระบบไม่ให้แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๓.๑.๖ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๓.๑.๗ จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน โดยผู้ใช้งานจะต้องป้อนรหัสผ่านภายในเวลา ๓๐ นาทีเพื่อเข้าใช้งานระบบ

๓.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติดังนี้

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดรหัสผ่านให้กับผู้ใช้งานตามหลักเกณฑ์การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของกรม

๓.๒.๒ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของกรม

๓.๒.๓ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นในการปฏิบัติ โดยจะต้องขออนุญาตใช้จาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และกำหนดกรอบเวลาการใช้งานที่ชัดเจน และยุติการใช้งานทันทีเมื่อพบความผิดปกติหรือหมดช่วงเวลาที่ยกขออนุญาตไว้

๓.๓ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) จำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

๓.๓.๑ ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติ หรืออนุญาตและยังไม่ผ่านการตรวจสอบ

๓.๓.๒ ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเอง และต่อหน่วยงาน

๓.๓.๓ จัดเก็บโปรแกรม ...

๓.๓.๓ จัดเก็บโปรแกรมมัลแวร์ป้องกันไวรัสในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ และเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๓.๓.๔ กำหนดให้มีการถอดถอนโปรแกรมมัลแวร์ป้องกันไวรัสที่ไม่จำเป็นออกจากระบบ รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมมัลแวร์ป้องกันไวรัสได้

๓.๓.๕ ให้ผู้ดูแลระบบทำบัญชีโปรแกรมที่อนุญาตให้ใช้งานได้

๓.๓.๖ จำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมมัลแวร์ป้องกันไวรัสเท่านั้น

๓.๔ การยุติการใช้งานระบบสารสนเทศ (Session Time-Out) เมื่อมีการว่างเว้นจากการใช้งาน ในระยะเวลาหนึ่ง ให้ดำเนินการดังนี้

๓.๔.๑ ต้องกำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลาการยุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้น หรือเป็นเวลา ๑๕ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๓.๔.๒ ถ้าไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบอัตโนมัติ

๓.๔.๓ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ

๓.๕ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๓.๕.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของกรมตามปกติเท่านั้น (วันจันทร์ ถึงวันศุกร์ เวลา ๘.๓๐ - ๑๖.๓๐ น.) หรือวันและเวลาอื่นเพิ่มเติมตามที่กรมกำหนด

๓.๕.๒ การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๓.๕.๓ กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงานที่มีความสำคัญสูง และระบบงานที่มีการใช้งานไปสถานที่ที่มีความเสี่ยง (ในที่สาธารณะ หรือพื้นที่ภายนอกกรม) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อไม่เกิน ๓ ชั่วโมงต่อครั้ง

๓.๖ การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๓.๖.๑ การกำหนดรหัสผ่านให้กับผู้ใช้งานตามหลักเกณฑ์ การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของกรม

๓.๖.๒ อนุญาตให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง โดยต้องกำหนดให้เป็นไปตามเงื่อนไขการกำหนดรหัสผ่าน

๔. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๔.๑ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๔.๑.๑ กำหนดให้มีรหัสผู้ใช้ (Username) และรหัสผ่าน (Password) ในการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

๔.๑.๒ กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ หากเกินกว่าที่กำหนดระบบต้องทำการ Lock ไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง

๔.๑.๓ ผู้ดูแลระบบต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามเกณฑ์การกำหนด ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของกรม

๔.๑.๔ ผู้ดูแลระบบตั้งระบบการล็อกหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานต้องทำการใส่รหัสผ่านเพื่อใช้งาน

๔.๑.๕ ผู้ดูแลระบบต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๔.๒ การควบคุมการให้บริการ Cloud Computing จากผู้ให้บริการภายนอก ด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ และระบบงานสารสนเทศ เพื่อการจัดเก็บข้อมูล การประมวลผล หรือดำเนินการใด ๆ ที่เกี่ยวข้องกับข้อมูลของหน่วยงาน ต้องให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูล ความถูกต้องเชื่อถือได้ ของข้อมูลและระบบสารสนเทศ และความพร้อมใช้งานของระบบสารสนเทศ ที่ให้บริการ รวมถึงกำหนดคุณสมบัติของผู้ให้บริการ เช่น ฐานะการเงิน ความเพียงพอของการให้บริการเพื่อให้มั่นใจได้ว่าผู้ให้บริการสามารถให้บริการตามความต้องการของหน่วยงานได้อย่างต่อเนื่อง ทั้งนี้ หน่วยงานต้องมีการติดตาม ประเมิน และทบทวนการให้บริการและคุณสมบัติของผู้ให้บริการ Cloud Computing เป็นประจำอย่างน้อยทุกปี

๔.๓ การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๔.๓.๑ มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหาย หรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

๔.๓.๒ ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของกรม

๔.๓.๓ การติดตั้ง หรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๔.๓.๔ ไม่ติดตั้ง Source Code Compiler ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

๔.๓.๕ กำหนดให้มีการจัดเก็บ Source Code และ Library สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความปลอดภัย

๔.๓.๖ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ เป็นต้น

๔.๓.๗ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบ

๔.๓.๘ ให้มีการจัดเก็บ ...

๔.๓.๘ ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่ต้องกลับไปใช้เวอร์ชันเก่านั้นตาม ระยะเวลาที่เหมาะสม สารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๔.๓.๙ ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุง ก่อนที่จะเริ่มต้นทำการพัฒนา

๔.๓.๑๐ ทำการปรับปรุง Library สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัย และสอดคล้องกับทั้งหมดที่ทำการติดตั้ง

๔.๓.๑๑ กำหนดให้ผู้ที่เกี่ยวข้องจัดทำแผนถอยหลังกลับ (Rollback Strategy) ก่อนที่จะดำเนินการติดตั้งระบบงานเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๔.๔ การทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลง

๔.๔.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๔.๔.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๔.๕ การพัฒนาซอฟต์แวร์และดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอก (Outsource Software Development)

๔.๕.๑ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก ผ่าน กระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔.๕.๒ กรมเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๔.๕.๓ ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพ และความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๔.๕.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้ง ก่อนดำเนินการติดตั้ง

๔.๕.๕ การดำเนินการพัฒนาซอฟต์แวร์และดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศของกรม ที่ดำเนินงานโดยหน่วยงานภายนอกนั้น หน่วยงานภายนอกจะต้องมีการลงนามในสัญญาการรักษาความลับรักษาข้อมูลของหน่วยงานก่อนการดำเนินใด ๆ รวมทั้งจะต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของหน่วยงานอย่างเคร่งครัด

๔.๕.๖ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

๔.๕.๗ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๔.๕.๘ การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนทุกครั้ง

๔.๖ ความเป็นเจ้าของและความรับผิดชอบ

๔.๖.๑ ต้องกำหนดผู้มีหน้าที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย โดยทำการ Update Service Pack หรือ Patch ต่าง ๆ ให้ทันสมัยอยู่เสมอ เพื่อปิดรูรั่วของตัวระบบปฏิบัติการและตัวโปรแกรมระบบ และต้องมีเอกสารในการปรับเปลี่ยนค่าการปรับแต่งบนเครื่องคอมพิวเตอร์แม่ข่าย โดยต้องมีการระบุรายละเอียดของเครื่องคอมพิวเตอร์แม่ข่ายในระบบการบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Enterprise Management System)

๔.๖.๒ กำหนด ชื่อ/รหัส ระดับสิทธิการใช้งาน ให้ผู้ใช้งานแต่ละคน

๔.๗ การติดตั้ง

๔.๗.๑ ห้ามเปิด Services และ Application ใด ๆ ที่ไม่เกี่ยวข้องกับของเครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ โดยเด็ดขาด

๔.๗.๒ เมื่อมีการปรับแต่ง หรือแก้ไขค่า ต้องมีการแจ้งผู้ดูแลรับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ

๔.๘ มาตรการควบคุมช่องโหว่ทางเทคนิค

๔.๘.๑ กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ต้องมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิต หรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๔.๘.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๔.๘.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

- มีการเฝ้าระวัง และติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของกรม
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้ง หรือทราบเกี่ยวกับช่องโหว่นั้น

๔.๘.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๔.๙ การเฝ้าดูและตรวจสอบ

๔.๙.๑ ต้องดำเนินการเก็บ Log และ Audit Trails ของเหตุการณ์ละเมิดความมั่นคงปลอดภัยดังต่อไปนี้

- Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา ๙๐ วัน

- ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า ๙๐ วัน ให้มีความปลอดภัยและพร้อมเรียกใช้งานได้ เมื่อพนักงานเจ้าหน้าที่ต้องการ และต้องสามารถนำออกมามอบให้กับพนักงานเจ้าหน้าที่ได้

๔.๙.๒ ผู้ดูแลระบบต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับผู้บังคับบัญชาทราบ ดังนี้

- การโจมตีในรูปแบบ Post – Scan
- การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิในการใช้งานระบบนั้น
- เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์แม่ข่ายที่เกิดขึ้น

