ประกาศกรมบังคับคดี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมบังคับคดี

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ อธิบดีกรมบังคับคดีโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมบังคับคดี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป

ข้อ ๓ ในประกาศนี้

๓.๑ **“ผู้ใช้งาน”** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร ผู้รับบริการและผู้ใช้งานทั่วไปของกรมบังคับคดี

๓.๒ **“บัญชีผู้ใช้งาน”** หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

๓.๓ **“สิทธิของผู้ใช้งาน”** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๓.๔ **“สินทรัพย์”** หมายความว่า เครื่องคอมพิวเตอร์ อุปกรณ์ประกอบคอมพิวเตอร์ อุปกรณ์เครือข่ายคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์

๓.๕ “ **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๓.๖ “**ความมั่นคงปลอดภัยด้านสารสนเทศ** ” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ

รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๓.๗ "**เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)**" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓.๘ "**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)**" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๓.๙ **"ข้อมูลอิเล็กทรอนิกส์"** หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๑๐ **"นโยบาย"** หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓.๑๑ **"ผู้บริหาร"** หมายความว่า อธิบดีหรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรม

๓.๑๒ **"หน่วยงาน"** หมายความว่า กรมบังคับคดีรวมถึงหน่วยงานในสังกัดกรมบังคับคดี

๓.๑๓ **"ผู้บริหารระดับสูง สุด"** หมายความว่า ผู้บริหาร ของหน่วยงาน ระดับสูงสุด (CEO) หรืออธิบดีกรม รับผิดชอบเกี่ยวกับความเสี่ยงและความเสียหายอันเกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

๓.๑๔ **"ศูนย์"** หมายความว่า ศูนย์สารสนเทศ

๓.๑๕ **"ระบบอินเทอร์เน็ต (Internet)"** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ทเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๓.๑๖ **"ระบบสารสนเทศ "** หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

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

๓.๑๘ **"หน่วยงานภายนอก "** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

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

๓.๒๐ **“สื่อบันทึกพกพา ”** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น

๓.๒๑ **“ชื่อผู้ใช้ (Username)”** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

๓.๒๒ **“รหัสผ่าน (Password)”** หมายความว่า ตัวอักษรหรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๓.๒๓ **“การเข้ารหัส (Encryption)”** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๓.๒๔ **“อุปกรณ์จัดเส้นทาง (Router)”** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๓.๒๕ **“การพิสูจน์ยืนยันตัวตน (Authentication)”** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๓.๒๖ **“SSID (Service Set Identifier)”** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๓.๒๗ **“WPA (Wi-Fi Protected Access)”** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๓.๒๘ **“MAC Address (Media Access Control Address)”** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด (Internet Card) โดยแต่ละการ์ดจะมีหลายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่รูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๓.๒๙ **“SSL-VPN (Secure Socket Layer Virtual Private Network)”** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓.๓๐ **“แผนผังระบบเครือข่าย (Network Diagram)”** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

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

๓.๓๒ "**Token**" หมายความว่า อุปกรณ์ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งานก่อนการเข้าใช้งาน

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของกรมบังคับคดี

(๓) กำหนดให้เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ของศูนย์เป็นผู้รับผิดชอบตามนโยบายและแนวปฏิบัติ ประกอบด้วย

- เจ้าหน้าที่ปฏิบัติการด้านพัฒนาโปรแกรมและฐานข้อมูล
- เจ้าหน้าที่ปฏิบัติการด้านระบบเครือข่าย
- เจ้าหน้าที่ปฏิบัติการด้านการซ่อมบำรุง

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๔.๒ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

มีนโยบายในการสร้างความรู้ความเข้าใจ 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 ความเข้าใจถึงภัยและผล กระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ต้องระมัดระวังหรือรู้เท่าไม่ถึงการณ์ 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

ทั้งนี้ สำหรับผู้ปฏิบัติงานใหม่ทุกคนจะต้องเข้ารับการอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศก่อนปฏิบัติงานทุกครั้ง

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 คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๘ มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายในนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(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) ต้องควบคุมการเข้า ถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้น ทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอด คล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่างอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(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 อย่างน้อยดังนี้

