ประกาศกรมสอบสวนคดีพิเศษ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมสอบสวนคดีพิเศษ
พ.ศ. ๒๕๖๖

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติมกำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานภาครัฐ โดยอาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ เพื่อให้การใช้งานด้านระบบเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษมีประสิทธิภาพ มีความมั่นคงปลอดภัย และเชื่อถือได้ กรมสอบสวนคดีพิเศษ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศกรมสอบสวนคดีพิเศษ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๖"

ข้อ ๒ ให้ยกเลิก "ประกาศกรมสอบสวนคดีพิเศษ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๒"

ข้อ ๓ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๔ ในประกาศนี้

(๑) **ผู้ใช้งาน (User)** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง หรือผู้ใช้งานทั่วไปที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

(๒) **บัญชีผู้ใช้ (User Account)** หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

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

(๔) **สินทรัพย์ (Asset)** หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

(๕) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๖) **ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)** หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (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) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๙) ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

(๑๐) นโยบาย (Policy) หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑๑) ผู้บริหาร หมายความว่า อธิบดีกรมสอบสวนคดีพิเศษ หรือรองอธิบดีกรมสอบสวนคดีพิเศษหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) หรือผู้ที่อธิบดีกรมสอบสวนคดีพิเศษมอบหมายให้ดูแลรับผิดชอบงานบริหารด้านเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษ หรือผู้อำนวยการกอง/สำนัก หรือเทียบเท่า

(๑๒) หน่วยงาน หมายความว่า กรมสอบสวนคดีพิเศษ และให้หมายความรวมถึงหน่วยงานภายในของกรมสอบสวนคดีพิเศษด้วย

(๑๓) ผู้บริหารระดับสูงสุด หมายความว่า อธิบดีกรมสอบสวนคดีพิเศษ

(๑๔) ระบบอินเทอร์เน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๑๕) ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศให้หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นองค์ประกอบ

(๑๖) ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง ให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๑๗) ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

(๑๘) หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานภายนอกกรมสอบสวนคดีพิเศษที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(๑๙) จดหมายอิเล็กทรอนิกส์ (E-Mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน โดยใช้มาตรฐาน SMTP, POP๓ หรือ IMAP

(๒๐) สื่อบันทึกพกพา หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล

(๒๑) ชื่อผู้ใช้ (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิการใช้งานไว้

(๒๒) รหัสผ่าน (Password) หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

(๒๓) การเข้ารหัส (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัส เพื่อป้องกันการลักลอบเข้าถึงข้อมูล ผู้ที่สามารถเปิดข้อมูลที่เข้ารหัสไว้ จะต้องมีโปรแกรมในการถอดรหัส เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

(๒๔) อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

(๒๕) การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า กระบวนการในการยืนยันความถูกต้องของผู้ใช้ที่แสดงตนว่าเป็นบุคคลที่กล่าวอ้างตามสิทธิที่กำหนดไว้

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

(๒๗) WPA (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในการแลกเปลี่ยนข้อมูลในระบบเครือข่ายไร้สาย

(๒๘) MAC Address (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่ายโดยจะมีหมายเลขที่ไม่ซ้ำกัน

(๒๙) SSL-VPN (Secure Socket Layer Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริง จะทำโดยการเข้ารหัสเฉพาะแล้วทำการรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่น ไม่สามารถเข้าถึงข้อมูลที่เข้ารหัสไว้ได้

(๓๐) แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผัง ซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

(๑) การจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑.๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการจัดทำ

(๑.๒) จัดทำนโยบายเป็นลายลักษณ์อักษร และประกาศให้ผู้ใช้งานได้ทราบผ่านเว็บไซต์ของหน่วยงานหรือช่องทางอื่นใดที่สามารถเข้าถึงได้อย่างสะดวก

(๑.๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติให้ชัดเจน

(๑.๔) มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

(๒) รายละเอียดของนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(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) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

(๒.๑.๘) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

(๒.๑.๙) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

(๒.๑.๑๐) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๒.๑.๑๑) การใช้ห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

(๒.๒) ระบบสารสนเทศและระบบสำรองของสารสนเทศ

กำหนดให้มีการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง พร้อมทั้งทบทวนและทดสอบอย่างน้อยปีละ ๑ ครั้ง

(๒.๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๒.๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ สร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ การใช้งานและการจัดการฝึกอบรม

ข้อ ๖ ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) มีอย่างน้อย ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๗ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งาน เพื่อการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ควบคุมไม่ให้สินทรัพย์สารสนเทศอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ ควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องมีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ(Remote Diagnostic and Configuration Port Protection) ต้องมีการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

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

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(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) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) อย่างน้อย ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ต้องกำหนดข้อปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกสำนักงาน

ข้อ ๑๒ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) พิจารณาคัดเลือกจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ และทบทวนแนวทางจัดทำระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) ความถี่ของการปฏิบัติในแต่ละข้อ มีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

ข้อ ๑๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

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

ข้อ ๑๔ ตรวจสอบและประเมินความเสี่ยง ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๕ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกรมสอบสวนคดีพิเศษ โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง "แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

ข้อ ๑๖ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบ ต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศ ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศหรือกรณีอื่นใดตามประกาศ กฎระเบียบหรือกฎหมายที่เกี่ยวข้องกำหนด

ข้อ ๑๗ บทบาทหน้าที่ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติ ดังนี้

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) มีหน้าที่กำกับดูแลการใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) ผู้อำนวยการศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบ การใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ

ประกาศ ณ วันที่ ๑๕ เดือน กันยายน พ.ศ. ๒๕๖๖

พันตำรวจตรี

(สุริยา สิงหกมล)

อธิบดีกรมสอบสวนคดีพิเศษ

บัญชีแนบท้ายประกาศกรมสอบสวนคดีพิเศษ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมสอบสวนคดีพิเศษ
พ.ศ. ๒๕๖๖

คำนำ

กรมสอบสวนคดีพิเศษ เป็นหน่วยงานบังคับใช้กฎหมายตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗ และที่แก้ไขเพิ่มเติม ซึ่งมีภารกิจเกี่ยวกับการป้องกัน การปราบปราม การสืบสวนและการสอบสวนคดีความผิดทางอาญาที่ต้องดำเนินการสืบสวนและสอบสวนโดยใช้วิธีการพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ ซึ่งกรมสอบสวนคดีพิเศษใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารในการขับเคลื่อนการดำเนินการตามภารกิจ เพื่อให้บรรลุผลตามวิสัยทัศน์ในการเป็นองค์การหลักในการบังคับใช้กฎหมายกับอาชญากรรมพิเศษตามมาตรฐานสากล ประกอบกับ ปัจจุบันกรมสอบสวนคดีพิเศษและหน่วยงานของรัฐต่างตกเป็นเป้าหมายของอาชญากรทางเทคโนโลยี ซึ่งอาศัยเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็วเป็นเครื่องมือในการโจมตี และมีการดำเนินการอย่างต่อเนื่อง

ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่กรมสอบสวนคดีพิเศษจะต้องทบทวน ปรับปรุง และยกระดับมาตรการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ รวมทั้งแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ ให้มีความทันสมัยและรองรับกับเทคโนโลยีในปัจจุบัน เพื่อเป็นแนวทางในการปฏิบัติในการป้องกันและรักษาความมั่นคงปลอดภัยด้านเสารสนเทศของกรมสอบสวนคดีพิเศษต่อไป จึงได้มีการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๖ เพื่อใช้เป็นแนวทางในการปฏิบัติโดยทั่วกัน

กรมสอบสวนคดีพิเศษ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

บทนำ

๑. หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานภาครัฐ เพื่อให้การใช้งานด้านระบบเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษมีประสิทธิภาพ มีความมั่นคงปลอดภัยของข้อมูล และเชื่อถือได้ จึงต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ กรมสอบสวนคดีพิเศษจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศต่อไป

๒. วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ ฉบับนี้มีวัตถุประสงค์เพื่อ

๑) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

๒) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล ระบบสารสนเทศ เทคโนโลยีและการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

๓) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของกรมสอบสวนคดีพิเศษมีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศของกรมสอบสวนคดีพิเศษ และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษ

๓. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ ประกอบด้วยวัตถุประสงค์ ผู้รับผิดชอบ และรายละเอียดหรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษ

๔. บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของกรมสอบสวนคดีพิเศษ บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุนและติดตามการประยุกต์ใช้โดยอธิบดีกรมสอบสวนคดีพิเศษ กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อธิบดีกรมสอบสวนคดีพิเศษเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๕. การเผยแพร่และทบทวน

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษฉบับนี้จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยแนวนโยบายและแนวปฏิบัติได้นำออกเผยแพร่ในระบบเว็บไซต์ภายใน (Intranet) ของกรมสอบสวนคดีพิเศษ รวมถึงมีการจัดทำบันทึกแจ้งเวียนเพื่อให้บุคลากรกรมสอบสวนคดีพิเศษและบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๖. คำนิยาม

(๑) ผู้ใช้งาน (User) หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง หรือผู้ใช้งานทั่วไปที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

(๒) บัญชีผู้ใช้ (User Account) หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

(๓) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๔) สินทรัพย์ (Asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

(๕) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๖) ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (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) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๙) ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

(๑๐) นโยบาย (Policy) หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑๑) ผู้บริหาร หมายความว่า อธิบดีกรมสอบสวนคดีพิเศษ หรือรองอธิบดีกรมสอบสวนคดีพิเศษหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) หรือผู้ที่อธิบดีกรมสอบสวนคดีพิเศษมอบหมายให้ดูแลรับผิดชอบงานบริหารด้านเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษ หรือผู้อำนวยการกอง/สำนัก หรือเทียบเท่า

(๑๒) หน่วยงาน หมายความว่า กรมสอบสวนคดีพิเศษ และให้หมายความรวมถึงหน่วยงานภายในของกรมสอบสวนคดีพิเศษด้วย

(๑๓) ผู้บริหารระดับสูงสุด หมายความว่า อธิบดีกรมสอบสวนคดีพิเศษ

(๑๔) ระบบอินเทอร์เน็ต หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๑๕) ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศให้หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นองค์ประกอบ