๔.๙.๓ ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ

๔.๙.๔ ต้องมีการประเมินความเสี่ยงทุก ๖ เดือน หรือตามความเหมาะสม พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอผู้บังคับบัญชา

๔.๑๐ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

๔.๑๐.๑ ข้อมูลชื่อบัญชีผู้ใช้งาน

๔.๑๐.๒ ข้อมูลวัน เวลาที่เข้าถึงระบบ

๔.๑๐.๓ ข้อมูลวัน เวลาที่ออกจากระบบ

๔.๑๐.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๔.๑๐.๕ ข้อมูลการล็อกอิน ทั้งที่สำเร็จ และไม่สำเร็จ

๔.๑๐.๖ ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จ และไม่สำเร็จ

๔.๑๐.๗ ข้อมูลการเปลี่ยนค่า Configuration ของระบบ

๔.๑๐.๘ ข้อมูลแสดงการใช้งานแอปพลิเคชัน

๔.๑๐.๙ ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

๔.๑๐.๑๐ ข้อมูล IP Address ที่เข้าถึง

๔.๑๐.๑๑ ข้อมูล Protocol เครือข่ายที่ใช้

๔.๑๐.๑๒ ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

๔.๑๐.๑๓ ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริหารเครือข่ายโดยไม่ได้รับอนุญาต มีแนวทางปฏิบัติอย่างน้อยดังนี้

๕.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ดังนี้

๕.๑.๑ มีการกำหนดระบบสารสนเทศที่ต้องการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๑.๒ ผู้ใช้งาน ...

๕.๑.๒ ผู้ใช้งานต้องใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่กรมกำหนดขึ้นมา เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยการให้สิทธิเฉพาะสำหรับใช้ ในการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้อง ทบทวน สิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีข้อปฏิบัติ หรือกระบวนการให้มีการยืนยันตัวบุคคล ก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศของกรมได้ ดังนี้

๕.๒.๑ การเข้าสู่เครือข่ายของกรมผ่านเครือข่ายภายนอก จะต้องมีการพิสูจน์ตัวตน โดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง

๕.๒.๒ การอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการ เข้าใช้งาน ต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิค รวมทั้งต้องได้รับความเห็นชอบจาก ผู้บังคับบัญชาก่อน

๕.๒.๓ หากหน่วยงาน หรือผู้ปฏิบัติที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน (Username) จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชา และศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน โดยจะต้อง รับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการ หรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่าย เป็นการ ยืนยันการเข้าถึง ดังนี้

๕.๓.๑ การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของกรม ต้องได้รับอนุญาตจาก ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนจึงจะสามารถดำเนินการได้

๕.๓.๒ ผู้ดูแลระบบมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาต และให้สิทธิในการ เชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด และสามารถระบุสัญญาณการเชื่อมต่อได้เมื่อ สิ้นสุดการอนุญาต

๕.๓.๓ จะต้องมีการจำกัดสิทธิการเข้าใช้งานอุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address

๕.๓.๔ จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่าย ขององค์กร โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์, IP Address, MAC Address, สถานที่ติดตั้ง, ผู้ใช้งาน เป็นต้น

๕.๓.๕ ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึง เครือข่ายของหน่วยงานได้

๕.๓.๖ จัดทำผังระบบเครือข่าย (Network Diagram) ซึ่งมีการระบุรายละเอียดอุปกรณ์ บนเครือข่ายอุปกรณ์ที่ติดตั้งในเครือข่าย และข้อมูลอื่น ๆ ที่จำเป็น

๕.๓.๗ แผนผังเครือข่ายเป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่าง น้อย ปีละ ๑ ครั้ง

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย ดังนี้

๕.๔.๑ ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหา และการตั้งค่า ระบบ ทั้งกายภาพ และโดยการล็อกอินเข้ามาใช้งาน

๕.๔.๒ ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า Configuration ไว้ในห้องคอมพิวเตอร์แม่ข่ายกลางที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์ และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๕.๔.๓ ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการ บำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

๕.๔.๔ ปิดพอร์ตที่มีความจำเป็นสำหรับการใช้งาน และยกเลิกหรือปิดพอร์ต หรือปิด พอร์ตบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๕.๔.๕ ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็น ในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๕.๔.๖ กำหนดสิทธิบุคคลในการเข้า - ออกห้องคอมพิวเตอร์แม่ข่าย (Server Room) โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

๕.๔.๗ มีการบันทึกการเข้า - ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่าย (Server Room) ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง เจ้าหน้าที่ผู้ดูแลระบบสารสนเทศ เป็นต้น

๕.๔.๘ ห้ามบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำเข้าไป

๕.๔.๙ มีการติดตั้งเครื่องควบคุมการบันทึกการเข้า - ออกห้องคอมพิวเตอร์แม่ข่าย ที่ประตูเข้า - ออก และติดตั้งกล้องวงจรปิดเพื่อป้องกันการโจรกรรม

๕.๔.๑๐ ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่าย ดังนี้

๕.๕.๑ ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายโดยใช้ VLAN แบ่งแยกเครือข่าย แต่ละ สำนัก/กอง/ศูนย์ หรือที่ตั้งอาคารออกจากกัน เพื่อป้องกันการละเมิดสิทธิและทรัพยากรเครือข่ายของแต่ละ หน่วยงาน

๕.๕.๒ ผู้ดูแลระบบจะต้องแบ่งแยกเครือข่ายออกเป็นโซนเพื่อความมั่นคงปลอดภัย ของ ระบบจากการบุกรุกทางเครือข่าย ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการ เข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติ อย่างน้อย ดังนี้

๕.๖.๑ การจำกัดสิทธิการเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

๕.๖.๒ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์ แม่ข่าย (Firewall, IDS/IPS)

๕.๖.๓ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๕.๖.๔ การเข้าใช้ ...

๕.๖.๔ การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

๕.๖.๕ ควบคุมไม่ให้มีการเปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบ ได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

๕.๖.๖ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๕.๖.๗ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

๕.๖.๗.๑ จำกัดสิทธิ์การเข้าใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่าย ที่ได้รับอนุญาตเท่านั้น

๕.๖.๗.๒ จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๕.๖.๗.๓ จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๕.๖.๗.๔ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๕.๖.๗.๕ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๕.๖.๗.๖ กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๖.๗.๗ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕.๖.๗.๘ IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๕.๖.๗.๙ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูล หรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๕.๗.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๕.๗.๒ กำหนด ...

๕.๗.๒ กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

๕.๗.๓ กำหนดมาตรการในการใช้เครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย ดังนี้

๕.๗.๓.๑ ผู้ใช้งานต้องมีสิทธิในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากร เครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตนเอง

๕.๗.๓.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

๕.๗.๓.๓ ผู้ใช้งานต้องไม่นำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

๕.๗.๓.๔ ผู้ดูแลระบบต้องทำการจำกัดสิทธิในการใช้งานระบบเครือข่ายร่วมกัน เช่น การแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่าย

๕.๗.๓.๕ ระบบเครือข่ายที่มีการเครือข่ายต่อไปยังเครือข่ายภายนอกต้องเชื่อมต่อผ่านอุปกรณ์รักษาความปลอดภัย IPS และ Firewall เป็นต้น

๕.๗.๔ ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่ายบนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๕.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก (Remote Connection)

๕.๘.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศ และ เครือข่ายของกรม ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรการเข้าสู่ระบบภายใน และต้องดูแลและจัดการอย่างรัดกุม ได้แก่ ช่องทางการเชื่อมต่อเครือข่ายแบบปลอดภัย SSL, VPN การควบคุม พอร์ต (Port) เป็นต้น

๕.๘.๒ การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ ตัวตนของผู้ใช้งาน โดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง

๕.๘.๓ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับ มอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้า สู่ระบบสารสนเทศอย่างเคร่งครัด

๕.๘.๔ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับกรมอย่างเพียงพอ และต้องได้รับอนุมัติจาก ผู้อำนวยการศูนย์ เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายอย่างเป็นทางการ

๕.๘.๕ การควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบ โดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่าง ถูกต้องและเหมาะสมแล้วเท่านั้น

๕.๘.๖ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความ จำเป็นเท่านั้น และไม่เปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องทำการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๖. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๖.๑ การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๖.๒ ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะ เป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

๖.๓ ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

๖.๔ กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

๖.๔.๑ ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall หรือหากมีความจำเป็นจริง ๆ ต้องวางในระบบเครือข่ายภายในที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

๖.๔.๒ ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๖.๔.๓ ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจาก โรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

๖.๔.๔ ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๖.๔.๕ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๖.๔.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

๖.๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบทันที

๗. นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่าง ๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๗.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของกรม

๗.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๗.๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๗.๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

๗.๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๗.๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๗.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๗.๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทางกรมอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน

๗.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบาย จะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยต้องระบุข้อมูลดังนี้

๗.๙.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๗.๙.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๗.๙.๓ วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้น ๆ