(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 โดยต้องปรับปรุงแผนเตรียมความพร้อม กรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๓ กำหนดให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน และต้องรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

ประกาศ ณ วันที่ ๑๘ มีนาคม พ.ศ.๒๕๕๘

(นางสาวรื่นวดี สุวรรณมงคล)
อธิบดีกรมบังคับคดี

เอกสารแนบท้ายประกาศ

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมบังคับคดี

ส่วนที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้รับผิดชอบและผู้ที่มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

๑.๑ จัดทำบัญชีทรัพย์สิน ซึ่งจะจำแนกกลุ่มทรัพยากรของระบบและการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิของผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

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

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

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้อง

- ขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตและกำหนดสิทธิการใช้งานเบื้องต้นจากผู้บังคับบัญชาก่อน
- ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร
- สำหรับรหัสการใช้งานจะแจ้ง โดยการใส่ซองปิดผนึกกลับไปยังผู้ที่ขออนุญาตใช้งาน
- กรณีตรวจสอบสิทธิการใช้งานแล้ว บุคคลดังกล่าวไม่มีสิทธิการใช้งานจะแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

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

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

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

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๖) การกำหนดเวลาที่ได้เข้าถึง

- ช่วงเวลาในเวลาราชการ คือ ในวันจันทร์ - ศุกร์ เวลา ๐๘.๓๐ - ๑๖.๓๐ น.
- ช่วงเวลานอกเวลาราชการที่ได้รับอนุญาต คือ ในวันจันทร์ - ศุกร์ เวลา ๑๖.๓๑ - ๒๐.๐๐ น.
- วันหยุดราชการและวันหยุดนักขัตฤกษ์ที่ได้รับอนุญาต เวลา ๐๘.๓๐ - ๑๖.๓๐ น.

(๗) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

- ผ่านช่องทาง Wire Line, Wireless Line โดยมีการจัดเก็บ Log

- ผ่านหน้าเว็บอินทราเน็ต โดยมีการตรวจสอบสิทธิเข้าใช้งาน

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต อย่างน้อยดังนี้

๒.๑ มีการประชาสัมพันธ์เผยแพร่ความรู้เกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness)

๒.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๓ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้

(๑) จัดแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๓) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๔) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๕) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(๖) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๗) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๘) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดจากการจ้าง เป็นต้น

๒.๔ มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

- ขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาต เบื้องต้นจากผู้บังคับบัญชาก่อน
- ผู้อำนวยการศูนย์พิจารณาอนุญาต เมื่อผ่านการพิจารณา ผู้อำนวยการศูนย์ส่งต่อให้ผู้ดูแลระบบตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร
- สำหรับรหัสการใช้งานจะแจ้ง โดยการใส่ซองปิดผนึกกลับไปยังผู้ที่ขออนุญาตใช้งาน

(๒) มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

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

(๓) การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

- มีการจัดเก็บเอกสารการร้องขอและการกำหนดสิทธิเป็นลายลักษณ์อักษร
- ในฐานข้อมูลมีการเก็บวัน/เดือน/ปีและรหัสของผู้ดูแลระบบที่เข้ามาดำเนินการกำหนดสิทธิ

๒.๕ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา โดยให้มีความแตกต่างและหลากหลาย

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

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านให้ยากต่อการเดา

(๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๒ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

๓.๑ มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password user) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๕ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือกลุ่มเหมือนกัน

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานต่าง ๆ ที่ตนใช้งาน

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๕) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๕) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๖) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

(๗) กำหนด Policy ผ่าน AD หากไม่มีการอนุญาตหรือขอปฏิบัติงานนอกเวลาจะไม่ให้ใช้งาน

๓.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ

อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) กำหนดมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่าง ๆ เช่น

- การจัดการบริเวณโดยรอบ
- การควบคุมการเข้า-ออก
- การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
- วัฒนธรรมองค์กร

(๓) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(๔) มีการกำหนดขอบเขตการป้องกัน ดังนี้

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

(๕) การควบคุมการใช้งาน

- ตรวจสอบรายชื่อผู้เข้าอาคาร
- ลงชื่อผู้ขอปฏิบัติงานนอกเวลาและเบิกกุญแจห้องที่ฝ่ายพัสดุ
- ใช้ AD ควบคุม Policy การใช้งาน
- มีการกำหนด session timeout ทุก ๓๐ นาที

๓.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

(๑) ต้องแสดงหลักเกณฑ์ในการกำหนดเรื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

- มีเอกสารหรือหนังสือแจ้งอย่างเป็นทางการ
- ผู้อำนวยการศูนย์แจ้งงานพัฒนาโปรแกรมกำหนดสิทธิข้อมูลที่เป็นความลับ

(๒) ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

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

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๔.๑ ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายให้ชัดเจนและรัดกุม เพื่อทำให้การควบคุมและป้องกันการบุกรุกเป็นไปอย่างมีประสิทธิภาพ

๔.๒ ผู้ดูแลระบบต้องมีวิธีในการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้ ดังนี้

- ควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
- ควบคุมการเข้าถึงระบบเครือข่าย
- ควบคุมการเข้าถึงระบบปฏิบัติการ
- ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless lan) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และ

ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างน้อยปีละ ๑ ครั้ง

๔.๓ การยืนยันตัวบุคคลสาหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

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

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

(๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน อย่างน้อย ๑ วิธี

(๔) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

๔.๔ ผู้ดูแลระบบทำการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน โดยควบคุมการเข้าถึงหรือการใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเข้าสู่เครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๔.๕ ผู้ดูแลระบบจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

๔.๖ ต้องมีการมอบหมายบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน

๔.๗ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานให้เชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เช่น Firewall เป็นต้น

๔.๘ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ระบุตามค่า ip address และให้ปฏิบัติตามวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(๒) มีการควบคุมการใช้งานอย่างเหมาะสม

(๓) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔.๙ ip address ของระบบเครือข่ายภายในหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อป้องกันไม่ให้บุคคลภายนอกเข้าสู่ระบบเครือข่ายได้โดยง่าย

๔.๑๐ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์หรือผู้ที่ได้รับอนุญาตเท่านั้น

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

(๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ต (port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

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

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

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

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาที่จำเป็น

๔.๑๒ ต้องทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็นโซน ดังนี้

(๑) Intranet Zone

(๒) Application Zone

(๓) Database Zone

(๔) Extranet Zone

(๕) DMZ Zone

๔.๑๓ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรืออุปกรณ์การประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้งานหมายเลขเครือข่าย (ip address)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

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

๕.๒ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

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

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

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

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card

๕.๔ การบริหารจัดการรหัสผ่าน (password management system) มีระบบบริหารจัดการรหัสผ่านที่สามารถทานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนด

รหัสผ่านที่มีคุณภาพ โดยการกำนหด AD Policy ใน AD เพื่อใช้ในการทำ password management ซึ่งทางกรมได้จัดทำโปรแกรมสำหรับตรวจสอบการเปลี่ยนรหัสดังกล่าว

เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

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

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๖ เมื่อมีการว่างเว้นจากการใช้งานระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๑) หลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามกำหนด

๕.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือความสำคัญสูง

(๑) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ใช้งานสามารถใช้งานได้นานที่สุด

ภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

(๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

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

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

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

(๑) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

(๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

- ระบบเครือข่ายที่ใช้การสื่อสารผ่านสายใยแก้วนำแสง (Fiber Optic) ต้องให้มีการร้อยท่อสายสัญญาณ เพื่อป้องกันการตัดสายสัญญาณและป้องกันสัตว์กัดสายสัญญาณ
- ตรวจสอบ และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น ระบบควบคุมอุณหภูมิ ระบบตรวจจับความชื้น ให้อยู่ในภาวะปกติ
- ห้ามนำอาหาร เครื่องดื่มเข้าทารับประทานหรือสูบบุหรี่ในบริเวณระบบเทคโนโลยีสารสนเทศกลาง (Data Center)

(๓) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้อง โดยมีขั้นตอนการ

ควบคุม ดังนี้

- ผู้ที่จะใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตเบื้องต้นจากผู้บังคับบัญชาก่อน
- ผู้อำนวยการศูนย์พิจารณาอนุญาต เมื่อผ่านการพิจารณา ผู้อำนวยการศูนย์ส่งต่อให้ผู้ดูแลระบบตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร
- สำหรับการขอเข้าใช้งานระบบสารสนเทศจากภายนอก (teleworking) รหัสการใช้งานจะแจ้ง โดยการใส่ซองปิดผนึกกลับไปยังผู้ที่ขออนุญาตใช้งาน
- สำหรับอุปกรณ์สื่อสารเคลื่อนที่ (mobile computing) ผู้ดูแลระบบตรวจสอบและดำเนินการเปิดสิทธิการใช้งาน โดยเพิ่มค่า Mac Address ของอุปกรณ์สื่อสารดังกล่าวในระบบควบคุมการใช้งาน และแจ้งกลับผู้ที่ขออนุญาตใช้งานทราบเป็นลายลักษณ์อักษร
- กรณีตรวจสอบสิทธิการใช้งานแล้ว บุคคลดังกล่าวไม่มีสิทธิการใช้งานจะแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์สื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยดำเนินการ ดังนี้

- กำหนดให้มีการจัดเก็บ Mac Address พร้อมรายละเอียดผู้ใช้งาน โดยมีระบบรองรับในการตรวจสอบ
- กำหนดสิทธิ์การเข้าระบบว่าสามารถเข้าถึงข้อมูลและระบบใดได้บ้าง เพียงใด
- ผู้ที่สามารถเข้าใช้งานได้จะต้องได้รับการอนุมัติหรืออนุญาตจาก CIO
- ผู้ดูแลระบบด้านเครือข่ายมีหน้าที่ตรวจสอบการเข้าใช้งานและผู้บุกรุกที่พยายามเข้าใช้งานโดยไม่ได้รับอนุญาต และรายงาน CIO ทราบ

๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน ดังนี้

- การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว
- การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุม และ

จำกัดสิทธิเพื่อเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม

- การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม
- การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ
- ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๗. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๗.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหาย หรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการอนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) ไม่ติดตั้งซอร์สโค้ด คอมไพเลอร์ (complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

(๕) กำหนดให้มีการจัดเก็บซอร์สโค้ด (source code) และไลบรารี่ (libraly) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ เป็นต้น

(๗) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(๘) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้นตามระยะเวลาที่เหมาะสม

(๙) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุง

ก่อนที่จะเริ่มต้นทำการพัฒนา

๗.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๗.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๗.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น และมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชัน (version) ที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

(๒) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการดังนี้

- มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

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

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการล็อกอิน (login) ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น (figuration) ของระบบ

(๘) ข้อมูลแสดงการใช้งานแอพพลิเคชั่น (application)

(๙) ข้อมูลการล็อกอิน (login) ทั้งที่สำเร็จและไม่สำเร็จ

(๑๐) ข้อมูลไอพีแอดเดรส (ip-address) ที่เข้าถึง

(๑๑) ข้อมูลโพรโตคอล (protocol) เครือข่ายที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)

๘.๑ ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (data center)

(๑) ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงานพื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือ

ระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

(๒) ให้ศูนย์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๓) ให้ศูนย์กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๔) ในกรณีที่หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

(๕) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำหรือเครื่องดับเพลิงระบบปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้สามารถมั่นใจได้ว่า ระบบทำงานตาม ปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๖) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๘.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (cabling security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ให้มีการปิดใส่กุญแจ เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

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

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับ

สัญญาณ โดยผู้ไม่ประสงค์ดี

๘.๓ การบำรุงรักษาอุปกรณ์ (equipment maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่ผู้ผลิตแนะนำ

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบ หรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้จับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘.๔ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (removal of property)

(๑) กำหนดให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกจากหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๘.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (security of equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) สร้างจิตสำนึกให้เจ้าหน้าที่รับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

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

(๑) กำหนดให้มีทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๙. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless)

๙.๑ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย

๙.๒ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๙.๓ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๙.๔ ผู้ดูแลระบบเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่

๙.๕ ผู้ดูแลระบบต้องกำหนดค่าของการใช้งานให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

๙.๖ ผู้ดูแลระบบต้องมีการแยก VLAN ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๙.๗ ผู้ดูแลระบบต้องใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

๑๐. การควบคุมการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑๐.๑ การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพา ผู้ใช้จะต้องนำมาลงทะเบียนที่ศูนย์ก่อน ซึ่งจะมีการกำหนดชื่อเครื่อง เพื่อง่ายต่อการตรวจสอบ หากก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์ของหน่วยงาน

(๒) การตั้งชื่อเครื่องคอมพิวเตร์แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ศูนย์เท่านั้น

(๓) เจ้าหน้าที่ศูนย์มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์แบบพกพาส่วนตัว

(๔) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหายและตรวจสอบ ซ่อมแซม หากเครื่องคอมพิวเตอร์แบบพกพาส่วนตัวเกิดความเสียหายด้วยตนเอง

๑๐.๒ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์

(๑) ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพาส่วนตัว

(๒) หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาส่วนตัวติดชุดคำสั่งไม่พึงประสงค์ ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

๑๑. การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑๑.๑ การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่อนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้น ผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ

(๒) โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

(๓) ไม่อนุญาตให้ ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๔) การตั้งชื่อเครื่องคอมพิวเตอร์จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เท่านั้น

(๕) การเคลื่อนย้ายจุดติดตั้งหรือตรวจซ่อมคอมพิวเตอร์จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เท่านั้น

(๖) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๗) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ใช้งานอยู่

(๘) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยปฏิบัติ ดังนี้

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๑๑.๒ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์

(๑) เจ้าหน้าที่ศูนย์มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้ต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk , Thumb Drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๓) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งานเสมอ

(๔) ผู้ใช้ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๑๑.๓ การสำรองข้อมูลและการกู้คืน

เจ้าหน้าที่ศูนย์ต้องรับผิดชอบในการสำรองข้อมูล และเก็บรักษาข้อมูล เมื่อผู้ใช้นำเครื่องคอมพิวเตอร์มาทำการตรวจสอบ ซ่อมแซม และหากทำการตรวจสอบ ซ่อมแซมจนเครื่องคอมพิวเตอร์สามารถใช้งานได้ตามปกติเป็นที่เรียบร้อยแล้ว ก็ต้องทำการเคลื่อนย้ายข้อมูลกลับไปให้คงเดิม

๑๒. การควบคุมการเข้า-ออกห้องศูนย์คอมพิวเตอร์

๑๒.๑ คำจำกัดความของผู้ที่เกี่ยวข้อง

(๑) ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศภายในศูนย์

(๒) เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ของหน่วยงานที่มีสิทธิ์ในการเข้าออกสถานที่ อาคาร ห้อง

ต่าง ๆ

(๓) ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือดูแล ซ่อมบำรุงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของศูนย์

๑๒.๒ บทบาทและความรับผิดชอบ

(๑) ผู้อำนวยการศูนย์

- อนุมัติสิทธิ์การเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
- อนุมัติกระบวนการควบคุมการเข้า-ออกห้องศูนย์คอมพิวเตอร์

(๒) ผู้ดูแลระบบ มีหน้าที่ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องศูนย์คอมพิวเตอร์

๑๒.๓ กระบวนการควบคุมการเข้า-ออกห้องศูนย์คอมพิวเตอร์

(๑) ผู้ดูแลระบบ และเจ้าหน้าที่ มีแนวทางปฏิบัติดังนี้

- ผู้ดูแลระบบ มีการจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เช่น ส่วนของห้อง SERVER ห้องทำงาน ห้องอบรมคอมพิวเตอร์ เป็นต้น เพื่อสะดวกในการปฏิบัติงานและการควบคุมดูแลให้มีประสิทธิภาพยิ่งขึ้น
- ศูนย์ต้องมีการกำหนดสิทธิ์บุคคลในการเข้าออกห้องศูนย์คอมพิวเตอร์
- สิทธิ์ในการเข้า-ออกห้องต่าง ๆ ภายในห้องศูนย์ของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนจะขึ้นอยู่กับหน้าที่ที่ต้องปฏิบัติหรือได้รับคำสั่งเท่านั้น
- เจ้าหน้าที่ทุกคนต้องทำบัตรผ่านเข้าออกแบบ Contactless เพื่อใช้ในการเข้า-ออกห้องศูนย์ และใช้ระบบ Finger Scan เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์
- ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกศูนย์และห้องควบคุมระบบคอมพิวเตอร์

(๒) ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

- ผู้ติดต่อจากหน่วยงานภายนอกต้องได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบจึงจะสามารถเข้า-ออกภายในศูนย์ได้
- ผู้ติดต่อจากหน่วยงานภายนอกทุกคน (รวมถึงผู้ติดตาม) จะต้องลงบันทึกรายละเอียดการขอเข้ามาดำเนินการลงในสมุดบันทึก “การเข้า-ออกห้องศูนย์คอมพิวเตอร์”
- หากมีบุคคลภายนอกเข้ามาดำเนินการ ผู้อำนวยการศูนย์จะต้องมอบหมายให้เจ้าหน้าที่ศูนย์คอยควบคุมดูแลทุกครั้ง
- ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในหน่วยงานจะต้องควบคุมดูแลอย่างรัดกุม และได้รับอนุญาตจาก

ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

- เจ้าหน้าที่ของศูนย์ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน
- เจ้าหน้าที่ของศูนย์ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมอ

๑๓. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๓.๑ การใช้งานสำหรับผู้ใช้งาน (User)

(๑) เจ้าหน้าที่ในสังกัด หากต้องการติดต่องานราชการหรือติดต่อกับบุคคลภายนอก ให้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน หรือของส่วนราชการที่กำหนดให้เท่านั้น ห้ามนำไปใช้ติดต่อในเรื่องส่วนตัว และห้ามติดต่องานราชการผ่านระบบจดหมายอิเล็กทรอนิกส์ของเว็บไซต์ผู้ให้บริการอื่น

(๒) สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบ ผู้ใช้ทุกคนจะต้องทำการเปลี่ยนรหัสผ่านใหม่โดยทันที

(๓) ห้ามผู้ใช้ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติของระบบจดหมายอิเล็กทรอนิกส์

(๔) ผู้ใช้ต้องระมัดระวังการใช้งานจดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงานหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และมาแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

(๕) ผู้ใช้ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(๖) ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของหน่วยงาน เพื่อการทำงานของหน่วยงานเท่านั้น

(๗) หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น และทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(๘) ผู้ใช้ต้องทำการตรวจเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น

Executable File เช่น .exe .com เป็นต้น

(๙) ผู้ใช้ต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๑๐) ห้ามผู้ใช้ใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์ และต้องระบุชื่อผู้รับและหัวข้อให้ชัดเจน

(๑๑) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ต้องระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(๑๒) ผู้ใช้ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(๑๓) ผู้ใช้ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

(๑๔) ผู้ใช้ต้องย้ายจดหมายอิเล็กทรอนิกส์ที่จำเป็นต้องนำมาใช้ในภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อป้องกันผู้อื่นแอบเข้าไปแอบอ่านจดหมายได้ ดังนั้น ไม่จัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

(๑๕) การใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน จะถือว่าผู้ที่เข้าใช้บริการรับทราบ ทำความเข้าใจและยอมรับนโยบายจดหมายอิเล็กทรอนิกส์ของหน่วยงานแล้ว

๑๓.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (Administrator)

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อให้ผู้ใช้รายใหม่พร้อมรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์

(๓) รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น ‘X’ , ‘O’ ในการพิมพ์แต่ละตัวอักษร

(๔) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไป ไม่เกิน ๓ ครั้ง

(๕) ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ และมีการ Logout ออกจากหน้าจอ เพื่อตัดการใช้งานของผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้

๑๔. การใช้งานระบบอินเตอร์เน็ต (Internet)

๑๔.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ การเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ได้จัดสรรไว้ให้เท่านั้น เช่น Proxy , Firewall เป็นต้น **ห้าม**มิให้ผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น

๑๔.๒ เครื่องคอมพิวเตอร์ส่วนบุคคล ก่อนทำการเชื่อมต่ออินเตอร์เน็ตจะต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์ และต้องมีการติดตั้งโปรแกรมป้องกันไวรัสก่อนเสมอ

๑๔.๓ เครื่องคอมพิวเตอร์แบบพกพาส่วนตัวไม่อนุญาตให้ใช้อินเตอร์เน็ต

๑๔.๔ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องผ่านระบบตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนจะทำการรับส่งข้อมูลทุกครั้ง

๑๔.๕ กำหนดให้หน้าแรกของ browser Internet เป็นหน้าเว็บ Intranet

๑๔.๖ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

๑๔.๗ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน

๑๔.๘ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

๑๔.๙ ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือ ภาพที่มีลักษณะลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

๑๔.๑๐ ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสื่อมเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๔.๑๑ ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๔.๑๒ ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเตอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๑๔.๑๓ ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความยั่วยุ เสียดสี ด่าทอ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน และเป็นการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น

๑๕. การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ (Conversion)

๑๕.๑ ข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลงต้องมีความหมายหรือรูปแบบเหมือนกับเอกสารและข้อความเดิม ซึ่งนำมาจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยผู้จัดทำหรือแปลงจะต้องตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์นั้น มีความหมายและรูปแบบเหมือนกับเอกสารและข้อความเดิม

๑๕.๒ ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงขึ้นด้วยวิธีการที่เชื่อถือได้ และมีการระบุตัวตนของผู้จัดทำหรือแปลงข้อมูลนั้น ๆ

๑๕.๓ ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงโดยมีเทคโนโลยีและมาตรการป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไขเกิดขึ้นกับข้อมูลนั้น เว้นแต่การรับรองหรือบันทึกเพิ่มเติม ซึ่งไม่มีผลต่อความหมายของข้อมูลอิเล็กทรอนิกส์

๑๕.๔ ผู้จัดทำหรือแปลงข้อมูลอิเล็กทรอนิกส์จะต้องรับผิดชอบในข้อผิดพลาดหรือความเสียหายที่เกิดจากข้อมูลที่ตนเป็นผู้จัดทำหรือแปลงนั้น

๑๖. การนำข้อมูลต่าง ๆ เผยแพร่ลงในเว็บไซต์ (Web Information)

๑๖.๑ ข้อมูลที่จะนำมาลงจะต้องได้รับความเห็นชอบ, อนุมัติหรือคำสั่งจากผู้บริหาร, ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการศูนย์

๑๖.๒ ข้อมูลจะนำมาลงจะต้องเป็นข้อมูลที่ไม่ก่อให้เกิดความเสียหายต่อผู้อื่น และหน่วยงาน หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม

๑๖.๓ ผู้มีหน้าที่ลงข้อมูลจะต้องได้รับอนุญาตจากผู้บริหาร, ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการศูนย์ และเป็นเจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมายเท่านั้น

๑๖.๔ กรณีเจ้าหน้าที่ในหน่วยงานที่ไม่อยู่ในสังกัดของศูนย์ ผู้ดูแลระบบจะต้องกำหนดสิทธิ์การเข้าถึง การลงข้อมูลให้แก่เจ้าหน้าที่ดังกล่าว เพื่อไม่ให้เกิดความเสียหายกับข้อมูลอื่นใดที่ไม่อยู่ในความรับผิดชอบ

๑๗. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๗.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๗.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๑๗.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๘. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

๑๘.๑ จัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง ชัดเจน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๑๘.๒ ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย

๑๘.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการเข้าใช้งานอินเตอร์เน็ตหรืออีเมล์ เป็นต้น

๑๙. การจัดการระบบเครือข่ายแบบรวมศูนย์ (Active Directory : AD)

เพื่อควบคุมความปลอดภัยของข้อมูล และให้สามารถกำหนดสิทธิของผู้ใช้งาน ให้ปฏิบัติดังต่อไปนี้

๑๙.๑ ทุกเครื่องที่อยู่ในระบบเครือข่ายจะต้องเข้าสู่ระบบเครือข่ายแบบรวมศูนย์

๑๙.๒ กำหนดให้ผู้ดูแลระบบมีหน้าที่ในการกำหนด Policy ต่าง ๆ และกำหนดสิทธิ์ของผู้ใช้งานโดยผ่านความเห็นชอบจากผู้บริหาร, ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการศูนย์

๑๙.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการเข้าใช้งานอินเตอร์เน็ตหรืออีเมล์ เป็นต้น

๒๐. การใช้งาน Token

๒๐ .๑ ทุกในการเข้าใช้ระบบคอมพิวเตอร์และอุปกรณ์ของกรมบังคับคดีทุกครั้ง ต้องยืนยันตัวบุคคลโดยใช้อุปกรณ์ Token หรือรหัสผ่านตามสิทธิการใช้งาน

๒๐ .๒ กรณีผู้ใช้งานลืมอุปกรณ์ Token ทำให้ไม่สามารถเข้าถึงระบบปฏิบัติการได้ ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว โดยจะเปิดสิทธิให้ใช้งาน ๑ วันทำการ

๒๐ .๓ ผู้ใช้งานสามารถเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตนเอง ให้ผู้ใช้งานใช้รหัสผู้ใช้(Username) และรหัสผ่าน(Password) จากอุปกรณ์ Token ของตนเอง เพื่อยืนยันตัวตนในการเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตนเอง

๒๐.๔ กรณีผู้ใช้ย้ายหน่วยงาน ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ เพื่อขอให้ทำการย้าย User Profile และกำหนดสิทธิของผู้ใช้งาน ให้กับเครื่องคอมพิวเตอร์เครื่องใหม่ และนำอุปกรณ์ Token ของตนเองติดตามตัวไปด้วย

๒๐.๕ กรณีอุปกรณ์ Token ชำรุดไม่สามารถใช้งานได้ ให้ผู้ใช้งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว พร้อมส่งคืนอุปกรณ์ Token เพื่อจะได้ดำเนินการแก้ไขต่อไป

๒๐.๖ กรณีอุปกรณ์ Token ชำรุดที่ไม่ได้เกิดจากการใช้งานตามปกติ ให้ผู้ใช้ งานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว ทางกรมจะดำเนินการซ่อมแซม และเรียกเก็บ ค่าใช้จ่ายที่เกิดขึ้น หากซ่อมไม่ได้ผู้ใช้ งานต้องชดใช้เงินตามราคาอุปกรณ์ Token

๒๐.๗ กรณีผู้ใช้ งาน ทำอุปกรณ์ Token สูญหาย ให้ผู้ใช้ งาน ทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อขอเปิดสิทธิของผู้ใช้งานชั่วคราว ผู้ใช้งานจะต้องชดใช้เงินตามราคาอุปกรณ์ Token

๒๐.๘ กรณีผู้ใช้ลาออก ให้ผู้ใช้งานส่งคืนอุปกรณ์ Token ตามหน่วยงานที่สังกัด และให้หน่วยงานทำบันทึกเสนอผู้บังคับบัญชาตามลำดับชั้นมาที่ผู้อำนวยการศูนย์สารสนเทศ พร้อมอุปกรณ์ Token

ส่วนที่ ๒

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถบริการได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางดังนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๑.๒ 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
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ด้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๒. ต้องจัดทำแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นเวลานาน ไฟไหม้ แผ่นดินไหว เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่ต้องการติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ที่มีความเกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนการเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ

๒. ผู้ตรวจสอบภายใน (Internal Auditor)

๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินงานโดยผู้ตรวจสอบภายในของหน่วยงาน เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อย ปีละ ๑ ครั้ง

๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๔

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของหน่วยงาน

๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน

๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ผ่านทางเว็บไซต์ของหน่วยงาน

๓. มีการประชาสัมพันธ์ให้ความรู้ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้โดยง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๔. มีการติดตามประเมินผล และสำรวจความต้องการของผู้ใช้งานอยู่เสมอ