(๑๖) ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง ให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๑๗) ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

(๑๘) หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานภายนอกกรมสอบสวนคดีพิเศษที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(๑๙) จดหมายอิเล็กทรอนิกส์ (E-Mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน โดยใช้มาตรฐาน SMTP, POP๓ หรือ IMAP

(๒๐) สื่อบันทึกพกพา หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล

(๒๑) ชื่อผู้ใช้ (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิการใช้งานไว้

(๒๒) **รหัสผ่าน** (Password) หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

(๒๓) **การเข้ารหัส** (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัส เพื่อป้องกันการลักลอบเข้าถึงข้อมูล ผู้ที่สามารถเปิดข้อมูลที่เข้ารหัสไว้ จะต้องมีโปรแกรมในการถอดรหัส เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

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

(๒๕) **การพิสูจน์ยืนยันตัวตน** (Authentication) หมายความว่า กระบวนการในการยืนยันความถูกต้องของผู้ใช้ที่แสดงตน ว่าเป็นบุคคลที่กล่าวอ้างตามสิทธิที่กำหนดไว้

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

(๒๗) WPA (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในการแลกเปลี่ยนข้อมูลในระบบเครือข่ายไร้สาย

(๒๘) MAC Address (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่ายโดยจะมีหมายเลขที่ไม่ซ้ำกัน

(๒๙) SSL-VPN (Secure Socket Layer Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริง จะทำโดยการเข้ารหัสเฉพาะแล้วทำการรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่น ไม่สามารถเข้าถึงข้อมูลที่เข้ารหัสไว้ได้

(๓๐) **แผนผังระบบเครือข่าย** (Network Diagram) หมายความว่า แผนผัง ซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

ส่วนที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อเป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้รับผิดชอบและผู้ที่เกี่ยวข้องได้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. ผู้ใช้งาน

แนวปฏิบัติ

๑๑.การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัย ให้ปฏิบัติดังนี้

๑.๑ จัดทำบัญชีสินทรัพย์ ซึ่งจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(๑) การกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ให้กำหนดตามที่แต่ละระบบออกแบบไว้

(๒) กำหนดเกณฑ์การระงับสิทธิการมอบอำนาจ ให้เป็นไปตามที่กำหนดไว้ในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการใช้งานระบบสารสนเทศของหน่วยงานจะต้องปฏิบัติดังนี้

(๓.๑) ขออนุญาตเป็นลายลักษณ์อักษรโดยใช้แบบฟอร์มที่กำหนดหรือจัดทำเป็นหนังสือหรือผ่านระบบสารสนเทศ และผ่านการพิจารณาเบื้องต้นจากผู้บังคับบัญชาก่อน

(๓.๒) ผู้อำนวยการศูนย์สารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมายตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน

(๓.๓) ผู้ดูแลระบบที่ได้รับมอบหมายแจ้งรหัสการใช้งานโดยใส่ซองปิดผนึกส่งกลับไปยังผู้ที่ขออนุญาตใช้งาน

(๓.๔) กรณีตรวจสอบแล้วพบว่าบุคคลดังกล่าวไม่มีสิทธิในการใช้งาน จะแจ้งกลับไปยังผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร

(๓.๕) ผู้ใช้งานจะต้องลงทะเบียนยืนยันตัวตนเพื่อใช้งานระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือตามที่ศูนย์สารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมายกำหนด

๑.๓ ขั้นตอนปฏิบัติในการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล แบ่งออกเป็น

(๑.๑) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ คำรับรองการปฏิบัติราชการ ข้อมูลบุคลากร งบประมาณ การเงินและบัญชี

(๑.๒) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ กฎหมายในชีวิตประจำวัน กฎหมายระเบียบ ข้อบังคับ คำสั่ง รวมถึงอนุบัญญัติที่กำหนดขึ้นตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.๒๕๔๗

(๑.๓) ข้อมูลสารสนเทศด้านการสืบสวนสอบสวนคดีพิเศษ ได้แก่ ข้อมูลเกี่ยวกับคดีพิเศษ ข้อมูลเกี่ยวกับคดีสืบสวน ข้อมูลอื่นที่เกี่ยวกับการสืบสวนสอบสวนคดีพิเศษ

(๒) การจัดแบ่งระดับความสำคัญของข้อมูล แบ่งออกเป็น

(๒.๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒.๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๒.๓) ข้อมูลที่มีระดับความสำคัญน้อย

(๓) การจัดแบ่งลำดับชั้นความลับของข้อมูล แบ่งออกเป็น

(๓.๑) ข้อมูลชั้นลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(๓.๒) ข้อมูลชั้นลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

(๓.๓) ข้อมูลชั้นลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

(๓.๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่ไม่มีความลับสามารถเปิดเผยได้

(๔) การแบ่งระดับชั้นการเข้าถึง แบ่งออกเป็น

(๔.๑) เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ

(๔.๒) เข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิจากเจ้าของระบบงานแล้วเท่านั้น

(๔.๓) เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง

(๔.๔) เข้าถึงได้ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว

(๕) การกำหนดเวลาที่เข้าถึงได้ แบ่งออกเป็น

(๕.๑) ในเวลาราชการ ได้แก่ วันจันทร์ – ศุกร์ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.

(๕.๒) นอกเวลาราชการที่ได้รับอนุญาต ได้แก่ วันจันทร์ – ศุกร์ เวลา ๑๖.๓๐ – ๒๐.๓๐ น.

(๕.๓) วันหยุดราชการและวันหยุดนักขัตฤกษ์ที่ได้รับอนุญาต ได้แก่ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.

(๕.๔) ตลอดเวลา

(๕.๕) เวลาอื่นตามที่ระบุไว้ให้เข้าถึงได้

(๖) การกำหนดช่องทางที่สามารถเข้าถึงได้ แบ่งออกเป็น

(๖.๑) อินทราเน็ต (Intranet)

(๖.๒) อินเทอร์เน็ต (Internet)

(๖.๓) เครือข่ายส่วนตัวเสมือน (VPN)

๒. การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

เพื่อควบคุมการเข้าถึงสารสนเทศตามภารกิจให้ปฏิบัติ ดังนี้

๒.๑ ต้องควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศให้สอดคล้องกับหน้าที่ความรับผิดชอบในการการปฏิบัติงาน ดังนี้

(๑) ผู้ดูแลระบบรับผิดชอบในการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

(๒) ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๒.๒ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

(๑) ทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เมื่อได้รับเอกสารแจ้งจากหน่วยงานต้นสังกัดของผู้ใช้งานระบบหรือกลุ่มบริหารทรัพยากรบุคคลหรือหน่วยงานอื่น เพื่อปรับปรุงการให้สิทธิ์แก่ผู้ใช้งานให้สอดคล้องกับการปฏิบัติงานที่เปลี่ยนไป เช่น เปลี่ยนแปลงตำแหน่งงาน ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน ภายในองค์กร เป็นต้น

(๒) หน่วยงานต้นสังกัดของผู้ใช้งานหรือกลุ่มบริหารทรัพยากรบุคคล ต้องแจ้งเอกสารอย่างเป็นทางการหรือแจ้งผ่านระบบสารสนเทศให้ ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบหรือผู้ดูแลระบบเพื่อกำหนดสิทธิ์ตามหน้าที่ความรับผิดชอบในการปฏิบัติงานเมื่อมีผู้ใช้งานใหม่เข้ามาปฏิบัติงานหรือยกเลิกสิทธิ์ต่าง ๆ ในการเข้าใช้ระบบสารสนเทศเมื่อมีผู้ใช้งานโยกย้ายหรือลาออก เป็นต้น

๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตให้ปฏิบัติ ดังนี้

๓.๑ ต้องประชาสัมพันธ์เผยแพร่ความรู้เกี่ยวกับการสร้างความตระหนัก เรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)

๓.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งานเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมาตรการเชิงป้องกันตามความเหมาะสม

๓.๓ การลงทะเบียนผู้ใช้งาน (User Registration)

(๑) ผู้ดูแลระบบจัดทำแบบคำขอใช้ระบบสารสนเทศ ตามที่ ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กำหนด โดยระบุข้อมูลพื้นฐาน ได้แก่ เลขประจำตัวประชาชน ชื่อ-นามสกุล ตำแหน่ง หน่วยงาน หมายเลขโทรศัพท์

(๒) ผู้ใช้งานกรอกข้อมูลคำขอตามแบบคำขอใช้ระบบสารสนเทศ และได้รับความเห็นชอบผู้บังคับบัญชาระดับผู้อำนวยการกอง/สำนัก หรือเทียบเท่า

(๓) ผู้ดูแลระบบต้องตรวจสอบและกำหนดสิทธิที่เหมาะสมในการเข้าถึงตามหน้าที่ความรับผิดชอบ

(๔) ผู้ดูแลระบบต้องจัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งผู้ขอใช้งานต้องลงนามรับทราบด้วย

(๕) ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) จากชื่อภาษาอังกฤษและตามด้วยอักษรสามตัวแรก ของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สี่ หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๖) ผู้ดูแลระบบต้องบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศและจัดเก็บย้อนหลังอย่างน้อย ๑ ปี

(๗) ผู้ดูแลระบบต้องกำหนดให้มีการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศทันทีเมื่อได้รับแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษรหรือผ่านระบบสารสนเทศ

๓.๔ กำหนดการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นๆที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๒) ผู้ดูแลระบบต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(๓) ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศให้เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ดูแลระบบ หรือผู้ใช้งานอื่นใดที่มีสิทธิในระดับสูง ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๕ กำหนดการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราวที่ยากต่อการคาดเดา และต้องมีความแตกต่างกัน

(๓) ผู้ดูแลระบบต้องกำหนดวันหมดอายุอย่างน้อยทุก ๓ เดือนสำหรับรหัสผ่านของผู้ใช้งานทุกคน

(๔) ผู้ดูแลระบบต้องส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ในการจัดส่งรหัสผ่าน

(๕) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนาม เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน ได้แก่ ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเข้าถึงระบบสารสนเทศ

(๖) ผู้ดูแลระบบต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบัน หรือข้อมูลอื่นที่สามารถยืนยันตัวตนของผู้ใช้งานได้ ให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๓.๖ ข้อกำหนดการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศโดยมีการปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง หรือเมื่อมีการเปลี่ยนแปลงอื่นใดในลักษณะเดียวกันนี้ และให้มีการทบทวนสิทธิผู้ใช้งานในระดับสูงอย่างน้อยปีละ ๒ ครั้ง พร้อมทั้งต้องบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่ได้ทำการทบทวน เพื่อใช้ในการตรวจสอบภายหลัง

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ การลักลอบทำสำเนาข้อมูลสารสนเทศ หรือการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้ปฏิบัติ ดังนี้

๔.๑ วิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งานเพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่านและการเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) กำหนดรหัสผ่าน ที่มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๑๐ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษเข้าด้วยกัน

(๔) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ตั้งรหัสผ่านโดยใช้ตัวเลขหรือตัวอักษรที่เรียงกัน หรือเหมือนกันทั้งหมด

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๙) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๐) ไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบหรือใช้งานแทนตน กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๑) ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๓ เดือน หรือเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้ต้องแจ้งให้ ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลตรวจสอบ ทราบทันที

(๑๒) ต้องเปลี่ยนรหัสผ่านสำหรับผู้ดูแลระบบ อย่างน้อยทุก ๆ ๑ เดือน

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

(๑๔) การเปลี่ยนรหัสผ่านต้องหลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๕) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น และไม่เก็บไว้ในระบบคอมพิวเตอร์

(๑๖) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานของตน เว้นแต่พิสูจน์ได้เป็นอย่างอื่น

(๑๗) ผู้ใช้งานจะได้รับการร้องขอจาก ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ ให้ทำการเปลี่ยนรหัสผ่านใหม่ ในกรณีที่รหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัยสามารถถูกคาดเดาหรือถูกล่วงละเมิดได้ง่าย ทั้งนี้ผู้ใช้งานต้องตรวจสอบ ความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวง

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ให้ปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๒) ผู้ใช้งานต้องตั้งค่าเครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๕ นาที โดยต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๓) ผู้ใช้งานต้องล็อคหรือใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

(๔) ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานและต้องปฏิบัติตามแนวปฏิบัติในการป้องกันนี้อย่างเคร่งครัด

๔.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(๑.๑) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย โดยห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน โดยผิดกฎหมาย

(๑.๒) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

(๑.๓) ปิดเครื่องคอมพิวเตอร์ทุกครั้งหลังเลิกงานหรือไม่ใช้งาน

(๑.๔) ออกจากระบบ (Log Out) ออกจากระบบสารสนเทศหรือระบบคอมพิวเตอร์ทันทีเมื่อใช้งานเสร็จหรือจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

(๑.๕) การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงานไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

(๑.๖) ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

(๑.๗) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์จัดเก็บข้อมูล Disk Drive

(๑.๘) ต้องใช้ความระมัดระวังในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์ โดยใส่กล่องหรือห่อหุ้มด้วยวัสดุป้องกันการกระแทก เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

(๑.๙) การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑.๑๐) หลีกเลี่ยงการใช้ปลายปากกา หรือวัสดุอื่นใดกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้

(๑.๑๑) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๑.๑๒) ติดตั้งหรือจัดเก็บอุปกรณ์คอมพิวเตอร์บนชั้นวางคอมพิวเตอร์ ตู้ติดตั้งอุปกรณ์เครือข่าย กล่องใส่แผ่น CD/DVD หรือสิ่งอื่นใดที่เป็นอุปกรณ์เฉพาะสำหรับติดตั้งหรือเก็บรักษาที่มั่นคงแข็งแรง

(๑.๑๓) เพื่อความเป็นระเบียบและปลอดภัยสำหรับอุปกรณ์คอมพิวเตอร์ที่พกพาประเภท CD/DVD Thumb Drive หรือสิ่งอื่นใดลักษณะเดียวกันนี้ ให้จัดเก็บไว้ในสถานที่หรืออุปกรณ์เฉพาะที่สามารถปิดล็อคได้

(๑.๑๔) ต้องกำหนดสิทธิการเข้าใช้งาน โดยตั้งรหัสผ่านการเข้าใช้งานเครื่องคอมพิวเตอร์และปฏิบัติตามข้อกำหนดในวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use)

(๑.๑๕) ตรวจสอบ สายไฟ สายเมาส์ สายแป้นพิมพ์ หรือสายสัญญาณของอุปกรณ์คอมพิวเตอร์ อื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์คอมพิวเตอร์ได้รับความเสียหาย

(๑.๑๖) ทำความสะอาดอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละออง ที่จะทำให้เครื่องคอมพิวเตอร์เกิดการขัดข้อง/เสียหาย

(๑.๑๗) ต้องใช้วิธีการทางเทคนิคในการเข้ารหัสข้อมูลเพื่อเข้ารหัสข้อมูลสำคัญในเครื่องคอมพิวเตอร์

(๑.๑๘) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันเครื่องคอมพิวเตอร์มิให้ถูกขโมยหรือสูญหาย โดยล๊อคเครื่องขณะไม่ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหายให้เก็บไว้ในตู้ที่สามารถล็อคได้หรือวิธีอื่นตามเหมาะสม

(๑.๑๙) ห้ามนำเครื่องคอมพิวเตอร์ที่ไม่ใช่ของหน่วยงานมาใช้กับเครือข่ายหน่วยงาน เว้นแต่ได้รับการตรวจสอบและได้รับอนุญาตจากผู้ดูแลระบบ หรือศูนย์สารสนเทศกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ ก่อนการใช้งาน

(๑.๒๐) ห้ามเปลี่ยนแปลงหมายเลขไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงาน

(๑.๒๑) ต้องสำรองข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

(๑.๒๒) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกแบบภายนอกชนิด CD, DVD, External Hard Disk หรืออื่น ๆ ที่เหมาะสม

(๑.๒๓) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๒) ผู้ใช้งานต้องป้องกันและแก้ไขไวรัสคอมพิวเตอร์หรือซอฟต์แวร์ไม่ประสงค์ดี (Antivirus)

(๒.๑) ตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานมีโปรแกรมป้องกันไวรัสติดตั้งอยู่และต้องเปิดใช้งานตลอดเวลาที่ใช้งาน

(๒.๒) ปรับปรุงฐานข้อมูลป้องกันไวรัส (Update Virus Signature) ให้เป็นปัจจุบัน

(๒.๓) ห้ามทำการใดเพื่อขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

(๒.๔) รับไฟล์อิเล็กทรอนิกส์เฉพาะจากบุคคลที่ตนรู้จักหรือจากช่องทางการติดต่อสื่อสารที่น่าเชื่อถือเท่านั้น

(๒.๕) ต้องตรวจสอบหาไวรัสทุกครั้งหลังจากรับไฟล์อิเล็กทรอนิกส์จากแหล่งใด ๆ ก็ตามก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒.๖) ผู้ใช้ระบบต้องทำการอัปเดต (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

(๒.๗) ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวังโดยไม่เปิดเว็บไซต์ลามกอนาจาร เว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมหรือไฟล์ต่าง ๆ หรือพฤติการณ์อื่นใดที่มีความเสี่ยงต่อการติดไวรัส

(๒.๘) ห้ามติดตั้งโปรแกรมหรือซอฟต์แวร์อื่นใด จากแหล่งที่ไม่น่าเชื่อถือ

(๒.๙) ไม่เปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่ไม่รู้จักหรือชื่อเรื่องที่ไม่เคยติดต่อกันมาก่อน หรือสงสัยว่าไม่ปลอดภัย

(๒.๑๐) ไม่เปิด Share Drive หากมีความจำเป็นให้เปิดเพียง Share Folder โดยต้องใช้รหัสผ่าน และอนุญาตให้อ่านอย่างเดียว

(๒.๑๑) ไม่คลิกเปิดหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม

(๒.๑๒) ห้ามสร้าง เก็บ หรือเผยแพร่ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ หรือซอฟต์แวร์ไม่พึงประสงค์ดีอื่นใด

(๒.๑๓) ต้องให้ความสำคัญกับการแจ้งเตือนจากโปรแกรมป้องกันไวรัส หากมีข้อสงสัยหรือพบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติหรือโปรแกรมป้องกันไวรัสมีการแจ้งเตือนมากผิดปกติให้แจ้งผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบทันที

(๓) การยับยั้งหรือจำกัดความเสียหาย เมื่อเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์หรือโปรแกรมประสงค์ร้ายให้ผู้ที่ทำหน้าที่ป้องกันและแก้ไขไวรัสปฏิบัติ ดังนี้

(๓.๑) ให้แยกเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติออกจากเครือข่ายของหน่วยงานโดยถอดสาย LAN หรือปิดอุปกรณ์ไร้สาย (Wireless LAN)

(๓.๒) สำรองข้อมูลสำคัญในเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติ

(๓.๓) ตรวจหาไวรัสที่อาจจะฝังตัวอยู่กับข้อมูลที่สำรองไว้ก่อนนำข้อมูลไปใช้กับเครื่องคอมพิวเตอร์อื่น

(๓.๔) ในกรณีที่พบไฟล์ที่ติดไวรัสหรือไฟล์ที่เป็นโปรแกรมประสงค์ร้าย และซอฟต์แวร์ตรวจสอบไวรัสสามารถแก้ไขไวรัสที่ติดได้ ให้แก้ไขโดยใช้ซอฟต์แวร์ตรวจสอบไวรัส หากซอฟต์แวร์ตรวจสอบไวรัสไม่สามารถแก้ไขไวรัสที่ติดได้ ให้ลบไฟล์ที่ติดไวรัสหรือไฟล์ที่เป็นโปรแกรมประสงค์ร้ายทิ้ง

(๓.๕) ติดตั้งโปรแกรมส่วนแก้ไข (Update Patch) ตามความเหมาะสม ปรับปรุงเวอร์ชั่นซอฟต์แวร์ตรวจสอบไวรัส และปรับปรุงฐานข้อมูลป้องกันไวรัส (Update Virus Signature) ให้เป็นปัจจุบัน เพื่อเพิ่มประสิทธิภาพในการป้องกันไวรัส

(๔) การจัดการเอกสารลับบนกระดาษหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

(๔.๑) ต้องจัดหมวดหมู่เอกสารลับไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างเพียงพอ

(๔.๒) จำกัดการสำเนาเอกสารลับเท่าที่จำเป็นต้องใช้งานเท่านั้น

(๔.๓) ระมัดระวังการกระจาย ส่ง หรือแจกจ่ายเอกสารลับไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับทราบ หรือใช้งานเอกสารนั้นเท่านั้น

(๔.๔) ใช้วิธีการตามกฎหมายที่หน่วยงานได้ถือปฏิบัติอยู่แล้วสำหรับการจัดส่งเอกสารลับทางไปรษณีย์

(๕) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

(๖) เจ้าของข้อมูลจะต้องทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๗) เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลายสื่อหรือข้อมูลอิเล็กทรอนิกส์ ดังนี้

(๗.๑) แฟลชไดรฟ์ (Flash Drive) ใช้วิธีการทุบหรือบดให้เสียหาย

(๗.๒) กระดาษ หรือ แผ่น CD/DVD ใช้วิธีการหั่นด้วยเครื่องหั่นทำลายเอกสาร

(๗.๓) เทป ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย

(๗.๔) ฮาร์ดดิสก์ (Hard Disk) ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.22-M ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ

(๘) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องมีการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล

(๙) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยปฏิบัติตามระเบียบ หรือกฎหมายที่เกี่ยวข้องกับการรักษาความลับทางราชการ

(๑๐) ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เพื่อส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม หรือจำหน่าย หรือเพื่อการอื่น ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

(๑๑) ป้องกันไม่ให้บุคคลภายนอกเข้าถึงหรือใช้งานกล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้ โดยไม่ได้รับอนุญาต

(๑๒) นำเอกสารออกจากเครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้ทันทีที่ใช้งานเสร็จ

(๑๓) ในกรณีที่ต้องการนำสินทรัพย์สารสนเทศต่าง ๆ ออกจากพื้นที่ใช้งาน ต้องขออนุญาตจากผู้บังคับบัญชาก่อนทุกครั้ง

(๑๔) ผู้ใช้งานต้องคืนสินทรัพย์ทั้งหมดที่เกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ เมื่อพ้นจากการปฏิบัติหน้าที่

(๑๕) ผู้ดูแลระบบต้องระงับสิทธิ หรือถอดถอนสิทธิ หรือเรียกคืนสินทรัพย์ตามเห็นควร หากผู้ใช้งานไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑๖) การเผยแพร่ข้อมูลข่าวสารบนเว็บไซต์

(๑๖.๑) ข้อมูลที่จะนำขึ้นเว็บไซต์ต้องไม่ก่อให้เกิดความเสียหาย ละเมิดสิทธิ หรือสร้างความรำคาญแก่ผู้อื่น หรือผิดกฎหมาย หรือขัดต่อศีลธรรมอันดีของประชาชน

(๑๖.๒) การนำข้อมูลขึ้นเว็บไซต์ต้องใช้แบบฟอร์มหรือจัดส่งคำขอเป็นหนังสือราชการ หรือระบบสารสนเทศ ตามที่ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ หรือนโยบายของกรมสอบสวนคดีพิเศษ กำหนด

(๑๖.๓) ข้อมูลที่จะนำขึ้นเว็บไซต์ต้องได้รับความเห็นชอบจากผู้บริหาร หรือ ผู้อำนวยการกอง/สำนัก หรือเทียบเท่า หรือผู้ที่ได้รับมอบหมายหรือมีหน้าที่เกี่ยวกับการประชาสัมพันธ์และภาพลักษณ์องค์กรของกรมสอบสวนคดีพิเศษ

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๕.๑ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๒ การใช้งานระบบเครือข่ายอินเทอร์เน็ต (Internet)

(๑) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายอินเทอร์เน็ตจะต้องทำการลงทะเบียนผู้ใช้งาน

(๒) ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้หน่วยงาน และบุคคลผู้ที่เกี่ยวข้องกับหน่วยงาน เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

(๓) การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ หน่วยงานขอสงวนสิทธิในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

(๔) ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบ Pop-up หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

(๕) ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

(๖) หน่วยงานต้องไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวผ่านทางเว็บบอร์ด บล็อก หรือสื่อสังคมออนไลน์อื่นใด ทั้งนี้ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของผู้นั้น

(๗) ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์จากเว็บไซต์ หรือแหล่งข้อมูลที่ไม่น่าเชื่อถือหรือไม่ปลอดภัยต่อระบบสารสนเทศ

(๘) กรณีที่มีความจำเป็นต้องดาวน์โหลดข้อมูลหรือไฟล์ขนาดใหญ่เกิน ๕๐๐ MB ผ่านอินเทอร์เน็ต ต้องกระทำนอกเวลาทำการ เพื่อป้องกันผลกระทบต่อปริมาณข้อมูลในเครือข่าย

(๙) ตรวจสอบไวรัสในข้อมูลหรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตทุกครั้ง ก่อนติดตั้งหรือใช้งาน

(๑๐) ผู้ใช้งานมีหน้าที่ระมัดระวังการใช้งาน และต้องรับผิดชอบต่องานหรือผลที่เกิดจากการเรียกใช้บริการบนอินเทอร์เน็ตดังต่อไปนี้

(๑๐.๑) ไม่ใช้เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อสิทธิ เสรีภาพ หรือสินทรัพย์ของผู้อื่น

(๑๐.๒) ไม่ใช้เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๑๐.๓) ไม่ใช้เพื่อการค้า หรือผลประโยชน์ทางธุรกิจ

(๑๐.๔) ไม่ใช้เพื่อกระทำการอันเป็นการละเมิดเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๑๐.๕) ไม่ใช้เพื่อเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่กรมสอบสวนคดีพิเศษ ไม่ว่าจะเป็นข้อมูลของกรมสอบสวนคดีพิเศษ หรือบุคคลภายนอกก็ตาม

(๑๐.๖) ไม่ใช้เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของกรมสอบสวนคดีพิเศษ หรือของบุคคลอื่น

(๑๐.๗) ไม่ใช้เพื่อรบกวน หรือขัดขวางการใช้งานระบบเครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ทั้งในและนอกกรมสอบสวนคดีพิเศษ ไม่ให้สามารถใช้งานได้ตามปกติ

(๑๐.๘) ไม่ใช้เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของกรมสอบสวนคดีพิเศษไปยังที่อยู่เว็บ (Web Site) ใด ๆ ในลักษณะที่อาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริงหรือก่อให้เกิดความขัดแย้งในสังคม

(๑๐.๙) ไม่ใช้เพื่อการอื่นใดที่อาจก่อให้เกิดความเสียหายแก่กรมสอบสวนคดีพิเศษ

(๑๐.๑๐) หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ผู้ใช้งานต้องทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

(๑๑) ผู้ดูแลระบบสามารถระงับหรือยกเลิกสิทธิในการเรียกใช้บริการบนอินเทอร์เน็ตได้ทันทีเมื่อพบว่าผู้ใช้มีการกระทำเข้าข่ายไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๓ การใช้งานระบบเครือข่ายไร้สาย (Wireless)

(๑) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องทำการลงทะเบียนผู้ใช้งาน

(๒) ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการ ดังนี้

(๒.๑) ต้องลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๒.๒) ต้องลงทะเบียนอุปกรณ์ที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๒.๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภานอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๒.๔) ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๒.๕) ต้องเปลี่ยนชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและต้องเลือกใช้ชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสได้ง่าย

(๒.๖) ใช้การเข้ารหัสข้อมูลในการใช้สัญญาณ Wireless ไม่ต่ำกว่าเทคโนโลยี WPA (Wi-Fi Protected Access) เพื่อยากต่อการดักจับและทำให้ปลอดภัยมากที่สุด

(๒.๗) การเข้าใช้งานระบบเครือข่ายไร้สาย ต้องใช้วิธีการควบคุม MAC Address (Media Access Control Address) โดยผู้ใช้งานที่มีสิทธิในการเข้าใช้งานต้องมี MAC Address ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

(๒.๘) ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๒.๙) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการศูนย์สารสนเทศ ทราบโดยทันที

(๓) ข้อกำหนดในการขอใช้เครือข่ายคอมพิวเตอร์ไร้สาย

(๓.๑) ต้องเป็นบุคลากรในสังกัดกรมสอบสวนคดีพิเศษ

(๓.๒) ผู้ขอใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานต้องลงทะเบียนใช้งาน

(๓.๓) ห้ามผู้ใช้งานติดตั้งอุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) โดยไม่ได้รับอนุญาต

(๓.๔) การใช้บริการทางอินเทอร์เน็ตต้องปฏิบัติตามข้อกำหนดในการเรียกใช้บริการบนอินเทอร์เน็ต

(๔) ขั้นตอนการขอใช้เครือข่ายคอมพิวเตอร์ไร้สาย

(๔.๑) ผู้ขอใช้งานต้องมีคุณสมบัติตามข้อกำหนดในการขอใช้เครือข่ายคอมพิวเตอร์ไร้สาย

(๔.๒) ผู้ขอใช้งาน ต้องลงทะเบียนเพื่อยืนยันตัวตนก่อนเข้าใช้ระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

(๔.๓) ผู้ดูแลระบบสามารถระงับหรือยกเลิกสิทธิการใช้เครือข่ายคอมพิวเตอร์ไร้สายได้ทันทีเมื่อพบว่าผู้ใช้งานมีการกระทำเข้าข่ายไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๔ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) มีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบสารสนเทศต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)

(๒) ต้องตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศ โดยการยืนยันตัวบุคคล (Authentication) ด้วยรหัสผ่าน (Password)

(๓) การใช้งานระบบสารสนเทศภายในของกรมสอบสวนคดีพิเศษผ่านระบบอินเทอร์เน็ต ต้องใช้งานโดยเชื่อมต่อกับเครือข่ายส่วนตัวเสมือน (VPN : Virtual Private Network) ของกรมสอบสวนคดีพิเศษ

๕.๕ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

(๑) ระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย IP Address และ Mac Address

(๒) ผู้ดูแลระบบจัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่เชื่อมต่อกับเครือข่าย ได้แก่ รายละเอียดเครื่องคอมพิวเตอร์, IP Address, Mac Address, สถานที่ติดตั้ง, ชื่อผู้ใช้บริการ

(๓) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ หรือผู้ที่ได้รับอนุญาตเท่านั้น

(๔) ต้องใช้ไฟร์วอลล์ (Firewall) กำหนดหมายเลขอุปกรณ์ ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

(๕) จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

(๖) ต้องทำการทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อย ปีละ ๑ ครั้ง

๕.๖ การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

(๑) การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๒) ป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่ายและเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

(๔) ทำการติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๕.๗ ข้อกำหนดการแบ่งแยกเครือข่าย (Segregation in Networks) ให้แยก ดังนี้

(๑) Management Zone เป็นระบบเครือข่ายที่ใช้ในการควบคุมการบริหารจัดการระบบคอมพิวเตอร์และเครือข่าย

(๒) DMZ Zone เป็นระบบคอมพิวเตอร์และเครือข่ายที่ให้บริการข้อมูลข่าวสารทั้งภายในหน่วยงาน (Intranet Zone) และภายนอกหน่วยงาน (Extranet Zone)

(๓) Intranet Zone เป็นระบบเครือข่ายภายในหน่วยงาน สำหรับการใช้งานข้อมูลสารสนเทศที่มีความสำคัญและเข้าถึงได้เฉพาะบุคลากรของหน่วยงานที่ได้รับอนุญาตเท่านั้น

(๔) Extranet Zone เป็นระบบเครือข่ายเชื่อมต่อกับภายนอกหน่วยงานสำหรับการรับ-ส่งข้อมูลกับหน่วยงานภายนอก หรือการให้บริการประชาชน

๕.๘ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

(๑) จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

(๒) ระบบเครือข่ายทั้งหมดต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (IDS/IPS, Firewall)

(๓) การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยเพื่อยืนยันตัวบุคคล

(๔) ควบคุมการเชื่อมต่อทางเครือข่ายของผู้ใช้งานตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน

๕.๙ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

(๑) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๒) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

(๓) ต้องมีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยเครือข่ายภายในและภายนอก

(๔) ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๕.๑๐ ข้อกำหนดการป้องการบุกรุก (Firewall Policy)

(๑) ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Firewall) ทั้งหมด

(๒) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

(๓) ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อกโดยไฟร์วอลล์ (Firewall)

(๔) ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งาน

(๕) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ (Firewall) ได้แก่ ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องบันทึกการเปลี่ยนแปลงทุกครั้ง

(๖) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น

(๗) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

(๘) กำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย โดยเปิดช่องทางการเชื่อมต่อ (Port) เฉพาะที่จำเป็นต้องใช้งานเท่านั้น

(๙) การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

(๑๐) ต้องสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์ (Firewall) และอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

(๑๑) ค่ารายการการป้องกันการเข้าถึง (Access Control Lists/ Firewall Rules) ต้องปรับปรุงและทบทวนให้สอดคล้องกับสถานภาพปัจจุบันด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

(๑๒) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

(๑๓) ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ มีสิทธิที่จะระงับหรือบล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(๑๔) การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ต้องบันทึกรายการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

(๑๕) ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall) จะถูกระงับการใช้งานทันที

๕.๑๑ ข้อกำหนดการตรวจจับการบุกรุก (IDS/IPS Policy)

(๑) ต้องบันทึกและบริหารจัดการข้อมูลจราจรคอมพิวเตอร์ให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และระเบียบ หรือกฎหมายอื่นที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลสำหรับการตรวจจับการบุกรุก

(๒) ต้องเฝ้าระวังและตรวจสอบ หรือเรียนรู้พฤติกรรมที่อาจเป็นความเสี่ยงหรือส่งผลกระทบต่อระบบสารสนเทศและเครือข่ายที่มีอยู่ของหน่วยงาน และสามารถยับยั้งการทำงานนั้นได้ทันที ในกรณีที่ตรวจสอบและพบว่ามีเหตุการณ์ของการบุกรุกและโจมตี จะต้องกำหนดวิธีการปฏิบัติหรือกิจกรรมและผู้รับผิดชอบที่ชัดเจน ในการแก้ไขหรือปรับปรุงเหตุการณ์ดังกล่าว

(๓) ระบบตรวจจับการบุกรุกระบบเครือข่าย ต้องมีการป้องกันการบุกรุกและโจมตีจากเครือข่ายภายในและภายนอก โดยการเรียนรู้พฤติกรรมการบุกรุกและโจมตีระบบเครือข่าย

(๔) ระบบตรวจจับการบุกรุกระบบเครือข่าย จะต้องมีการปรับปรุงการกำหนดค่าด้านความมั่นคงปลอดภัยที่สามารถเรียนรู้พฤติกรรมการบุกรุกและโจมตีระบบเครือข่าย เพื่อให้สามารถเรียนรู้พฤติกรรมการบุกรุกและการโจมตีระบบรูปแบบใหม่ ๆ ได้

(๕) ระบบตรวจจับการบุกรุกระบบเครือข่าย ต้องมีมาตรการในการป้องกันการโจมตี การทำงานของระบบตรวจจับการบุกรุกระบบเครือข่ายไม่ให้ทำงานผิดพลาด โดยต้องไม่เปิดเผยให้สามารถตรวจสอบ IP

หรือเส้นทาง (Path) ในระบบเครือข่าย หรือมาตรการอื่นใดในการป้องกันการโจมตี ทั้งนี้ให้มีการตรวจสอบและทบทวนมาตรการให้มีความสอดคล้องกับสถานภาพด้านเครือข่ายในปัจจุบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมด้านเครือข่ายที่มีผลกระทบ

๕.๑๒ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs)

(๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

(๒) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) มีดังนี้

(๒.๑) Firewall/Proxy/Gateway ข้อมูล IP Address ของเครื่องทั้งภายในและภายนอกที่มีการเชื่อมต่อกับเครือข่ายของหน่วยงาน

(๒.๒) Authentication ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ การพิสูจน์ตัวตนของผู้ใช้งาน

(๒.๓) Web Server ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ การเข้าถึงเครื่องแม่ข่าย

(๒.๔) Web Application ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ การพิสูจน์ตัวตนและการเข้าถึงข้อมูลของผู้ใช้งาน

(๓) ต้องมีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) รายละเอียดของระบบป้องกันการบุกรุก การเข้า – ออกระบบ การพยายามเข้าสู่ระบบ หรือสิ่งอื่นใดเพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตให้ปฏิบัติ ดังนี้

๖.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการต้องมีการยืนยันตัวตนที่มีความมั่นคงปลอดภัยโดยให้ปฏิบัติ ดังนี้

(๑) ต้องไม่ให้ระบบปฏิบัติการแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบปฏิบัติการสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line ที่อาจสร้างความเสียหายให้กับระบบได้

๖.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึงโดยปฏิบัติ ดังนี้

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

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นในด้านเทคนิค หรือความสอดคล้องกับการปฏิบัติงาน

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

(๑) ต้องใช้เทคนิคการตรวจสอบการกำหนดรหัสผ่านซึ่งประกอบด้วยอักขระ ตัวเลข และอักขระพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๒) เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๖.๔ ข้อปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ที่ไม่ได้ใช้งานเป็นประจำไว้ในสื่อภายนอก

(๔) เก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) ห้ามติดตั้งหรือใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์หรือโปรแกรมที่มีนโยบายห้ามไม่ให้เข้าถึงการติดตั้งหรือใช้งาน รวมไปถึงใช้วิธีการในการหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดหรือที่มีอยู่แล้วด้วย

(๗) หน่วยงานไม่สนับสนุนการติดตั้งและ/หรือใช้งานโปรแกรมละเมิดลิขสิทธิ์หากเกิดข้อพิพาทผู้ที่ติดตั้งและ/หรือใช้งานโปรแกรมดังกล่าวต้องเป็นผู้รับผิดชอบ

๖.๕ การกำหนดเวลาเพื่อยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน (Session Time-Out)

(๑) ระบบสารสนเทศต้องมีการตัดและหมดเวลาการใช้งานรวมถึงปิดการใช้งานหลังจากที่ว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาที

(๒) ระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง ต้องมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๖.๖ ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ดังนี้

(๑) ระบบสารสนเทศต้องมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานระบบสารสนเทศแต่ละครั้งไม่เกิน ๔ ชั่วโมง โดยจะต้องระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ และหากไม่มีการใช้งานนานเกิน ๖๐ นาที ต้องยกเลิกการเชื่อมต่อระบบ

(๒) ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงต้องมีการจำกัดช่วงระยะเวลาการเชื่อมต่อให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้นและมีการจำกัดระยะเวลาการเชื่อมต่อที่สั้นขึ้น

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๗.๑ ต้องจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงาน ตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูลต่าง ๆ

(๒) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด ต้องยกเลิกการเชื่อมต่อระบบ

(๓) ผู้ให้บริการภายนอก (Outsource) ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของหน่วยงาน

(๔) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(๕) ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ทุกครั้ง

๗.๒ การบริหารจัดการระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

(๑) ต้องระบุความสำคัญของระบบงานซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อหน่วยงาน

(๒) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ

(๓) ต้องประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่น ๆ ที่มีความสำคัญน้อยกว่า

(๔) ต้องควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(๕) ต้องสำรองและทดสอบการกู้คืนระบบ ตามนโยบายระบบสารสนเทศและระบบสำรองสารสนเทศ

(๖) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(๗) ต้องควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก ตามข้อกำหนดที่ตั้งค่าไว้ในไฟร์วอลล์ (Firewall)

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ (Mobile Computing) เพื่อควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต จากการสูญหาย เสียหาย ถูกขโมย ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) การควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๑.๑) การป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ครอบคลุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา เช่น โทรศัพท์มือถือ Smart Phone, Notebook, Tablet หรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้

(๑.๒) ต้องกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๑.๓) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๑.๔) ใช้วิธีการทางเทคนิคในการเข้ารหัสข้อมูลเพื่อเข้ารหัสข้อมูลสำคัญในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๑.๕) เมื่อพบซอฟต์แวร์ไม่ประสงค์ดีในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้ปฏิบัติตามข้อปฏิบัติในการป้องกันซอฟต์แวร์ไม่ประสงค์ดีและที่เกี่ยวข้อง

(๑.๖) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่มิให้ถูกขโมยหรือสูญหาย โดยการล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหายโดยทำการล็อคอุปกรณ์ไว้กับโต๊ะ หรือนำไปเก็บไว้ในตู้ที่สามารถล็อคได้ หรือวิธีการอื่นใดที่เหมาะสม

(๑.๗) ต้องสำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างสม่ำเสมอ

(๑.๘) ต้องมีการป้องกันการเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เข้ากับเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต

(๑.๙) ต้องใส่ซองกันกระแทกหรือกระเป๋าสำหรับอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือนจากการตกจากโต๊ะทำงาน หลุดมือ หรือพฤติการณ์อื่นใด

(๑.๑๐) หลีกเลี่ยงการใช้ปลายปากกา หรือวัสดุอื่นใดกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้

(๑.๑๑) ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ใกล้อาหาร น้ำ หรือสิ่งอื่นใดที่เป็นของเหลวมีความชื้นซึ่งอาจเป็นอันตรายต่ออุปกรณ์ดังกล่าวได้

(๑.๑๒) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

(๑.๑๓) ให้ติดตั้งหรือจัดเก็บอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่บนโต๊ะ ชั้นวางของ หรือสิ่งอื่นใดที่เป็นอุปกรณ์เฉพาะสำหรับติดตั้งหรือเก็บรักษาที่มั่นคงแข็งแรง

(๑.๑๔) เพื่อความเป็นระเบียบและปลอดภัยสำหรับอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้จัดเก็บสายชาร์ต สายเชื่อมต่อกับระบบคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องอื่นใด ไว้ในสถานที่หรืออุปกรณ์เฉพาะที่สามารถปิดล็อคได้เพื่อป้องกันการสูญหาย

(๑.๑๕) ตรวจสอบสายสัญญาณของอุปกรณ์สื่อสาร สายชาร์ต สายเชื่อมต่อกับระบบคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องอื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์สื่อสารได้รับความเสียหายทำความสะอาดอุปกรณ์สื่อสารอย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละอองที่จะทำให้อุปกรณ์สื่อสารเกิดการขัดข้องเสียหาย

(๒) การควบคุมการติดตั้งระบบหรืออุปกรณ์ต่าง ๆ เพิ่มเติม ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๒.๑) ห้ามติดตั้งโปรแกรมเพิ่มเติมนอกเหนือจากที่หน่วยงานได้ติดตั้งไว้ให้ใช้งาน

(๒.๒) ห้ามติดตั้งโปรแกรมที่สามารถตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

(๒.๓) ห้ามติดตั้งโปรแกรมหรืออุปกรณ์อื่นใดเพิ่มเติม เพื่อให้บุคคลอื่นสามารถใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ หรือเครือข่ายของหน่วยงานได้

(๒.๔) ห้ามนำอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ไม่ใช่ของหน่วยงานมาใช้กับเครือข่ายหน่วยงาน เว้นแต่ได้รับการตรวจสอบความปลอดภัยและตั้งค่าการใช้งานจากผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องก่อนการใช้งาน

(๓) ข้อกำหนดในการสำรองข้อมูลและการกู้คืน

(๓.๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกประเภท CD, DVD, External Hard Disk หรือสื่อบันทึกอื่นใดที่เหมาะสม ในการใช้สำรองข้อมูลจากเครื่องคอมพิวเตอร์

(๓.๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) เพื่อป้องกันการใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาตจากการปฏิบัติงานจากภายนอกหน่วยงานให้ปฏิบัติ ดังนี้

(๑) ต้องเข้ารหัส (Encryption) ด้วย SSL, VPN, Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่าง ๆ ภายในหน่วยงาน ทั้งนี้ให้มีความเหมาะสมกับรูปแบบการสื่อสารของความสำคัญของข้อมูล

(๒) การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจาก ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบและจะต้องเข้าใช้งานผ่านเครือข่ายส่วนตัวเสมือน (VPN)

(๓) การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของหน่วยงานจะต้องเข้าใช้งานผ่านเครือข่ายส่วนตัวเสมือน (VPN)

(๔) การขอใช้งานระบบเครือข่ายส่วนตัวเสมือน (VPN) ผู้ใช้งานจะต้องลงทะเบียนขอใช้งานตามแบบฟอร์ม หรือวิธีการอื่นใด ที่ผู้ดูแลระบบ หรือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบกำหนด

(๕) การเข้าสู่ระบบสารสนเทศภายในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๖) ผู้ได้รับอนุญาตเท่านั้นเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงาน โดยห้ามมิให้สมาชิกในครอบครัวหรือบุคคลใด ๆ ที่ไม่ได้รับอนุญาต และขอสงวนสิทธิในการระงับหรือยกเลิกสิทธิหากพบว่าไม่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง

(๗) ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

(๘) ต้องทบทวนปรับปรุงสิทธิการอนุญาตให้ใช้ปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

๘. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

เพื่อให้มีการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม ไม่ก่อให้เกิดความเสี่ยงในการเข้าถึงระบบสารสนเทศและเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาตและให้เครื่องคอมพิวเตอร์แม่ข่ายทำงานได้อย่างมีประสิทธิภาพ ถูกต้อง น่าเชื่อถือ และพร้อมใช้งานให้ปฏิบัติ ดังนี้

๘.๑ การควบคุมการติดตั้งซอฟต์แวร์ลงในระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ต้องควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ผู้ดูแลระบบที่ได้รับการอบรมแล้วหรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ที่อาจกระทบต่อการให้บริการของระบบสารสนเทศต้องมีการขออนุมัติจากผู้อำนวยการศูนย์สารสนเทศ ให้ติดตั้งก่อนดำเนินการ

(๔) ต้องมีการจัดเก็บซอร์สโค้ด (Source Code) และไลบรารี่สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๕) ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ หรือซอฟต์แวร์หรือระบบสารสนเทศอื่นใด ตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๖) ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(๗) ต้องมีการจัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชั่นเก่าเหล่านั้นตามระยะเวลาที่เหมาะสม

(๘) ต้องระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๘.๒ ข้อกำหนดในการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๘.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ต้องมีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

(๒) ต้องระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด (Source Code) ในการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก

(๓) กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ต้องตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบ และฐานข้อมูลที่ใช้งาน เลือกสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

๘.๔ มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

(๑) ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการศูนย์สารสนเทศ

(๒) ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

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

(๔) การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากผู้อำนวยการศูนย์สารสนเทศ ก่อนทุกครั้ง

๘.๕ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) ต้องจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้นและต้องบันทึก ดังนี้

(๑.๑) ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน

(๑.๒) สถานที่ที่ติดตั้ง

(๑.๓) เครื่องที่ติดตั้ง

(๑.๔) ผู้ผลิตซอฟต์แวร์

(๑.๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

(๒) ต้องมีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการดังนี้

(๓.๑) ต้องเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(๓.๒) กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน

(๓.๓) ผู้ที่เกี่ยวข้องต้องทำการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัด โดยกำหนดระยะเวลาเท่าที่จำเป็น

๘.๖ ข้อกำหนดในการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) และการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการล็อกอิน (Login) ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนค่า Configuration ของระบบ

(๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน

(๙) ข้อมูลแสดงการเปิด ปิด เขียน อ่านไฟล์ หรือลักษณะอื่นใดในการกระทำกับไฟล์

(๑๐) ข้อมูลไอพีแอดเดรส (IP Address) ที่ใช้ และที่เข้าถึง

(๑๑) ข้อมูลโปรโตคอล (Protocol) เครือข่ายที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๙. **การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)**

เพื่อรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

๙.๑ การรักษาความมั่นคงปลอดภัยบริเวณศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center) ให้ปฏิบัติ ดังนี้

(๑) พื้นที่ใช้งานระบบสารสนเทศแบ่งออกเป็น พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย พื้นที่ปฏิบัติงาน และพื้นที่สำหรับผู้มาติดต่อ

(๒) จัดทำแผนผังพื้นที่ใช้งานระบบสารสนเทศ

(๓) ผู้อำนวยการศูนย์สารสนเทศ เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ

(๔) ควบคุมการเปิด-ปิดห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center) ให้ปฏิบัติตามข้อ ๑๑. การใช้ห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

(๕) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน ต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

(๖) ต้องมีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยมีระบบสำรองไฟฟ้า ระบบน้ำ ระบบดับเพลิง ระบบปรับอากาศ ระบบควบคุมความชื้น ทั้งนี้ต้องมีการตรวจสอบและทดสอบระบบสนับสนุนเหล่านี้

(๗) ติดตั้งระบบแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

(๘) เครื่องคอมพิวเตอร์หรือระบบสารสนเทศที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก และสำนักงานหรือห้องจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๙) เจ้าหน้าที่ผู้ได้รับมอบหมายต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ที่ตนได้รับมอบหมายเป็นประจำ เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก อุปกรณ์ต่าง ๆ สื่อบันทึกข้อมูลที่สำคัญถูกจัดเก็บหรือได้รับการปิดล็อคอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๙.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security) ดำเนินการ ดังนี้

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ต้องร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ต้องเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) จัดทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการเชื่อมต่อสายสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ให้มีการป้องกันการเข้าถึงจากบุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติกแทนสายสัญญาณสื่อสารแบบเดิม สำหรับระบบสารสนเทศ ที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๙.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) ให้ปฏิบัติ ดังนี้

(๑) ต้องบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๙.๔ การนำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน (Removal of Property) ให้ปฏิบัติ ดังนี้

(๑) ต้องขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์นั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงานเมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๔) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๙.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises) ให้ปฏิบัติ ดังนี้

(๑) ต้องป้องกันอุปกรณ์มิให้โดนกระแทก แตกหักในระหว่างการขนส่งหรือเคลื่อนย้าย

(๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) ในการนำอุปกรณ์ไปใช้งานภายนอกหน่วยงานให้ผู้รับผิดชอบได้รับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

๙.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment) ให้ปฏิบัติ ดังนี้

(๑) ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) กำหนดมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ หรือทำลาย เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

๙.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ ให้ปฏิบัติ ดังนี้

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ต้องควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ

๑๐.การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๐.๑ ขั้นตอนการขอใช้ E-Mail ของกรมสอบสวนคดีพิเศษ

(๑) ผู้ขอใช้ E-Mail ต้องเป็นบุคลากรในสังกัดกรมสอบสวนคดีพิเศษ

(๒) ผู้ใช้งานต้องดำเนินการขอใช้งานระบบสารสนเทศตามข้อ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

๑๐.๒ การใช้ E-Mail ของกรมสอบสวนคดีพิเศษ ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) ผู้ใช้งาน E-Mail ทั้งหมดของหน่วยงาน ต้องมี E-Mail Account เป็นของตนเอง

(๒) E-Mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำ E-Mail ไปใช้ในทางที่ผิด

(๓) E-Mail Account ที่มีวัตถุประสงค์พิเศษ เช่น webmaster@dsi.go.th ซึ่งสร้างขึ้นเพื่อใช้งานตามภารกิจหรือมีผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป ต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-Mail Accountนั้น และต้องขอเปิดใช้งานบัญชี E-Mail ในลักษณะดังกล่าวเป็นหนังสือลงนามโดยหัวหน้าหน่วยงานนั้น ๆ

(๔) E-Mail Account ทั้งหมด และ E-Mail ทุกฉบับ (รวมถึง E-Mail ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของหน่วยงาน ถือเป็นสินทรัพย์ของหน่วยงาน

(๕) ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบ E-Mail ของหน่วยงาน

(๖) หลังจากการใช้งาน E-Mail เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งาน E-Mail โดยไม่ได้รับอนุญาต

(๗) พื้นที่เก็บ E-Mail บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณของ E-Mail มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ ให้ผู้ใช้งานแจ้งผู้ดูแลระบบเพื่อขอขยายพื้นที่จัดเก็บดังกล่าวให้เหมาะสมกับการใช้งานเป็นรายบุคคล และถ้าหากปริมาณของ E-Mail มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่ง E-Mail ได้ตามปกติอีกต่อไป

(๘) ห้ามใช้ E-Mail Account ของหน่วยงานเพื่อการโฆษณา การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ หรือเพื่อการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือเพื่อการส่วนตัว

(๙) ห้ามใช้ E-Mail Account ของหน่วยงานในการประกาศข้อมูลใด ๆ ในเว็บบอร์ด บล็อก กระดานข่าว หรือสื่อสังคมออนไลน์อื่นใด เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับหน่วยงาน

(๑๐) ห้ามผู้ใช้งานทำการปลอมแปลงข้อความใน E-Mail หัวจดหมาย E-Mail ลายเซ็นใน E-Mail หรือ E-Mail Account ของบุคคลอื่นโดยเด็ดขาด

(๑๑) การแจ้ง E-Mail address ของหน่วยงาน ให้บุคคลอื่นใช้เพื่อการผลประโยชน์ทางราชการเท่านั้น

(๑๒) ห้ามใช้ E-Mail ของหน่วยงานในการติดต่อเรื่องส่วนตัวกับบุคคลหรือหน่วยงานที่ไม่รู้จักหรือไม่น่าเชื่อถือ

(๑๓) ขอสงวนสิทธิในการเพิกถอนสิทธิการใช้งาน E-Mail หากพบว่า E-Mail ดังกล่าวถูกนำไปใช้งานขัดต่อนโยบายของหน่วยงาน หรือระเบียบปฏิบัติ หรือกฎหมายที่เกี่ยวข้อง

๑๐.๓ การส่ง E-Mail ของหน่วยงาน ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ห้ามผู้ใช้งานส่ง E-Mail ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อหน่วยงาน

(๒) ซอฟต์แวร์สำหรับใช้งาน E-Mail ต้องได้รับการตั้งค่าให้ E-Mail ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน และเบอร์โทรศัพท์ติดต่อ

(๓) ห้ามผู้ใช้งานส่งหรือส่งต่อ E-Mail ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศหรือ E-Mail ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม ศาสนา และ E-Mail ที่ส่งผลกระทบต่อความมั่นคงของชาติหรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

(๔) ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง E-Mail หลอกลวงหรือการส่ง E-Mail ในลักษณะลูกโซ่โดยเด็ดขาด

(๕) ห้ามผู้ใช้งานส่ง E-Mail ขยะ (Junk Mail) โฆษณาสินค้าต่าง ๆ (Spam Mail) หรือ E-Mail อื่นใดที่ผู้รับไม่ได้ต้องการ

(๖) ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่ง E-Mail โดยใช้ E-Mail Account ของตนโดยเด็ดขาด

(๗) ผู้ใช้งานต้องร่างเนื้อหาของ E-Mail ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออก E-Mail นั้นในนามตัวแทนของหน่วยงาน

(๘) ไฟล์เอกสารที่แนบมาพร้อมกับ E-Mail จะต้องอยู่ในรูปแบบ PDF, DOC, TXT, CSV, XLS, JPG, GIF, PPT, HTML หรือในรูปแบบตามมาตรฐานอื่นใดซึ่งผู้รับสามารถเปิดอ่านได้ด้วยซอฟต์แวร์พื้นฐานบนทุกระบบปฏิบัติการ

(๙) ห้ามส่งข้อมูลลับแนบกับ E-Mail เว้นแต่กรณีที่มีความจำเป็นซึ่งต้องเข้ารหัสก่อน

(๑๐) การส่ง E-Mail ที่มีไฟล์แนบขนาดใหญ่ต้องบีบอัดไฟล์แนบให้เล็กลงก่อนส่ง

๑๐.๔ การรับ E-Mail ของหน่วยงาน ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่าเครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่ง E-Mail โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

(๒) ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส E-Mail Bomb หรือโปรแกรมประสงค์ร้ายต่าง ๆ

(๓) ผู้ใช้งานต้องลบ E-Mail ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บ E-Mail ให้เป็นไปตามขนาดที่หน่วยงานกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษา E-Mail ที่เกี่ยวข้องกับการทำงาน และ E-Mail ที่ไม่ขัดต่อกฎหมายเท่านั้น

(๔) ไม่เปิดไฟล์แนบสกุล .exe, .com, .bat หรือไฟล์ประเภทโปรแกรมกระทำการอื่นใดที่ไม่เกี่ยวข้องกับงาน

(๕) ในกรณีที่ได้รับ E-Mail ฉบับเดียวกันซ้ำหลายครั้งหรือได้รับ E-Mail จากบุคคลที่ไม่รู้จักเป็นประจำ หรือลักษณะอื่นใดที่สงสัยว่ามีการใช้ E-Mail ที่ผิดปกติเกิดขึ้น ให้รีบแจ้งผู้ดูแลระบบ ดำเนินการตรวจสอบทันที

๑๐.๕ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

(๑) กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒) กำหนดสิทธิบัญชีรายชื่อผู้ใช้งาน E-mail รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน

(๓) จัดทำระบบให้สามารถบังคับให้เปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการเข้าสู่ระบบในครั้งแรกสำหรับผู้ใช้งานใหม่ซึ่งได้รับรหัสผ่านครั้งแรก (Default Password)

(๔) จัดทำระบบการปกปิดการเข้ารหัสผ่านจดหมายอิเล็กทรอนิกส์เมื่อใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาให้แสดงในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นในการพิมพ์อักขระแต่ละตัว

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๕ ครั้ง

(๖) ทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง หรือเมื่อมีการเปลี่ยนแปลงอื่นใดในทำนองเดียวกันนี้

(๗) ควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๑. การใช้ห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

เพื่อควบคุมการเข้าถึงทางกายภาพให้เข้าได้เฉพาะผู้ได้รับอนุญาตเท่านั้น เพื่อป้องกันสินทรัพย์ในห้องศูนย์คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์จากการสูญหาย เสียหาย รวมถึงการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต ให้ปฏิบัติ ดังนี้

๑๑.๑ การขออนุญาตเข้าปฏิบัติงานห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๑) หน่วยงานที่ขอเข้าปฏิบัติงานต้องทำหนังสือขออนุญาตเพื่อให้ผู้อำนวยการศูนย์สารสนเทศเป็นผู้พิจารณาอนุญาต ได้แก่

(๑.๑) หน่วยงานในกรมสอบสวนคดีพิเศษ

(๑.๒) หน่วยงานภายนอกกรมสอบสวนคดีพิเศษ

(๑.๓) บริษัทที่เป็นผู้รับจ้างดำเนินงานโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารของกรมสอบสวนคดีพิเศษ

(๑.๔) บริษัทหรือหน่วยงานอื่น ๆ ที่ได้รับอนุญาตให้เข้าดำเนินการทดสอบระบบเพื่อเป็นประโยชน์ทางราชการ

(๒) ให้ระบุรายละเอียดการขอเข้าปฏิบัติงานในหนังสือขอเข้าปฏิบัติงาน ดังนี้

(๒.๑) วัน – ช่วงเวลาในการเข้าปฏิบัติงาน

(๒.๒) รายชื่อเจ้าหน้าที่ประสานงาน

(๒.๓) รายชื่อเจ้าหน้าที่ที่จะเข้าปฏิบัติงาน

(๒.๔) วัตถุประสงค์การเข้าปฏิบัติงาน

(๓) หากมีการติดตั้งอุปกรณ์ให้แนบรายละเอียดอุปกรณ์ พร้อมรายละเอียดโครงการที่เกี่ยวข้องกับการติดตั้งอุปกรณ์

๑๑.๒ การใช้ห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ต้องลงทะเบียนตามแบบฟอร์มทะเบียนผู้เข้าปฏิบัติงานห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ แม่ข่ายก่อนเข้าห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๒) ห้ามเปิดประตูห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในโดยเด็ดขาด

(๓) ห้ามสวมรองเท้าที่จัดเตรียมไว้ให้ก่อนเข้าห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๔) ห้ามนำกระเป๋าเข้าห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๕) ห้ามสูบบุหรี่ หรือกระทำการอื่นใดที่อาจก่อให้เกิดฝุ่นละออง หรืออัคคีภัย

(๖) ห้ามนำอาหารหรือเครื่องดื่มเข้ามาในห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๗) ห้ามนำกล่องเครื่องมือหรือหีบห่อเข้าและออกห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาตจากผู้ดูแล

(๘) ก่อนนำอุปกรณ์เข้าห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ ต้องให้ผู้ดูแลตรวจสอบก่อน

(๙) การนำอุปกรณ์เข้าติดตั้งชั่วคราวให้กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ก่อนและต้องได้รับอนุมัติก่อนจึงจะสามารถนำอุปกรณ์เข้าห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ และขอสำเนาแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์เพื่อใช้เป็นหลักฐานในกรณีนำอุปกรณ์ออก

(๑๐) การนำอุปกรณ์ออกต้องแสดงสำเนาแบบฟอร์มการเคลื่อนย้ายเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ที่เคยขออนุมัติใน ๑๑.๒ (๑๑) ให้เจ้าหน้าที่ผู้ดูแลตรวจสอบก่อน ในกรณีที่ไม่มีให้กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ก่อนและต้องได้รับอนุมัติ จึงจะสามารถนำอุปกรณ์ออกจากห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ได้

(๑๑) เมื่อปฏิบัติงานเสร็จแล้ว ต้องกรอกแบบรายงานการเข้าปฏิบัติงานห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์แล้วให้ผู้ดูแลตรวจสอบก่อน

(๑๒) เวลาในการเข้าปฏิบัติงานห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๑๒.๑) ในเวลาราชการ ตอนเช้า เวลา ๐๘.๐๐ น. – ๑๒.๐๐ น.
ตอนบ่ายเวลา ๑๓.๐๐ น. – ๑๖.๓๐ น.

(๑๒.๒) นอกเวลาราชการให้ทำหนังสือขออนุญาต ตามขั้นตอนการขออนุญาตเข้าปฏิบัติงานห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ ตาม ๑๑.๑

๑๑.๓ ข้อกำหนดในการดูแลห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ ให้ผู้ดูแลระบบปฏิบัติ ดังนี้

(๑) บันทึกและจัดเก็บภาพของกล้องโทรทัศน์วงจรปิด (CCTV) ไว้อย่างน้อย ๑ เดือน เพื่อใช้ในการตรวจสอบในภายหลัง

(๒) ตรวจสอบประตูเข้า – ออกห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ให้ปิดล็อคอยู่เสมอ

(๓) ต้องมีความระมัดระวังดูแลสินทรัพย์สารสนเทศและต้องมีการบำรุงรักษาวัสดุอุปกรณ์รวมทั้งระบบดับเพลิง ระบบปรับอากาศ ระบบไฟฟ้า หรือระบบอื่นใดที่ติดตั้งในห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ตามระยะเวลาที่เหมาะสม ให้มีสภาพพร้อมใช้งานอยู่เสมอ

(๔) ต้องมีการดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์อย่างสม่ำเสมอ

ส่วนที่ ๒
นโยบายระบบสารสนเทศและระบบสำรองสารสนเทศ
(Information Backup)

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศและเครือข่ายของหน่วยงานสามารถใช้งานได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ให้ปฏิบัติ ดังนี้

๑.๑ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบสารสนเทศแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ชนิดข้อมูลที่ต้องสำรองอย่างน้อยต้องประกอบด้วย

(๑) ค่า Configuration สำหรับระบบ

(๒) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ

(๓) ฐานข้อมูลของระบบสารสนเทศของหน่วยงาน

(๔) ซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่นใดที่ต้องทำการสำรอง

๑.๓ ต้องกำหนดขั้นตอนและความถี่ในการสำรองและกู้คืนข้อมูลอย่างถูกต้องและชัดเจน

๑.๔ ต้องกำหนดรูปแบบการสำรองข้อมูล การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) ให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

๑.๕ ต้องบันทึกข้อมูล ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการสำรองข้อมูล

๑.๖ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

๑.๗ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วัน/เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๑.๘ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน และดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล

๑.๙ ต้องมีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๑.๑๐ วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (Restore) โดยในการทดสอบต้องจัดทำบันทึกการทดสอบไว้เป็นหลักฐาน

๒. การกู้คืนระบบ

๒.๑ ต้องมีขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๒ ผู้ดูแลระบบต้องบันทึกการกู้คืนระบบทุกครั้งที่มีการกู้คืนระบบ แล้วรายงานให้ผู้บังคับบัญชาทราบ

๒.๓ ผู้ดูแลระบบต้องทำการแก้ไขหากเกิดปัญหารวมถึงรายงานผู้บังคับบัญชาถึงปัญหาและวิธีการแก้ไขการกู้คืนระบบ

๒.๔ ผู้ดูแลระบบต้องทำการกู้คืนระบบโดยใช้ข้อมูลสำรองที่ทันสมัยที่สุด (Last update) ที่ได้สำรองไว้

๒.๕ ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยระบบละ ๑ ครั้งต่อปี

๓. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๓.๑ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ต้องประเมินสถานการณ์ความเสี่ยงสำหรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

(๓) กำหนดช่องทางในการติดต่อผู้ให้บริการภายนอกที่จะต้องติดต่อเมื่อเกิดเหตุจำเป็นฉุกเฉิน

(๔) สร้างความตระหนักให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน หรือความรู้อื่นใดในการเตรียมความพร้อมกรณีฉุกเฉิน

๓.๒ ต้องทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๓.๓ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓.๔ กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(IT Risk Management)

วัตถุประสงค์

๑. เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของหน่วยงานมีความครอบคลุมและทันต่อสถานการณ์

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

๒. ผู้ตรวจสอบภายใน (Internal Audit)

๓. ผู้ตรวจสอบภายนอก (External Audit)

๔. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ข้อกำหนดในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ให้ปฏิบัติ ดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๓ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๔ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายนอกหน่วยงาน (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. ข้อกำหนดในการประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ ระบุความเสี่ยง สาเหตุของความเสี่ยงและผลกระทบที่เกิดขึ้นจากความเสี่ยง

๒.๒ จัดลำดับความสำคัญของความเสี่ยง

๒.๓ จัดทำมาตรการในการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน และมาตรการในภาวะฉุกเฉิน

๒.๔ จัดทำรายงานการควบคุมความเสี่ยงประจำปี

๒.๕ หากมีความเสี่ยงที่เกิดขึ้นใหม่ ให้มีการจัดทำรายงานและวิเคราะห์การแก้ไขความเสี่ยง เพื่อไม่ให้เกิดขึ้นซ้ำอีก เป็นการดำเนินการต่อเนื่องว่าแผนบริหารความเสี่ยงมีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลงไปหรือไม่ รวมถึงทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอนและพัฒนาระบบให้ดียิ่งขึ้น

๓. ข้อกำหนดในการดำเนินการตรวจสอบประเมินระบบสารสนเทศ ให้ปฏิบัติดังนี้

๓.๑ ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๓.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งให้มีการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๓.๓ ต้องระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๓.๔ ต้องเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลประวัติแสดงการเข้าถึงนั้น (Logs) ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ

๓.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ แยกการติดตั้งเครื่องมือ ที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๔. ข้อกำหนดในการบริหารความต่อเนื่องของระบบสารสนเทศ ให้ปฏิบัติดังนี้

๔.๑ ต้องมีระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศสอดคล้องกับการใช้งานตามภารกิจหน่วยงาน

๔.๒ ต้องมีการปรับปรุงระบบสารสนเทศ ระบบสำรอง และแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ทั้งนี้ให้ความถี่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

๔.๓ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ทั้งนี้ให้ความถี่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

๔.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

๔.๕ ในการสำรองข้อมูลให้มีการคัดเลือกและจัดทำระบบสำรองที่เหมาะสม

๔.๖ จัดทำคู่มือที่เกี่ยวข้องกับการปฏิบัติงานตามแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

๕. ข้อกำหนดการแจ้งเหตุด้านความมั่นคงปลอดภัย ให้ปฏิบัติดังนี้

๕.๑ แจ้งไปยังผู้ดูแลระบบโดยทันที เมื่อพบเหตุการกระทำที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนี้

(๑) การกระทำที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(๒) การกระทำที่ขัดต่อความมั่นคงของชาติ

(๓) การใช้ทรัพยากรสารสนเทศของหน่วยงานไม่เหมาะสม ผิดวัตถุประสงค์

(๔) หน้าเว็บไซต์หลัก หรือระบบสารสนเทศของหน่วยงานถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดี

(๕) ข้อมูลเว็บไซต์หลัก หรือระบบสารสนเทศของหน่วยงานไม่ถูกต้อง หรือคลาดเคลื่อนจากความเป็นจริง

(๖) ข้อมูลสารสนเทศสำคัญของหน่วยงานหรือส่วนตัวถูกเปิดเผย เปลี่ยนแปลง ลบ หรือสูญหายโดยไม่ได้รับอนุญาต

(๗) มีการนำข้อมูลสารสนเทศสำคัญของหน่วยงานไปใช้ผิดวัตถุประสงค์

(๘) ทรัพยากรสารสนเทศถูกขโมย

(๙) มีบุคคลภายนอกเข้าใช้งานระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

(๑๐) มีการแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักฟัง ดักดูข้อมูลในระบบเครือข่ายของหน่วยงาน

(๑๑) มีการใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม

(๑๒) มีการบุกรุกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ของหน่วยงาน

(๑๓) มีการบุกรุกหรือการใช้โปรแกรมของผู้ไม่ประสงค์ดี

(๑๔) เหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๕.๒ การจัดการกับเหตุด้านความมั่นคงปลอดภัยเมื่อได้รับรายงานเหตุด้านความมั่นคงปลอดภัย ให้ผู้ดูแลที่ได้รับมอบหมายปฏิบัติตามขั้นตอนปฏิบัติตามแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๕.๓ ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลระบบที่เกี่ยวข้องในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา และผู้ดูแลระบบที่เกี่ยวข้อง

ส่วนที่ ๔
นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์
(IT Awareness)

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของหน่วยงานเพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน ให้ปฏิบัติดังนี้

๑.๑ จัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๑.๒ จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๑.๓ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ หรือจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๑.๔ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาต้องจัดปีละไม่น้อยกว่า ๑ ครั้ง หรือจัดร่วมกับการสัมมนาอื่นด้วย โดยมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดให้ความรู้

๑.๕ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๑.๖ ระดมความคิดการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน