(สำเนา)

ประกาศกรมบังคับคดี
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๖

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัยเช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้ ดังนั้น ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีความสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ อธิบดีกรมบังคับคดีจึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศกรมบังคับคดี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

(๑) **"ผู้ใช้งาน"** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร ผู้รับบริการและผู้ใช้งานทั่วไปของกรมบังคับคดี

(๒) **"บัญชีผู้ใช้งาน"** หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

(๓) **"สิทธิของผู้ใช้งาน"** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๔) **"สินทรัพย์"** หมายความว่า เครื่องคอมพิวเตอร์ อุปกรณ์ประกอบคอมพิวเตอร์ อุปกรณ์เครือข่ายคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์

(๕) **"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ"** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๖) **"ความมั่นคงปลอดภัยด้านสารสนเทศ"** หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๗) **"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)"**หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๘) **"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)"** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

(๙) **"ข้อมูลอิเล็กทรอนิกส์"** หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

(๑๐) **"นโยบาย"** หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๑๑) **"ผู้บริหาร"** หมายความว่า อธิบดีหรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมบังคับคดี

(๑๒) **"หน่วยงาน"** หมายความว่า กรมบังคับคดีรวมถึงหน่วยงานในสังกัดกรมบังคับคดี

(๑๓) **"ผู้บริหารระดับสูงสุด"** หมายความว่า ผู้บริหาร ของหน่วยงาน ระดับสูงสุด (CEO) หรืออธิบดีกรม รับผิดชอบเกี่ยวกับความเสี่ยงและความเสียหายอันเกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

(๑๔) **"ศูนย์"** หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๑๕) **"ระบบอินเทอร์เน็ต (Internet)"** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๑๖) **"ระบบสารสนเทศ "** หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

(๑๗) **"ผู้ดูแลระบบ (System Administrator)"** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

(๑๘) **"หน่วยงานภายนอก"** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

(๑๙) **"จดหมายอิเล็กทรอนิกส์ (E-Mail)"** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP , POP๓ และ IMAP เป็นต้น

(๒๐) **"สื่อบันทึกพกพา"** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น

(๒๑) **"ชื่อผู้ใช้ (Username)"** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

(๒๒) **"รหัสผ่าน (Password)"** หมายความว่า ตัวอักษรหรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๒๓) **"การเข้ารหัส (Encryption)"** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

(๒๔) **"อุปกรณ์จัดเส้นทาง (Router)"** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

(๒๕) **"การพิสูจน์ยืนยันตัวตน (Authentication)"** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

(๒๖) **"SSID (Service Set Identifier)"** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

(๒๗) **"WPA (Wi-Fi Protected Access)"** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

(๒๘) **"MAC Address (Media Access Control Address)"** หมายความว่าหมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด (Internet Card) โดยแต่ละการ์ดจะมีหลายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่รูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

(๒๙) **"SSL-VPN (Secure Socket Layer Virtual Private Network)"** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

(๓๐) **"แผนผังระบบเครือข่าย (Network Diagram)"** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

(๓๑) **"ระบบเครือข่ายแบบรวมศูนย์ (Active Directory)"** หมายความว่า ข้อมูลที่ถูกจัดเก็บในระบบเครือข่าย ผู้ที่สามารถเข้าใช้งานจะต้องผ่านกระบวนการพิสูจน์ตัวตนจากเครื่องแม่ข่าย

(๓๒) **"Token"** หมายความว่า อุปกรณ์ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งานก่อนการเข้าใช้งาน

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๑.๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๑.๒) จัดทำนโยบายเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของกรมบังคับคดี

(๑.๓) กำหนดให้เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ของศูนย์เป็นผู้รับผิดชอบตามนโยบายและแนวปฏิบัติประกอบด้วย

- เจ้าหน้าที่ปฏิบัติการด้านพัฒนาโปรแกรมและฐานข้อมูล
- เจ้าหน้าที่ปฏิบัติการด้านระบบเครือข่าย
- เจ้าหน้าที่ปฏิบัติการด้านการซ่อมบำรุง

(๑.๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

(๒) รายละเอียดของแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒.๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒.๑.๑) การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

(๒.๑.๒) การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

(๒.๑.๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๒.๑.๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

(๒.๑.๕) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๒.๑.๖) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๒.๑.๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๒.๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ กำหนดให้มีการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์ พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง พร้อมทั้งทบทวนและทดสอบอย่างน้อยปีละ ๑ ครั้ง

(๒.๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๒.๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือการใช้งานและการจัดการฝึกอบรม

ข้อ ๕ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ต้องระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ทั้งนี้สำหรับผู้ปฏิบัติงานใหม่ทุกคนจะต้องเข้ารับการอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศก่อนปฏิบัติงานทุกครั้ง

ข้อ ๗ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๘ มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายในนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ต (Port) ที่สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อย ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๑ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๓ กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศ ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือกรณีอื่นใดตามประกาศ กฎระเบียบหรือกฎหมายที่เกี่ยวข้องกำหนด

ข้อ ๑๔ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกรมบังคับคดี โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศเรื่อง “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยเชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

ข้อ ๑๕ บทบาทหน้าที่ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติ ดังนี้

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) มีหน้าที่กำกับดูแลการใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบ การใช้งานระบบงานสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของกรมบังคับคดีตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี

ประกาศ ณ วันที่ ๑๑ เดือน เมษายน พ.ศ. ๒๕๖๖

(ลงชื่อ) ทัศนีย์ เปาอินทร์

(นางทัศนีย์ เปาอินทร์)
อธิบดีกรมบังคับคดี

สำเนาถูกต้อง

(นางสาวอรอุมา เกงทางดี)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

กฤติน ร่าง/พิมพ์
อรอุมา ทาน

เอกสารแนบท้ายประกาศ

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมบังคับคดี
พ.ศ.2566

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอ ในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมมั่นคงปลอดภัยในระบบสารสนเทศ ที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553 ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

กรมบังคับคดีจึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมบังคับคดีประจำปี พ.ศ.2566 ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในกรมบังคับคดี และบุคลากรทุกคนในกรมบังคับคดีมีความรู้ เข้าใจในนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี สามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

กรมบังคับคดี

สารบัญ

หน้า

บทนำ

1. หลักการและเหตุผล 1
2. วัตถุประสงค์ 1
3. องค์ประกอบของนโยบาย 2
4. บทบังคับใช้ 2
5. การเผยแพร่และทบทวน 2

คำนิยาม 3

ส่วนที่ 1 นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ 6

1. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control) 6
2. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for access control 8
3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) 9
4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) 12
5. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) 16
6. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operation system access control) 21
7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ 21
8. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย 25
9. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental security) 29
10. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless) 30
11. การควบคุมการใช้งานเครื่องคอมพิวเตอร์แบบพกพา 30
12. การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล 31
13. การควบคุมการเข้า-ออกห้องศูนย์คอมพิวเตอร์ 32
14. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) 32

หน้า

15. การใช้งานระบบอินเตอร์เน็ต (Internet) 33
16. การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ (Conversion) 33
17. การนำข้อมูลต่างๆ เผยแพร่ลงในเว็บไซต์ (Web Information) 33
18. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) 34
19. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) 34
20. การจัดการระบบเครือข่ายแบบรวมศูนย์ (Active Directory : AD) 34
21. การใช้งาน Token 35
ส่วนที่ 2 นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ 36
ส่วนที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ 39
ส่วนที่ 4 นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ 41

บทนำ

1. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ในมาตรา 5 *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กร ซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

2. วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี ฉบับนี้มีวัตถุประสงค์เพื่อ

1) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดีที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

2) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศ เทคโนโลยีและการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

3) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของกรมบังคับคดี มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศกรมบังคับคดี และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

3. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ อ้างอิงตามที่พระราช

กฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553 โดยแนวทางปฏิบัตินี้ ประกอบด้วย วัตถุประสงค์ ผู้รับผิดชอบ และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

4. บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของกรมบังคับคดี บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้ โดยอธิบดีกรมบังคับคดี

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อธิบดีกรมบังคับคดีเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

5. การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) กรมบังคับคดี จัดพิมพ์เผยแพร่เพื่อให้บุคลากรกรมบังคับคดี บุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

คำนิยาม

1. **องค์กร หรือ หน่วยงาน** หมายถึง กรมบังคับคดี

2. **ผู้ใช้งาน** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร ผู้รับบริการ และผู้ใช้งานทั่วไปของกรมบังคับคดี

3. **บัญชีผู้ใช้งาน** หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

4. **สิทธิ์ของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

5. **สินทรัพย์** หรือ ทรัพย์สิน หมายความว่า เครื่องคอมพิวเตอร์ อุปกรณ์ประกอบคอมพิวเตอร์ อุปกรณ์เครือข่ายคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์

6. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

7. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

8. **เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

9. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

10. **ข้อมูลอิเล็กทรอนิกส์** หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

11. **นโยบาย** หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

12. **ผู้บริหาร** หมายความว่า อธิบดีหรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรม

13. **หน่วยงาน** หมายความว่า กรมบังคับคดี รวมถึงหน่วยงานในสังกัดกรมบังคับคดี

14. **ผู้บริหารระดับสูงสุด** หมายความว่า ผู้บริหารของหน่วยงานระดับสูงสุด (CEO) หรืออธิบดีกรม รับผิดชอบเกี่ยวกับความเสี่ยงและความเสียหายอันเกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

15. **ศูนย์** หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

16. **ระบบอินเทอร์เน็ต (Internet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

17. ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

18. ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

19. หน่วยงานภายนอก หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

20. จดหมายอิเล็กทรอนิกส์ (E-Mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

21. สื่อบันทึกพกพา หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น

22. ชื่อผู้ใช้ (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

23. รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

24. การเข้ารหัส (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

25. อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

26. การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

27. SSID (Service Set Identifier) หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

28. WPA (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

29. MAC Address (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด (Internet Card) โดยแต่ละการ์ดจะมีหลายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่รูปของ เลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

30. SSL-VPN (Secure Socket Layer Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

31. แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

32. ระบบเครือข่ายแบบรวมศูนย์ (Active Directory) หมายความว่า ข้อมูลที่ถูกจัดเก็บในระบบเครือข่าย ผู้ที่สามารถเข้าใช้งานจะต้องผ่านกระบวนการพิสูจน์ตัวตนจากเครื่องแม่ข่าย

33. Token หมายความว่า อุปกรณ์ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งาน ก่อนการเข้าใช้งาน

34. Outsource คือ องค์กร หรือหน่วยงานภายนอกที่กรมบังคับคดีอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของกรมบังคับคดี

35. การเชื่อมโยงข้อมูล คือ การเชื่อมโยงข้อมูลจากฐานข้อมูลหนึ่ง ไปยังอีกฐานข้อมูลหนึ่งได้อย่างรวดเร็ว

36. บันทึกข้อตกลง (Memorandum of Understanding : MOU) คือ เอกสารหรือหนังสือบันทึกข้อตกลง ความเข้าใจที่ตรงกัน หรือ ข้อตกลงที่จะร่วมมือระหว่างกัน โดยที่แต่ละฝ่ายอาจเป็นองค์กร หน่วยงานของรัฐ หน่วยงานหรือบริษัทเอกชน หรือระหว่างรัฐกับรัฐ

37. DCIO คือ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม

ส่วนที่ 1

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

2. เพื่อให้ผู้รับผิดชอบและผู้ที่มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

1. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

1.1 จัดทำบัญชีทรัพย์สิน ซึ่งจะจำแนกกลุ่มทรัพยากรของระบบและการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิของผู้ใช้งาน

1.2 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว สำหรับ กลุ่มผู้บริหาร
- สร้างข้อมูล สำหรับ กลุ่มผู้ดูแลระบบ
- ป้อนข้อมูล สำหรับ กลุ่มหัวหน้างานและกลุ่มผู้ปฏิบัติงาน
- แก้ไข สำหรับ กลุ่มผู้ดูแลระบบ,กลุ่มผู้อำนวยการและกลุ่มหัวหน้างาน
- อนุมัติ สำหรับ กลุ่มผู้อำนวยการ
- ไม่มีสิทธิ

(2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้อง

- ขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตและกำหนดสิทธิการใช้งานเบื้องต้นจากผู้บังคับบัญชาก่อน
- ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร
- สำหรับรหัสการใช้งานจะแจ้ง โดยการใส่ซองปิดผนึกส่งกลับไปยังผู้ที่ขออนุญาตใช้งานสารสนเทศ

- กรณีตรวจสอบสิทธิการใช้งานแล้ว บุคคลดังกล่าวไม่มีสิทธิการใช้งานจะแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร

1.3 ขั้นตอนปฏิบัติเพื่อการบริหารจัดการข้อมูล

(1) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการให้บริการ เช่น ข้อมูลตรวจบุคคลล้มละลาย ข้อมูลตรวจฟื้นฟูกิจการของลูกหนี้ ข้อมูลประกาศขายทอดตลาด เป็นต้น

(2) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(3) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

กำหนดให้ผู้ใช้งานนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.2544 ซึ่งมีแนวปฏิบัติ ดังนี้

1. ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน
2. กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล
3. การจัดเก็บ username และ password ของระบบสารสนเทศในฐานข้อมูลตามภารกิจหลัก จะต้องทำการเข้ารหัสด้วย SHA256 เป็นอย่างน้อย ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง
4. ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล https สำหรับระบบสารสนเทศ แบบ web application เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราว์เซอร์และเว็บเซิร์ฟเวอร์
5. กำหนดช่องทางการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสม สำหรับช่องทางดังต่อไปนี้
   - ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต
   - เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย

(4) จัดแบ่งระดับชั้นการเข้าถึง ผู้ดูแลระบบได้บริหารจัดการสิทธิ์ของผู้ใช้งาน ดังต่อไปนี้

(4.1) ระดับชั้นสำหรับผู้บริหาร ได้แก่

- ผู้บริหารระดับสูง (อธิบดี, รองอธิบดี, ผู้บริหารเทคโนโลยีระดับสูง เป็นต้น)
- ผู้บริหารระดับกลาง (ผู้อำนวยการ)

(4.2) ระดับชั้นสำหรับผู้ใช้งานทั่วไป ได้แก่

- ระดับชำนาญการ
- ระดับปฏิบัติการ (เจ้าหน้าที่ทั่วไป)
- Outsource
- บุคคลภายนอก (ประชาชนทั่วไป หรืออื่นๆ)

(4.3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

- ผู้ดูแลระบบ
- ผู้ที่ได้รับมอบหมาย (มีกำหนดเวลาในการใช้งาน)

(5) การกำหนดเวลาที่ได้เข้าถึง

- ช่วงเวลาในเวลาราชการ คือ ในวันจันทร์ - ศุกร์ เวลา 08.30 - 16.30 น.
- ช่วงเวลานอกเวลาราชการที่ได้รับอนุญาต คือ ในวันจันทร์ - ศุกร์ เวลา 16.31 - 20.00 น.
- วันหยุดราชการและวันหยุดนักขัตฤกษ์ที่ได้รับอนุญาต เวลา 08.30 - 16.30 น.

(6) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

- ผ่านช่องทาง Wire Line, Wireless Line โดยมีการจัดเก็บ Log
- ผ่านหน้าเว็บอินทราเน็ต โดยมีการตรวจสอบสิทธิเข้าใช้งาน

2. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for access control)

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศขององค์กร และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย การใช้งานตามภารกิจเอควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติดังนี้

2.1 การควบคุมการเข้าถึงสารสนเทศ

1. กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานให้สอดคลองกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้งานระบบสารสนเทศของหน่วยงาน

2. ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

3. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

2.2 จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภาระกิจดังนี้

1. กลุ่มผู้บริหาร ได้แก่ อธิบดี, รองอธิบดี, ผู้ตรวจราชการ, ผู้เชี่ยวชาญ และผู้อำนวยการสำนัก/กอง/สาขา
2. กลุ่มของผู้ดูแลระบบศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
3. กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของหน่วยงาน
4. กลุ่มที่ปรึกษาหรือผู้ว่าจ้างที่มีระยะสัญญาจ้างกับหน่วยงาน
5. ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

2.3 การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

1. ทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อได้รับเอกสารแจ้งจากหน่วยงานต้นสังกัดของผู้ใช้งานระบบ เพื่อปรับปรุงการให้สิทธิ์แก่ผู้ใช้งานให้สอดคล้องกับการปฏิบัติงานที่เปลี่ยนไป เช่น เมื่อเปลี่ยนแปลงตำแหน่งงาน ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงานภายในองค์กร เป็นต้น

2. หน่วยงานต้นสังกัดของผู้ใช้งานต้องแจ้งเอกสารอย่างเป็นทางการแก่ผู้ดูแลระบบให้กำนดสิทธิ์ตามหน้าที่ความรับผิดชอบในการปฏิบัติงานเมื่อมีผู้ใช้งานใหม่เข้ามาปฏิบัติงาน หรือยกเลิกสิทธิ์ต่างๆ ในการเข้าใช้ระบบสารสนเทศเมื่อผู้ใช้งานโยกย้าย หรือลาออก เป็นต้น

3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต อย่างน้อยดังนี้

3.1 มีการประชาสัมพันธ์เผยแพร่ความรู้เกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness)

3.2 ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

3.3 มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้

(1) จัดแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(2) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(3) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าจำเป็น

(4) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(5) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(6) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(7) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(8) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดจากการจ้าง เป็นต้น

3.4 มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(1) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

- ขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาต เบื้องต้นจากผู้บังคับบัญชาก่อน

- ผู้อำนวยการศูนย์พิจารณาอนุญาต เมื่อผ่านการพิจารณา ผู้อำนวยการศูนย์ส่งต่อให้ผู้ดูแลระบบตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร

- สำหรับรหัสการใช้งานจะแจ้ง โดยการใส่ซองปิดผนึกกลับไปยังผู้ที่ขออนุญาตใช้งานสารสนเทศ

(2) มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

- ระดับผู้บริหาร ดูข้อมูลอย่างเดียว (ทุกระบบ)
- ระดับผู้อำนวยการ ดูข้อมูล/แก้ไขข้อมูล (เฉพาะระบบที่อยู่ในความรับผิดชอบ)
- ระดับหัวหน้างาน ดูข้อมูล/แก้ไขข้อมูล/ลบข้อมูล (เฉพาะระบบที่อยู่ในความรับผิดชอบ)
- ระดับปฏิบัติงาน ดูข้อมูล/เพิ่มข้อมูล (เฉพาะระบบที่อยู่ในความรับผิดชอบ)

(3) การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(4) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

- มีการจัดเก็บเอกสารการร้องขอและการกำหนดสิทธิเป็นลายลักษณ์อักษร
- ในฐานข้อมูลมีการเก็บวัน/เดือน/ปีและรหัสของผู้ดูแลระบบที่เข้ามาดำเนินการกำหนดสิทธิ

3.5 มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(1) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา โดยให้มีความแตกต่างและหลากหลาย

(3) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานต้องตอบกลับทันที หลังจากได้รับรหัสผ่าน

(4) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านให้ยากต่อการคาดเดา

(5) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(6) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(7) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(8) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

3.6 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง เป็นต้น โดยมีแนวปฏิบัติดังนี้

(1) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิที่ได้รับของแต่ละบุคคล

(2) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

(3) ผู้บังคับบัญชาของหน่วยงานดำเนินการแก้ไขข้อมูลสิทธิ์ต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับผู้ดูแลระบบ

(4) สำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน 3 วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 7 วันหลังจากได้รับแจ้งจากหน่วยงาน

4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

4.1 มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password user) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(2) ต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

(3) ต้องกำหนดรหัสผ่าน ให้มีตัวอักษรอย่างน้อย 8 ตัวอักษร หรือเข้ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(4) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือกลุ่มเหมือนกัน

(5) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(6) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(7) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(8) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(9) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(10) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(11) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(12) ต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาทุกๆ 180 วัน หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(13) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานต่างๆ ที่ตนใช้งาน

(14) หลีกเลี่ยงการใช้รหัสผ่านเดิมเมื่อเปลี่ยนรหัสผ่านใหม่

(15) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน ถี่กว่าผู้ใช้งานทั่วไป

4.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(1) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(2) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(3) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(4) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(5) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 15 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(6) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

(7) กำหนด Policy ผ่าน AD หากไม่มีการอนุญาตหรือขอปฏิบัติงานนอกเวลาจะไม่ให้ใช้งาน

4.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(1) กำหนดมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ เช่น

- การจัดการบริเวณโดยรอบ
- การควบคุมการเข้า-ออก
- การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่ปลอดภัย

(2) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(3) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(4) มีการกำหนดขอบเขตการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องถ่ายสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(5) การควบคุมการใช้งาน

- ตรวจสอบรายชื่อผู้เข้าอาคาร
- ลงชื่อผู้ขอปฏิบัติงานนอกเวลาและเบิกกุญแจห้องที่ฝ่ายพัสดุ
- ใช้ AD ควบคุม Policy การใช้งาน
- มีการกำหนด session timeout ทุก 30 นาที

(6) กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์ ดังนี้

(6.1) ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในแผ่น CD/DVD ใช้วิธีการย่อยทำลาย

(6.2) ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในเทป DAT จะต้องทำการลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป

(6.3) ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices เช่น USB flash drive, SD cards ให้ทำลายข้อมูล โดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD 5220-22M ของกระทรวงกลาโหม สหรัฐอเมริกา ว่าด้วยการลบข้อมูลในฮาร์ดดิสก์ ดังนี้

- ใช้ซอฟต์แวร์ Disk Wipe (http://www.diskwipe.org) ในการทำลายข้อมูลทั้ง Hard Disk หรือ Memory Devices ก่อนการถอดทำลาย โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://www.diskwipe.org/download.php

- ใช้ซอฟต์แวร์ Eraser (http://eraser.heidi.ie) ในการลบแฟ้มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php

4.4 ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.2544 ดังนี้

(1) ต้องแสดงหลักเกณฑ์ในการกำหนดเรื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

- มีเอกสารหรือหนังสือแจ้งอย่างเป็นทางการ
- ผู้อำนวยการศูนย์แจ้งงานพัฒนาโปรแกรมกำหนดสิทธิข้อมูลที่เป็นความลับ

(2) ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

- มีเอกสารหรือหนังสืออนุญาตอย่างเป็นทางการจากผู้บริหารระดับสูง
- ผู้อำนวยการศูนย์มอบหมายให้ผู้ดูแลระบบดำเนินการ
- ผู้ดูแลระบบกำหนดสิทธิการเข้าถึง และแจ้งรหัสแก่ผู้ใช้งานที่ได้รับมอบหมายให้เข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด
- หากมีเอกสารหรือหนังสือจากผู้บริหารระดับสูงให้ยกเลิกสิทธิการใช้งาน หรือหมดวาระการใช้งาน ให้ระงับสิทธิการใช้งานของผู้ใช้งานทันที

5. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

5.1 การใช้งานบริการเครือข่าย

(1) ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายให้ชัดเจนและรัดกุม เพื่อทำให้การควบคุมและป้องกันการบุกรุกเป็นไปอย่างมีประสิทธิภาพ

(2) ผู้ดูแลระบบต้องมีวิธีในการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(3) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้ ดังนี้

- ควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
- ควบคุมการเข้าถึงระบบเครือข่าย
- ควบคุมการเข้าถึงระบบปฏิบัติการ

- ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(4) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(5) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างน้อยปีละ 1 ครั้ง

5.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(1) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) ทุกครั้ง

(2) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (password)

(3) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน อย่างน้อย 1 วิธี

(4) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และให้มีการตรวจสอบผู้ใช้งานด้วย VPN

5.3 การระบุอุปกรณ์บนเครือข่าย (Equipment identification in network)

(1) กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย IP Address และ MAC Address

(2) จัดทำบัญชีเครื่องคอมพิวเตอร์และระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์, IP Address, MAC Address, สถานที่ติดตั้ง, ผู้ใช้งาน เป็นต้น

(3) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์หรือผู้ได้รับอนุญาตเท่านั้น

(4) ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

(5) จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

(6) แผนผังเครือข่าย จะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง

(7) IP address ของระบบเครือข่ายภายในหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อป้องกันไม่ให้บุคคลภายนอกเข้าสู่ระบบเครือข่ายได้โดยง่าย

5.4 การป้องกันพอร์ต (port) ที่ใช้งานสำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ต (port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

(1) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ต (port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

- ตรวจสอบโปรโตคอล (protocol) และพอร์ต (port) ที่ใช้
- ตรวจสอบว่ามีแอพพลิเคชั่นใดทำงานบนเครื่องเป้าหมาย
- ตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(2) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

- ทำการปิดบริการ (service) และพอร์ต (port) ที่ไม่จำเป็น
- ใช้เครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

(3) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาที่จำเป็น

(4) ต้องมีการมอบหมายบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน

5.5 การแบ่งแยกเครือข่าย (Segregation in network) กำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้

(1) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(2) แบ่งแยกเครือข่าย สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็นโซน ดังนี้

(1) Intranet Zone

(2) Application Zone

(3) Database Zone

(4) Extranet Zone

(5) DMZ Zone

5.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติดังนี้

(1) จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

(2) ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)

(3) การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น

(4) ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(5) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(6) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

(7) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานให้เชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เช่น Firewall เป็นต้น

5.7 การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรืออุปกรณ์การประยุกต์ใช้งานตามภารกิจ ดังนี้

(1) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้งานหมายเลขเครือข่าย (IP address)

(2) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

(3) กำหนดมาตรการการบังคับใช้เส้นทางบนเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

(4) กำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

6. การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

6.1 ผู้ดูแลระบบ (system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

6.2 กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(1) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(3) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

6.3 ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

(1) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(2) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค หรือสอดคล้องกับการปฏิบัติงาน

(3) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card, Finger scan

6.4 การบริหารจัดการรหัสผ่าน (password management system) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยการกำหนด AD Policy ใน AD เพื่อใช้ในการทำ password management ซึ่งทางกรมได้จัดทำโปรแกรมสำหรับตรวจสอบการเปลี่ยนรหัสดังกล่าว

เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

6.5 การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ต้องจำกัดและควบคุมการใช้งาน โปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

(1) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(2) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(3) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(4) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(5) กำหนดให้มีการถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(6) ห้ามติดตั้งหรือใช้งานโปรแกรมละเมิดลิขสิทธิ์ หรือโปรแกรมที่มีนโยบายห้ามไม่ให้เข้าถึงหรือติดตั้ง หรือใช้งาน

6.6 เมื่อมีการว่างเว้นจากการใช้งานระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(1) หลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาที เป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อ

ว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา 15 นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(2) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(3) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามกำหนด

6.7 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือความสำคัญสูง

(1) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ใช้งานสามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ 3 ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

(2) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(3) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

7.1 การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ ซึ่งได้มีการกำหนด Access Right คือ กำหนดให้ผู้ใช้แต่ละรายมีสิทธิเข้าถึงระบบ แต่ละระบบได้เพียงใด โดยดำเนินการดังนี้

(1) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูล

(2) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่างๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

(3) ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน

(4) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(5) ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

7.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

(1) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

(2) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

- ควบคุมการเข้าถึงอุปกรณ์ และระบบ โดยติดตั้งไว้ในในพื้นที่ปลอดภัย

- ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณ์ผิดปกติ

(3) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว โดยมีขั้นตอนการควบคุมดังนี้

- ผู้ที่จะใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตเบื้องต้นจากผู้บังคับบัญชาก่อน

- ผู้อำนวยการศูนย์พิจารณาอนุญาต เมื่อผ่านการพิจารณา ผู้อำนวยการศูนย์ส่งต่อให้ผู้ดูแลระบบตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร

- สำหรับการขอเข้าใช้งานระบบสารสนเทศจากภายนอก (teleworking) ต้องขออนุมัติการใช้งานจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รหัสการใช้งานจะแจ้งโดยการใส่ซองปิดผนึกกลับไปยังผู้ที่ขออนุญาตใช้งาน

7.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์สื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยดำเนินการ ดังนี้

- อุปกรณ์สื่อสารเคลื่อนที่ (mobile computing) ผู้ดูแลระบบจะต้องตรวจสอบและดำเนินการเปิดสิทธิการใช้งาน โดยเพิ่มค่า Mac Address ของอุปกรณ์สื่อสารดังกล่าว ในระบบควบคุมการใช้งาน และแจ้งกลับผู้ที่ขออนุญาตใช้งานทราบเป็นลายลักษณ์อักษร

- กำหนดให้มีการจัดเก็บ Mac Address พร้อมรายละเอียดผู้ใช้งาน โดยมีระบบรองรับในการตรวจสอบ

- กำหนดสิทธิ์การเข้าระบบว่าสามารถเข้าถึงข้อมูลและระบบใดได้บ้าง เพียงใด

- ผู้ที่สามารถเข้าใช้งานได้จะต้องได้รับการอนุมัติหรืออนุญาตจาก DCIO

- ผู้ดูแลระบบด้านเครือข่ายมีหน้าที่ตรวจสอบการเข้าใช้งานและผู้บุกรุกที่พยายามเข้าใช้งานโดยไม่ได้รับอนุญาต และรายงาน DCIO ทราบ

- ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลความลับด้วยอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

7.4 การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน ดังนี้

(1) ให้มีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่างๆ ภายในหน่วยงาน

(2) การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(3) การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียดดังนี้

(3.1) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน

(3.2) รายละเอียดและลักษณะของระบบงาน

(3.3) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

(3.4) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

(3.5) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน

(4) ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

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

(6) ผู้ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงานโดย ไม่ให้สมาชิกภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

(7) ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

(8) ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(9) ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ 1 ครั้ง

7.5 การควบคุม Outsource กรณีมีการจ้างเหมาบริการจากภายนอกในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ต้องกำหนดแนวปฏิบัติ ดังนี้

(1) กำหนดให้ผู้อำนวยการศูนย์ เป็นผู้อนุมัติสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ โดย Outsource จะต้องจัดทำเอกสารขออนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงานเป็นลายลักษณ์อักษร โดยจะต้องมีรายละเอียดประกอบในเอกสารอย่างน้อย ดังนี้

- เหตุผลในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- ระยะเวลาในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- คำยินยอมจากเจ้าหน้าที่ของหน่วยงานที่รับผิดชอบในการนำ Outsource เข้ามาปฏิบัติงานภายในสำนักงาน

(2) Outsource ที่มาปฏิบัติงานให้กับหน่วยงาน ไม่ว่าจะปฏิบัติงานภายใน หรือภายนอกหน่วยงาน จะต้องลงนามในสัญญาจ้างเรื่องการไม่เปิดเผยข้อมูลของสำนักงาน โดยจะต้องจัดทำสัญญาจ้างให้เสร็จสิ้นก่อนการกำหนดสิทธิ์ให้ Outsource นั้น เข้าถึงระบบเทคโนโลยีสารสนเทศ

(3) เจ้าหน้าที่ของหน่วยงานซึ่งเป็นเจ้าของโครงการที่มีการเข้าถึงข้อมูลโดย Outsource จะต้องกำหนดสิทธิ์การเข้าถึงให้เฉพาะบุคคลที่จำเป็นเท่านั้น

(4) สำหรับการปฏิบัติงานในโครงการใหญ่ ผู้ดูแลระบบจะต้องควบคุมให้ Outsource รักษาความมั่นคงปลอดภัย ทั้งทางด้านการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาให้ระบบพร้อมให้บริการอยู่เสมอ (Availability)

(5) ควรกำหนดให้ Outsource จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้องในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน รวมทั้งให้มีการปรับปรุงอย่างสม่ำเสมอ เพื่อใช้ในการควบคุมและตรวจสอบการปฏิบัติงานของ Outsource ให้เป็นไปตามขอบเขตที่ได้กำหนดไว้

(6) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(7) มอบหมายเจ้าหน้าที่ หรือผู้ดูแลระบบทำหน้าที่ในการควบคุม ดูแล ตรวจสอบการปฏิบัติงานของ Outsource

8. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

8.1 ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(1) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหาย หรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(2) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

(3) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการอนุมัติให้ติดตั้งก่อนดำเนินการ

(4) ไม่ติดตั้งซอร์สโค้ด คอมไพเลอร์ (complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นๆ

(5) กำหนดให้มีการจัดเก็บซอร์สโค้ด (source code) และไลบรารี่ (library) สำหรับ ซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(6) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ เป็นต้น

(7) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(8) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

(9) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

8.2 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(1) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(2) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

8.3 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(1) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

(2) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก

(3) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

8.4 มาตรการควบคุมช่องโหว่ทางเทคนิค

(1) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น และมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชัน (version) ที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

(2) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(3) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการดังนี้

- มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(4) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

8.5 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้ระบบสารสนเทศ (audit logging) มีการบันทึกพฤติกรรมการใช้งาน (log) การเข้าถึงระบบสารสนเทศ ดังนี้

(1) ข้อมูลชื่อบัญชีผู้ใช้งาน

(2) ข้อมูลวันเวลาที่เข้าถึงระบบ

(3) ข้อมูลวันเวลาที่ออกจากระบบ

(4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(5) ข้อมูลการล็อกอิน (login) ทั้งที่สำเร็จและไม่สำเร็จ

(6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(7) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น (figuration) ของระบบ

(8) ข้อมูลแสดงการใช้งานแอพพลิเคชั่น (application)

(9) ข้อมูลการล็อกอิน (login) ทั้งที่สำเร็จและไม่สำเร็จ

(10) ข้อมูลไอพีแอดเดรส (IP-address) ที่เข้าถึง

(11) ข้อมูลโพรโตคอล (protocol) เครือข่ายที่ใช้

(12) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(13) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

9. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)

9.1 ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (data center)

(1) ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงานพื้นที่ติดตั้ง และจัดเก็บอุปกรณ์ระบบสารสนเทศ หรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

(2) ให้ศูนย์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(3) ให้ศูนย์กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(4) ในกรณีที่หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงานจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

(5) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำหรือเครื่องดับเพลิงระบบปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้สามารถมั่นใจได้ว่า ระบบทำงานตาม ปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(6) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

9.2 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (cabling security)

(1) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(2) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(3) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(4) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(5) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(6) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ให้มีการปิดใส่กุญแจ เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(7) พิจารณาใช้งานสายไฟเบอร์ออฟติก (fiber optic) แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(8) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณ โดยผู้ไม่ประสงค์ดี

9.3 การบำรุงรักษาอุปกรณ์ (equipment maintenance)

(1) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่ผู้ผลิตแนะนำ

(2) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบ หรือประเมินในภายหลัง

(4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(5) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(6) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้จับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

9.4 การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (removal of property)

(1) กำหนดให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(2) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกจากหน่วยงาน

(3) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(4) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(5) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

9.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (security of equipment off-premises)

(1) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(2) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(3) สร้างจิตสำนึกให้เจ้าหน้าที่รับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

9.6 การจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (secure disposal or re-use of equipment)

(1) กำหนดให้มีทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(2) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

9.7 การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

(1) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(2) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(3) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

(4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

10. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless)

10.1 ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย

10.2 ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

10.3 ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

10.4 ผู้ดูแลระบบเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่

10.5 ผู้ดูแลระบบต้องกำหนดค่าของการใช้งานให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

10.6 ผู้ดูแลระบบต้องมีการแยก VLAN ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

10.7 ผู้ดูแลระบบต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

10.8 ผู้ดูแลระบบต้องใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

11. การควบคุมการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

11.1 การใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์แบบพกพา ผู้ใช้จะต้องนำมาลงทะเบียนที่ศูนย์ก่อน ซึ่งจะมีการกำหนดชื่อเครื่อง เพื่อง่ายต่อการตรวจสอบ หากก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์ของหน่วยงาน

(2) การตั้งชื่อเครื่องคอมพิวเตร์แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ศูนย์เท่านั้น

(3) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

(4) เจ้าหน้าที่ศูนย์มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์แบบพกพาส่วนตัว

(5) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหายและตรวจสอบ ซ่อมแซม หากเครื่องคอมพิวเตอร์แบบพกพาส่วนตัวเกิดความเสียหายด้วยตนเอง

11.2 การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์

(1) ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพาส่วนตัว

(2) หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาส่วนตัวติดชุดคำสั่งไม่พึงประสงค์ ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

12. การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

12.1 การใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์ที่อนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ

(2) โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

(3) ไม่อนุญาตให้ ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(4) การตั้งชื่อเครื่องคอมพิวเตอร์จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เท่านั้น

(5) ห้ามคัดลอกโปรแกรมต่างๆ ที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานซึ่งมีลิขสิทธิ์ถูกต้องตามกฎหมาย นำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(6) การเคลื่อนย้ายจุดติดตั้งหรือตรวจซ่อมคอมพิวเตอร์จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เท่านั้น

(7) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(8) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ใช้งานอยู่

(9) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยปฏิบัติ ดังนี้

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

12.2 การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์

(1) เจ้าหน้าที่ศูนย์มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์

(2) ผู้ใช้ต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(3) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งานเสมอ

(4) ผู้ใช้ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

12.3 การสำรองข้อมูลและการกู้คืน

เจ้าหน้าที่ศูนย์ต้องรับผิดชอบในการสำรองข้อมูล และเก็บรักษาข้อมูล เมื่อผู้ใช้นำเครื่องคอมพิวเตอร์มาทำการตรวจสอบ ซ่อมแซม และหากทำการตรวจสอบ ซ่อมแซมจนเครื่องคอมพิวเตอร์สามารถใช้งานได้ตามปกติเป็นที่เรียบร้อยแล้ว ก็ต้องทำการเคลื่อนย้ายข้อมูลกลับไปให้คงเดิม

13. การควบคุมการเข้า-ออกห้องศูนย์คอมพิวเตอร์

13.1 คำจำกัดความของผู้ที่เกี่ยวข้อง

(1) ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศภายในศูนย์

(2) เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ของหน่วยงานที่มีสิทธิ์ในการเข้าออกสถานที่ อาคาร ห้องต่างๆ

(3) ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือดูแล ซ่อมบำรุงหรือใช้ข้อมูลหรือทรัพย์สินต่างๆ ของศูนย์

13.2 บทบาทและความรับผิดชอบ

(1) ผู้อำนวยการศูนย์

- อนุมัติสิทธิ์การเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
- อนุมัติกระบวนการควบคุมการเข้า-ออกห้องศูนย์คอมพิวเตอร์

(2) ผู้ดูแลระบบ มีหน้าที่ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องศูนย์คอมพิวเตอร์

13.3 กระบวนการควบคุมการเข้า-ออกห้องศูนย์คอมพิวเตอร์

(1) ผู้ดูแลระบบ และเจ้าหน้าที่ มีแนวทางปฏิบัติดังนี้

- ผู้ดูแลระบบ มีการจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เช่น ส่วนของห้อง SERVER ห้องทำงาน ห้องอบรมคอมพิวเตอร์ เป็นต้น เพื่อสะดวกในการปฏิบัติงานและการควบคุมดูแลให้มีประสิทธิภาพยิ่งขึ้น

- ศูนย์ต้องมีการกำหนดสิทธิ์บุคคลในการเข้าออกห้องศูนย์คอมพิวเตอร์

- สิทธิ์ในการเข้า-ออกห้องต่างๆ ภายในห้องศูนย์ของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนจะขึ้นอยู่กับหน้าที่ที่ต้องปฏิบัติหรือได้รับคำสั่งเท่านั้น

- เจ้าหน้าที่ทุกคนต้องทำบัตรผ่านเข้าออกแบบ Contactless เพื่อใช้ในการเข้า-ออกห้องศูนย์ และใช้ระบบ Finger Scan เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์

- ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกศูนย์และห้องควบคุมระบบคอมพิวเตอร์

(2) ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

- ผู้ติดต่อจากหน่วยงานภายนอกต้องได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบจึงจะสามารถเข้า-ออกภายในศูนย์ได้

- ผู้ติดต่อจากหน่วยงานภายนอกทุกคน (รวมถึงผู้ติดตาม) จะต้องลงบันทึกรายละเอียดการขอเข้ามาดำเนินการลงในสมุดบันทึก “การเข้า-ออกห้องศูนย์คอมพิวเตอร์”

- หากมีบุคคลภายนอกเข้ามาดำเนินการ ผู้อำนวยการศูนย์จะต้องมอบหมายให้เจ้าหน้าที่ศูนย์คอยควบคุมดูแลทุกครั้ง

- ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในหน่วยงานจะต้องควบคุมดูแลอย่างรัดกุม และได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

- เจ้าหน้าที่ของศูนย์ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

- เจ้าหน้าที่ของศูนย์ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมอ

14. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

14.1 การใช้งานสำหรับผู้ใช้งาน (User)

(1) เจ้าหน้าที่ในสังกัด หากต้องการติดต่องานราชการหรือติดต่อกับบุคคลภายนอก ให้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน หรือของส่วนราชการที่กำหนดให้เท่านั้น ห้ามนำไปใช้ติดต่อในเรื่องส่วนตัว และห้ามติดต่องานราชการผ่านระบบจดหมายอิเล็กทรอนิกส์ของเว็บไซต์ผู้ให้บริการอื่น

(2) สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบ ผู้ใช้ทุกคนจะต้องทำการเปลี่ยนรหัสผ่านใหม่โดยทันที

(3) ห้ามผู้ใช้ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติของระบบจดหมายอิเล็กทรอนิกส์

(4) ผู้ใช้ต้องระมัดระวังการใช้งานจดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงานหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และมาแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

(5) ผู้ใช้ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(6) ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของหน่วยงาน เพื่อการทำงานของหน่วยงานเท่านั้น

(7) หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น และทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(8) ผู้ใช้ต้องทำการตรวจเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

(9) ผู้ใช้ต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(10) ห้ามผู้ใช้ใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์ และต้องระบุชื่อผู้รับและหัวข้อให้ชัดเจน

(11) หลีกเลี่ยงการส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่านบัญชีผู้ใช้งาน หมายเลขบัตรประชาชน ผ่านจดหมายอิเล็กทรอนิกส์

(12) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ต้องระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(13) ผู้ใช้ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(14) ผู้ใช้ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

(15) ผู้ใช้ต้องย้ายจดหมายอิเล็กทรอนิกส์ที่จำเป็นต้องนำมาใช้ในภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อป้องกันผู้อื่นแอบเข้าไปแอบอ่านจดหมายได้

(16) ไม่จัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

(17) การใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน จะถือว่าผู้ที่เข้าใช้บริการรับทราบ ทำความเข้าใจและยอมรับนโยบายจดหมายอิเล็กทรอนิกส์ของหน่วยงานแล้ว

14.2 แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (Administrator)

(1) ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้

(2) ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อให้ผู้ใช้รายใหม่พร้อมรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์

(3) จัดทำระบบการปกปิดการเข้ารหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น 'X', 'O' ในการพิมพ์แต่ละตัวอักษร

(4) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไป ไม่เกิน 3 ครั้ง

(5) ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ และมีการ Logout ออกจากหน้าจอ เพื่อตัดการใช้งานของผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้

15. การใช้งานระบบอินเตอร์เน็ต (Internet)

15.1 ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ การเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ได้จัดสรรไว้ให้เท่านั้น เช่น Proxy, Firewall เป็นต้น ห้ามมิให้ผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น

15.2 เครื่องคอมพิวเตอร์ส่วนบุคคล ก่อนทำการเชื่อมต่ออินเตอร์เน็ตจะต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์ และต้องมีการติดตั้งโปรแกรมป้องกันไวรัสก่อนเสมอ

15.3 เครื่องคอมพิวเตอร์แบบพกพาส่วนตัวไม่อนุญาตให้ใช้อินเตอร์เน็ต

15.4 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องผ่านระบบตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนจะทำการรับส่งข้อมูลทุกครั้ง

15.5 กำหนดให้หน้าแรกของ browser Internet เป็นหน้าเว็บ Intranet

15.6 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

15.7 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน

15.8 ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

15.9 ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

15.10 ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสื่อมเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

15.11 ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตก่อนนำข้อมูลไปใช้งาน

15.12 ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเตอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

15.13 ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความยั่วยุ เสียดสี ด่าทอ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน และเป็นการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น

15.14 ห้ามผู้ใช้งานใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมาก หรือเป็นเวลานาน

16. การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ (Conversion)

16.1 ข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลงต้องมีความหมายหรือรูปแบบเหมือนกับเอกสารและข้อความเดิม ซึ่งนำมาจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยผู้จัดทำหรือแปลงจะต้องตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์นั้น มีความหมายและรูปแบบเหมือนกับเอกสารและข้อความเดิม

16.2 ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงขึ้นด้วยวิธีการที่เชื่อถือได้ และมีการระบุตัวตนของผู้จัดทำหรือแปลงข้อมูลนั้นๆ

16.3 ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงโดยมีเทคโนโลยีและมาตรการป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไขเกิดขึ้นกับข้อมูลนั้น เว้นแต่การรับรองหรือบันทึกเพิ่มเติม ซึ่งไม่มีผลต่อความหมายของข้อมูลอิเล็กทรอนิกส์

16.4 ผู้จัดทำหรือแปลงข้อมูลอิเล็กทรอนิกส์จะต้องรับผิดชอบในข้อผิดพลาดหรือความเสียหายที่เกิดจากข้อมูลที่ตนเป็นผู้จัดทำหรือแปลงนั้น

17. การนำข้อมูลต่างๆ เผยแพร่ลงในเว็บไซต์ (Web Information)

17.1 ข้อมูลที่จะนำมาลงจะต้องได้รับความเห็นชอบ, อนุมัติหรือคำสั่งจากผู้บริหาร, ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการศูนย์

17.2 ข้อมูลจะนำมาลงจะต้องเป็นข้อมูลที่ไม่ก่อให้เกิดความเสียหายต่อผู้อื่น และหน่วยงาน หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม

17.3 ผู้มีหน้าที่ลงข้อมูลจะต้องได้รับอนุญาตจากผู้บริหาร, ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการศูนย์ และเป็นเจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมายเท่านั้น

17.4 กรณีเจ้าหน้าที่ในหน่วยงานที่ไม่อยู่ในสังกัดของศูนย์ ผู้ดูแลระบบจะต้องกำหนดสิทธิ์การเข้าถึงการลงข้อมูลให้แก่เจ้าหน้าที่ดังกล่าว เพื่อไม่ให้เกิดความเสียหายกับข้อมูลอื่นใดที่ไม่อยู่ในความรับผิดชอบ

18. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

18.1 อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

18.2 ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องไม่เปิดเผยข้อมูลสำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของหน่วยงาน

18.3 ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

18.4 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

19. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

19.1 จัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องชัดเจน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

19.2 ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงานหรือบุคคลที่หน่วยงานมอบหมาย

19.3 กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการเข้าใช้งานอินเตอร์เน็ตหรืออีเมล์ เป็นต้น

19.4 กำหนดระยะเวลาจัดเก็บ Log ไม่น้อยกว่า 90 วัน

20. การจัดการระบบเครือข่ายแบบรวมศูนย์ (Active Directory: AD)

เพื่อควบคุมความปลอดภัยของข้อมูล และให้สามารถกำหนดสิทธิของผู้ใช้งาน ให้ปฏิบัติดังต่อไปนี้

20.1 ทุกเครื่องที่อยู่ในระบบเครือข่ายจะต้องเข้าสู่ระบบเครือข่ายแบบรวมศูนย์

20.2 กำหนดให้ผู้ดูแลระบบมีหน้าที่ในการกำหนด Policy ต่างๆ และกำหนดสิทธิ์ของผู้ใช้งาน โดยผ่านความเห็นชอบจากผู้บริหาร, ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการศูนย์

20.3 กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการเข้าใช้งานอินเตอร์เน็ตหรืออีเมล์ เป็นต้น

21. การใช้งาน Token

21.1 กำหนดให้การเข้าใช้ระบบคอมพิวเตอร์และอุปกรณ์ของกรมบังคับคดีทุกครั้ง ต้องยืนยันตัวบุคคลโดยใช้อุปกรณ์ Token หรือรหัสผ่านตามสิทธิการใช้งาน

21.2 กรณีผู้ใช้งานลืมอุปกรณ์ Token ทำให้ไม่สามารถเข้าถึงระบบปฏิบัติการได้ ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว โดยจะเปิดสิทธิให้ใช้งาน 1 วันทำการ

21.3 ผู้ใช้งานสามารถเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตนเอง ให้ผู้ใช้งานใช้รหัสผู้ใช้ (Username) และรหัสผ่าน (Password) จากอุปกรณ์ Token ของตนเอง เพื่อยืนยันตัวตนในการเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตนเอง

21.4 กรณีผู้ใช้ย้ายหน่วยงาน ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ เพื่อขอให้ทำการย้าย User Profile และกำหนดสิทธิของผู้ใช้งาน ให้กับเครื่องคอมพิวเตอร์เครื่องใหม่ และนำอุปกรณ์ Token ของตนเองติดตามตัวไปด้วย

21.5 กรณีอุปกรณ์ Token ชำรุดไม่สามารถใช้งานได้ ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว พร้อมส่งคืนอุปกรณ์ Token เพื่อจะได้ดำเนินการแก้ไขต่อไป

21.6 กรณีอุปกรณ์ Token ชำรุดที่ไม่ได้เกิดจากการใช้งานตามปกติ ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว ทางกรมจะดำเนินการซ่อมแซม และเรียกเก็บค่าใช้จ่ายที่เกิดขึ้น หากซ่อมไม่ได้ผู้ใช้งานต้องชดใช้เงินตามราคาอุปกรณ์ Token

21.7 กรณีผู้ใช้งานทำอุปกรณ์ Token สูญหาย ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว ผู้ใช้งานจะต้องชดใช้เงินตามราคาอุปกรณ์ Token

21.8 กรณีผู้ใช้ลาออก ให้ผู้ใช้งานส่งคืนอุปกรณ์ Token ตามหน่วยงานที่สังกัด และให้หน่วยงานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ พร้อมอุปกรณ์ Token

ส่วนที่ 2

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถบริการได้อย่างต่อเนื่อง

2. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

1. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางดังนี้

1.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดความถี่ให้มีการสำรองข้อมูลมากขึ้น โดยให้มีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบในการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น Data Backup หรือ System Backup
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ข้อมูลที่สำรอง วัน/เวลา สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการเขียนชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงวันที่สำรองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ซึ่งระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

- ทดสอบบันทึกข้อมูลอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ดำสำรองเก็บไว้

- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

2. ต้องจัดทำแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

2.1 มีการจัดทำแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(1) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นเวลานาน ไฟไหม้ แผ่นดินไหว เป็นต้น

(3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่ต้องการติดต่อ

(6) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ที่มีความเกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อม กรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

3. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนการเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

3.1 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความคิดเห็นเสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ต่างๆ

3.2 ผู้อำนวยการศูนย์ รับผิดชอบ ดังนี้

- วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดาเนินการให้ผู้บังคับบัญชาระดับสูงทราบ

- กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งาน การปฏิบัติงานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

- กำกับดูแล ตรวจสอบ การบำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ตามปกติ

- กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการในหน่วยงาน

- กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของห้อง Server ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

- แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

- รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ

- กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก โดยไม่ได้รับอนุญาต

4. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

5. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 3
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
2. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. ผู้ตรวจสอบภายใน (Internal Auditor)
3. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

1.1 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

1.2 ตรวจสอบและประเมินความเสี่ยงที่ดำเนินงานโดยผู้ตรวจสอบภายในของหน่วยงาน เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

2. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

2.1 มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ 1 ครั้ง

2.2 มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

2.3 มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

2.4 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(1) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว

(2) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี

(3) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำปีนต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(4) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

(5) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ 4

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

1. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของหน่วยงาน

2. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

3. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

1. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ 1 ครั้ง

2. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ผ่านทางเว็บไซต์ของหน่วยงาน

3. มีการประชาสัมพันธ์ให้ความรู้ในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้โดยง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

4. มีการติดตามประเมินผล และสำรวจความต้องการของผู้ใช้งานอยู่เสมอ