๗.๙.๔ วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

๗.๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๗.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๗.๑๒ กรม มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มี พฤติกรรม การใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช หรือ กฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

๗.๑๓ ภายหลังจากการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของกรม หรือกฎหมาย หรืออาจทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือ ทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางศูนย์เทคโนโลยีสารสนเทศ และการสื่อสารจะ ยกเลิกการให้บริการทันที

๗.๑๔ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรือ อุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากกรมก่อน

๘. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึง จากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

๘.๑ กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่อง ต่อไปนี้

๘.๑.๑ จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูล ลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๘.๑.๒ ระบุข้อมูลผู้ใช้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

๘.๑.๓ กำหนดชื่อผู้ใช้งาน (Username) จะกำหนดจากชื่อภาษาอังกฤษ หากชื่อ ภาษาอังกฤษซ้ำกัน จะตามด้วยตัวอักษรแรกของนามสกุล หากให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับ ชื่อผู้ใช้งานคนอื่น

๘.๑.๔ จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาต ให้ใช้เท่าที่จำเป็น

๘.๑.๕ ตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือความต้องการตามภารกิจ

๘.๑.๖ จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานและมาตรการ ด้านความมั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศ ซึ่งต้องลงนามรับทราบด้วย

๘.๑.๗ ทำบันทึกและจัดเก็บข้อมูลการขออนุมัติใช้ระบบสารสนเทศ

๘.๑.๘ การอนุญาตให้เข้าถึงระบบสารสนเทศ จะต้องได้รับการพิจารณาอนุญาต จากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน

๘.๑.๙ การยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออก จากทะเบียนของผู้ใช้งาน จะดำเนินการเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๘.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียด ที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความ เหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวกับการเข้าถึง ดังนี้

๘.๒.๑ แสดงกระบวนการ ...

๘.๒.๑ แสดงกระบวนการในการมอบหมาย หรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน ดังนี้

ระดับชั้นการเข้าถึง	สิทธิการใช้งาน
ผู้บริหาร	อนุมัติ, อ่านอย่างเดียว
ผู้ใช้งานทั่วไป	ป้อนข้อมูล, แก้ไขข้อมูล, อ่านอย่างเดียว
ผู้ดูแลระบบ/ผู้ที่ได้รับมอบหมาย	สร้างข้อมูล, ป้อนข้อมูล, แก้ไขข้อมูล, อ่านอย่างเดียว, ลบข้อมูล

๘.๒.๒ กำหนดระดับสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสมหน้ากับความรับผิดชอบ และตามความจำเป็นในการเข้าใช้งานให้กับผู้ใช้งาน เจ้าหน้าที่ และบุคคลภายนอกที่กรมอนุญาตให้ใช้งาน

๘.๒.๓ ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนดจะต้องได้รับการอนุมัติเห็นชอบจากต้นสังกัด และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จัดทำคำร้องเป็นลายลักษณ์อักษร โดยการให้สิทธิพิเศษดังกล่าวจะต้องกำหนดช่วงเวลาชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษ จะต้องระงับการใช้งานทันที

๘.๒.๔ การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

๘.๒.๕ การบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๘.๒.๖ ทบทวนสิทธิการใช้งานสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๘.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๘.๓.๑ กำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๘.๓.๑.๑ การกำหนดรหัสผ่านให้มีความยาวอย่างน้อย ๘ อักขระ และลักษณะอย่างน้อย ๓ ใน ๕ ของลักษณะดังนี้

- อักขระตัวพิมพ์เล็ก (Lowercase letters) เช่น a, b, c เป็นต้น
- อักขระตัวพิมพ์ใหญ่ (Uppercase letters) เช่น A, B, C เป็นต้น
- ตัวเลข (Numbers) คือ ๐, ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘, ๙
- สัญลักษณ์ (Symbols) เช่น () `~!@#\$%^&* -+ = | \ {} [] ; : " ' <> , . ? / เป็นต้น

- อักขระแบบยูนิโค้ด (Unicode characters) คือ €, ?, ?, และ ?

๘.๓.๑.๒ รหัสผ่านต้องไม่เป็นตัวอักษรที่มีอยู่ในชื่อ user name เกินกว่า ๓ ตัวอักษร

๘.๓.๑.๓ เพื่อให้มีความปลอดภัยเพิ่มขึ้นให้ทำการเปลี่ยนรหัสผ่านเป็นประจำอย่างน้อยทุก ๆ ๑๘๐ วัน

๘.๓.๑.๔ ไม่ใช้รหัสผ่านซ้ำกับรหัสผ่านที่เคยใช้มาแล้ว

๘.๓.๑.๕ อย่าเขียนรหัสผ่านลงกระดาษโดยเด็ดขาด

๘.๓.๒ การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

๘.๓.๓ ส่งมอบ ...

๘.๓.๓ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการให้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ในการจัดส่งรหัสผ่าน และกำหนดให้ผู้ใช้งานต้องลงนามรับรหัสผ่าน เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน และรับทราบแนวปฏิบัติในการใช้งานของกรม

๘.๓.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที หรือภายใน ๗ วัน หลังจากได้รับรหัสผ่านชั่วคราว และเปลี่ยนตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของกรม

๘.๓.๕ เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

๘.๓.๖ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

๘.๓.๗ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๘.๓.๘ กำหนดให้การเข้ารหัสผิดได้ ไม่เกิน ๓ ครั้ง กรณีบัญชีผู้ใช้งานไม่สามารถเข้าใช้งานได้เนื่องจากเข้ารหัสผิดเกินจำนวนครั้งที่กำหนด ให้ติดต่อผู้ดูแลระบบและแจ้งความจำนงค์ขอตั้งรหัสผ่านใหม่

๘.๓.๙ กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ ๑๘๐ วัน

๘.๓.๑๐ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เพื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๘.๔ กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และสารสนเทศในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๙. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of Access Right)

ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ และปรับปรุงบัญชี

๙.๑ ทบทวนสิทธิอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๙.๒ ทบทวนสิทธิผู้ที่มีสิทธิในระดับสูง เช่น สิทธิผู้ดูแลระบบ ด้วยความถี่กว่าสิทธิระดับผู้ใช้งานขั้นต้น โดยมีแนวปฏิบัติในการทบทวนสิทธิ ดังนี้

๙.๒.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน พร้อมรายละเอียด

๙.๒.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

๙.๒.๓ ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับผู้ดูแลระบบ

๙.๒.๔ ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วัน

๑๐. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีแนวปฏิบัติอย่างน้อยดังนี้

๑๐.๑ การกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

๑๐.๑.๑ เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

๑๐.๑.๒ ต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

๑๐.๑.๓ ต้องกำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่า หรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๑๐.๑.๔ ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๑๐.๑.๕ ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

๑๐.๑.๖ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑๐.๑.๗ เก็บรักษารหัสผ่านทั้งของตนเอง และของกลุ่มไว้เป็นความลับ

๑๐.๑.๘ ไม่จด หรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

๑๐.๑.๙ ต้องไม่กำหนดให้มีการบันทึก หรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

๑๐.๑.๑๐ ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

๑๐.๑.๑๑ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้วให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๑๐.๑.๑๒ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

๑๐.๑.๑๓ หลีกเลี่ยงการใช้รหัสผ่านเดิม ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๑๐.๑.๑๔ ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน ถัดจากผู้ใช้งานทั่วไป

๑๐.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของกรม ในขณะที่ไม่มีผู้ดูแล ดังนี้

๑๐.๒.๑ ออกจากระบบสารสนเทศ (Log out) ทันทีที่เสร็จสิ้นการใช้งาน

๑๐.๒.๒ ต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๑๐.๒.๓ ตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งาน หรือถือครองให้มีการล็อก (Lock) หน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที

๑๐.๒.๔ มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยให้ครอบคลุมเรื่องต่าง ๆ คือ การจัดการบริเวณล้อมรอบ การควบคุมการเข้าออก การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์ โดยบุคคลภายนอก การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย

๑๐.๓ การควบคุมทรัพย์สินสารสนเทศ และการใช้งานระบบคอมพิวเตอร์ (Clear Desk an Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสารสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน ดังนี้

๑๐.๓.๑ ทุกคนต้องตระหนักและปฏิบัติตามใด ๆ เพื่อป้องกันทรัพย์สินของกรม

๑๐.๓.๒ ลงชื่อออกจากระบบงาน (Log out) โดยทันทีเมื่อเสร็จสิ้นงาน หรือเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๑๐.๓.๓ ต้องจัดเก็บ/สำรองข้อมูลสารสนเทศที่มีความสำคัญของกรมไว้ในที่ที่ปลอดภัย เช่น เก็บไว้ในตู้เอกสารที่มีระบบรักษาความปลอดภัย

๑๐.๓.๔ ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อไม่มีการใช้งานเกิน ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ต้องให้บริการและมีการใช้งานตลอด ๒๔ ชั่วโมง

๑๐.๓.๕ ล็อกเครื่องคอมพิวเตอร์ อุปกรณ์ สื่อบันทึกข้อมูล เมื่อไม่ได้ใช้งาน

- ตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งาน หรือถือครองให้มีการล็อก (Lock) หน้าจอโดยอัตโนมัติเมื่อไม่มีการใช้งานนานเกินกว่า ๓๐ นาที

- ต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูลที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๑๐.๓.๖ กรณีข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูลแฟลชไดรฟ์ หรือ ฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๑๐.๓.๗ ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

๑๐.๓.๘ ต้องทำการขออนุมัติจากผู้บังคับบัญชา ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสารสื่อบันทึก อุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกกรมทุกครั้ง

๑๐.๓.๙ ระมัดระวังและดูแลทรัพย์สินของกรมที่ตนเองใช้งาน หรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดการสูญหายโดยประมาทเลินเล่อต้องรับผิดชอบ หรือชดเชยต่อความเสียหายนั้น

๑๐.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตาม ระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL หรือ VPN เมื่อมีการรับ - ส่งข้อมูลที่สำคัญ หรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

๑๐.๕ การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศขององค์กร กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

๑๐.๕.๑ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๑๐.๕.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านลืตกี้ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๑๐.๕.๓ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นขององค์กร หรือเป็นบุคคลภายนอก

๑๐.๕.๔ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการ ครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑๐.๕.๕ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ต้องกรตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับองค์กร ซึ่งองค์กรอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๑๐.๕.๖ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกัน หรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent) อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑๐.๕.๗ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์

๑๐.๕.๘ ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือ กระทบต่อภารกิจขององค์กร

๑๐.๕.๙ ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อ ภารกิจขององค์กร

๑๐.๕.๑๐ ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อประโยชน์ทางการค้า

๑๐.๕.๑๑ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตามห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๑๑. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์สื่อสารเคลื่อนที่ (Personal Computer and Mobile Computing)

๑๑.๑ การใช้งานทั่วไป

๑๑.๑.๑ เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินของหน่วยงาน ซึ่งจะขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ดังนั้นผู้ใช้งานต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๑๑.๑.๒ โปรแกรม ...

๑๑.๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๑.๑.๓ ผู้ใช้งานต้องศึกษา และปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๑๑.๑.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของกรมเท่านั้น

๑๑.๑.๕ ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาที่ต้องการ Update Service Pack และ Hot Fix ให้เป็นเวอร์ชันล่าสุดจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น

๑๑.๑.๖ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ในเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาของกรม เว้นแต่ได้รับคำปรึกษา หรือคำแนะนำจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น

๑๑.๑.๗ ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ให้มีสภาพดั้งเดิม

๑๑.๑.๘ การนำเครื่องคอมพิวเตอร์แบบพกพาออกไปใช้งานนอกกรม เมื่อนำกลับมาที่กรม ต้องทำการเชื่อมต่อระบบเครือข่ายภายในกรมเพื่อทำการ Update ข้อมูล ไวรัสคอมพิวเตอร์ (Virus Pattern) ของโปรแกรมป้องกันไวรัสให้เป็นปัจจุบัน

๑๑.๑.๙ การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น การนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกนอกหน่วยงานเพื่อการใดก็ตาม ต้องขออนุมัติผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษรเท่านั้น

๑๑.๑.๑๐ ห้ามเจ้าหน้าที่ผู้ใช้งานทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาของกรมทุกเครื่อง และต้องดูแลมิให้เครื่องคอมพิวเตอร์ที่ถือครองถูกแก้ไข ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ถูกแก้ไข ผู้ถือครองเครื่องคอมพิวเตอร์จะปฏิเสธความรับผิดชอบไม่ได้ เมื่อรู้ว่าเครื่องคอมพิวเตอร์มีการแก้ไขการตั้งค่าเวลาต้องทำการแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบทันที

๑๑.๑.๑๑ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์ โดยใช้โปรแกรมป้องกันไวรัส

๑๑.๑.๑๒ ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

๑๑.๑.๑๓ ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ให้กับผู้ถือครองเครื่องรายใหม่พร้อมทั้งทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้เครื่องคอมพิวเตอร์ทุกครั้ง

๑๑.๑.๑๔ กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์ คอมพิวเตอร์ และสื่อสารเคลื่อนที่ ซึ่งจะต้องแสดงตัวตนเมื่อเข้าใช้งาน

๑๑.๑.๑๕ ไม่อนุญาต ...

๑๑.๑.๑๕ ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของตนเอง

๑๑.๑.๑๖ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัว หรือเครื่องคอมพิวเตอร์แบบพกพา ที่มีได้ขึ้นทะเบียนอุปกรณ์กับผู้ดูแลระบบ มาใช้งานและเชื่อมต่อกับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับอนุญาตเป็นลายลักษณ์อักษรและนำมาขึ้นทะเบียนกับผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

๑๑.๑.๑๗ ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ลงบนสื่อจัดเก็บที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย หรือกำหนดรหัสการเข้าสู่อินเทอร์เน็ต รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑.๒ ความปลอดภัยทางกายภาพ

๑๑.๒.๑ ไม่นำอาหาร หรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๑๑.๒.๒ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอคอมพิวเตอร์ หรือ Disk Drive

๑๑.๒.๓ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น และควรหลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทาง เพราะอาจถูกกดทับเกิดความเสียหายได้

๑๑.๒.๔ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดให้ทำการปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๑.๒.๕ หลีกเลี่ยงการใช้นิ้ว หรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๑.๒.๖ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑๑.๒.๗ การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๑.๒.๘ ไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๑๑.๒.๙ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ให้ล็อก เครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๑.๒.๑๐ ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

๑๑.๒.๑๑ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๑๑.๒.๑๒ การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดด้วยความระมัดระวัง ควรเช็ดไปในแนวทางเดียวกัน ไม่ควรเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๑๑.๓ การเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และรหัสผ่าน

๑๑.๓.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาที่ตนถือครอง

๑๑.๓.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพที่ดี ตามเกณฑ์การกำหนด ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของกรม

๑๑.๓ การเข้าใช้ ...

๑๑.๓.๓ ผู้ใช้งานต้องใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน และต้องทำการใส่รหัสผ่านเมื่อต้องการใช้งาน

๑๑.๓.๔ ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันที เมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑๑.๓.๕ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๑๑.๔ การสำรองข้อมูลและการกู้คืน

๑๑.๔.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๑๑.๔.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑.๔.๓ ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ต้องไม่เป็นข้อมูลสำคัญที่เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไม่เกิดผลกระทบต่อการทำงานของหน่วยงาน

๑๑.๕ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๑๑.๕.๑ ผู้ใช้งานต้องทำการตรวจสอบหาไวรัสคอมพิวเตอร์จากสื่อต่าง ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๑๑.๕.๒ ผู้ใช้งานต้องตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (e-Mail) หรือ File ที่ทำการดาวน์โหลดจากอินเทอร์เน็ต ด้วยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนใช้งาน

๑๑.๕.๓ ผู้ใช้งานต้องทำการตรวจสอบข้อมูลคอมพิวเตอร์ที่คาดว่าจะมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย เพื่อป้องกันไม่ให้ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหายจากการถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ จากชุดคำสั่งไม่พึงประสงค์ (Malware)

๑๒. การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)

๑๒.๑ การใช้งานสำหรับผู้ใช้งาน

๑๒.๑.๑ ผู้ใช้งานที่ต้องการใช้งาน e-Mail ของกรม ต้องทำการกรอกข้อมูลคำขอเข้าใช้งาน และยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งานรายใหม่ และรหัสผ่าน (Password)

๑๒.๑.๒ เมื่อได้รับรหัสผ่าน (Password) จะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันทีเมื่อได้รับรหัสผ่าน (Default Password) ในการเข้าสู่ระบบในครั้งแรก

๑๒.๑.๓ ต้องใช้ e-Mail ของกรม เพื่อติดต่อกับงานของราชการเท่านั้น

๑๒.๑.๔ ไม่ใช้ e-Mail Address ของผู้อื่นเพื่อ อ่าน รับ - ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ e-Mail และให้ถือว่าเจ้าของ e-Mail เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ใน e-Mail ของตน

๑๒.๑.๕ หลังจากการใช้งาน ต้องลงชื่อออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

๑๒.๑.๖ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑๒.๑.๗ ทำการ ...

๑๒.๑.๗ ทำการตรวจสอบ และลบ e-Mail ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบ e-Mail ให้เหลือจำนวนน้อยที่สุด

๑๒.๑.๘ ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๑๒.๑.๙ ปฏิบัติตามวิธีการใช้งานรหัสผ่าน (Password Use) ที่กำหนดไว้อย่างเคร่งครัด

๑๒.๑.๑๐ ห้ามผู้ใช้งานตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๒.๑.๑๑ ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

๑๒.๑.๑๒ ผู้ใช้งานไม่เปิด หรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จักในเครื่องที่อยู่ในระบบเครือข่ายของกรม และผู้ใช้งานควรตรวจสอบเอกสารแนบ จาก e-mail ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัส โดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

๑๒.๑.๑๓ ผู้ใช้งานต้องไม่ส่ง หรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้

- ข้อมูลคอมพิวเตอร์อันเป็นเท็จ
- ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
- ข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
- ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกอนาจาร

๑๒.๑.๑๔ ผู้ใช้งานต้องไม่ใช่ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของกรม ทำให้เกิดความแตกแยกระหว่างกรม ผ่านทางจดหมายอิเล็กทรอนิกส์

๑๒.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

๑๒.๒.๑ กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมให้เหมาะสมกับการให้บริการของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของผู้ใช้งาน

๑๒.๒.๒ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๕ ครั้ง

๑๒.๒.๓ มีการทบทวนสิทธิการเข้าใช้งาน และปรับปรุงบัญชีผู้ใช้งานอย่าง น้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๑๒.๒.๔ มีการควบคุมการเข้าถึงระบบตามทางการบริหารจัดการการเข้าถึงผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๓. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๓.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial - Up Modem ยกเว้น แต่ว่ามีเหตุผลความจำเป็น และได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายแล้วเท่านั้น

๑๓.๒ การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอัปเดตซอฟต์แวร์ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ของระบบปฏิบัติการ

๑๓.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่าย และความปลอดภัยของข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ตของกรมเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น

๑๓.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๓.๕ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๑๓.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับของกรม ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรม การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๑๓.๗ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๑๓.๘ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๓.๙ ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ อย่างเคร่งครัด

๑๓.๑๐ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๔.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบ และลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๔.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับกรมจากการใช้งาน เครือข่ายสังคมออนไลน์

๑๔.๓ ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

๑๔.๔ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับกรม ผู้ใช้งานต้องแจ้งต่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

ส่วนที่ ๔

นโยบายความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยในกรม และกำหนดมาตรการป้องกันที่เหมาะสมตามระดับความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศของกรมขึ้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับอนุญาต ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคาม และการรบกวนไม่ว่าโดยความตั้งใจ หรือจากภัยธรรมชาติ เช่น การโจรกรรม อัคคีภัย หรือสนามแม่เหล็กไฟฟ้า เป็นต้น

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบ/ผู้ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room)

๑.๑ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดพื้นที่ใช้งานสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็น พื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศและระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๑.๒ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

๑.๓ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดมาตรการควบคุมการเข้า - ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

๑.๓.๑ ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิการเข้าใช้งานพื้นที่เท่านั้น

๑.๓.๒ ควบคุมการเข้าใช้งานในพื้นที่โดย แบบพิมพ์นิ้วมือ (Finger Scan)

๑.๓.๓ ติดตั้งกล้องวงจรปิดเพื่อติดตาม/เฝ้าระวัง การเข้าพื้นที่ศูนย์ข้อมูลและเครือข่าย

คอมพิวเตอร์

๑.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์แบบพกพา หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในกรม จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานระบบเครือข่ายไร้สาย และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑.๕ มีระบบสนับสนุนการทำงานของระบบสารสนเทศของกรม ที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ ระบบตรวจจับความชื้น ระบบดับเพลิงสำหรับห้องคอมพิวเตอร์แม่ข่าย ระบบปรับอากาศและควบคุมความชื้น ระบบสำรองไฟ และให้มีการตรวจสอบ หรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้มั่นใจว่า ระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๑.๖ ติดตั้ง ...

๑.๖ ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องคอมพิวเตอร์แม่ข่ายทำงานผิดปกติ หรือหยุดทำงาน

๒. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัด สายสัญญาณ เพื่อทำให้เกิดความเสียหาย

๒.๓ ให้เดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๒.๔ ทำป้ายชื่อสำหรับสายสัญญาณ และบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๒.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง

๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก (Fiber Optic) แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๒.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๓. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๓.๑ ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๓.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามผู้ผลิตแนะนำ

๓.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อให้บริการตรวจสอบ หรือประเมินในภายหลัง

๓.๔ จัดเก็บบันทึกปัญหา และข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๓.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในกรม ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบจะต้องอยู่ในพื้นที่ทุกครั้ง

๓.๖ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔. การนำทรัพย์สินของกรมออกนอกกรม (Removal of Property)

๔.๑ ให้มีการขออนุญาตจาก ผู้บังคับบัญชาในหน่วยงาน ก่อนนำอุปกรณ์ หรือทรัพย์สินนั้นออกไปใช้งานนอกกรม

๔.๒ กำหนดผู้มีอำนาจในการเคลื่อนย้าย หรือนำอุปกรณ์ออกนอกกรม

๔.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกกรม และติดตามให้ทรัพย์สินดังกล่าวกลับมาตามเวลาที่กำหนด

๔.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๔.๕ บันทึกข้อมูลการนำอุปกรณ์ของกรมออกไปใช้งานนอกกรม เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๕. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกกรม (Security of Equipment Off – Premises)

๕.๒ กำหนดมาตรการความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือ ทรัพย์สินของกรมออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๕.๓ ไม่ทิ้งอุปกรณ์ หรือทรัพย์สินของกรมไว้โดยลำพังในที่สาธารณะ

๕.๔ เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์ หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๖. การกำจัดอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment)

๖.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้อนุมัติในการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

๖.๓ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๖.๔ มีมาตรการ หรือเทคนิคในการลบ หรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๖.๕ เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

๖.๕.๑ คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับและไม่แน่ใจว่าลับหรือไม่ ในอยู่ในกลุ่มเอกสารลับ

๖.๕.๒ ทำลายเอกสารลับเหล่านั้นโดยใช้วิธีการดังนี้

ประเภทสื่อข้อมูล	วิธีการทำลาย
Flash Drive	ทุบหรือบดให้เสียหาย
กระดาษ	ทำลายกระดาษด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ทำลายแผ่น CD/DVD ด้วยเครื่องทำลายแผ่น CD/DVD
เทป	ทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลฮาร์ดดิสก์ ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M ซึ่งเป็นการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ

๗. การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

๗.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๗.๒ ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๗.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บ หรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึง หรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

ส่วนที่ ๕

นโยบายจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

(Information System Acquisition, Development and Maintenance Policy)

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของหน่วยงาน มีความมั่นคงปลอดภัย และมีการควบคุมที่เพียงพอ โดยหน่วยงานและผู้พัฒนาระบบ จะต้องคำนึงถึงความมั่นคงปลอดภัยของระบบงาน และการควบคุมภายใน ระบบงานต่าง ๆ เช่น แนวทางการจัดจ้างพัฒนาระบบ การตรวจสอบความถูกต้องของข้อมูล เป็นต้น

ผู้รับผิดชอบ

๑. หน่วยงานเจ้าของระบบ
๒. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๓. ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย

๑.๑ หน่วยงานเจ้าของระบบสารสนเทศ ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานก่อนที่จะพัฒนา หรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นเอกสาร ซึ่งถือว่าเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน

๑.๒ หน่วยงานที่เกี่ยวข้องกับการพัฒนาระบบงานต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของกรม ในการพัฒนาระบบงานและโปรแกรมประยุกต์

๒. การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล

๒.๑ การตรวจข้อมูลนำเข้า

๒.๑.๑ โปรแกรมประยุกต์ของกรมที่มีการป้อนข้อมูลเข้าสู่ระบบ จะต้องมีการ ตรวจสอบความถูกต้องของข้อมูลที่ได้รับจากการป้อนข้อมูล ก่อนที่จะนำข้อมูลนั้นไปประมวลผลต่อ

๒.๑.๒ ในระบบประมวลผลที่สำคัญของหน่วยงาน ต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลที่ป้อนเข้า รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการป้อนข้อมูล

๒.๒ การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล

๒.๒.๑ ระบบประมวลผลต้องออกแบบให้มีความสามารถแจ้งถึงความผิดพลาดต่าง ๆ จากการประมวลผลการสอบทาน เพื่อตรวจจับกรณีการประมวลผลข้อมูลมีความผิดพลาด หรือเสียหาย

๒.๒.๒ ระบบประมวลผลที่สำคัญ ต้องมีการตรวจสอบความถูกต้องของการประมวลผลอย่างสม่ำเสมอ

๒.๓ การตรวจสอบความถูกต้องของข้อมูล

สำหรับระบบที่มีความสำคัญและต้องการความครบถ้วนถูกต้องของข้อมูล ต้องมีการพิจารณาใช้เทคนิคที่เหมาะสมมาใช้กับระบบงาน โดยประโยชน์ของการใช้งานรับรองข้อมูล ได้แก่

๒.๓.๑ รักษา ...

๒.๓.๑ รักษาความถูกต้องของข้อมูล

๒.๓.๒ ตรวจสอบการลักลอบแก้ไขข้อมูล

๒.๔ การตรวจสอบข้อมูลผลลัพธ์

๒.๔.๑ กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อมั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์ ทั้งนี้ การตรวจสอบครอบคลุมถึง

- การสอบเทียบความครบถ้วนของข้อมูลผลลัพธ์ที่ได้จากการประมวลผล
- การตรวจสอบถึงความผิดพลาดต่าง ๆ ของรายงาน
- กำหนดให้มีระเบียบปฏิบัติในการทดสอบข้อมูลผลลัพธ์

๒.๔.๒ ในระบบประมวลผลที่สำคัญของกรม ต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลผลลัพธ์ รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการนำข้อมูลผลลัพธ์ไปใช้

๓. มาตรการในการเข้ารหัสข้อมูล

๓.๑ นโยบายการใช้งานการเข้ารหัสข้อมูล

๓.๑.๑ กำหนดให้มีระเบียบปฏิบัติในเรื่องการใช้อุปกรณ์เข้ารหัส รวมถึงซอฟต์แวร์และมาตรฐานวิธีการเข้ารหัสที่หน่วยงานอนุญาตให้ใช้งานสำหรับข้อมูลในลำดับชั้นต่าง ๆ

๓.๑.๒ ต้องมีการปรับปรุงรายชื่อซอฟต์แวร์ และมาตรฐานในด้านการเข้ารหัสให้ทันสมัยอยู่เสมอ

๓.๑.๓ ต้องมีการพิจารณาถึงลำดับชั้นของข้อมูล และแนวทางในการจัดการข้อมูลในลำดับชั้นดังกล่าวประกอบการพิจารณาในการใช้งานการเข้ารหัส

๓.๑.๔ ต้องมีการประเมินความเสี่ยง และพิจารณาผลการประเมินความเสี่ยงก่อนในการเลือกวิธีในการเข้ารหัสมาใช้งานในระบบงาน

๓.๒ การบริหารจัดการกุญแจเข้ารหัสข้อมูล

ผู้ดูแลระบบแต่ละระบบเป็นผู้จัดการกุญแจรหัสในระบบ และต้องกำหนดการป้องกันด้วยวิธีที่เหมาะสม การจัดการดังกล่าวรวมถึงขั้นตอนการปฏิบัติงานต่าง ๆ ดังนี้

๓.๒.๑ การสร้างและการแจกจ่ายกุญแจรหัส

๓.๒.๒ ความลับของกุญแจส่วนบุคคล

๓.๒.๓ ความถูกต้องของกุญแจสาธารณะ

๓.๒.๔ การยกเลิกการใช้กุญแจรหัส

๓.๒.๕ การกู้คืนกุญแจรหัส

๓.๒.๖ การสำรองข้อมูลกุญแจรหัส

๓.๒.๗ การยกเลิกและทำลายกุญแจรหัสที่ไม่ใช้งานแล้ว

๓.๒.๘ การจัดการที่ไม่ขัดแย้งต่อกฎหมายใด ๆ

๓.๒.๙ การจำกัดให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นในการเข้าใช้อุปกรณ์ที่ใช้ในการสร้างเก็บ หรือสำรองกุญแจรหัส

๔. การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

๔.๑ การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ หรือระบบที่ใช้งานจริง

๔.๑.๑ ก่อนมีการปรับปรุงโปรแกรมเวอร์ชันใหม่ในระบบที่ใช้งานจริงจะต้องได้รับเอกสารการอนุมัติการใช้โปรแกรมเวอร์ชันใหม่ และหลักฐานประกอบอื่น ๆ เช่น รายการผลการทดสอบ เพื่อการรับรองความถูกต้องจากผู้ใช้ และต้องปรับเปลี่ยน Source Code ในสมุดทะเบียน (Library) ให้สอดคล้องกัน

๔.๑.๒ เจ้าหน้าที่ผู้ดูแลสมุดทะเบียน (Library) ที่ได้รับการอนุญาตจากผู้บริหารเท่านั้นที่จะเป็นผู้ดำเนินการปรับปรุงซอฟต์แวร์ที่อยู่ในระบบใช้งานจริงเฉพาะส่วนที่ตนเองรับผิดชอบ

๔.๑.๓ ไม่จัดเก็บ Source Code ของโปรแกรมไว้ในระบบที่ใช้งานจริง

๔.๑.๔ ต้องจัดเก็บรายการบันทึกเพื่อการตรวจสอบต่าง ๆ ของการแก้ไข Source code และโปรแกรม

๔.๑.๕ ต้องมีการสำรองและจัดเก็บโปรแกรมเวอร์ชันก่อนการแก้ไขเพื่อนำกลับมาใช้เมื่อมีความจำเป็น

๔.๑.๖ ก่อนที่จะอนุญาตให้ผู้ให้บริการ/เจ้าหน้าที่ระบบเข้าถึงระบบที่ใช้งานจริงเพื่อติดตั้ง แก้ปัญหา และ/หรือดูแลรักษาระบบ จะต้องได้รับการอนุมัติจากผู้บริหาร โดยมีเจ้าหน้าที่หรือผู้ที่ได้รับมอบหมายของกรม ในการติดตามดูแลกิจกรรมต่าง ๆ ของผู้ให้บริการ/เจ้าหน้าที่

๔.๑.๗ การลงโปรแกรมแก้ไข (Software Patches) เมื่อผู้ผลิตได้ออกโปรแกรม ดังกล่าวเพื่อใช้ในการแก้ไขหรือกำจัดข้อบกพร่องด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลักษณะการใช้งาน ซอฟต์แวร์ในปัจจุบัน

๔.๒ การป้องกันข้อมูลที่ใช้สำหรับการทดสอบระบบ

ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงไปใช้เพื่อการทดสอบระบบงานที่พัฒนาใหม่ ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง โดยการควบคุมต่าง ๆ ต้องประกอบด้วย

๔.๒.๑ ต้องได้รับอนุญาตก่อนการนำสำเนาข้อมูลจริงไปใช้ในระบบงานทดสอบในแต่ละครั้ง

๔.๒.๒ มีการควบคุมการเข้าถึงข้อมูลที่ใช้ทำการทดสอบระบบ

๔.๒.๓ มีการดัดแปลงข้อมูลจริงบางส่วนก่อนนำมาใช้ในการทดสอบ

๔.๒.๔ ทำการลบข้อมูลทดสอบออกจากระบบทันทีที่เมื่อเสร็จสิ้นการทดสอบ

๔.๒.๕ มีการจัดเก็บบันทึกการทำรายการในระบบ (Audit Log) เพื่อตรวจสอบ

๔.๓ การควบคุมการเข้าถึง Source Code ของโปรแกรม

๔.๓.๑ แต่งตั้งเจ้าหน้าที่ผู้ดูแลสมุดทะเบียน (Library) ที่เก็บ Source Code ของแต่ละระบบในความรับผิดชอบ และต้องมีการจำกัดสิทธิในการเข้าถึง Library ที่เก็บ Source Code ของโปรแกรม

๔.๓.๒ การอัปเดต Source Code ของโปรแกรมใน Library และการนำ Source Code ของโปรแกรมให้กับผู้พัฒนาระบบ จะต้องดำเนินการโดยเจ้าหน้าที่ผู้ดูแล Library ที่ได้รับมอบหมายในแต่ละระบบ

๔.๓.๓ ต้องมีการจัดเก็บบันทึกการทำรายการในระบบ (Audit Log) เพื่อตรวจสอบการเข้าถึง Library ต่าง ๆ

๔.๓.๔ บันทึก ...

๔.๓.๔ บันทึกรายละเอียดโปรแกรมเวอร์ชันเก่าที่จะทำการจัดเก็บอย่างชัดเจน โดยมี รายละเอียดต่าง ๆ เช่น วัน-เดือน-ปี ที่โปรแกรมเวอร์ชันนี้ได้ใช้งานอยู่ในระบบใช้งานจริง ซอฟต์แวร์ต่าง ๆ ที่ทำงานร่วมกันกับโปรแกรมนี้ เป็นต้น

๔.๓.๕ การปรับปรุงเปลี่ยนแปลง และการทำสำเนา Library จะต้องปฏิบัติตามข้อพิจารณาในการควบคุมการเปลี่ยนแปลงของระบบ

๕. การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและการสนับสนุน

๕.๑ ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลง หรือแก้ไขระบบ

๕.๑.๑ การปรับปรุงแก้ไขระบบงาน หรือโปรแกรมต่าง ๆ ต้องปฏิบัติตามระเบียบปฏิบัติของหน่วยงานว่าด้วยเรื่องการปรับปรุงแก้ไขระบบงานหรือโปรแกรม

๕.๑.๒ การปรับปรุงแก้ไขระบบงานต่าง ๆ ต้องจัดทำเป็นเอกสารและสามารถติดตามสถานะได้รวมถึงต้องมีเอกสารสนับสนุน เช่น แผนการทดสอบการปรับปรุงแก้ไขโปรแกรม และผลการทดสอบ

๕.๑.๓ การปรับปรุงแก้ไขระบบงานให้พิจารณาถึง

- การอนุมัติโดยหน่วยงานเจ้าของระบบงาน
- การระบุถึงเครื่องคอมพิวเตอร์ ซอฟต์แวร์ ระบบฐานข้อมูล ที่จะต้องเปลี่ยนแปลง

- การป้องกันผลกระทบที่อาจเกิดขึ้นกับการทำงาน
- การสำรองข้อมูลก่อนการปรับปรุงแก้ไข หรือบำรุงรักษาระบบ
- การจัดทำเอกสารประกอบการเปลี่ยนแปลงให้ทันสมัย
- การควบคุมเวอร์ชันของซอฟต์แวร์ที่เปลี่ยนแปลง
- การจัดเก็บบันทึกเพื่อการตรวจสอบการแก้ไข

๕.๑.๔ การปรับปรุงแก้ไขระบบต้องจัดทำเป็นหนังสือขออนุมัติแก้ไขระบบงาน หรือโปรแกรมซึ่งประกอบด้วยรายละเอียดตามมาตรฐานที่หน่วยงานกำหนด

๕.๒ การตรวจสอบการทำงานของโปรแกรมประยุกต์ภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๕.๒.๑ ทบทวนมาตรการควบคุม และขั้นตอนปฏิบัติของโปรแกรมประยุกต์ ในด้านความสมบูรณ์ถูกต้องภายหลังการเปลี่ยนแปลงระบบปฏิบัติการ

๕.๒.๒ ดำเนินการแจ้งการเปลี่ยนแปลงระบบปฏิบัติการให้กับผู้ที่เกี่ยวข้องทราบ ในเวลาที่เหมาะสมเพียงพอสำหรับการเตรียมการทดสอบและการทบทวนก่อนที่จะติดตั้งใช้งานจริง

๕.๒.๓ แต่งตั้งกลุ่มบุคคลเฉพาะเพื่อรับผิดชอบในการตรวจเฝ้าระวังช่องโหว่ และการแก้ไข อุดช่องโหว่ของผู้ให้บริการ/จำหน่ายระบบ

๕.๓ การจำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่มาจากผู้ผลิต

ซอฟต์แวร์สำเร็จรูปต้องใช้งานโดยปราศจากการแก้ไข ถ้ามีความจำเป็นในการเปลี่ยนแปลง แก้ไขซอฟต์แวร์สำเร็จรูปต้องมีการพิจารณาการควบคุมต่าง ๆ ดังนี้

๕.๓.๑ ความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ซึ่งอาจมีการละเลยการควบคุมด้านความมั่นคงปลอดภัย

๕.๓.๒ การได้รับความยินยอมในการแก้ไขจากผู้จำหน่ายซอฟต์แวร์

๕.๓.๓ ข้อกำหนดความต้องการต่าง ๆ ด้านเทคนิคจากผู้จำหน่ายซอฟต์แวร์

๕.๓.๔ ผลกระทบ ...

๕.๓.๔ ผลกระทบและการดูแลรักษาระบบภายหลังการเปลี่ยนแปลง

๕.๓.๕ การจัดทำสำเนาของซอฟต์แวร์ก่อนการเปลี่ยนแปลง

๕.๓.๖ การทดสอบการเปลี่ยนแปลง

๕.๓.๗ การจัดทำเอกสารประกอบการเปลี่ยนแปลง

๕.๔ การป้องกันการรั่วไหลของข้อมูลสารสนเทศ

กรมต้องมีการควบคุมเพื่อป้องกันการรั่วไหลของข้อมูลสารสนเทศ ซึ่งมีโอกาสที่จะเกิดขึ้นได้จากผลของชุดคำสั่งที่แอบแฝงมากับซอฟต์แวร์สำเร็จรูป ส่งผลกระทบให้ระบบทำงานผิดพลาด หรือแอบเปิดเผยข้อมูลของกรม ดังนั้น จึงต้องมีการควบคุมเพื่อป้องกันโปรแกรม หรือชุดคำสั่งที่อาจแอบแฝงมากับซอฟต์แวร์สำเร็จรูปก่อนการจัดซื้อซอฟต์แวร์สำเร็จรูปต้องพิจารณาการควบคุม ดังต่อไปนี้

๕.๔.๑ จัดซื้อซอฟต์แวร์ที่เป็นเวอร์ชันซึ่งจัดจำหน่ายในเชิงพาณิชย์แล้ว (ไม่ใช่เวอร์ชันทดลอง) โดยจัดซื้อซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น

๕.๔.๒ ถ้าเป็นไปได้ให้นำ Source Code มาตรวจสอบก่อนนำมาใช้งานจริง โดยทำการสแกนหาข้อมูล หรือชุดคำสั่งแอบแฝง ตลอดจนการทดสอบก่อนที่จะนำไปติดตั้งในระบบใช้งานจริง

๕.๔.๓ มีการควบคุมการเข้าถึง Source Code เพื่อป้องกันการแก้ไขโดยไม่ได้รับอนุญาต

๕.๔.๔ ตรวจสอบและเฝ้าระวังการใช้ทรัพยากรในระบบคอมพิวเตอร์หลังจากที่นำซอฟต์แวร์ใช้งาน

๕.๕ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

การใช้หน่วยงานภายนอกพัฒนาซอฟต์แวร์เพื่อใช้งานภายในกรมต้องพิจารณาหัวข้อ

๕.๕.๑ สิทธิบัตร หรือลิขสิทธิ์ความเป็นเจ้าของซอฟต์แวร์

๕.๕.๒ สิทธิความเป็นเจ้าของใน Source Code ของโปรแกรม

๕.๕.๓ สัญญา หรือข้อตกลงด้านความมั่นคงปลอดภัยในการพัฒนาโปรแกรม เช่น การไม่เขียนโปรแกรมแอบแฝง เป็นต้น

๕.๕.๔ ความรับผิดชอบหากเกิดปัญหาในซอฟต์แวร์

๕.๕.๕ ความน่าเชื่อถือของหน่วยงานภายนอก

๕.๕.๖ การทดลองการติดตั้งเพื่อป้องกันชุดคำสั่ง หรือโปรแกรมแอบแฝง

๕.๕.๗ ข้อตกลงการเข้าใช้ Source Code ในกรณีที่บริษัทผู้ผลิตไม่สามารถให้บริการได้ (Escrow Arrangement)

๕.๕.๘ การอบรมให้ความรู้แก่ข้าราชการ พนักงานราชการ และพนักงานจ้างเหมาของกรมได้

๕.๕.๙ เอกสารประกอบระบบงาน

๖. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

กรมต้องทำการตรวจสอบความเสี่ยงของช่องโหว่ ปรับปรุงโปรแกรมตลอดจนติดตามข้อมูลข่าวสารที่เกี่ยวกับช่องโหว่ในระบบต่าง ๆ อย่างสม่ำเสมอเป็นระยะ ๆ โดยมีแนวทางปฏิบัติ ดังนี้

๖.๑ กำหนดบทบาท และหน้าที่ความรับผิดชอบ เพื่อบอกหมายให้มีผู้รับผิดชอบในการบริหารจัดการช่องโหว่ ซึ่งรวมถึงการเฝ้าระวังภัยจากช่องโหว่ การประเมินความเสี่ยงที่มีจากช่องโหว่ การอุดช่องโหว่ การติดตามทรัพย์สินสารสนเทศ และการประสานงานตามที่เป็นในการบริหารจัดการควบคุมช่องโหว่

๖.๒ มีแหล่งข้อมูล ...

๖.๒ มีแหล่งข้อมูลที่เชื่อถือได้ในการติดตามข่าวสารภัยช่องโหว่ และการจัดการด้านเทคนิค เพื่อให้ตระหนักถึงช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์และเทคโนโลยีอื่น ๆ

๖.๓ จัดการแก้ไขช่องโหว่ตามความรุนแรงของเหตุการณ์

๖.๔ หากไม่มีชุดคำสั่งอุดช่องโหว่ (Patch) ให้ดำเนินการประเมินความเสี่ยงในการติดตั้งชุดคำสั่งดังกล่าว โดยเปรียบเทียบกับความเสี่ยงจากภัยที่มีจากช่องโหว่

๖.๕ ทำการทดสอบชุดคำสั่งอุดช่องโหว่ (Patch) และทำการประเมินก่อนที่จะติดตั้งแก้ไขระบบ

๖.๖ หากไม่มีคำสั่งอุดช่องโหว่ (Patch) ให้พิจารณามาตรการควบคุมอื่น ๆ อย่างเช่น

๖.๖.๑ ปิดการให้บริการ หรือการใช้ระบบในส่วนที่เกี่ยวข้องกับช่องโหว่

๖.๖.๒ ดัดแปลง หรือเพิ่มมาตรการควบคุม เช่น กำหนดค่าบน Firewall เป็นต้น

๖.๖.๓ เผื่อระวังมากขึ้นเพื่อตรวจจับ หรือป้องกันการบุกรุกจริง

๖.๖.๔ แจ้งข่าวสาร หรือเพิ่มความตระหนักถึงภัยช่องโหว่

๖.๗ จัดเก็บ Audit Log ตามระเบียบปฏิบัติ

๖.๘ ทำการติดตามและประเมินกระบวนการในการบริหารจัดการช่องโหว่อย่างสม่ำเสมอ

๖.๙ ในกรณีระบบที่มีความเสี่ยงสูง ต้องมีการจัดการอย่างเข้มงวด

ส่วนที่ ๖

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ (Backup and Recovery)

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของกรม ให้บริการได้อย่างต่อเนื่อง
๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติ และความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับกรมเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทางต่อไปนี้
 - ๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของกรม พร้อมทั้งกำหนดระบบสารสนเทศที่จะทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง
 - ๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย กำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มี วิธีการสำรองข้อมูลดังนี้
 - ๑.๒.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
 - ๑.๒.๑.๑ ข้อมูลคอนฟิกูเรชัน (Configuration) สำหรับระบบ
 - ๑.๒.๑.๒ ฐานข้อมูล (Database) ในระบบสารสนเทศ
 - ๑.๒.๑.๓ ซอฟต์แวร์ (Software) ต่าง ๆ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่น ๆ ที่สำคัญ
 - ๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
 - ๑.๒.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา/ชื่อข้อมูลสำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
 - ๑.๒.๔ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น
 - ๑.๒.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
 - ๑.๒.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับกรมจะต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับกรม เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว เป็นต้น

๑.๒.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล
นอกสถานที่

๑.๒.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึง
ข้อมูลได้ตามปกติ

๑.๒.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองเก็บไว้

๑.๒.๑๐ ตรวจสอบและทดสอบประสิทธิภาพ และประสิทธิผลของขั้นตอนปฏิบัติ
ในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑.๒.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๑.๓ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๑.๔ กำหนดชนิดของระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้อง
ประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์
ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้อง

๑.๕ กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับ
ความเสี่ยงที่กำหนดโดยเจ้าของข้อมูลหรือระบบ

๑.๖ กำหนดขั้นตอนการดำเนินการสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง

๑.๗ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับ
การกู้คืนระบบ

๑.๘ การเก็บสื่อบันทึกข้อมูลสำรองต้องถูกเก็บไว้ ณ บริเวณพื้นที่ภายนอกอาคารของกรม
เดือนละ ๑ ครั้ง

๑.๙ ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูล
ในการสำรองข้อมูลทุกครั้ง

๑.๑๐ ต้องทำการทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการ
ทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่าง
สมบูรณ์ โดยการทดสอบต้องจัดทำบันทึกการทดสอบไว้เป็นหลักฐาน

๑.๑๑ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถทำการกู้คืนระบบกลับคืนได้
ภายในระยะเวลาที่กำหนด

๑.๑๒ การสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสาร และมีการ
ตรวจสอบความถูกต้องเป็นระยะ ๆ

๑.๑๓ ต้องมีการตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำ ทุกปี

๑.๑๔ สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนสื่อบันทึกข้อมูลตามอายุการใช้งานของสื่อ
ตามประเภทของสื่อบันทึกข้อมูลแต่ละชนิด

๒. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง
อิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความ
พร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ
ตามแนวทางต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อยดังนี้

๒.๑.๑ มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๑.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟฟ้าดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว น้ำท่วม การชุมนุม ประท้วงทำให้ไม่สามารถเข้าใช้ระบบงานได้ เป็นต้น

๒.๑.๓ มีการกำหนดขั้นตอนการกู้คืนระบบสารสนเทศ และระยะเวลาในการกู้คืน ระบบที่สอดคล้องตามเป้าหมายที่กรมกำหนดไว้

๒.๑.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๑.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๒.๑.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้ อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละกรม อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๗

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment)

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ตรวจสอบภายใน (Internal Auditor)
๓. คู่มือระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้
 - ๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง
 - ๑.๒ ตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของกรม (Internal Auditor) เพื่อให้กรมได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยทางไซเบอร์ และสารสนเทศของกรม
๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อย ดังนี้
 - ๒.๑ มีการทบทวนให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่เป็นต้องตรวจสอบได้แบบอ่านได้
อย่างเดียว
 - ๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
อย่างน้อยปีละ ๑ ครั้ง
 - ๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
 - ๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้
 - ๒.๔.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่เป็นต้องตรวจสอบได้แบบอ่านได้
อย่างเดียว
 - ๒.๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้
ผู้ตรวจสอบใช้งาน รวมทั้งทำลาย หรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็น
อย่างดี
 - ๒.๔.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบ
บริหารจัดการความมั่นคงปลอดภัย
 - ๒.๔.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล
Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ
 - ๒.๔.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยก
การติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการ
จัดเก็บป้องกันเครื่องมือจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๘

นโยบายการรับมือภัยคุกคามทางไซเบอร์

วัตถุประสงค์

๑. เพื่อให้มีแผนการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์และแนวทางแก้ไขปัญหา
๒. เพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์
๓. เพื่อให้ระบบสารสนเทศสามารถให้บริการอย่างต่อเนื่อง

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

จัดให้มีมาตรการในการรับมือและตอบสนองเมื่อตรวจพบภัยคุกคามทางไซเบอร์ สามารถตอบสนองได้อย่างทันการณ์ ดังนี้

๑. การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์
 - ๑.๑ จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใด ที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น
 - ๑.๒ จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์
 - ๑.๓ ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศ
 - ๑.๔ จัดเตรียมรายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เพื่อข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์
 - ๑.๕ พิจารณาช่องบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น
 - ๑.๖ จัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) ที่มีผลกระทบกับความมั่นคงปลอดภัยทางไซเบอร์ของกรม และดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) โดยจะต้องมีการบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร
 - ๑.๗ กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง
 - ๑.๘ จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ

๑.๙ ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยต้องมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ เท่านั้น

๑.๑๐ ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing)

๑.๑๑ รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence)

๑.๑๒ พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ เพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบช่องโหว่หรือจุดอ่อนต่าง ๆ

๑.๑๓ กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์

๑.๑๔ จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว

๑.๑๕ สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์

๒. การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

๒.๑ จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้

๒.๒ จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๒.๓ จัดให้มีข้อควรปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัยด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) และจัดให้มีข้อควรปฏิบัติที่สูงขึ้นสำหรับระบบงานที่มีความสำคัญมากขึ้น

๒.๔ วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษา และค้นหาความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation)

๒.๕ ทันท่วงทีที่พบว่ามีหรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์ ช่องโหว่ที่อาจถูกใช้ในการโจมตี สถานการณ์ของการโจมตี (กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้เวลา ประทับ ข้อมูล payload และข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยกรมจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguard incident data) เป็นพยานหลักฐานในการดำเนินคดี และจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

๒.๖ ระบุหมวดหมู่ ...

๒.๖ ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าวจะสิ้นสุด โดยพิจารณาอ้างอิงจากข้อมูล “ภาคผนวก ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔”

๒.๗ จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ให้ทันทั่วทั้ง โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

๒.๘ ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์ รวมถึงจุดอ่อนของระบบที่ถูกโจมตี

๒.๙ ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัยหรือช่องทางที่สำนักงานกำหนด โดยต้องคำนึงถึงระดับขั้นความลับและความสำคัญของข้อมูล เพื่อให้ผู้รับผิดชอบดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

๒.๑๐ รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบภายในระยะเวลาที่กรมกำหนด

๓. การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปรามปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, eradication, and recovery)

๓.๑ ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประกอบการตัดสินใจในการดำเนินการ

๓.๑.๑ การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น

๓.๑.๒ การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของกรม การสื่อสารทั้งภายในและภายนอกกรม เป็นต้น

๓.๑.๓ การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด

๓.๒ ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้ เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี

๓.๓ ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาที่มาของการโจมตีจาก แหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น

๓.๔ ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้องผ่านทางช่องทางที่มีความเหมาะสมและปลอดภัยภายในระยะเวลาที่กรมกำหนด

๓.๕ ดำเนินการ ...

๓.๕ ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม

๓.๖ ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติ ภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น

๓.๗ สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ ที่มี ลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต

๓.๘ ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญ ด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของกรมทำได้อย่างรวดเร็ว

๔. การดำเนินงานที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) ให้กรมพิจารณาดำเนินการดังนี้

๔.๑ นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีผลกระทบรุนแรงมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของกรมนโยบายและกระบวนการการฝึกอบรมบุคลากร การระบุผู้มีอำนาจ การดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง

๔.๒ รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์เป็นรายเดือน เช่น จำนวนของภัยคุกคามทางไซเบอร์ ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และ วัตถุประสงค์ของการโจมตี เป็นต้น เสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในกรม

๔.๓ ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน

๔.๔ เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ตามแนวทางและระยะเวลาการเก็บรักษา หลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

ส่วนที่ ๙

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของหน่วยงาน
๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน
๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. สำนักงานเลขานุการกรม

แนวปฏิบัติ

๑. กำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training)
๒. ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
๓. จัดให้มีการเผยแพร่ประชาสัมพันธ์ความรู้ความเข้าใจกับผู้ใช้งาน เหตุการณ์ด้านความมั่นคงปลอดภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมทั้งกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
๔. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของกรม อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
๕. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของกรม
๖. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของกรม
๗. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาจะจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดให้ความรู้
๘. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ
๙. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน