

ประกาศ

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ



เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงาน ป.ป.ท. พ.ศ. ๒๕๖๔

ประกาศ

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ



เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงาน ป.ป.ท. พ.ศ. ๒๕๖๔



ประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๔

เพื่อเป็นมาตรฐานและแนวปฏิบัติให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และสามารถดำเนินการได้อย่างต่อเนื่อง อันเป็นการป้องกันปัญหาที่อาจเกิดจากการใช้งานระบบสารสนเทศที่ไม่ถูกต้อง ทั้งที่เกิดจากความตั้งใจ และไม่ตั้งใจก็ตาม รวมถึงการป้องกันภัยคุกคามต่างๆ จากภายในและภายนอกองค์กร อันเป็นส่งผลให้เกิดความเสียหายต่อสำนักงาน ป.ป.ท. และเพื่อเป็นการรักษาไว้ซึ่งความสามารถในการดำเนินงานได้อย่างมีประสิทธิภาพ

สำนักงาน ป.ป.ท. จึงได้จัดทำ นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๔ โดยสอดคล้องตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เมื่อวันที่ ๑๘ มกราคม ๒๕๕๙ เรียบร้อยแล้ว

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ จึงออกประกาศดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ เรื่อง “นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๔”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓. ให้ยกเลิกประกาศ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ เรื่อง “นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๕๙” ลงวันที่ ๑๑ เมษายน ๒๕๕๙ (แก้ไขใหม่)

/ข้อ ๔. คำนิยาม...

ข้อ ๔. คำนิยาม ประกอบด้วย

- (๑) หน่วยงาน หมายความว่า สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ
- (๒) ศูนย์ หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- (๓) ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) หมายความว่า เลขาธิการคณะกรรมการ ป.ป.ท.
- (๔) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) หมายความว่า รองเลขาธิการคณะกรรมการ ป.ป.ท.
- (๕) ผู้ใช้งาน หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ/ชั่วคราว ลูกจ้างตามสัญญาจ้างในสำนักงาน ป.ป.ท. หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่าย สำนักงาน ป.ป.ท.
- (๖) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ของสำนักงาน ป.ป.ท.
- (๗) สินทรัพย์ หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับหน่วยงาน ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- (๘) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
- (๙) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดชอบ ปฏิเสธความผิด และความน่าเชื่อถือ
- (๑๐) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุงการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิด การฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- (๑๑) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
- (๑๒) ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
- (๑๓) ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น
- (๑๔) ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
- (๑๕) หน่วยงานภายนอก หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับข้อมูล

/(๑๖) จดหมายอิเล็กทรอนิกส์...

- (๑๖) จดหมายอิเล็กทรอนิกส์ (E-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว โดยที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น
- (๑๗) สื่อบันทึกพกพา หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น
- (๑๘) ชื่อผู้ใช้ (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้
- (๑๙) รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- (๒๐) การเข้ารหัส (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
- (๒๑) อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
- (๒๒) การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทัวไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
- (๒๓) SSID (Service Set Identifier) หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน
- (๒๔) WEP (Wired Equivalent Privacy) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้
- (๒๕) WPA (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP
- (๒๖) MAC Address (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหลายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่รูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
- (๒๗) VPN (Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ - ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
- (๒๘) แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

ข้อ ๔. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ มี ๒ ส่วน ดังนี้
๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕
๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๖ - ๑๔ ซึ่งเป็นเอกสารแนบท้ายประกาศ

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสำนักงาน ป.ป.ท.

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงเพิ่มเติมในส่วนที่มีผลกระทบในเนื้อหารายละเอียดที่สำคัญ

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) กำหนดนโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

กำหนดนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งาน โดยให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) กำหนดนโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

กำหนดนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) กำหนดนโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

กำหนดนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงเพิ่มเติม ในส่วนที่มีผลกระทบในเนื้อหา รายละเอียดที่สำคัญ

(๔) กำหนดนโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

กำหนดนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

(๕) กำหนดผู้รับผิดชอบ

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๖. มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อยดังนี้

(๑) มีการจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน และมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

/(๒) ในการกำหนด...

- (๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงาน
- (๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้น การเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง
- (๔) ต้องกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

ข้อ ๗. บริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

- (๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิด จากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิง ป้องกันตามความเหมาะสม
- (๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียน ผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการ ยกเลิกเพิกถอนการอนุญาตดังกล่าว
- (๓) การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิ์ อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง
- (๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม
- (๕) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวน สิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาลักษณะอย่างน้อยดังนี้

- (๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้ ใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ
- (๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มี สิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล
- (๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อ ว่างเว้นจากการใช้งาน
- (๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษา ความลับทางราชการ พ.ศ. ๒๕๔๔

/ข้อ ๘. ควบคุม...

ข้อ ๙. ควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

- (๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- (๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้
- (๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่าย เพื่อใช้ในการระบุอุปกรณ์บนเครือข่ายของหน่วยงานได้
- (๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย
- (๕) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
- (๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง
- (๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐. มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

- (๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย
- (๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง
- (๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ
- (๔) การใช้งานโปรแกรมรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว
- (๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

/(๖) การจำกัด ...

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑. มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

- (๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้
- (๒) ระบบซึ่งไวต่อการถูกรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ
- (๓) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- (๔) การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกหน่วยงาน

ข้อ ๑๒. จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

- (๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
- (๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
- (๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- (๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง
- (๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๓. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาลักษณะอย่างน้อยดังนี้

- (๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง
- (๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

/ข้อ ๑๔. กำหนดให้ ...

ข้อ ๑๔. กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตราย ใดๆ แก่สำนักงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน การปฏิบัติตามแนวนโยบายและ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ทั้งนี้ ให้รองเลขาธิการสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ ในตำแหน่ง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) ของสำนักงาน ป.ป.ท. เป็นผู้รับผิดชอบต่อนโยบาย ในฐานะกำกับ ดูแล ติดตาม ทบทวน แนวนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงาน ป.ป.ท.

ประกาศ ณ วันที่ ๘ มีนาคม พ.ศ. ๒๕๖๔

พันตำรวจโท 
(วันนพ สมจินตนากุล)

เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

เอกสารแนบท้ายประกาศ

เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๔

สารบัญ

	หน้า
ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ.....	๓
๑. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control).....	๓
๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management).....	๕
๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities).....	๖
๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control).....	๙
๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control).....	๑๒
๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control).....	๑๓
๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control).....	๑๔
๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security).....	๑๕
๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย.....	๑๗
๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา.....	๑๙
๑๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ.....	๒๑
๑๒. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail).....	๒๑
๑๓. การใช้งานระบบอินเทอร์เน็ต (Internet).....	๒๒
๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network).....	๒๓
๑๕. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log).....	๒๓
๑๖. การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection System : IDS and Intrusion Prevention System : IPS).....	๒๓
ส่วนที่ ๒ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ.....	๒๕
ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ.....	๒๗
ส่วนที่ ๔ นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์.....	๒๘
ส่วนที่ ๕ การกำหนดผู้รับผิดชอบ.....	๒๙

ส่วนที่ ๑

นโยบายควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศของหน่วยงาน
๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับหน่วยงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

- ๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน
- ๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้
 - (๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง
 - อ่านอย่างเดียว
 - สร้างข้อมูล
 - ป้อนข้อมูล
 - แก้ไข
 - อนุมัติ
 - ไม่มีสิทธิ์
 - (๒) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้
 - (๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย
- ๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล
 - (๑) จัดแบ่งประเภทของข้อมูล
 - ข้อมูลสารสนเทศด้านการบริหาร ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

/- ข้อมูลสารสนเทศ...

- ข้อมูลสารสนเทศด้านการป้องกันและปราบปรามการทุจริตในภาครัฐที่ให้บริการ ข้อมูลการรับเรื่องร้องเรียน

(๒) จัดแบ่งระดับความสำคัญของข้อมูล

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึงหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึงหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึงหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึงข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับขั้นการเข้าถึงข้อมูล โดยแบ่งสิทธิการเข้าถึงตามประเภทของข้อมูล

- ประเภทของข้อมูลทั่วไป กำหนดสิทธิ์ให้สามารถเข้าถึงข้อมูลได้ทุกคน
- ประเภทของข้อมูลที่ต้องกำหนดสิทธิการเข้าถึง มีระดับการเข้าถึงดังนี้
 - ระดับผู้ปฏิบัติงาน
 - ระดับผู้ตรวจสอบข้อมูล
 - ระดับผู้ลงนามรับรองผล/อนุมัติ
 - ระดับในการเข้าถึงรายงานสรุปผล
 - ระดับผู้ดูแลระบบระดับหน่วยงาน
 - ระดับผู้ดูแลระบบย่อย ตามคำสั่งหน่วยงานผู้รับผิดชอบข้อมูล
 - ระดับผู้ดูแลระบบสูงสุด

ในกรณีผู้ใช้งานมีความจำเป็นต้องใช้สิทธิ์สูงกว่าปกติ ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่งหรือพ้นจากอำนาจหน้าที่

(๕) การกำหนดเวลาที่ได้เข้าถึง

- ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอดเวลา
- ระบบงานภายในสำนักงาน ป.ป.ท. (Back Office) สามารถเข้าถึงได้ตลอดเวลา

(๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

- ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)
- ระบบโทรศัพท์ (เข้าถึงได้ในเวลาราชการ)
- หนังสือหรือบันทึกข้อความ (เข้าถึงได้ทุกช่วงเวลา)
- ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

- ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
- ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
- ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)
- เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนดเวลา)
- การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และช่วงเวลาพิเศษเป็นรายครั้ง)

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) ดังนี้

- (๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ
- (๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและเพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต มีแนวปฏิบัติอย่างน้อย ดังนี้

- ๒.๑ ให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
- ๒.๒ กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่องต่อไปนี้
 - (๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิ์และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
 - (๒) ต้องระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
 - (๓) การกำหนดชื่อผู้ใช้งาน (Username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น
 - (๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น
 - (๕) ต้องตรวจสอบและมอบหมายสิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และหรือความต้องการทางธุรกิจ
 - (๖) จัดทำเอกสารแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย
 - (๗) ต้องทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ
 - (๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย
 - (๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง
- ๒.๓ ต้องบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ์เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

/(๑) กำหนดให้มี...

(๑) กำหนดให้มีกระบวนการบริหารจัดการสิทธิ์หรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งาน ได้แก่

- จัดให้มีระบบบริหารจัดการสิทธิ์จากส่วนกลางที่เป็นมาตรฐาน
- กำหนดสิทธิ์ในการเข้าถึงที่เหมาะสมต่อความจำเป็นในการใช้งานเท่านั้น
- ทบทวนสิทธิ์ หรือปรับปรุงสิทธิ์ให้ทันสมัยและถูกต้องอยู่เสมอ

(๒) ต้องกำหนดระดับสิทธิ์ในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

(๓) การมอบหมายสิทธิ์ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๒.๔ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) มีขั้นตอนปฏิบัติสำหรับการติดตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๕ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีแนวปฏิบัติอย่างน้อย ดังนี้

๓.๑ กำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ตั้งรหัสผ่านที่ยากต่อการคาดเดา

/ (๓) กำหนดรหัสผ่าน...

- (๓) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
 - (๔) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
 - (๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน
 - (๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
 - (๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
 - (๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์
 - (๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)
 - (๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
 - (๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้วทำการเปลี่ยนรหัสผ่านโดยทันที
 - (๑๒) เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
 - (๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ตนใช้งาน
 - (๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิม
 - (๑๕) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถึงกว่าผู้ใช้งานทั่วไป
- ๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้
- (๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
 - (๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว
 - (๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน
 - (๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน
 - (๕) ตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้
 - (๖) ต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว
- ๓.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้
- (๑) มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้เกิดการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ เช่น
 - การจัดการบริเวณล้อมรอบ

- การควบคุมการเข้า-ออก
 - การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
 - การวางอุปกรณ์
 - ระบบและอุปกรณ์สนับสนุนการทำงาน
- (๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้
- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
 - กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
 - วัฒนธรรมองค์กร
- (๓) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
- (๔) มีการกำหนดขอบเขตของการป้องกัน ดังนี้
- ทุกคนต้องตระหนักและปฏิบัติตามใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
 - ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
 - จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
 - ล็อกเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
 - ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
 - ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
 - ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
 - นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- (๕) มาตรการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์
- ต้องทำการล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนการส่งซ่อมหรือเปลี่ยนอุปกรณ์
 - ต้องทำการลบข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนการทำลายหรือจำหน่าย
 - ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล และเจ้าของข้อมูลในการลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล
- ๓.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ดังนี้
- (๑) มีหลักเกณฑ์ในการกำหนดเรื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด
- (๒) มีข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด ดังนี้
- ผู้ดูแลระบบ
- (๒.๑) ต้องกำหนดให้มีการเข้ารหัสในสิ่งต่อไปนี้
- (๒.๑.๑) การเชื่อมต่อแบบ VPN
 - (๒.๑.๒) การรับ – ส่งข้อมูลระดับชั้นความลับบนเครือข่ายคอมพิวเตอร์
 - (๒.๑.๓) รับ – ส่งข้อมูลระดับชั้นความลับตั้งแต่ “ลับ” ขึ้นไปทุกกรณี
- /(๒.๒) การประเมิน...

- (๒.๒) การประเมินผลิตภัณฑ์ในการเข้ารหัสข้อมูล ต้องพิจารณาจากสิ่งต่อไปนี้
 - (๒.๒.๑) วิธีการและความแข็งแกร่งในการเข้ารหัส
 - (๒.๒.๒) ขนาดคีย์ (Key Space) และความน่าเชื่อถือของผู้ผลิต
- (๒.๓) ศึกษา วิเคราะห์อัลกอริทึมเพื่อใช้ในการเข้ารหัสข้อมูล ลดความเสี่ยงจากการรั่วไหลของข้อมูล
- (๒.๔) พิจารณาให้มีการใช้งานเว็บไซต์ผ่านโปรโตคอล https สำหรับระบบที่ให้ความสำคัญ

ผู้ใช้งาน

- ๒.๕ ปฏิบัติตามขั้นตอนการใช้งานอย่างเคร่งครัด
- ๒.๖ หากพบปัญหาหรือสิ่งผิดปกติ ให้แจ้งต่อผู้ดูแลระบบทันที
- ๒.๗ มีความระมัดระวังในการใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ

๔. การควบคุมการเข้าถึงเครือข่าย (network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต มีแนวปฏิบัติอย่างน้อย ดังนี้

- ๔.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ดังนี้
 - (๑) ต้องกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้
 - (๒) มีข้อปฏิบัติสำหรับผู้ใช้ให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
 - (๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น ลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง
- ๔.๒ การยืนยันตัวตนบุคคลสำหรับผู้ใช้ที่อยู่นอกหน่วยงาน (User Authentication for External Connections) ต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่นอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ดังนี้
 - (๑) ผู้ใช้ที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง
 - (๒) ให้มีการตรวจสอบผู้ใช้ทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวตน (Authentication) เพื่อแสดงว่าเป็นผู้ใช้จริง โดยการเข้ารหัสผ่าน (Password)
 - (๓) ให้มีการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน ดังนี้

/ผู้ใช้งาน...

ผู้ใช้งาน

- ผู้มีสิทธิ์เข้าถึงระบบงานอินเทอร์เน็ตหรือระบบเครือข่ายจากภายนอก ต้องเป็นข้าราชการสำนักงาน ป.ป.ท. และได้รับอนุญาตในการเข้าถึงระบบนั้น ๆ
- การใช้งานจากเครือข่ายสาธารณะนอกสำนักงาน ผู้ใช้งานต้องเขียนเป็นลายลักษณ์อักษรเพื่อลงทะเบียนเปิดสิทธิ์ในระบบอินเทอร์เน็ต
- การเข้าถึงระบบงานจากระยะไกลต้องมีการพิสูจน์เครื่องคอมพิวเตอร์ว่าได้รับอนุญาตให้เข้าถึง และต้องพิสูจน์ตัวตนจากระบบอินเทอร์เน็ตของสำนักงาน
- ไม่เชื่อมต่ออินเทอร์เน็ตอื่น ขณะใช้งานอินเทอร์เน็ตของสำนักงาน

ผู้ดูแลระบบ

- ลงทะเบียนบัญชีผู้ใช้งานและเปิดสิทธิ์เพื่อเข้าสู่ระบบและควบคุมให้สามารถใช้งานได้เฉพาะเครื่องคอมพิวเตอร์ที่ลงทะเบียนไว้เท่านั้น
 - (๔) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย
- ๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้
- (๑) ใช้หมายเลขเฉพาะที่อ้างอิงถึงอุปกรณ์ที่เชื่อมต่อกับเครือข่าย Mac Address / IP Address ในการระบุว่าอุปกรณ์นี้ได้รับการอนุญาตให้เชื่อมต่อ
 - (๒) จัดทำทะเบียนอุปกรณ์ สถานที่ตั้งอุปกรณ์
 - (๓) ใช้ระบบบริหารจัดการอุปกรณ์จากส่วนกลาง และตรวจสอบอุปกรณ์ที่เชื่อมต่อด้วยอย่างสม่ำเสมอ
- ๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้
- (๑) กำหนดหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย ดังนี้
 - ผู้ดูแลระบบต้องกำหนดการเปิด - ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์
 - (๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย ดังนี้
 - ต้องยกเลิกหรือปิดพอร์ต และบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน
 - ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๒ ครั้ง

/ (๓) ปิดการใช้งาน...

- (ก) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร
- ๔.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก
- ๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้
- (๑) ต้องตรวจสอบการเชื่อมต่อเครือข่าย
 - (๒) จำกัดสิทธิ์ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย
 - (๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย
 - (๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย
 - (๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต
- ๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้
- (๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)
 - (๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย
 - (๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่าย
- ๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก ดังนี้
- (๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) ผู้ระบบสารสนเทศและเครือข่ายของหน่วยงาน ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
 - (๒) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น
 - (๓) วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด
 - (๔) ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายอย่างเป็นทางการ

/(๕) มีการควบคุม...

(๕) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(๖) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรมีเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต มีแนวปฏิบัติอย่างน้อย ดังนี้

๕.๑ ระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติอย่างน้อย ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card เป็นต้น

๕.๒ การบริหารจัดการรหัสผ่าน (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๕.๓ การใช้งานโปรแกรมมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้รู้สึกเสี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

(๑) จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) ซอฟต์แวร์ที่ติดตั้งต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกซอฟต์แวร์ต่าง ๆ และนำไปติดตั้งหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๕.๔ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out) มีแนวปฏิบัติอย่างน้อย ดังนี้

/(๑) ให้ยุติการใช้...

- (๑) ให้ยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- (๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ
- (๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๕.๕ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

- (๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น กำหนดให้ใช้งานได้ ๓ ชม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น
- (๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย
- (๓) กำหนดให้ระบบสารสนเทศ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๕.๖ กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยการเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคง ปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

- (๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่จะเข้าสู่ระบบจะเสร็จสมบูรณ์
- (๒) ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีภัยคุกคามคาดเดารหัสผ่านจากเครื่องปลายทาง
- (๓) จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยมีแนวปฏิบัติอย่างน้อย ดังนี้

- ๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้
- ๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

/ (๑) ต้องแยกระบบ...

- (๑) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน
 - (๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ
 - (๓) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว
- ผู้ใช้งาน
- ข้าราชการ กรอกแบบฟอร์มการขอใช้บริการอินเทอร์เน็ต จากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
 - เรียนรู้การใช้งานอินเทอร์เน็ตผ่านเครือข่ายสาธารณะ จากผู้ดูแลระบบ
 - ไม่ใช้งานอินเทอร์เน็ตระหว่างการใช้งานอินเทอร์เน็ตของสำนักงาน
 - การเชื่อมต่อคอมพิวเตอร์ประเภทพกพาที่ระบบอินเทอร์เน็ตของสำนักงาน ต้องติดตั้งโปรแกรมป้องกันไวรัสที่มีการอัปเดต Signature อย่างสม่ำเสมอและ Full Scan อย่างน้อยเดือนละครั้ง
 - ระยะเวลาการใช้งานอินเทอร์เน็ตของสำนักงาน จากเครือข่ายสาธารณะสามารถใช้งานได้ต่อเนื่องตามระยะเวลาที่กำหนด

ผู้ดูแลระบบ

- ลงทะเบียนบัญชีผู้ใช้งานและเปิดสิทธิ์เพื่อเข้าสู่ระบบและควบคุมให้สามารถใช้งานได้เฉพาะเครื่องคอมพิวเตอร์ที่ได้ลงทะเบียนไว้เท่านั้น
 - คืนเครื่องคอมพิวเตอร์แก่ผู้ใช้ พร้อมสอนการใช้งานอินเทอร์เน็ต
 - ทบทวนสิทธิ์การใช้งานอินเทอร์เน็ตของผู้ใช้งานทุกปี
- ๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ การเชื่อมต่อระบบเครือข่าย โดยใช้อุปกรณ์ต่อพ่วง เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่
- ๖.๔ การปฏิบัติงานจากภายนอกหน่วยงานต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกหน่วยงาน
๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)
- ๗.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย
 - ๗.๒ ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการดังต่อไปนี้
 - (๑) ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

/(๒) ต้องทำการ...

- (๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
- (๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
- (๔) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
- (๕) ควรเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้อาจเดาหรือเจาะรหัสได้โดยง่าย
- (๖) ต้องกำหนดค่าใช้ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น
- (๗) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
- (๘) ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน
- (๙) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์ทราบโดยทันที

๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environmental Security)

๘.๑ ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data center)

- (๑) ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น
- (๒) ให้ศูนย์เป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร
- (๓) ให้ศูนย์กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร
- (๔) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

/(๕) มีระบบสนับสนุน...

- (๕) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำและเครื่องดับเพลิงระบบปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้มั่นใจได้ว่า ระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- (๖) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๘.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

- (๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้
- (๒) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย
- (๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- (๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น
- (๕) จัดทำฝั้งสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง
- (๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก
- (๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ
- (๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๘.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

- (๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
- (๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามผู้ผลิตแนะนำ
- (๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง
- (๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- (๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน
- (๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘.๔ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

- (๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน
- (๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน
- (๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

/ (๔) เมื่อมีการนำ...

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๘.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๘.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลสำคัญนั้นได้

๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) ไม่ติดตั้งซอร์สโค้ด คอมไพเลอร์ (Compiler) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นๆ

(๕) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ เป็นต้น

/(๗) ให้ผู้ที่เกี่ยวข้อง...

- (๗) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ
 - (๘) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม
 - (๙) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุง ก่อนที่จะเริ่มต้นทำการพัฒนา
- ๙.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ
- (๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ
 - (๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่
- ๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก
- (๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก
 - (๒) ให้ระบุว่ามีใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก
 - (๓) ให้กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น
 - (๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง
- ๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค
- (๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศ เพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้
 - ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
 - สถานที่ที่ติดตั้ง
 - เครื่องที่ติดตั้ง
 - ผู้ผลิตซอฟต์แวร์
 - ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ
 - (๒) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที
 - (๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบการดำเนินการ ดังนี้
 - มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
 - ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน

- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๙.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ อย่างน้อยดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนคอนฟิกูเรชันของระบบ

(๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน

(๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๑๐) ข้อมูลไอพีแอดเดรสที่เข้าถึง

(๑๑) ข้อมูลโพรโตคอลเครือข่ายที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๙.๖ การจ้างเหมาดำเนินการพัฒนา บำรุงรักษา ระบบสารสนเทศและ ระบบเครือข่าย มีมาตรการควบคุม Outsource ดังนี้

(๑) กำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

(๒) สัญญาต้องระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตและเงื่อนไขการให้บริการ (Service level agreement) อย่างชัดเจน

๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑๐.๑ การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ผู้ใช้งาน ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

/(๔) การเคลื่อนย้าย...

- (๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น
- (๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- (๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่
- (๗) ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- (๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive
- (๙) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- (๑๐) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อน จัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- (๑๑) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้อจอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- (๑๒) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (๑๓) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
- (๑๔) ไม่ใช่หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น
- (๑๕) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น
- (๑๖) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๑๐.๒ การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น
- (๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
- (๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๑๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

- ๑๑.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- ๑๑.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของขงสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน เหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- ๑๑.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล
- ๑๑.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- ๑๑.๕ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
- ๑๑.๖ เอกสารที่มีระดับชั้นความลับจะต้องมีการใช้เทคโนโลยี Digital Signature หรือลายเซ็นอิเล็กทรอนิกส์ตามที่หน่วยงานกำหนด เพื่อพิสูจน์ยืนยันความถูกต้องของข้อมูล

๑๒. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๑๒.๑ การใช้งานสำหรับผู้ใช้งาน

- (๑) ผู้ใช้งานที่ต้องการใช้งาน E-mail ของหน่วยงานต้องทำการกรอกข้อมูลคำขอเข้าใช้งานและยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Password)
- (๒) เมื่อได้รับรหัสผ่าน (Password) จะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันที หลังจากการเข้าสู่ระบบเป็นครั้งแรก
- (๓) ต้องใช้ E-mail ของหน่วยงานเพื่อติดต่อกับงานของราชการเท่านั้น
- (๔) ไม่ควรใช้ E-mail Address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ E-mail และให้ถือว่าเจ้าของ E-mail เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ใน E-mail ของตน
- (๕) หลังจากการใช้งาน ควรลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ
- (๖) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- (๗) ควรตรวจสอบและลบ E-mail ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบ E-mail ให้เหลือจำนวนน้อยที่สุด
- (๘) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง
- (๙) ปฏิบัติตามวิธีการใช้งานรหัสผ่าน (Password use) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๒.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

- (๑) กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการ
เข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน
- (๒) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๕ ครั้ง
- (๓) มีการทบทวนสิทธิ์การเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อ
มีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง
เป็นต้น
- (๔) มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (User Access
Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๓. การใช้งานระบบอินเทอร์เน็ต (Internet)

- ๑๓.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อ
ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น
ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem
ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับการอนุมัติจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบ
ที่ได้รับมอบหมายแล้วเท่านั้น
- ๑๓.๒ การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่
ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ของระบบปฏิบัติการ
- ๑๓.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของ
ระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ต
ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่
เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัย
ต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิด
สิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น
- ๑๓.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ
อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต
- ๑๓.๕ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการ
ดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สิน
ทางปัญญา
- ๑๓.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็น
ความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ุให้ร้าย ที่จะทำให้เกิดความ
เสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ
- ๑๓.๗ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการ
เข้าใช้งานโดยบุคคลอื่นๆ

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

- ๑๔.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น
- ๑๔.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์
- ๑๔.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๕. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้มีแนวปฏิบัติอย่างน้อย ดังนี้

- ๑๕.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง
 - ๑๕.๒ ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย
 - ๑๕.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง
 - ๑๕.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
- #### ๑๖. การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection System : IDS and Intrusion Prevention System : IPS) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้
- ๑๖.๑ ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ (IDS/IPS) เหตุการณ์ผิดปกติและการแจ้งเตือนต่างๆ ที่อุปกรณ์ตรวจพบจะถูกทำการวิเคราะห์และหาสาเหตุของการบุกรุกในระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด ซึ่งเป็นการป้องกันก่อนที่จะเกิดการโจมตี
 - ๑๖.๒ ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่บุกรุกหรือโจมตีหน่วยงานเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น Firewall เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตรายที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ Hacker รวมทั้งไวรัสประเภทต่างๆ เป็นต้น
 - ๑๖.๓ ผู้ดูแลระบบต้องมีการบริหารจัดการเหตุการณ์บุกรุกระบบ (Incident Management) เป็นการตอบสนองต่อเหตุการณ์บุกรุกทางเครือข่าย สามารถช่วยวิเคราะห์ลักษณะการบุกรุกทางเครือข่าย และทำให้สามารถแก้ไขสถานการณ์ได้อย่างถูกต้อง ลดความเสี่ยงและผลกระทบที่

/อาจเกิดขึ้นจาก...

อาจเกิดขึ้นจากการบุกรุก โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับหน่วยงานและจัดทำวิธีปฏิบัติที่ถูกต้องให้กับหน่วยงานเพื่อป้องกันเหตุการณ์เกิดซ้ำ การตอบสนองต่อเหตุการณ์การบุกรุกแบ่งเป็น ๔ ขั้นตอน คือ

(๑) จำกัดขอบเขต (Containment) จำกัดพื้นที่ที่เสี่ยงต่อการบุกรุกและจำกัดความรุนแรงของการบุกรุก

(๒) กำจัดต้นเหตุ (Eradication) กำจัดต้นเหตุของการบุกรุก รวมถึงปิดกั้นช่องทางของการบุกรุก

(๓) กู้คืนระบบ (Recovery) แก้ไขระบบที่ถูกบุกรุกให้สามารถกลับมาทำงานได้ตามปกติ

(๔) ติดตามผล (Follow - Up) บันทึกผลกระทบของเหตุการณ์และแนะนำวิธีปฏิบัติเพื่อป้องกันเหตุการณ์เกิดซ้ำ

๑๖.๔ ผู้ดูแลระบบต้องกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละ ๑ ครั้ง

๑๖.๕ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๑๖.๖ การใช้เครื่องมือต่างๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๑๖.๗ ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอต้องประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง

ส่วนที่ ๒

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงาน ให้บริการได้อย่างต่อเนื่อง
๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. กลุ่มงานคอมพิวเตอร์และการสื่อสาร
๓. กลุ่มงานบริหารเทคโนโลยีและพัฒนาระบบ

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้
 - ๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง
 - ๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้
 - กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
 - กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
 - บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
 - ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น
 - จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่/เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
 - จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

/- ดำเนินการ...

- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
 - ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
 - จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองเก็บไว้
 - ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
 - กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้
๒. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้
- ๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้
- (๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
 - (๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
 - (๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
 - (๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
 - (๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
 - (๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น
- ๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง
๓. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง
๕. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ตรวจสอบภายใน โดย กลุ่มงานตรวจสอบภายใน สำนักงาน ป.ป.ท.
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อยดังนี้
 - ๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง
 - ๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ
๒. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้
 - ๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง
 - ๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
 - ๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
 - ๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้
 - (๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
 - (๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลาย ลบ โดยทันทีที่ตรวจสอบเสร็จ และต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
 - (๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
 - (๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
 - (๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนี้จากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๔

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของหน่วยงาน
๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน
๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง หรือ ทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน
๓. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
๔. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดให้ความรู้
๕. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ
๖. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๕ การกำหนดผู้รับผิดชอบ

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. ระดับนโยบาย

ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร เป็นผู้รับผิดชอบในการสั่งการตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงาน ป.ป.ท. รวมถึงการกำกับติดตาม ดูแล ควบคุม ตรวจสอบ และให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๒. ระดับปฏิบัติ

๒.๑ กลุ่มงานคอมพิวเตอร์และการสื่อสาร รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

- ๒.๑.๑ ควบคุมการเข้า – ออกห้องแม่ข่ายตามการกำหนดสิทธิ์การเข้าถึงเครื่องแม่ข่าย
- ๒.๑.๒ กำกับดูแล ตรวจสอบ บำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์เชื่อมต่อเครือข่าย (Network) ที่ให้บริการในสำนักงาน ป.ป.ท. ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง
- ๒.๑.๓ กำกับดูแล การติดตั้ง รื้อถอน ตรวจสอบ การเชื่อมต่อเครือข่ายสื่อสารผ่านเครือข่ายทางระบบเครือข่ายที่ให้บริการในสำนักงาน ป.ป.ท.
- ๒.๑.๔ กำกับดูแลการแก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมต่อเครือข่ายของสำนักงาน ป.ป.ท.
- ๒.๑.๕ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบในกรณีที่มีภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๑.๖ กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต
- ๒.๑.๗ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมด ที่ให้บริการสามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง
- ๒.๑.๘ กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบ
- ๒.๑.๙ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามกรอบระยะเวลาที่กำหนด

๒.๑.๑๐ บริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๒.๑.๑๑ อื่นๆ ตามที่ได้รับมอบหมาย

๒.๒ กลุ่มงานบริหารเทคโนโลยีและพัฒนาระบบ รับผิดชอบดังนี้

๒.๒.๑ กำกับ แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศที่เกิดจากการถูกเจาะระบบจากบุคคลภายนอก (Hack) และการถูกทำลายจากโปรแกรมไวรัส

๒.๒.๒ กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิ์การเข้าถึงระบบสารสนเทศ

๒.๒.๓ กำกับการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบงานสารสนเทศ

๒.๒.๔ รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบฐานข้อมูลและสารสนเทศที่ถูกทำลายจากบุคคลภายนอก (Hacker) และจากไวรัส (Virus)

๒.๒.๕ ประสานการปฏิบัติงานตามแผนจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๒.๖ รายงานผลการปฏิบัติงานตามแผนให้ผู้บังคับบัญชาทราบ

๒.๒.๗ อื่นๆ ตามที่ได้รับมอบหมาย

๓. การกำหนดผู้รับผิดชอบ

๓.๑ รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

นายภูมิวิศาล เกษมสุข รองเลขาธิการคณะกรรมการ ป.ป.ท.

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม

นายจิรวัดน์ สุภาพ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒ ผู้รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้รับผิดชอบ ได้แก่

นายมรุต อากาศุล นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

นายนักสิทธิ์ อึ้งสกุล นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

๓.๓ รับผิดชอบดูแลบำรุงรักษา ระบบเครื่อง ระบบเครือข่ายและการสำเนาฐานข้อมูล ผู้รับผิดชอบ ได้แก่

นายพชฎ ศรีพันธ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายวิกร แก้วกำไร นักวิชาการคอมพิวเตอร์ปฏิบัติการ

หน้าที่รับผิดชอบ มีดังนี้

๓.๓.๑ ควบคุมการเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์ตามการกำหนดสิทธิ์การเข้าถึงห้องควบคุมระบบคอมพิวเตอร์

๓.๓.๒ ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ เครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมด

๓.๓.๓ ควบคุม ติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิ์การเข้าถึงระบบ

/๓.๓.๔ ทำการสำรอง...

๓.๓.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๓.๓.๕ ป้องกันการถูกเจาะระบบ และ แก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๓.๓.๖ ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก

๓.๔ รับผิดชอบในการรักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล ผู้รับผิดชอบ ได้แก่

นางสาวณัฐกฤตา วงษ์สายตา นักวิชาการคอมพิวเตอร์ชำนาญการ

นายวิกร แก้วกำไร นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายอานันท์ มากบัวแก้ว นักวิชาการคอมพิวเตอร์ปฏิบัติการ

หน้าที่รับผิดชอบ มีดังนี้

๓.๔.๑ ทำการสำรองข้อมูลและเรียกคืนข้อมูลของระบบฐานข้อมูลสารสนเทศ (Backup and Recovery)

๓.๔.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓.๕ รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต ผู้รับผิดชอบ ได้แก่

นายพชฎ ศรีพันธุ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายศรนรินทร์ วุฒิเพย นักวิชาการคอมพิวเตอร์ปฏิบัติการ

หน้าที่รับผิดชอบ มีดังนี้

ควบคุมการใช้งานของผู้ใช้งานระบบอินเทอร์เน็ต ของสำนักงาน ป.ป.ท.รวมถึงบุคคลภายนอกที่เข้ามาขอใช้งาน

๓.๖ รับผิดชอบความปลอดภัยทั่วไป ผู้รับผิดชอบ ได้แก่

นางสาวพรทิพย์ อยู่สุข นักจัดการงานทั่วไปชำนาญการ

หน้าที่รับผิดชอบ มีดังนี้

ติดต่อประสานงานกับทางฝ่ายอาคาร สถานที่ หากเกิดเหตุการณ์ต่าง ๆ อาทิเช่น ไฟฟ้าดับ
สถานการณ์ทางการเมือง
