ประกาศกรมส่งเสริมอุตสาหกรรม
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมส่งเสริมอุตสาหกรรม
ประจำปี พ.ศ. ๒๕๖๙

โดยที่เป็นการสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมอุตสาหกรรม เพื่อรองรับเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วในสถานการณ์ปัจจุบัน ตลอดจนเพื่อให้การดำเนินการเป็นไปตาม มาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมส่งเสริมอุตสาหกรรมจึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมอุตสาหกรรม ตามเอกสารแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๙ พฤษภาคม พ.ศ. ๒๕๖๙

(นางสาวณัฏฐิญา เนตยสุภา)
อธิบดีกรมส่งเสริมอุตสาหกรรม

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมส่งเสริมอุตสาหกรรม
ประจำปี พ.ศ. ๒๕๖๙

สารบัญ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมส่งเสริมอุตสาหกรรม ประจำปี พ.ศ. ๒๕๖๙

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมส่งเสริมอุตสาหกรรมมีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินธุรกรรมมีความถูกต้องและแม่นยำน่าเชื่อถือ ตลอดจนเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมส่งเสริมอุตสาหกรรมจึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

ข้อ ๑ คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน ประกอบด้วย

๑. “กสอ”	หมายถึง กรมส่งเสริมอุตสาหกรรม
๒. “หน่วยงาน”	หมายถึง กอง/ศูนย์/กลุ่มงาน หรือที่เรียกชื่อเป็นอย่างอื่น ในสังกัดกรมส่งเสริมอุตสาหกรรม
๓. “ศส.”	หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง ติดตั้ง บำรุงรักษาระบบคอมพิวเตอร์ระบบ ชุดคำสั่ง โปรแกรม และเครือข่ายใน กสอ.
๔. “สารสนเทศ”	หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
๕. “ระบบสารสนเทศ”	หมายถึง ระบบงานที่ใช้จัดเก็บและประมวลผลข้อมูลซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผลให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการ วางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสารได้

๖. “ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ กสอ. ได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)

๗. “สินทรัพย์” หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับ กสอ. ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อ กสอ.

๘. “ผู้บริหารสูงสุด” CEO (Chief Executive Officer) หมายถึง อธิบดีกรมส่งเสริมอุตสาหกรรม

๙. “ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” CIO (Chief Information Officer) หมายถึง ผู้ที่อธิบดีกรมส่งเสริมอุตสาหกรรม มอบหมายให้ รับผิดชอบสั่งการและกำกับดูแล ติดตามการดำเนินงานด้าน เทคโนโลยีสารสนเทศของ กสอ.

๑๐. “ผู้บริหาร” หมายถึง ผู้อำนวยการกอง/ศูนย์ ผู้เชี่ยวชาญ ผู้อำนวยการกลุ่มงานของ กสอ. เป็นผู้มีอำนาจสั่งการตามโครงสร้างการแบ่งส่วนราชการ

๑๑. “ผู้อำนวยการ” หมายถึง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ผอ.ศส.) รับผิดชอบในการกำหนดนโยบาย การควบคุมกำกับดูแลการใช้งานระบบสารสนเทศและระบบเครือข่าย

๑๒. “ผู้ใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแล รักษาระบบเทคโนโลยีสารสนเทศของ กสอ. โดยมีสิทธิและหน้าที่ขึ้นอยู่ กับบทบาท ซึ่งกำหนดตามข้อ (๑๓) (๑๔) (๑๕) (๑๖) และ (๑๗)

๑๓. “ผู้ดูแลระบบ” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บริหารระดับสูง หรือ ผู้อำนวยการให้มีหน้าที่รับผิดชอบในการดูแลรักษาข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย ซึ่งสามารถเข้าถึง และปรับปรุงให้ระบบสามารถใช้งานได้ดีและมีประสิทธิภาพ

๑๔. “ผู้รับผิดชอบระบบสารสนเทศ” หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่ดูแลระบบงานของ กสอ. ในภาพรวม

๑๕. “เจ้าหน้าที่” หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ และพนักงานจ้างเหมาบริการ ของ กสอ.

๑๖. “ผู้ใช้งานที่เกี่ยวข้อง” หมายถึง บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของ กสอ. หรือเจ้าหน้าที่ ที่ได้รับมอบหมาย ซึ่งจำเป็นต้องใช้งานระบบสารสนเทศและระบบเครือข่ายของ กสอ.

๑๗. “ผู้ใช้งานภายนอก” หมายถึง บุคคล หรือนิติบุคคลที่นอกเหนือจากข้อ (๑๕) และ (๑๖) ที่มีความจำเป็นต้องใช้งานเครือข่ายของ กสอ.

๑๘. “ผู้รับบริการ” หมายถึง ประชาชนทั่วไป นักเรียน นิสิต นักศึกษา

๑๙. “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง ความมั่นคงและความปลอดภัยสำหรับ ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กสอ. โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๒๐. “สิทธิของผู้ใช้งาน” หมายถึง ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศของเจ้าหน้าที่และผู้ใช้งานที่เกี่ยวข้อง ได้แก่ สิทธิทั่วไป สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ กสอ.

๒๑. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ หรือ การมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือ ระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ เอาไว้ด้วยก็ได้

๒๒. “บัญชีผู้ใช้งาน” หมายถึง บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับเจ้าหน้าที่ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก

๒๓. “Active Directory” หมายถึง เครื่องมือสำหรับใช้บริหารจัดการ ที่มีมาพร้อมกับระบบปฏิบัติการ Windows Server ทำหน้าที่ในการเก็บและบริหารจัดการ บัญชีผู้ใช้งาน กลุ่มผู้ใช้งาน สิทธิในการเข้าถึง และ การกำหนดนโยบายการใช้งาน

๒๔. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และ ความมั่นคงปลอดภัยถูกคุกคาม

๒๕. “จดหมายอิเล็กทรอนิกส์ (e-Mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ผู้ส่ง สามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน ผ่านโปรโตคอล มาตรฐานที่ใช้ในการรับ-ส่ง ข้อมูล ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น โดยชื่อที่ใช้ ในการรับส่งจดหมายอิเล็กทรอนิกส์จะประกอบ ด้วย ๒ ส่วน คือ ชื่อผู้ใช้งาน และชื่อโดเมน เช่น mail...@diprom.go.th

๒๖. “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๒๗. “ชื่อผู้ใช้งาน (Username)” หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้ในระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

๒๘. “รหัสผ่าน (Password)” หมายถึง ชุดของตัวอักษร หรืออักขระ หรือตัวเลข ที่ถูกกำหนดขึ้นเพื่อใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคลในการควบคุมการเข้าถึงข้อมูลและระบบเครือข่าย

๒๙. “การเข้ารหัสลับ (Encryption)” หมายถึง การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๓๐. “การพิสูจน์ยืนยันตัวตน (Authentication)” หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน

๓๑. “ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์ หรือ ชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงาน เข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓๒. “ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ต่าง ๆ ของ กสอ. เข้ากับเครือข่ายอินเทอร์เน็ตสากล

๓๓. “SSID (Service Set Identifier)” หมายถึง ชื่อที่ใช้ระบุเครือข่ายไร้สาย

๓๔. “MAC Address (Media Access Control Address)” หมายถึง หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้ สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๓๕. “VPN (Virtual Private Network)” หมายถึง เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่ง ข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๖. “WPA (Wi-Fi Protected Access)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายพัฒนาขึ้นมาใหม่มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๓๗. “แผนผังระบบเครือข่าย (Network Diagram)” หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของ กสอ.

๓๘. “ไฟร์วอลล์ (Firewall)” หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๓๙. “ช่องโหว่ (Vulnerability)” หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔๐. “โปรแกรมประสงค์ร้าย (Malware)” หมายถึง โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอนคอมพิวเตอร์ (Worm) หรือม้าโทรจัน (Trojan Horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

ข้อ ๒ แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมอุตสาหกรรม
กำหนดประเด็นสำคัญ ดังต่อไปนี้

๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผล ข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่ เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิเพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตาม แนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๑.๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

๑.๓ การบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งานตรวจสอบบัญชีผู้ใช้งานอนุมัติและกำหนดรหัสผ่านการได้ลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิเท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งานต้องมีการทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๑.๔ การเข้าถึงข้อมูลตามระดับชั้นความลับ ต้องมีการจัดลำดับชั้นความลับ ให้ใช้หลักเกณฑ์ตาม พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ มีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนด วิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการจำหน่ายหรือการนำอุปกรณ์กลับมาใช้ใหม่

๑.๕ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่ กสอ. จัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งานเพื่อทำให้การควบคุม และป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๑.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ โปรแกรมประยุกต์ และโปรแกรมอรรถประโยชน์ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์ โปรแกรมอรรถประโยชน์ หรือ แอพพลิเคชั่นต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ อินเตอร์เน็ต (Internet) และระบบงานต่าง ๆ ต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความ เห็นชอบจากหัวหน้าส่วนราชการเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑.๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอพพลิเคชั่นต้องกำหนดสิทธิการจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของ กสอ. สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นจากมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๑.๘ การควบคุมการเข้าถึงเครือข่ายไร้สาย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายไร้สายโดยไม่ได้รับอนุญาต ผู้ที่จะเข้าใช้งานต้องกรอกแบบฟอร์มขอใช้บริการระบบเครือข่าย WIFI ลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Default ของ SSID (Service Set Identifier) ที่ตั้งค่ามาจากผู้ผลิต ผู้ดูแลระบบต้องสร้าง SSID เป็น ๒ กลุ่มคือ กลุ่มผู้ใช้งานที่มีบัญชีผู้ใช้งานอยู่ใน AD (Active Directory) กับผู้มาติดต่องานกับ กสอ. (Guest) ซึ่งต้องปฏิบัติตามขั้นตอนการลงทะเบียน (User Register) ตามที่ กสอ. กำหนดเพื่อขอสิทธิ์ในการใช้งานเครือข่ายไร้สายต่อไป

๑.๙ การรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์กำหนดหน้าที่และความรับผิดชอบของผู้ใช้งานในการใช้งานจดหมายอิเล็กทรอนิกส์ โดยเจ้าหน้าที่ของ กสอ. ต้องใช้จดหมายอิเล็กทรอนิกส์ของ กสอ. ในการติดต่องานที่เกี่ยวกับภารกิจของ กสอ. กำหนดข้อห้าม ข้อควรระวัง การถูกระงับในการใช้งาน สิทธิในการใช้งานจะหมดลงก็ต่อเมื่อพ้นสภาพการเป็นเจ้าหน้าที่ของ กสอ.

หมายเหตุ: เจ้าหน้าที่ของ กสอ. สามารถใช้จดหมายอิเล็กทรอนิกส์อื่นได้ ในกรณีที่จดหมายอิเล็กทรอนิกส์ของ กสอ. ไม่สามารถรองรับการทำงานที่เกี่ยวข้องกับภารกิจของ กสอ. ได้ เช่น การส่งข้อมูลขนาดใหญ่มาก หรือจดหมายอิเล็กทรอนิกส์ของ กสอ. ไม่สามารถใช้งานได้ในขณะนั้น เป็นต้น

๑.๑๐ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยข้อมูลระบบสารสนเทศ ต้องกำหนดรายละเอียดที่เกี่ยวกับการใช้งานรหัสผ่าน (Password Use) การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended User Equipment) และการเก็บรักษาทรัพย์สินขององค์กรไว้ในที่ที่ปลอดภัยและการป้องกันหน้าจอเครื่องคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) เพื่อให้ผู้ใช้งานได้รับทราบวิธีปฏิบัติในการป้องกันการเข้าถึงข้อมูลสารสนเทศหรือข้อมูลที่มีความสำคัญทั้งของผู้ใช้งานและของ กสอ.

๒ การสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

๒.๑ การสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน ต้องมีการจัดทำระบบสำรองข้อมูลเพื่อให้ระบบสารสนเทศของ กสอ. สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ พร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และการกู้คืนต้องมีการทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน ได้แก่ การประเมินสถานการณ์ความเสี่ยง แผนการสำรองข้อมูลและระบบงาน (Back Up) แผนการป้องกันไวรัสคอมพิวเตอร์ แผนการป้องกันและแก้ไขปัญหาที่เกิดจากไฟฟ้าดับ แผนการป้องกันความเสี่ยงจากไฟไหม้ แผนการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ (Hacker) แผนการป้องกันอุปกรณ์เครื่องแม่ข่ายชำรุด และแผนการป้องกันความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานระบบงานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๒.๒ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ต้องมีการกำหนดหรือระบุเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของ กสอ. เพื่อเป็นแนวทางให้กับผู้ใช้งานได้ประเมินว่าเหตุการณ์ที่พบมีผลกระทบต่อระบบสารสนเทศ ต้องกำหนดขั้นตอนการแจ้งเหตุเมื่อพบเหตุการณ์ด้านความมั่นคงปลอดภัย มีการกำหนดหน้าที่ความรับผิดชอบและวิธีปฏิบัติในการจัดการกับเหตุการณ์ที่เกิดขึ้น

๓ การตรวจสอบและประเมินความเสี่ยง

ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของ กสอ. (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๔ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยมั่นคงสารสนเทศ

ต้องสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ให้ดำเนินการดังนี้

๔.๑ จัดอบรมแนวปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กสอ. อย่างสม่ำเสมอ โดยอาจเพิ่มเนื้อหาที่เกี่ยวข้องกับเทคโนโลยีหรือภัยในรูปแบบใหม่ ๆ รวมทั้งกฎหมายระเบียบ ที่เกี่ยวข้องกับการใช้งาน

๔.๒ เผยแพร่นโยบายและแนวปฏิบัติในการรักษามั่นคงปลอดภัยสารสนเทศด้านสารสนเทศทางเว็บไซต์ กสอ. หรือห้องสมุดของ กสอ. เพื่อให้ผู้ใช้งานและบุคคลทั่วไปเข้าถึงได้

๔.๓ มีมาตรการเชิงป้องกัน โดยให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ ข้อควร ระวังในการใช้งานระบบสารสนเทศ รวมถึงต้องมีการกำหนดบทลงโทษเมื่อพบว่ามีการใช้ระบบสารสนเทศที่ไม่ถูกต้อง ได้แก่ การระงับการเข้าถึง หรือการระงับสิทธิการใช้งาน

หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อกำหนดการควบคุมการเข้าถึงข้อมูลสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยด้านสารสนเทศ

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิและการมอบอำนาจของ กสอ.

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๔. เพื่อให้การตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

แนวปฏิบัติ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ (Access Control)

ข้อ ๑ ผู้ดูแลระบบต้องจัดทำบัญชีหรือทะเบียนสินทรัพย์ เพื่อใช้ในการบริหารจัดการและกำหนด สิทธิในการเข้าถึงและใช้งาน

ข้อ ๒ ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานระบบสารสนเทศแต่ละกลุ่ม อย่างน้อยดังนี้

- อ่านอย่างเดียว
- สร้าง/บันทึกข้อมูล
- แก้ไข/ปรับปรุง
- ลบข้อมูล
- สิทธิการอนุมัติ/อนุญาต
- ระงับสิทธิ

ข้อ ๓ ผู้ดูแลระบบต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

๓.๑ ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๒ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ กล่าวคือ ในการขออนุญาตเข้าระบบงานนั้น ผู้ใช้งานจะต้องมีการกรอกเอกสารลงทะเบียนขอใช้งานตามที่ กสอ. กำหนด เพื่อขออนุญาตเข้าสู่ระบบสารสนเทศ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน จากนั้น ผู้ดูแลระบบจะ สร้างบัญชีผู้ใช้งานสำหรับการเข้าถึงโดยเฉพาะในส่วนที่จำเป็นและได้รับอนุญาตให้เข้าถึงเท่านั้น โดยคำนึงถึง ประเภทของข้อมูล ลำดับความสำคัญ และชั้นความลับ รวมถึงระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ต้องแยกออกจากระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อ กสอ.

๓.๓ ผู้ดูแลระบบต้องจัดเก็บบัญชีรายชื่อของผู้ใช้งานระบบปฏิบัติการไว้ใน Active Directory และต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิดเกิน ๓ ครั้ง จนกว่าจะยื่นเรื่องพร้อมหลักฐานแสดงความเป็นตัวตนต่อเจ้าหน้าที่ดูแลระบบ เพื่อขอรหัสผ่านใหม่อีกครั้ง

๓.๔ ผู้ดูแลระบบ ต้องกำหนดให้การ Log-in เพื่อเข้าระบบงานใด ๆ จะต้องมีการตรวจจับการเปิดระบบงานไว้ เมื่อไม่มีการใช้งานจะทำการ Log-out ระบบให้อัตโนมัติในระยะเวลาที่เหมาะสม

๓.๕ ผู้ดูแลระบบ ต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๖ กรณีมีการอนุญาตให้ผู้ใช้งานภายนอก ผู้เกี่ยวข้อง เข้าถึงระบบสารสนเทศของ กสอ. เพื่อดำเนินการใด ๆ เมื่อได้ใช้งานเสร็จแล้วผู้ดูแลระบบต้องยกเลิกสิทธิกับผู้ใช้เหล่านั้นในทันที สำหรับผู้รับจ้างพัฒนาและดูแลระบบสารสนเทศต้องเข้าผ่านระบบ VPN (Virtual Private Network) เท่านั้น และหากพบว่าการดำเนินการนั้นมีผลกระทบหรือทำให้เกิดความเสียหายต่อระบบสารสนเทศ ผู้ใช้งานต้องเป็นผู้รับผิดชอบ

๓.๗ กำหนดระยะเวลาการใช้งานระบบสารสนเทศของ กสอ. ดังนี้

๓.๗.๑ ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอกตลอด ๒๔ ชั่วโมง ไม่เว้นวันหยุดราชการ

๓.๗.๒ ระบบงานภายใน (Back Office) หรือโปรแกรมที่มีความเสี่ยงสูงสำหรับเจ้าหน้าที่ ให้เข้าถึงในเวลาราชการ (๘.๓๐ – ๑๖.๓๐ น.) เท่านั้น เว้นแต่ได้รับอนุญาต

ข้อ ๔ ผู้ดูแลระบบ ต้องจัดการรักษาความปลอดภัยทางกายภาพ (Physical Security Management) ดังนี้

๔.๑ จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ มีจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้น โดยกำหนดพื้นที่ ดังนี้

๔.๑.๑ พื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตุการณ์ระบบ

๔.๑.๒ พื้นที่จำกัดการเข้าถึง ได้แก่ ห้องที่มีการติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศ หรือระบบเครือข่าย โดยต้องติดตั้งระบบควบคุมการการเข้าถึงพื้นที่ทางกายภาพ

๔.๒ การเดินสายสัญญาณเครือข่ายต่าง ๆ ที่ต้องผ่านเข้าไปในบริเวณที่เป็นมุมอับลับตา หรือบริเวณที่บุคคลภายนอกเข้าถึงได้ ต้องมีการร้อยท่อสัญญาณ เพื่อป้องกันการดักจับสัญญาณ การตัด หรือการกัดของสัตว์ต่าง ๆ

๔.๓ ติดตั้งระบบดับเพลิงชนิดที่ใช้สำหรับอุปกรณ์ไฟฟ้าและทำความเสียหายให้กับระบบน้อยที่สุดเมื่อมีการใช้งาน

๔.๔ ติดตั้งระบบไฟฉุกเฉินให้เพียงพอสำหรับการทำงานเมื่อเกิดกรณีไฟฟ้าดับ

ข้อ ๕ ผู้ดูแลระบบ ต้องจัดการควบคุมการเข้า - ออก พื้นที่ควบคุม ดังนี้

๕.๑ ให้มีการแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึง (พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชม หรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีระบบคอมพิวเตอร์และเครือข่ายติดตั้งอยู่)

๕.๒ ให้มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

๕.๓ ดูแลผู้มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๕.๔ การเข้า - ออก พื้นที่ควบคุมของบุคคลภายนอก ต้องจัดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของ กสอ. และระบุเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าวอย่างชัดเจน

๕.๕ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๕.๖ ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้น เจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหาร หน่วยงานนำเข้าเยี่ยมชม

๕.๗ มีการพิสูจน์ตัวตน เพื่อควบคุมการเข้า - ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะในห้อง Server การควบคุมการเข้า - ออก ให้ยืนยันตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพได้แก่ ระบบสแกนลายนิ้วมือของแต่ละบุคคล (Authentication by Biometric Traits)

๕.๘ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะในห้อง Server เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๕.๙ จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๕.๑๐ บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากผู้อำนวยการกลุ่มระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และจะต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๕.๑๑ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากหัวหน้าส่วนงาน

ข้อ ๖ ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศ ต้องกำหนดการบำรุงรักษาอุปกรณ์ ดังนี้

๖.๑ กำหนดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

๖.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๖.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๖.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๖.๕ ควบคุมและดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายใน กสอ.

๖.๖ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีความสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๗ ผู้ดูแลระบบต้องควบคุมการนำอุปกรณ์คอมพิวเตอร์ของ กสอ. ออกภายนอก ดังนี้

๗.๑ ต้องมีการกรอกใบคำร้อง เสนอต่อ ผอ.ศส. และต้องได้รับอนุมัติก่อนที่จะนำอุปกรณ์หรือทรัพย์สินออกนอกหน่วยงานได้

๗.๒ ต้องมีการบันทึกข้อมูลการนำอุปกรณ์ของ กสอ. ออกนอกหน่วยงาน และต้องมีการลงลายมือชื่อตอนรับอุปกรณ์เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ มาส่งคืน

ข้อ ๘ ผู้ดูแลระบบ ต้องจัดการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน

๘.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์คอมพิวเตอร์ของ กสอ. ออกไปใช้งานนอกสถานที่

๘.๒ ห้ามผู้ใช้งานละทิ้งอุปกรณ์คอมพิวเตอร์ของ กสอ. ไว้โดยลำพังในที่สาธารณะ

๘.๓ ให้ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์คอมพิวเตอร์ของ กสอ. เสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๙ ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศ ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

๙.๑ ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะส่งจำหน่ายอุปกรณ์ดังกล่าว

๙.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ข้อ ๑๐ ผู้ใช้งานระบบสารสนเทศของหน่วยงานภายใน กสอ. ต้องกำหนดรหัสผ่าน และใช้งานรหัสผ่านอย่างปลอดภัย ดังนี้

๑๐.๑ ลงนามรับบัญชีผู้ใช้งานของตนเอง หากพบว่าบัญชีผู้ใช้งานนั้นถูกเปิดออกให้แจ้งผู้ดูแลระบบทันที

๑๐.๒ เปลี่ยนรหัสผ่านของตนเองทันทีหลังจากได้รับรหัสผ่านชั่วคราว โดยการตั้งรหัสผ่านใหม่จะต้องดำเนินการแนวทางการกำหนดรหัสผ่านในระบบบริหารจัดการบัญชีผู้ใช้งาน

๑๐.๓ ตั้งค่าเครื่องไม่ให้บันทึกรหัสผ่าน เพื่อให้การใช้งานรหัสผ่านมีความปลอดภัย ผู้ใช้งานควรจัดเก็บและรักษารหัสผ่านของตนเองไว้ให้เป็นความลับและระมัดระวังมิให้ผู้อื่นล่วงรู้ รวมทั้งไม่จดบันทึกรหัสผ่านไว้ในที่สามารถสังเกตเห็นได้โดยง่าย หรือไม่บันทึกรหัสผ่านไว้ในเครื่อง ทั้งนี้ ผู้ใช้งานสามารถปฏิเสธความรับผิดชอบหากผู้อื่นล่วงรู้และนำบัญชีผู้ใช้งานนี้ไปใช้งาน

๑๐.๔ การใช้บัญชีผู้ใช้งานของผู้อื่นจะต้องได้รับอนุญาตจากเจ้าของบัญชีผู้ใช้งานและเจ้าของบัญชีผู้ใช้งานไม่อาจปฏิเสธความรับผิดชอบหากบัญชีผู้ใช้งานดังกล่าวถูกใช้ไปในทางมิชอบ

ข้อ ๑๑ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึง (Business Requirements for Access Control)

๑๑.๑ กสอ. ได้จัดให้มีการบริการสารสนเทศรวมทั้งระบบเทคโนโลยีสารสนเทศ เพื่อใช้ประโยชน์ตามภารกิจของ กสอ. ได้แก่ ข้อมูลผู้ประกอบการ การบริการ ข้อมูลสารสนเทศของอุตสาหกรรม การบริหารจัดการระบบหนังสือราชการ ทั้งนี้การใช้งานตามภารกิจต้องอยู่บนพื้นฐานของการเคารพสิทธิของบุคคลอื่น การปฏิบัติให้ถูกต้องตาม พรบ. และกฎหมาย ที่เกี่ยวข้อง โดยกำหนดสิทธิการเข้าถึง จะแบ่งตามลำดับชั้นการบริหารจัดการของผู้บริหาร ดังนี้

๑๑.๑.๑ ผู้บริหารระดับสูง ได้แก่ อธิบดีกรมส่งเสริมอุตสาหกรรม รองอธิบดีกรมส่งเสริมอุตสาหกรรม สามารถเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับ มอบหมายให้กำกับดูแล

๑๑.๑.๒ ผู้บริหารระดับหน่วยงาน ได้แก่ ผู้อำนวยการกอง/ศูนย์ ผู้อำนวยการกลุ่มงาน สามารถ เข้าถึงข้อมูลภายใต้ความรับผิดชอบดูแล

๑๑.๑.๓ ผู้ปฏิบัติงาน สามารถเข้าถึงได้เฉพาะส่วนงานที่ตนเองได้รับมอบหมาย

๑๑.๒ การอนุญาตและการทบทวนสิทธิการเข้าถึงตามภารกิจ

๑๑.๒.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากหน่วยงานเจ้าของข้อมูลและผู้ดูแลระบบตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๑๑.๒.๒ เจ้าของข้อมูลและเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะส่วนที่จำเป็นตามหน้าที่ที่ได้รับมอบหมายเท่านั้น

๑๑.๒.๓ ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน ซึ่งต้องมีการจัดทำเอกสารขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ

๑๑.๓ ข้อมูลพื้นฐานที่ใช้ประกอบการควบคุมและจำกัดสิทธิสำหรับผู้ใช้งาน

๑๑.๓.๑ ชื่อ นามสกุล ของผู้ขอใช้บริการ
๑๑.๓.๒ ตำแหน่ง และ หน่วยงานต้นสังกัด
๑๑.๓.๓ คำสั่งมอบหมายและหน้าที่ความรับผิดชอบ
๑๑.๓.๔ วันที่เริ่มมีผลบังคับใช้ วันที่สิ้นสุด
๑๑.๓.๕ ลายเซ็นอนุมัติจากหัวหน้าส่วนราชการ

ส่วนที่ ๒ การบริหารจัดการสิทธิการเข้าถึง (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

ข้อ ๑ การสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

๑.๑ มีการเผยแพร่นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้งานได้รับทราบ

๑.๒ มีการจัดฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๑.๓ เสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึง ระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว โดย ปฏิบัติตามแนวทางดังนี้

๒.๑ ผู้ขอใช้งานต้องปฏิบัติตามขั้นตอนการลงทะเบียน (User Register) ตามที่ กสอ. กำหนดในภาคผนวก ข. โดยที่ผู้ขอใช้งานจะต้องลงนามรับทราบนโยบายความมั่นคงปลอดภัยและแนวปฏิบัติของ กสอ. อย่างเคร่งครัด

๒.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๒.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒.๔ จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นลายลักษณ์อักษร

๒.๕ มีการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๒.๖ การอนุญาตให้เข้าถึงระบบสารสนเทศต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการกอง/ศูนย์ที่เป็นเจ้าของระบบสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๗ ต้องดำเนินการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและตัดออกจากทะเบียน ผู้ใช้งานทันที เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

ข้อ ๓ การบริหารจัดการบัญชีผู้ใช้งาน (User Account) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งาน ดังนี้

๓.๑ ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายใน กสอ. จัดทำบัญชีผู้ใช้งานกลาง โดยกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อให้สามารถระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ตามสิทธิการเข้าถึง

๓.๒ ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายใน กสอ. ต้องกำหนดชื่อผู้ใช้งานในบัญชีผู้ใช้งาน ดังนี้

๓.๒.๑ ชื่อผู้ใช้งานต้องไม่ซ้ำกัน

๓.๒.๒ ชื่อผู้ใช้งานต้องสื่อถึงชื่อผู้เป็นเจ้าของบัญชีผู้ใช้งานหรือหน่วยงาน

๓.๓ ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายใน กสอ. ต้องมีการทบทวนสิทธิของผู้ใช้งานอย่างสม่ำเสมอ การตรวจสอบสิทธิจะต้องอ้างอิงจากหนังสือคำสั่งต่าง ๆ ได้แก่ คำสั่งให้ลาออก คำสั่งโยกย้าย คำสั่งบรรจุบุคลากร ในการเปลี่ยนแปลงสิทธิการเข้าใช้งานระบบสารสนเทศจะต้องกระทำหลังจากจัดเก็บสำเนาเอกสารคำสั่งแล้วเท่านั้น

๓.๔ สำนักงานเลขานุการกรม มีหน้าที่รายงานความเคลื่อนไหวของบัญชีเจ้าหน้าที่ต่อ ศส. โดยเร่งด่วน ในกรณีบรรจุใหม่ ลาออก ออกจากราชการ ย้ายหน่วยงาน เกษียณอายุ หรือถึงแก่กรรม ยกเว้นกรณีที่เกี่ยวกับการมอบอำนาจหรือยกเลิกในการลงนามโดยลายมือชื่ออิเล็กทรอนิกส์ให้ดำเนินการโดยด่วนที่สุด

๓.๕ การขอบัญชีผู้ใช้งาน

๓.๕.๑ ผู้บริหารสูงสุด ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และผู้บริหารได้รับบัญชีผู้ใช้งานโดยมิต้องร้องขอ

๓.๕.๒ เจ้าหน้าที่ หรือผู้ที่เกี่ยวข้อง ต้องปฏิบัติตามขั้นตอนการลงทะเบียน (User Register) ตามที่ กสอ. กำหนดในภาคผนวก ข. โดยที่ผู้ขอใช้งานจะต้องลงนามรับทราบนโยบายความมั่นคงปลอดภัยและแนวปฏิบัติของ กสอ. อย่างเคร่งครัด

๓.๕.๓ ในกรณีที่บัญชีเจ้าหน้าที่และผู้ใช้งานที่เกี่ยวข้องถูกระงับชั่วคราว หากเจ้าหน้าที่หรือผู้ใช้งานที่เกี่ยวข้องประสงค์จะใช้งานบัญชีผู้ใช้งานนั้นใหม่ให้ผู้อำนวยการ กอง/ศูนย์มีบันทึกข้อความขอบัญชีผู้ใช้งานใหม่พร้อมเอกสารใบคำร้องเพื่อขอบัญชีผู้ใช้งาน

๓.๖ การระงับบัญชีผู้ใช้งาน

๓.๖.๑ เมื่อฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและหัวหน้าส่วนราชการมีคำสั่งให้ระงับบัญชีผู้ใช้งานเป็นการชั่วคราว

๓.๖.๒ เมื่อฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศหลายครั้งและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง มีคำสั่งให้ระงับบัญชีผู้ใช้งาน

๓.๖.๓ เมื่อผู้บริหารร้องขอ

๓.๗ การยกเลิกบัญชีผู้ใช้งาน

๓.๗.๑ เมื่อฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศหลายครั้งและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง มีคำสั่งให้ยกเลิกบัญชีผู้ใช้งานอย่างถาวร

๓.๗.๒ เมื่อผู้บริหารร้องขอ

๓.๗.๓ เมื่อสิ้นสุดสัญญา (สำหรับผู้ใช้งานที่เกี่ยวข้อง)

๓.๗.๔ เมื่อหมดเวลาการใช้งานที่ ศส. กำหนด (สำหรับผู้ใช้งานภายนอก)

ข้อ ๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อ เข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิทั่วไป สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับการเข้าถึง โดยปฏิบัติตามแนวทางดังนีดังนี้

๔.๑ การขอสิทธิของผู้ใช้งาน

๔.๑.๑ ผู้บริหารระดับสูง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และผู้บริหารได้รับสิทธิพิเศษซึ่งเป็นสิทธิที่มีการจำกัดการใช้งานน้อยที่สุด โดยมิต้องร้องขอ

๔.๑.๒ เจ้าหน้าที่ ผู้ที่เกี่ยวข้อง ผู้ดูแลระบบ และผู้รับผิดชอบระบบสารสนเทศ ต้องปฏิบัติตามขั้นตอนการลงทะเบียน (User Register) ตามที่ กสอ.กำหนดในภาคผนวก ข. เพื่อให้มีสิทธิในการเข้าถึงและใช้งานระบบสารสนเทศตามภารกิจและความจำเป็น ดังนี้

- สิทธิทั่วไป หมายถึง สิทธิในการเข้าถึงเครือข่ายของ กสอ. เพื่อ Download ข้อมูลเผยแพร่หรือเอกสารที่ใช้สำหรับการประชุม การใช้งาน Internet หรืออุปกรณ์บนเครือข่าย เช่น Printer Network

- สิทธิของผู้ใช้งานระบบสารสนเทศหรือระบบงาน หมายถึง สิทธิในการเข้าถึง ข้อมูลในระบบสารสนเทศซึ่งผู้ขอใช้งานต้องระบุวัตถุประสงค์และระดับของข้อมูลตามภารกิจที่จะเข้าถึงอย่าง ชัดเจนตามความจำเป็นในการปฏิบัติหน้าที่และต้องได้รับการอนุมัติ ก่อนเข้าใช้งาน

- สิทธิสูงสุด หมายถึง สิทธิของผู้ดูแลระบบหรือผู้รับผิดชอบระบบสารสนเทศเป็นสิทธิพิเศษที่ผู้ขอต้องเป็นผู้ที่เกี่ยวข้องและมีหน้าที่หรือภารกิจที่ได้รับมอบหมายให้ดูแล บริหารจัดการพัฒนาและบำรุงรักษาระบบสารสนเทศ ของ กสอ.

๔.๑.๓ ผู้ใช้งานภายนอกต้องเขียนเอกสารใบคำร้องขอใช้บริการยื่นด้วยตนเองต่อ เจ้าหน้าที่ ศส. เพื่อเสนออนุมัติต่อ ผอ.ศส. ซึ่งจะได้รับสิทธิขั้นพื้นฐานที่เป็นการใช้งานชั่วคราวตาม ระยะเวลาที่กำหนด

๔.๑.๔ ในกรณีถูกระงับสิทธิให้เขียนใบคำร้องเพื่อขอเปิดสิทธิการใช้งาน

๔.๒ การระงับสิทธิผู้ใช้งาน

๔.๒.๑ เมื่อฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และ ผู้อำนวยการกอง/ศูนย์มีคำสั่งให้ระงับสิทธิผู้ใช้งานทั้งหมดหรือบางส่วน

๔.๒.๒ เมื่อผู้อำนวยการกอง/ศูนย์ร้องขอให้ระงับสิทธิผู้ใช้งานทั้งหมดหรือบางส่วน

๔.๒.๓ เมื่อ Login ผิดเกิน ๓ ครั้งติดต่อกัน

๔.๓ การยกเลิกสิทธิผู้ใช้งาน

๔.๓.๑ เมื่อฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศหลายครั้ง และ ผู้บริหารเทคโนโลยีสารสนเทศ มีคำสั่งให้ยกเลิกสิทธิผู้ใช้งาน

๔.๓.๒ เมื่อผู้อำนวยการกอง/ศูนย์ร้องขอให้ยกเลิกสิทธิผู้ใช้งาน

๔.๓.๓ เมื่อสิ้นสุดสัญญา (สำหรับผู้ใช้งานที่เกี่ยวข้อง)

๔.๓.๔ เมื่อหมดเวลาการใช้งานที่ ศส. กำหนด (สำหรับผู้ใช้งานภายนอก)

ข้อ ๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้อย่างรัดกุม โดยปฏิบัติตาม แนวทางดังนี้

๕.๑ ผู้ดูแลระบบต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๕.๒ การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

๕.๓ ต้องกำหนดรหัสผ่านตามเงื่อนไข ดังนี้

๕.๓.๑ มีความยาวไม่น้อยกว่า ๘ ตัวอักษร

๕.๓.๒ ประกอบด้วยตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ อักขระสัญลักษณ์ ตัวเลข

๕.๓.๓ ไม่มีความหมายในพจนานุกรมภาษาใด ๆ ทั้งสิ้น

๕.๓.๔ ไม่กำหนดรหัสผ่านจากชื่อหรือนามสกุลของตนเอง ชื่อเล่น ชื่อบุคคลในครอบครัว ชื่อบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน และจากคำศัพท์ที่ใช้ในพจนานุกรม

๕.๔ ส่งมอบรหัสผ่านชั่วคราว ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ไม่ใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่าน

๕.๕ การเปลี่ยนแปลงรหัสผ่าน สามารถกระทำได้ ๒ วิธี ดังนี้

๕.๕.๑ การเปลี่ยนแปลงรหัสผ่านโดยผู้ใช้งาน ควรทำเมื่อได้รับรหัสผ่านชั่วคราวหรือเกิดความไม่มั่นใจในความปลอดภัย สามารถกระทำผ่านหน้าจอจัดการข้อมูลรหัสผ่านภายในระบบปฏิบัติการของตน

๕.๕.๒ การเปลี่ยนรหัสผ่านโดยผู้ดูแลระบบ เนื่องจากผู้ใช้จำรหัสผ่านไม่ได้ ผู้ใช้จะต้องทำการกรอกแบบฟอร์มขอใช้บริการทางด้านเทคโนโลยีสารสนเทศ เสนอต่อผู้บังคับบัญชาตามลำดับ ไปยัง ผอ.ศส. เพื่อพิจารณาอนุมัติ หลังจากนั้นผู้ดูแลระบบจึงดำเนินการตั้งรหัสผ่าน ชั่วคราวให้ใหม่ ผู้ใช้งานจะต้องทำการเข้าสู่ระบบเพื่อแก้ไขรหัสผ่านด้วยตนเองอีกครั้ง ทั้งนี้การเปลี่ยนรหัสผ่านควรเปลี่ยนรหัสผ่านตามรอบระยะเวลา ดังนี้

- ผู้ดูแลระบบ ต้องเปลี่ยนรหัสผ่านอย่างน้อย ทุก ๓ เดือน
- ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านอย่างน้อย ทุก ๖ เดือน
- เปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๕.๖ การยกเลิกรหัสผ่าน คือการยกเลิกสิทธิจะถูกดำเนินการผ่านขั้นตอนการทบทวนสิทธิ ผู้ใช้งานโดยเมื่อมีคำสั่งโยกย้าย ให้ลาออก หรือคำสั่งจัดการทรัพยากรบุคคลอื่น ๆ ที่ทำให้จำเป็นต้องยกเลิก สิทธิให้ผู้ดูแลระบบทำการจัดเก็บสำเนาคำสั่งแล้วดำเนินการระงับการใช้งานหรือลบบัญชีผู้ใช้งานผ่านระบบ Active Directory ตามแต่กรณี

๕.๗ กรณีผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้อง จดจำ รหัสผ่านหลายตัว ผู้ใช้งานสามารถใช้รหัสผ่านเดียว สำหรับการเข้าถึง ทุกระบบได้ ซึ่งระบบเหล่านั้นควรมีการ รักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

๕.๘ ไม่ส่งรหัสผ่าน ผ่านระบบเครือข่ายโดยไม่ดำเนินการเข้ารหัสเพื่อรักษาความลับก่อน

๕.๙ ต้องกำหนดให้ผู้ใช้งานป้อนรหัสผู้ใช้งานและรหัสผ่านในการใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

ข้อ ๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

๖.๑ สำนักงานเลขานุการกรม ต้องแจ้งให้ ศส. ทราบทันทีเมื่อ

- มีการบรรจุ
- มีการเปลี่ยนแปลงตำแหน่งหน้าที่ความรับผิดชอบ
- มีการลาออกจากงานหรือสิ้นสุดการเป็นผู้บริหาร บุคลากร และลูกจ้าง หรือการถึงแก่กรรม
- มีการโยกย้ายหน่วยงาน
- มีการพักงาน การลงโทษทางวินัย หรือถูกระงับการปฏิบัติหน้าที่

๖.๒ ต้องจัดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชี ผู้ใช้งานปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ดังนี้

๖.๒.๑ ผู้ดูแลระบบต้องดำเนินการแก้ไขสิทธิการเข้าถึงของผู้ใช้ทันทีที่ได้รับแจ้งการเปลี่ยนแปลงจากสำนักงานเลขานุการกรม

๖.๒.๒ ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิการเข้าถึงระดับ สูงสุด ได้แก่ สิทธิผู้ดูแลระบบสูงสุดระดับหน่วยงาน สิทธิผู้ดูแลระบบย่อยตามคำสั่งมอบหมายของหน่วยงานเจ้าของระบบสารสนเทศด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๖.๒.๓ ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ การเข้าถึงในระดับสูงสุด เพื่อใช้ในการทบทวนในภายหลัง

๖.๒.๔ ผู้ดูแลระบบดำเนินการเพิกถอนสิทธิผู้ใช้งานที่พ้นสภาพการเป็นข้าราชการหรือ เจ้าหน้าที่และบุคลากร ของ กสอ. ภายใน ๖ เดือน

๖.๒.๕ ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยี สารสนเทศ โดย ทันทีเมื่อผู้ใช้งานนั้นทำการลาออก/เปลี่ยนตำแหน่งงาน/โอนย้ายข้ามหน่วยงานราชการ/ ถึงแก่กรรม โดยอ้างอิงหนังสือราชการจากสำนักงานเลขานุการกรม

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ ๑ ผู้ดูแลระบบ ต้องกำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ โดยแบ่งชั้นความลับของข้อมูล เป็น ๓ ระดับ ดังนี้

๑.๑ ลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งภาครัฐร้ายแรงที่สุด

๑.๒ ลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

๑.๓ ลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความ เสียหายแก่ประโยชน์แห่งรัฐ

ข้อ ๒ การจัดลำดับชั้นความลับและการบริหารจัดการกับข้อมูลตามข้อ ๑ ให้ใช้หลักเกณฑ์ตาม พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ โดยแสดงระดับชั้นความลับของเอกสารข้อมูลลับอย่างชัดเจนในเอกสารที่เกี่ยวข้องทุกหน้า

ข้อ ๓ การจัดลำดับชั้นความลับและการบริหารจัดการกับข้อมูลตามข้อ ๒ ให้อยู่ในดุลพินิจของผู้บริหาร

ข้อ ๔ การบริหารจัดการกับข้อมูลตามข้อ ๓ ต้องมีการตรวจสอบความถูกต้องเหมาะสมของข้อมูลที่จะเผยแพร่ออกสู่สาธารณะผ่านทางเว็บไซต์ ข้อมูลดังกล่าวจะต้องไม่ขัดต่อกฎหมายและมีกลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาต และห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

ข้อ ๕ การรับ ส่ง และจัดเก็บข้อมูลอิเล็กทรอนิกส์ที่ประสงค์จะให้เป็นความลับได้อย่างปลอดภัย สามารถขอคำปรึกษาหรือการสนับสนุนในการเข้ารหัสจากผู้ดูแลระบบได้โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๖ ประเภทของข้อมูลแบ่งออกเป็น ๓ ประเภท ดังนี้

๖.๑ ข้อมูลที่ใช้ในการบริหารจัดการ ได้แก่ ข้อมูล นโยบาย ยุทธศาสตร์ บุคลากร งบประมาณ คำรับรองการปฏิบัติราชการ การเงินและบัญชี

๖.๒ ข้อมูลที่ใช้ในการดำเนินงาน ได้แก่ ข้อมูล กฎหมาย ระเบียบ ข้อมูลที่เกี่ยวกับภารกิจหน้าที่ของ กสอ.

๖.๓ ข้อมูลเพื่อการบริการ ได้แก่ รายงานทางวิชาการ แผนที่ภาพถ่ายดาวเทียม องค์ความรู้

ข้อ ๗ ลำดับความสำคัญของข้อมูล แบ่งออกเป็น ๓ ระดับ ดังนี้

๗.๑ ข้อมูลที่มีความสำคัญมากที่สุด ได้แก่ ข้อมูลส่วนตัวของผู้ประกอบการ และข้อมูลนิติบุคคล

๗.๒ ข้อมูลที่มีความสำคัญปานกลาง ได้แก่ ข้อมูลอื่น ๆ ของผู้ประกอบการ

๗.๓ ข้อมูลที่มีความสำคัญน้อย ได้แก่ ข้อมูลตามภารกิจของ กสอ. ที่ไม่อยู่ในข้อ (๑) และ (๒)

ข้อ ๘ ระดับการเข้าถึงข้อมูล แบ่งออกเป็น ๓ ระดับ ดังนี้

๘.๑ ข้อมูลที่เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุด เพื่อเข้าไปบริหารจัดการระบบสารสนเทศ ได้แก่ ผู้ดูแลระบบ

๘.๒ ข้อมูลที่เข้าถึงได้เฉพาะผู้ได้รับอนุมัติสิทธิ หมายถึง ข้อมูลที่ผู้ใช้งานต้องได้รับการอนุญาตจากผู้รับผิดชอบระบบสารสนเทศหรือผู้ดูแลระบบ ตามภาระหน้าที่และความจำเป็น

๘.๓ ข้อมูลที่เข้าถึงได้ทุกกลุ่มผู้ใช้งาน หมายถึงข้อมูลพื้นฐานที่ได้รับอนุญาตจากผู้รับผิดชอบระบบสารสนเทศหรือผู้ดูแลระบบ พิจารณาแล้วว่าสามารถเข้าถึงได้

ข้อ ๙ การกำหนดช่องทางการเข้าถึงระบบสารสนเทศของ กสอ. ต้องกำหนด ดังนี้

๙.๑ ต้องให้ผู้รับบริการสามารถเข้าถึงได้ทั้งจากภายในและภายนอก กสอ.

๙.๒ ผู้รับบริการสามารถรับบริการข้อมูลข่าวสารผ่านเว็บไซต์ของ กสอ. โดยไม่ต้องลงทะเบียน

๙.๓ ผู้รับบริการสามารถใช้บริการสอบถามข้อมูลต่าง ๆ ผ่านกระดานถามตอบที่ กสอ. จัดเตรียมไว้ให้ ซึ่งผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ หรือ เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน โดย กสอ. สงวนสิทธิในการลบข้อความที่เข้าข่ายดังกล่าว หรือข้อความที่ขัดต่อกฎหมาย ใด ๆ รวมทั้งขัดต่อศีลธรรมอันดี ออกจากระบบโดยไม่จำเป็นต้องแจ้งให้ทราบ

ส่วนที่ ๔ การบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ข้อ ๑ กำหนดมาตรการทางเครือข่ายสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่าย ระบบงาน หรือบริการต่าง ๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๑.๑ กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ งานที่ต้องรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

๑.๒ กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๑.๓ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๔ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๑.๕ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๑.๖ มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์แม่ข่ายและเครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๑.๗ มีการใช้ฮาร์ดแวร์หรือซอฟต์แวร์ สำหรับการบริหารจัดการเครือข่าย เพื่อเฝ้าระบุเฝ้าตรวจ ติดตามสถานะ อุปกรณ์ในระบบสารสนเทศของ กสอ.

๑.๘ ทำทะเบียนข้อมูลอุปกรณ์ ครุภัณฑ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่และระบบเครือข่าย รวมทั้งหมายเลข Media Access Control Address (MAC Address) เพื่อให้สามารถระบุอุปกรณ์บนระบบเครือข่ายได้

๑.๙ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๒ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒.๑ การใช้งานบริการเครือข่าย

๒.๑.๑ ผู้ดูแลระบบ ดำเนินการออกแบบระบบเครือข่ายตามกลุ่มการให้บริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานตามกลุ่มผู้ใช้และกลุ่มของระบบสารสนเทศ และกำหนดให้ผู้ใช้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น เพื่อเป็นการควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ และให้คำนึงถึงความมั่นคงปลอดภัยเป็นสำคัญ

๒.๑.๒ การเข้าสู่ระบบเครือข่ายของ กสอ. ต้องปฏิบัติตามขั้นตอนการลงทะเบียน (User Register) ตามที่ กสอ. กำหนดในภาคผนวก ข. โดยที่ผู้ขอใช้งานจะต้องลงนามรับทราบนโยบายความมั่นคงปลอดภัยและแนวปฏิบัติของ กสอ. อย่างเคร่งครัด และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตเป็นลายลักษณ์อักษรและจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหน่วยงานต้นสังกัดและผ่านความเห็นชอบจากผู้อำนวยการกอง/ศูนย์ก่อนที่จะสามารถใช้งานได้

๒.๑.๓ การใช้งานระบบสารสนเทศที่สำคัญต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิปีละ ๑ ครั้ง

๒.๑.๔ สิทธิการใช้งานเครือข่ายเป็นสิทธิพิเศษ (Privilege) ที่ กสอ. มอบให้บุคคล หรือหน่วยงานที่ได้รับสิทธิเฉพาะบริการหรือระบบสารสนเทศที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ไม่สามารถโอนสิทธิให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

๒.๑.๕ ผู้ใช้ที่ฝ่าฝืนระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์จะถูกพิจารณาระงับและ/หรือ ยกเลิกบัญชีผู้ใช้งาน และ ศส. จะแจ้งหน่วยงานต้นสังกัดเพื่อพิจารณาโทษผู้ใช้ที่ฝ่าฝืนระเบียบด้วย

๒.๑.๖ การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

๒.๑.๖.๑ การใช้ระบบเครือข่ายคอมพิวเตอร์ เพื่อการกระทำสิ่งที่ผิดกฎหมาย

๒.๑.๖.๒ การเข้าใช้ระบบคอมพิวเตอร์ด้วยบัญชีรายชื่อของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

๒.๑.๖.๓ การเข้าถึงข้อมูลของผู้อื่นเพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต

๒.๑.๖.๔ การใช้งานที่เป็นสาเหตุทำให้มีผลต่อประสิทธิภาพการทำงานของระบบเครือข่ายลดลง หรือทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหาย เช่น การเปิดไฟล์ที่ไม่ทราบแหล่งที่มาที่แน่ชัด เพื่อป้องกันโปรแกรมประสงค์ร้าย (Malware) เข้าสู่ระบบเครือข่าย รวมถึงห้ามมิให้ผู้ใช้งาน ทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการ ป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจาก ผู้ดูแลระบบ (System Administrator)

๒.๑.๖.๕ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับ ระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของไวรัสไปยังเครื่องคอมพิวเตอร์อื่น ๆ

๒.๑.๖.๖ การเผยแพร่และ/หรือการเขาถึงสื่อลามกอนาจาร

๒.๑.๖.๗ การใช้ทรัพยากรและระบบเครือขายคอมพิวเตอร์เพื่อประกอบธุรกิจ หรือเข้าข่ายลักษณะเพื่อการค้าหรือเพื่อแสวงหากำไรผ่านเครื่องคอมพิวเตอร์ และเครื่องแม่ข่าย ได้แก่ การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การบริการโฆษณาสินค้า

๒.๑.๖.๘ ไม่อนุญาตให้ใช้งานโปรแกรมแชร์ข้อมูลประเภท Peer to Peer Network

๒.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections) สำหรับผู้ใช้ที่อยู่ภายนอก กสอ. ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวบุคคล ก่อนที่จะอนุญาตเข้าใช้งานเครือข่ายและระบบสารสนเทศของ กสอ. ดังนี้

๒.๒.๑ ในการเชื่อมต่อเข้าสู่ระบบเครือข่ายของ กสอ. ผู้ใช้งานต้องมีการ Login เพื่อแสดงตัวตนด้วย Username และ Password และพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๒.๒.๒ การเข้าสู่ระบบสารสนเทศของ กสอ. จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนผู้ใช้งานอีกครั้ง จึงอนุญาตให้เข้าถึงระบบข้อมูลได้

๒.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

๒.๓.๑ ผู้ดูแลระบบดำเนินการสำรวจข้อมูลอุปกรณ์ที่เชื่อมต่อบนเครือข่ายของทุก หน่วยงานในอาคารของ กสอ. ตามรอบการบำรุงรักษาระบบ (Preventive Maintenance) และจัดทำเอกสารผลการสำรวจ จำนวน ๒ รายการ ได้แก่

๒.๓.๑.๑ แผนภาพที่แสดงตำแหน่งที่ตั้งอุปกรณ์ภายในอาคารสถานที่

๒.๓.๑.๒ เอกสารแสดงการจัดเก็บข้อมูลในรูปแบบตารางที่แสดงความสัมพันธ์ระหว่างข้อมูล อย่างน้อย ดังนี้

- ชื่อของผู้ใช้/ผู้รับผิดชอบอุปกรณ์
- ชื่ออุปกรณ์และ Domain ของอุปกรณ์
- หมายเลข IP Address
- ชื่อส่วนงานที่ใช้อุปกรณ์
- หมายเลขครุภัณฑ์
- วัน เดือน ปี ที่ทำการสำรวจ

๒.๓.๒ ผู้ดูแลระบบดำเนินการจัดทำแผ่นป้าย (Label) ที่ระบุข้อมูลของอุปกรณ์ตามผลการสำรวจ สำหรับติดกำกับที่อุปกรณ์เพื่อความสะดวกในการจำแนกประเภทและชนิดของอุปกรณ์บนเครือข่าย

๒.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

๒.๔.๑ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้อง Server จะต้อง ลงชื่อเข้า - ออก พื้นที่ ให้ถูกต้องและได้รับการอนุมัติจาก ผอ.ศส. ก่อน และต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๔.๒ บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษาระบบ ปรับแต่งหรือบริหารจัดการ พอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับอนุมัติจากผู้อำนวยการกอง/ศูนย์ก่อน

๒.๔.๓ ผู้ดูแลระบบต้องกำหนดการเปิด - ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงต่อการก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์

๒.๔.๔ ทำการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ด้วยการปิดการเข้าถึงโดยตรงจากภายนอกทั้งหมด ผู้ใช้ที่ต้องการเข้าถึงพอร์ตจะต้องทำการล๊อกอินเชื่อมต่อกับ VPN ก่อนจึงสามารถใช้งานได้กายภาพ และโดยการล๊อกอินเข้ามาใช้งาน

๒.๔.๕ ผู้ดูแลระบบต้องทำการ ตรวจสอบเพื่อ เปิด – ปิด พอร์ตของระบบหรืออุปกรณ์ตามความจำเป็นต่อการใช้งานอย่างน้อยสัปดาห์ละ ๒ ครั้ง

๒.๕ การแบ่งแยกเครือข่าย (Segregation in Networks)

๒.๕.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มการให้บริการระบบ เทคโนโลยีสารสนเทศที่มีการใช้งาน ตามกลุ่มผู้ใช้ และกลุ่มของระบบสารสนเทศ เพื่อเป็นการควบคุมและ ป้องกันการบุกรุกได้อย่างเป็นระบบ และให้คำนึงถึงความมั่นคงปลอดภัยเป็นสำคัญ

๒.๕.๒ ผู้ดูแลระบบ ดำเนินการจัดแบ่งระบบเครือข่าย (VLAN) ของเครื่องคอมพิวเตอร์ ลูกข่ายออกเป็นเครือข่ายย่อย ตามโครงสร้างอย่างเหมาะสมในการปฏิบัติงานและการบริหารจัดการ

๒.๕.๓ ผู้ดูแลระบบ ดำเนินการแยกเครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการข้อมูลสารสนเทศ กับเครื่องคอมพิวเตอร์สำหรับผู้ใช้งาน โดยใช้ Core Switch และ Firewall หรืออุปกรณ์เครือข่ายอื่น ๆ เพื่อจำกัดให้เฉพาะกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้น จึงจะสามารถเชื่อมต่อเข้าไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นได้

๒.๕.๔ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่าย ภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกันให้ สอดคล้องกับแนวปฏิบัติการควบคุม การเข้าถึง ดังนี้

๒.๖.๑ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ IPS, Firewall, Proxy และ Mail Gateway

๒.๖.๒ ติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) สำหรับตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติผ่านเครือข่ายหรือมีการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๒.๖.๓ การเชื่อมต่อเข้าสู่ระบบเครือข่ายของ กสอ. ผู้ใช้งานต้องมีการ Login ด้วย Username และ Password และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๒.๖.๔ ในกรณีที่ผู้ดูแลระบบตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลักของ กสอ. จะทำการหยุดให้บริการโดยการตัดการเชื่อมต่อกับระบบเครือข่ายกลาง โดยไม่มีการแจ้งให้ทราบล่วงหน้า จนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

๒.๖.๕ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขต (Zone) ของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๖.๖ ให้ผู้ดูแลระบบใช้เครื่องมือ (Tool) ได้แก่ FortiGate Firewall และ Cacti Monitor เพื่อทำการตรวจสอบการเชื่อมต่อระบบเครือข่าย

๒.๖.๗ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก ได้แก่ บันทึกการ เข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน หรือไม่ต่ำกว่า ๙๐ วัน

๒.๖.๘ กำหนดให้มีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัด สิทธิการเข้าถึงบันทึกต่าง ๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒.๖.๙ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๒.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

๒.๗.๑ ผู้ดูแลระบบ ดำเนินการกำหนดตารางการใช้เส้นทางบนระบบเครือข่ายบนอุปกรณ์ค้นหาเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมการใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๒.๗.๒ ผู้ดูแลระบบ ต้องจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเพื่อการวิเคราะห์ปัญหาและตั้งค่าระบบ ให้กำหนดเฉพาะชุด IP Address ของผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงได้

๒.๗.๓ กำหนดบุคคลที่รับผิดชอบในการกำหนด ตั้งค่า แก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง

๒.๗.๔ ข้อมูลหมายเลขชุดอินเตอร์เน็ตของคอมพิวเตอร์ (IP Address) ภายใน (Local) ของระบบงานเครือข่ายภายในของ กสอ. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของ กสอ. ได้โดยง่าย

๒.๗.๕ ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการ ติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ ศส. หรือผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบ เท่านั้น

ข้อ ๓ การเข้าถึงระบบเครือข่ายหรือระบบสารสนเทศจากระบบเครือข่ายภายนอก ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายใน กสอ. ต้องดูแลรักษาความปลอดภัยโดยต้องควบคุมและจำกัดให้ดำเนินการใช้ได้เฉพาะเท่าที่จำเป็นเท่านั้น โดยมีแนวทางปฏิบัติ ดังนี้

๓.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของ กสอ. ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของ กสอ. การควบคุมบุคคลที่เข้าสู่ระบบของ กสอ. จากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน ผู้ใช้งานต้องทำการเชื่อมต่อผ่านระบบ VPN

๓.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๓.๓ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ กสอ. อย่างเพียงพอและต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อน

๓.๔ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๓.๕ ให้ ศส. จัดทำระบบ VPN (Virtual Private Network) โดยเป็นช่องทางเฉพาะที่มีการเข้ารหัสเพื่อป้องกันการดักจับข้อมูลระหว่างทาง โดยผู้ใช้งานจะสามารถเข้าถึงระบบสารสนเทศหรือระบบงานได้เฉพาะที่ตนเองมีสิทธิเท่านั้น ทั้งนี้ ผู้ใช้งานจะต้อง Login โดยใช้ Username และ Password ตามบัญชีผู้ใช้งานทุกครั้ง เพื่อพิสูจน์ยืนยันตัวตน (User Authentication) ก่อนใช้งาน

ข้อ ๔ ข้อกำหนดของห้องควบคุมระบบ (Computer Room)

๔.๑ แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น Router, Switch และ Server ต่าง ๆ

๔.๒ มีการจัดเก็บอุปกรณ์ต่าง ๆ ในตู้ Rack ที่เหมาะสม เพื่อสะดวกในการบำรุงรักษา

๔.๓ ไม่ควรวางอุปกรณ์ต่าง ๆ ในตำแหน่งใกล้ประตูหน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น

๔.๔ การจัดวางสายสัญญาณและสายไฟฟ้าควรมีการเก็บสายให้เรียบร้อยเพื่อป้องกันการเดินสะดุด

๔.๕ ติดประกาศการบำรุงรักษาอุปกรณ์ เช่น ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

๔.๖ ติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV ระบบป้องกันการเข้าออกห้องโดยระบบ Key Card หรือ Fingerprint Scan เป็นต้น

๔.๗ มีระบบป้องกันอัคคีภัย

๔.๘ มีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง

๔.๙ มีระบบป้องกันไฟฟ้าจากฟ้าผ่า

๔.๑๐ ระบบปรับอากาศแบบควบคุมอุณหภูมิ (๑๐-๒๖°C) และความชื้น (๒๐- ๘๐%)

๔.๑๑ ติดตั้งฉนวนกันไฟไหม้ ที่ฝ้าเพดานและผนังกำแพง

๔.๑๒ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๔.๑๓ ไม่อนุญาตให้มีการเข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

๔.๑๔ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อ ทรัพย์สินจะอนุญาตให้เข้าไปในพื้นที่จำกัด การเข้าถึงได้โดยได้รับความเห็นชอบจากผู้บริหารฝ่าย IT

ส่วนที่ ๕ การบริหารจัดการระบบสารสนเทศ

ข้อ ๑ การพัฒนาระบบสารสนเทศของ กสอ. จะต้องควบคุมการพัฒนาระบบสารสนเทศให้มีมาตรฐานด้านความมั่นคงปลอดภัย ดังนี้

๑.๑ มีการพิสูจน์ตัวตนของผู้ใช้งานและแจ้งเตือนเมื่อการพิสูจน์ตัวตนผิดพลาด

๑.๒ สามารถแยก Function การทำงานตามภาระหน้าที่

๑.๓ สามารถสร้างกลุ่มผู้ใช้ได้ตามสิทธิของผู้ใช้งาน

๑.๔ สามารถจัดเก็บ Log การใช้งาน

๑.๕ สามารถยืนยันหรือแจ้งเตือนการเปลี่ยนแปลงแก้ไขข้อมูล

๑.๖ มี Function ในการปรับปรุงสิทธิของผู้ใช้งาน

ข้อ ๒ ผู้ดูแลระบบเป็นผู้ตรวจสอบ Function (s) ด้านความมั่นคงปลอดภัย ตามข้อ ๑

ข้อ ๓ ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศ ของหน่วยงานภายใน กสอ. ต้องกำหนดระยะเวลาการใช้งานระบบสารสนเทศ (Session Time-Out) ดังนี้

๓.๑ กำหนดให้ระบบสารสนเทศ ได้แก่ ระบบงาน ระบบเครือข่าย มีการตัดการติดต่อและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๓.๒ กำหนดให้ระบบสารสนเทศมีการตัดการติดต่อและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบงานที่มีการจัดลำดับว่าเป็นข้อมูลที่มีความสำคัญมาก หรือระบบงานที่มีการกำหนดชั้นความลับ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๓ แนวทางปฏิบัติ

๓.๓.๑ เมื่อผู้ใช้งานไม่ได้ใช้งานหรือว่างเว้นจากการใช้งานในระยะเวลา ๑๕ นาที หรือตามที่ผู้รับผิดชอบกำหนด ให้มีการตัดการเชื่อมต่อการใช้งานออกจากระบบสารสนเทศโดยอัตโนมัติ

๓.๓.๒ ถ้ามีความพยายามเข้าสู่ระบบใหม่ ให้ยืนยันการใช้งานโดยใส่ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หรือวิธีการที่ปลอดภัยในการยืนยันตัวบุคคลในทุก ๆ ครั้ง

ข้อ ๔ ผู้ดูแลระบบและผู้รับผิดชอบระบบสารสนเทศ ของหน่วยงานภายใน กสอ. ต้องกำหนดการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection) ดังนี้

๔.๑ กำหนดให้ระบบงานที่มีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น

๔.๒ กำหนดให้ระบบสารสนเทศ ได้แก่ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) ระบบงานที่กำหนดชั้นความลับ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อเพื่อป้องกันบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึงข้อมูลได้โดยง่าย

๔.๓ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของ กสอ. มีแนวทางปฏิบัติดังนี้

๔.๓.๑ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของ กสอ. กำหนดให้ใช้งานได้ ๒ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หรือตามผู้บังคับบัญชาเห็นสมควร

๔.๓.๒ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของ กสอ. กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.) เท่านั้น

๔.๓.๓ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของ กสอ. ถ้ากระทำในช่วงนอกเวลาทำงานตามปกติ ต้องแจ้งขอใช้งานจากผู้ดูแลระบบก่อนเพื่อให้มีการบันทึกไว้ตรวจสอบ

ข้อ ๕ การควบคุมผู้รับเหมา (Outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ มีวิธีการปฏิบัติดังนี้

๕.๑ มีกระบวนการคัดเลือกผู้รับเหมาโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาที่ชัดเจน เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ ดังนี้

๕.๑.๑ ต้องมีประสบการณ์

๕.๑.๒ มีลูกค้าอ้างอิงน่าเชื่อถือ

๕.๑.๓ มีใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล

๕.๑.๔ มีความพร้อมด้านเทคโนโลยีของการรับเหมาช่วงทั้งในส่วนของฮาร์ดแวร์และซอฟท์แวร์รวมถึงระบบสนับสนุนอื่น ๆ

๕.๒ มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาและ ต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาต้องนำเสนอรายละเอียดขอบเขตงานอย่างครบถ้วน

๕.๓ กสอ. มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่า กสอ. สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น ดังนี้

๕.๓.๑ รายละเอียดเกี่ยวกับวิธีการทำงาน

๕.๓.๒ การกำหนดระยะเวลาตรวจติดตามคุณภาพของผู้รับเหมาเป็นระยะ ๆ หรือ แบบสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาช่วงใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้รับเหมาในการกระทำตามข้อกำหนดของหน่วยงาน

๕.๔ ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง และต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจาก ผอ.ศส. โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

๕.๔.๑ เหตุผลในการขอใช้งาน

๕.๔.๒ ระยะเวลาในการใช้งาน

๕.๔.๓ การตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย

๕.๔.๔ การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

๕.๕ มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๕.๖ ผู้รับเหมาที่ทำงานให้กับ กสอ. ทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายใน หรือนอกสถานที่จำเป็นต้องลงนามใน “สัญญาการไม่เปิดเผยข้อมูลของ กสอ.” โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ และ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability) และให้กำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น

๕.๗ ผู้รับเหมาต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

ข้อ ๖ ระบบสารสนเทศที่มีผลกระทบต่อองค์กร ต้องมีการจัดทำระบบสำรองข้อมูล

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ โปรแกรมประยุกต์ และโปรแกรมอรรถประโยชน์

ข้อ ๑ การติดตั้งโปรแกรมระบบปฏิบัติการ โปรแกรมประยุกต์ และโปรแกรมอรรถประโยชน์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย รวมทั้งเครื่องคอมพิวเตอร์ลูกข่ายของ กสอ. ให้กระทำโดยผู้ดูแลระบบ โดย โปรแกรมดังกล่าวต้องไม่ละเมิดลิขสิทธิ

ข้อ ๒ การควบคุมการเข้าถึงระบบปฏิบัติการ ให้ดำเนินการ ดังนี้

๒.๑ กรณีเครื่องแม่ข่าย (Server Computer)

๒.๑.๑ ผู้ดูแลระบบดำเนินการเชื่อมต่อเครื่องแม่ข่ายสำหรับให้บริการทุกเครื่องเข้ากับระบบ Domain Controller ที่ทำหน้าที่บริหารจัดการเครื่องคอมพิวเตอร์ เพื่อใช้บริหารจัดการกำหนดนโยบายควบคุมดูแลบัญชีผู้ใช้งานตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องของ กสอ.

๒.๑.๒ สร้างบัญชีผู้ใช้งานและให้สิทธิในการเข้าถึงระบบปฏิบัติการเท่าที่จำเป็น และต้องคอยตรวจสอบบัญชีรายชื่ออย่างน้อยเดือนละ ๑ ครั้ง เพื่อยกเลิกบัญชีที่ไม่ได้ใช้งาน

๒.๑.๓ หลีกเลี่ยงการใช้บัญชี Administrator ในการเข้าระบบ โดยให้สร้างและใช้บัญชีผู้ใช้งานที่ระบุได้ว่าเป็นผู้ใดกำลังใช้งานอยู่

๒.๑.๔ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งาน

๒.๑.๕ ผู้ดูแลระบบต้องตรวจสอบ Event Log เป็นประจำเพื่อดูว่ามีผู้ไม่ประสงค์ดีพยายามบุกรุกเข้าถึงระบบโดยไม่ได้รับอนุญาตหรือไม่

๒.๑.๖ การเข้าใช้งานระบบปฏิบัติการจากเครือข่ายภายนอกจะต้องผ่าน VPN ที่กำหนดให้เท่านั้น

๒.๒ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client Computer)

๒.๒.๑ การตั้งค่า BIOS บน Mainboard ให้ตั้งรหัสผ่านเพื่อป้องกันการแก้ไข

๒.๒.๒ ให้สิทธิการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ลูกข่ายที่ระดับ User พร้อมกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๒.๒.๓ ผู้ใช้งานต้องตั้งค่าโปรแกรมพักหน้าจอ (Screen Saver) ให้มีรหัสผ่านเพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งานเกินกว่า ๕ นาที

๒.๒.๔ ผู้ใช้งานต้องทำการลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเอง และลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๓ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ผู้ใช้งานต้องแสดง ตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน สำหรับการใช้งานระบบสารสนเทศ ดังนี้

๓.๑ การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

๓.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนโดยใช้ Username และ Password ของตนเองทุกครั้งก่อนใช้ระบบสารสนเทศและเครือข่าย เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานดำเนินการแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๓ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

๓.๔ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๕ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ข้อ ๔ การบริหารจัดการรหัสผ่าน (Password Management System)

ผู้ดูแลระบบต้องจัดทำหรือจัดให้มีระบบบริหาร จัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยต้องปฏิบัติดังนี้

๔.๑ จำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการล็อคสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อคให้

๔.๒ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

๔.๓ มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๔.๔ จัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

๔.๕ ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๔.๖ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

ข้อ ๕ โปรแกรมประยุกต์และโปรแกรมอรรถประโยชน์ ที่เป็นโปรแกรมมาตรฐานซึ่งผู้ดูแลระบบติดตั้งให้เมื่อมีการส่งมอบเครื่องคอมพิวเตอร์แก่ผู้ใช้งาน มีดังนี้

๕.๑ Microsoft Office

๕.๒ Microsoft Windows

๕.๓ Acrobat Reader

๕.๔ Antivirus

๕.๕ WinRAR/WinZip

๕.๖ Google Chrome

ข้อ ๖ ในกรณีที่ผู้ใช้งานของหน่วยงานใดต้องการใช้งานโปรแกรมอื่น ๆ นอกเหนือจากข้อ ๕ ให้แจ้งเหตุผลความจำเป็นมาที่ ศส. เพื่อพิจารณาดำเนินการให้ต่อไป

ส่วนที่ ๗ การบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่ายไร้สาย

ข้อ ๑ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) มีแนวทางปฏิบัติ ดังนี้

๑.๑ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๑.๒ ผู้ดูแลระบบทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๑.๓ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๑.๔ ผู้ดูแลระบบเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) หรือ ชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และ/หรือชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๑.๕ ผู้ดูแลระบบมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๑.๖ ผู้ดูและระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาให้ทราบทันที

๑.๗ ผู้ใช้งานที่มีความประสงค์จะใช้งานระบบเครือข่ายไร้สาย (Wireless) ต้องปฏิบัติตามขั้นตอนการลงทะเบียน (User Register) ตามที่ กสอ. กำหนดในภาคผนวก ข. เพื่อให้มีสิทธิในการใช้ระบบเครือข่ายไร้สาย (Wireless) ตามภารกิจและความจำเป็น

๑.๘ ผู้ขอใช้งานที่ได้รับอนุมัติแล้วจะต้องนำอุปกรณ์ไปทำการลงทะเบียนกับผู้ดูแลระบบก่อนการใช้งาน

ข้อ ๒ การใช้งานระบบเครือข่ายไร้สาย มีแนวปฏิบัติ ดังนี้

๒.๑ ห้ามผู้ใช้งานนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB Client หรือ Wireless Card

๒.๒ ห้ามผู้ใช้งานเปิดแชร์ Internet แบบ ad-hoc หรือ peer-to-peer Network หรือเปิดแชร์ด้วย Hotspot Bluetooth USB ผ่านโทรศัพท์มือถือ หรือสมาร์ทโฟน โดยไม่ได้รับอนุญาต

๒.๓ ผู้ใช้งานต้อง Login เพื่อพิสูจน์ตัวตน โดยใช้ Username และ Password ตามบัญชีผู้ใช้งานทุกครั้ง

ส่วนที่ ๘ การรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์

ข้อ ๑ ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของ กสอ. มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๑.๑ ผู้มีความประสงค์จะใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกแบบฟอร์มการขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงาน โดยยื่นคำขอผ่านหน่วยงานที่สังกัดตามขั้นตอน

๑.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที

๑.๓ ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๑.๔ ไม่เปิดอ่านจดหมายที่ไม่ปรากฏชื่อเรื่อง (Subject) หรือชื่อผู้ส่งไม่ชัดเจน

๑.๕ ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

๑.๖ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของหน่วยงาน ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของ กสอ. เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของ กสอ. ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๑.๗ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๑.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคลโดยอ้างว่าเป็นความเห็นของ กสอ.

๑.๙ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของ กสอ. เพื่อเผยแพร่ ข้อความ รูปภาพ วิดีโอ เสียงที่มีลักษณะ หยาบคาย หรือลามกอนาจารหรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของ กสอ. ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการ กสอ.

๑.๑๐ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของ กสอ. เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น

๑.๑๑ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑.๑๒ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

ข้อ ๒ การระงับบัญชีจดหมายอิเล็กทรอนิกส์

บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่ผู้ใช้ไม่สามารถโอนสิทธิให้แก่ผู้ใช้อื่นได้ กสอ. คงไว้ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบาย หรืออาจก่อให้เกิดปัญหา ความมั่นคงปลอดภัย หรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์ มีแนวปฏิบัติดังนี้

๒.๑ เมื่อผู้ใช้พ้นสภาพการอยู่ในสังกัดของ กสอ. ผู้ดูแลระบบสามารถระงับบัญชีผู้ใช้ ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย

๒.๒ ผู้ใช้สามารถร้องขอการขยายสิทธิการใช้บัญชีผู้ใช้เพื่อคงสิทธิการใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้เมื่อต้องพ้นสภาพการอยู่ในสังกัดของ กสอ. โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัดพร้อมแนบเหตุผลความจำเป็นส่งถึง ศส. การอนุญาตและระยะเวลาการขยายสิทธิให้เป็นอำนาจของ ผอ.ศส. หรือผู้บริหารสูงสุดมอบหมาย

๒.๓ บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งาน โดยคำร้องขอจากผู้บริหารสูงสุดหรือผู้บริหาร หากพบว่ามีการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้

๒.๔ บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งานโดยทันทีโดยผู้ดูแลระบบหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบให้ประสิทธิภาพระบบเครือข่ายด้อยลงหรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้หรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้ ศส. มีสิทธิระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

ส่วนที่ ๙ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยข้อมูลระบบสารสนเทศ

ข้อ ๑ การใช้งานรหัสผ่าน (Password Use) โดยมีแนวทางปฏิบัติ ดังนี้

๑.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน โดยการตั้งรหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร (โดยมีการผสมผสานกันระหว่างตัวอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ต่าง ๆ เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อหรือชื่อสกุลของผู้ใช้ บุคคลที่มีความสัมพันธ์กับตนหรือ คำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์)

๑.๒ ผู้ใช้งานควรทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานทุก ๓ - ๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๑.๓ จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย ไม่ติดรหัสผ่านไว้บริเวณเครื่องคอมพิวเตอร์หรือโต๊ะทำงาน

๑.๔ ต้องเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๑.๕ เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๑.๖ เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้

๑.๗ ไม่กำหนดให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ ได้แก่การบันทึกไว้ในหน้าจอล็อคอิน ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อคอินในภายหลัง จะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง

ข้อ ๒ การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended User Equipment)

ผู้ใช้งานควรมีความตระหนักและเอาใจใส่ว่าอุปกรณ์ขององค์กรในบางช่วงระยะเวลา ที่ไม่มีผู้ดูแล ควรมีการป้องกันที่เหมาะสม (เพื่อป้องกันการสูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต) แนวทางปฏิบัติ

๒.๑ ผู้ใช้งานต้องป้องกันอุปกรณ์คอมพิวเตอร์ที่ตนเองใช้งานเพื่อป้องกันการสูญหาย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

๒.๒ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๒.๓ เพื่อรักษาความปลอดภัยของคอมพิวเตอร์จากการใช้งานที่ไม่ถูกต้อง ผู้ใช้ควรมีการตั้งค่ารหัสผ่านในการเข้าใช้งาน และตั้งค่ารหัสผ่านการล็อคหน้าจอเมื่อไม่มีการใช้งานเกินกว่า ๑๐ นาทีเพื่อป้องกันไม่ให้ผู้อื่นเข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศขององค์กรโดยหลังจากที่มีการล็อคหน้าจอแล้ว ผู้ใช้งานต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบสารสนเทศได้

๒.๔ ควรล็อคอุปกรณ์คอมพิวเตอร์สำคัญเมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราวเพื่อป้องกันการสูญหายหรือถูกขโมย

๒.๕ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) เพื่อควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญ ได้แก่ เอกสาร สื่อบันทึกข้อมูลต่าง ๆ ให้อยู่ในสถานที่ที่ไม่ปลอดภัย หรือสถานที่ที่สามารถเข้าถึงได้ทางกายภาพ ซึ่งอยู่ในบริเวณที่เปิดหรือที่สาธารณะที่ผู้อื่นสามารถเข้าถึงได้ รวมถึงการป้องกันหน้าจอเครื่องคอมพิวเตอร์จากการถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยมีแนวทางปฏิบัติ ดังนี้

๓.๑ มีการป้องกันสินทรัพย์ของหน่วยงาน และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ไม่ปลอดภัย โดยมีการจัดการบริเวณล้อมรอบ การควบคุม การเข้า - ออก การจัดบริเวณการเข้าถึงการส่งผลิตภัณฑ์โดยบุคคลภายนอก การวางอุปกรณ์ และระบบสนับสนุนการทำงาน

๓.๒ มีการกำหนดขอบเขตของการป้องกัน ดังนี้

๓.๒.๑ ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันสินทรัพย์ของหน่วยงาน

๓.๒.๒ ลงชื่อออกจากระบบงานและระบบปฏิบัติการคอมพิวเตอร์ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๓.๒.๓ จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

๓.๒.๔ ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

๓.๒.๕ ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน

๓.๒.๖ ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน

๓.๒.๗ ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

๓.๒.๘ ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร

๓.๒.๙ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๓ ควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของหรือผู้ที่ได้รับมอบหมายเท่านั้น

๓.๔ การลบ หรือเขียนข้อมูลทับบนข้อมูลที่สำคัญ ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุมัติให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เปลี่ยนทดแทน หรือ ทำลาย เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

๓.๕ สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๖ กำหนดมาตรการควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

๓.๖.๑ ให้ทำลายข้อมูลลับหรือข้อมูลสำคัญในสื่อบันทึกข้อมูลประเภทต่าง ๆ ก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว เพื่อป้องกันการเข้าถึงข้อมูลสำคัญที่ยังคงค้างอยู่บนสื่อบันทึกข้อมูลนั้น และให้ปฏิบัติตามแนวทางการทำลายสื่อบันทึกข้อมูล ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive, Thumb Drive, USB Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการ Format ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DoD 5220.22-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลาย CD/DVD

๓.๖.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๓.๗ ผู้ใช้งานควรทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

ข้อ ๔ แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๔.๑ เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๔.๒ ผู้ใช้งานควรทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๔.๓ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกัน โปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๔.๔ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์อื่น ๆ

๔.๕ ก่อนการใช้งานสื่อบันทึกพกพา ควรมีการตรวจสอบ เพื่อป้องกัน และกำจัดโปรแกรมประสงค์ร้าย (Malware)

๔.๖ ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่าย ผู้ใช้งานต้องทำการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

๔.๗ ผู้ใช้งานควรทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Malware) เป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

ข้อ ๕ แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ. คอมพิวเตอร์

๕.๑ ห้ามไม่ให้ผู้ใช้งานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๕.๒ ห้ามไม่ให้ผู้ใช้งานนำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๕.๓ ห้ามไม่ให้ผู้ใช้งานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๕.๔ ห้ามไม่ให้ผู้ใช้งานกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๕.๕ ห้ามไม่ให้ผู้ใช้งานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงหรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

๕.๖ ห้ามไม่ให้ผู้ใช้งานกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวางหรือรบกวนจนไม่สามารถทำงานตามปกติได้

๕.๗ ห้ามไม่ให้ผู้ใช้งานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

๕.๘ ห้ามไม่ให้ผู้ใช้งานกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๕.๙ ห้ามไม่ให้ผู้ใช้งานจำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม พ.ร.บ. คอมพิวเตอร์

๕.๑๐ ห้ามไม่ให้ผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรหรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๕.๑๑ ห้ามไม่ให้ผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๕.๑๒ ห้ามไม่ให้ผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๕.๑๓ ห้ามไม่ให้ผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๕.๑๔ ห้ามไม่ให้ผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

๕.๑๕ ห้ามไม่ให้ผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดทั้งนั้น โดยประการที่น่าจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้ความอับอาย

๕.๑๖ ศส. ต้องมีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน

หมวดที่ ๒ การจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายใน กสอ. ต้องกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล ดังนี้

๑.๑ กำหนด คัดเลือก และจัดลำดับระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้ให้สามารถพร้อมนำ กลับมาใช้งานได้อย่างสมบูรณ์

๑.๒ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ที่ดูแลระบบสารสนเทศ ระบบสำรองข้อมูล และการกู้คืน การจัดทำแผนรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) จากกรณีฉุกเฉินที่ไม่สามารถดำเนินการทางอิเล็กทรอนิกส์ได้

๑.๓ กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ โดยมีหลักเกณฑ์การคัดเลือก

๑.๓.๑ ระบบที่มีผลกับการให้บริการประชาชน ได้แก่ Website, e-Service

๑.๓.๒ ระบบติดต่อสื่อสารของ กสอ. ได้แก่ ระบบจดหมายอิเล็กทรอนิกส์

๑.๓.๓ ระบบที่ใช้ปฏิบัติงานตามภารกิจของ กสอ. ได้แก่ ระบบสารบรรณ ระบบบุคลากร ระบบฐานข้อมูลผู้ประกอบการ

๑.๔ กำหนดความถี่โดยจัดทำแผนในการสำรองข้อมูลของระบบปฏิบัติการและระบบงาน หากระบบงานที่มีการเปลี่ยนแปลงบ่อยจะต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๑.๕ กำหนดขั้นตอนการสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์ที่ใช้ในการสำรองข้อมูล

๑.๖ ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ ไปยังศูนย์คอมพิวเตอร์สำรอง (Dr Site)

๑.๗ ทำการตรวจสอบว่าการสำรองข้อมูลที่เกิดขึ้นนั้น สำเร็จครบถ้วนหรือไม่

๑.๘ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

๑.๙ แนวปฏิบัติสำหรับการสำรองข้อมูล ดังนี้

๑.๙.๑ ผู้ดูแลระบบต้องจัดให้มีการสำรองข้อมูลและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ

๑.๙.๒ การจัดทำบันทึกการสำรองข้อมูล (Operation Logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ดังนี้

- ผู้ปฏิบัติงาน
- เวลาปฏิบัติงาน
- รายละเอียดการปฏิบัติงาน
- ปัญหาที่เกิดขึ้นและการแก้ไข
- สถานะของระบบ
- ผู้ตรวจทานการปฏิบัติงาน

๑.๙.๓ มีการพิมพ์ชื่อบนสื่อ เก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๑.๙.๔ การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่แก้ไขด้วย

๑.๙.๕ ให้ผู้ดูแลระบบมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

๑.๙.๖ ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้อำนวยการกอง/ศูนย์ทราบ

๑.๙.๗ ให้ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

๑.๙.๘ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๑.๑๐ จัดทำแผนรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency plan) เพื่อให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะเวลาที่กำหนด และมีรายละเอียดดังต่อไปนี้

๑.๑๐.๑ กำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๑.๑๐.๒ ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยง กรณีไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้

๑.๑๐.๓ กำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ การไฟฟ้า การประปา โทรศัพท์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ

๑.๑๐.๔ ทำการทบทวนปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๑.๑๐.๕ จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน รวมทั้งเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบ

๑.๑๑ จัดทำแนวการปฏิบัติการจัดทำการป้องกันระบบไฟฟ้าขัดข้อง

๑.๑๑.๑ มีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ

๑.๑๑.๒ มีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์เพื่อให้การดำเนินงานมีความต่อเนื่อง

ส่วนที่ ๒ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑ การตรวจสอบและแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย

๑.๑ ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้งไปยัง ศส. ทันทีที่พบเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของ กสอ. อันได้แก่

๑.๑.๑ มีโปรแกรมไม่ประสงค์ดีเข้ามาในระบบ

๑.๑.๒ มีการบุกรุกเข้ามาในเครือข่าย

๑.๑.๓ มีการใช้งานในลักษณะที่ผิดปกติ

๑.๑.๔ ข้อมูลสำคัญเปลี่ยนแปลงหรือสูญหาย

๑.๑.๕ มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๑.๑.๖ มีการนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์

๑.๑.๗ มีการใช้ระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์

๑.๑.๘ พบจุดอ่อนในระบบงาน ซอฟต์แวร์ หรือฮาร์ดแวร์ที่ใช้งาน

๑.๑.๙ มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้

๑.๑.๑๐ ระบบเทคโนโลยีสารสนเทศชำรุดหรือสูญหาย

๑.๑.๑๑ มีการใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๑.๑.๑๒ บุคคลภายนอกเข้าใช้ระบบงานของ กสอ. โดยไม่ได้รับอนุญาต

๑.๑.๑๓ มีการติดตั้งซอฟต์แวร์เพื่อขโมยข้อมูลหรือเข้าถึงข้อมูลในเครือข่าย

๑.๑.๑๔ มีเหตุการณ์ที่เป็นการละเมิดความมั่นคงปลอดภัยของ กสอ.

๑.๒ ให้ความร่วมมือและอำนวยความสะดวก รวมทั้งปฏิบัติตามคำแนะนำของผู้บริหาร หรือ ศส. ในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น

ข้อ ๒ ความรับผิดชอบของผู้ดูระบบและผู้รับผิดชอบระบบสารสนเทศของ กสอ. เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่ตรวจพบด้วยตนเอง ให้ปฏิบัติตามขั้นตอนดังต่อไป

๒.๑ ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด (สูง กลาง หรือต่ำ)

๒.๒ แจ้ง ผู้อำนวยการกลุ่ม เพื่อรายงานผู้บังคับบัญชาตามลำดับชั้นให้ได้รับทราบตามระดับของผลกระทบ

๒.๓ วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็น กรณีการบุกรุก การโจมตีระบบ หรือระบบได้รับความเสียหาย ประสานงานขอความช่วยเหลือจากผู้รู้ ได้แก่ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (Thai CERT)

๒.๔ กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัยและจำกัดการเข้าถึงหลักฐานนั้น

๒.๕ จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลางขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ

ข้อ ๓ ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัติ ดังนี้

๓.๑ ให้แจ้งรายงานตามสายการบังคับบัญชาให้หน่วยงานที่เกี่ยวข้องทราบ

๓.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๓.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันไม่ให้เหตุการณ์เกิดซ้ำอีก

ข้อ ๔ ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้หน่วยงานเจ้าของระบบสารสนเทศดำเนินการดังนี้

๔.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่าง ๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบเสียหายอย่างใดหรือไม่

๔.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันที อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ ๕ ความรับผิดชอบผู้ใช้งานต่อประกาศฉบับนี้ มีดังนี้

๕.๑ ปฏิบัติตามประกาศนี้อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของ ตนเอง

๕.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของ กสอ.

๕.๓ ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ของ กสอ.

๕.๔ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยัง ศส. โดยเร็วที่สุด

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อำจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) มีวิธีการปฏิบัติ ดังนี้

๑.๑.๑ มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านระบบสารสนเทศ

๑.๑.๒ มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการด้านความมั่นคงปลอดภัย

๑.๑.๓ มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

๑.๑.๔ มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) อย่างน้อย ๑ ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ มีวิธีการปฏิบัติ ดังนี้

๑.๒.๑ กำหนดให้มีคณะทำงานตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ซึ่งประกอบด้วยหน่วยตรวจสอบภายในของหน่วยงาน (internal auditor) ผู้แทนจากกอง/ศูนย์ต่าง ๆ ใน กสอ. และ/หรือ ผู้ที่ได้รับมอบหมายจากคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร กสอ. เป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศ และให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อย ๑ ครั้งต่อปี

๑.๒.๒ มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

๑.๒.๓ มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว

๑.๒.๔ มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

๑.๒.๕ มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

๑.๒.๖ มีการทำลาย หรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

๑.๒.๗ มีวิธีการแบบปลอดภัยสำหรับการเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจสอบ

๑.๒.๘ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ

๑.๒.๙ มีการกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแล หรือรับผิดชอบ)

ข้อ ๒ มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อยดังนี้

๒.๑ แนวทางในการตรวจสอบและประเมินความเสี่ยง

๒.๑.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๒.๑.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายการพร้อมข้อเสนอแนะให้ผู้บริหารพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

๒.๒ มาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๒.๒.๑ ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๒.๒.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งดำเนินการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๒.๒.๓ มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๒.๔ มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อคแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ

๒.๒.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ต้องแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓ รายการที่สอบทาน

๒.๓.๑ การป้องกันการบุกรุกระบบ

๒.๓.๒ การสำรองข้อมูล

๒.๓.๓ การควบคุมการเข้าห้องควบคุมระบบเครือข่าย

๒.๓.๔ การซ้อมรับสถานการณ์ฉุกเฉิน

๒.๓.๕ สอบทานการเข้าถึงระบบสารสนเทศ

๒.๓.๖ สอบทานการกำหนดการใช้งานตามภารกิจ

๒.๔ การกำกับดูแลการปฏิบัติตามด้านเทคนิค

๒.๔.๑ ผู้บริหารต้องกำกับดูแลเพื่อให้มั่นใจว่าเจ้าหน้าที่ทราบถึงความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและได้มีการปฏิบัติในทางที่เหมาะสม

๒.๔.๒ สอบทานและตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศเพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่

๒.๔.๓ ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านปลอดภัย

๒.๔.๔ เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ระบบงานและเอกสารที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้อง จากการลักลอบใช้งานหรือใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูลซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของ กสอ.

แนวปฏิบัติ

ข้อ ๑ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ระบบเครือข่ายคอมพิวเตอร์หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒ ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ต้องมีลักษณะ ดังนี้

๒.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า – ออก ของบุคคลเป็นจำนวนมาก

๒.๓ ต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๒.๔ ต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

๒.๕ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด

๒.๖ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบ ตามความเหมาะสมจากผู้ที่ไม่ได้รับอนุญาต

ข้อ ๓ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ ต้องจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้น

๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔ การควบคุมการเข้าออก อาคารสถานที่

๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๔.๒ การเข้าถึงอาคารของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรประชาชน ใบอนุญาตขับขี่ หรือบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๔.๓ ต้องมีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔.๔ ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๔.๕ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๔.๖ ต้องจัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๔.๗ ต้องจัดให้มีเจ้าหน้าที่ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๔.๘ ต้องมีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๔.๙ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๐ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๔.๑๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๔.๑๒ มีการพิสูจน์ตัวตน โดยใช้บัตรรูด รหัสผ่าน หรือนิ้วมือ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๔.๑๓ ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

ข้อ ๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังต่อไปนี้

๕.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS)

๕.๑.๒ ระบบปรับอากาศ และควบคุมความชื้น

๕.๒ ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๖.๒ ต้องมีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๖.๓ ต้องเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๖.๔ ต้องทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๖.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๖.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่กุญแจให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๖.๗ ใช้งานสายไฟเบอร์ออฟติก (Fiber Optic) แทนสายสัญญาณสื่อสารแบบเดิม (Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๖.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณจากผู้ไม่ประสงค์ดี

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๗.๑ กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๗.๖ กำหนดการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างที่ให้บริการจากภายนอก (ทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๘.๑ ขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๘.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๘.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๘.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน ทั้งอุบัติเหตุระหว่างการขนส่ง หรือการเกิดอุบัติเหตุกับอุปกรณ์

๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๙.๓ เจ้าหน้าที่ที่รับผิดชอบจะต้องดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

๑๐.๑ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ข้อ ๑๑ การป้องกันภัยในห้องแม่ข่าย

๑๑.๑ กำหนดให้มีเจ้าหน้าที่ดูแลระบบดับเพลิง (Fire Suppression System) เมื่อมีสัญญานแจ้งเตือนต้องตรวจสอบทันที

๑๑.๒ กำหนดให้มีเจ้าหน้าที่ดูแลระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detector System) เมื่อมีสัญญานแจ้งเตือนต้องตรวจสอบทันที

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑ ระบบป้องกันผู้บุกรุก ให้ปฏิบัติ ดังนี้

ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก ดังนี้

(๑) มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด

(๒) ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่

(๓) ระดับความรุนแรงมากน้อยเพียงใด

(๔) หมายเลขไอพี (IP Address)ของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒ ระบบไฟร์วอลล์ ให้ปฏิบัติ ดังนี้

๒.๑ ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒.๒ ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของ Firewall ดังนี้

๒.๒.๑ Packet ที่ Firewall ได้ทำการ Block

๒.๒.๒ ลักษณะของ Packet ที่ถูก Block

๒.๒.๓ Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๒.๓ กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงานหรือผู้รับผิดชอบซึ่งได้รับมอบหมาย เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓ ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต (ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ประกอบด้วย ไวรัสคอมพิวเตอร์ หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์)

๓.๑ ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ดังนี้

๓.๑.๑ มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก

๓.๑.๒ มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด

๓.๑.๓ มีการส่งมัลแวร์จากเครือข่ายภายในหน่วยงานไปยังภายนอกหรือไม่

๓.๒ ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

๓.๓ หากตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่ายทันที แล้วทำการแก้ไขเครื่องนั้นให้สามารถใช้งานได้ตามปกติ ต่อไป

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของ กสอ.

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑ ต้องมีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๓ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร ซึ่งการจัดสัมมนาต้องมีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๔ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖ สร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดีเพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการกอง/ศูนย์ ผู้อำนวยการกลุ่มงาน เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ ระดับนโยบาย ผู้รับผิดชอบ ได้แก่ ผู้บริหารสูงสุด ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) โดยมีหน้าที่ความรับผิดชอบ ดังนี้

- รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ
- รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูล สารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ

ข้อ ๒ ระดับบริหาร ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการกอง/ศูนย์ หรือเทียบเท่า ผู้อำนวยการกลุ่ม หรือเทียบเท่า โดยมีหน้าที่ความรับผิดชอบ ดังนี้

- รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ
- รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล
- รับผิดชอบวางแผน จัดทำ ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๓ ระดับปฏิบัติ ผู้รับผิดชอบ คือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าหน่วนงานให้เป็นผู้ดูแลระบบ หรือ ผู้รับผิดชอบระบบสารสนเทศ ได้แก่ นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์ และนักวิชาการอุตสาหกรรม โดยมีหน้าที่ความรับผิดชอบ ดังนี้

- ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
- รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
- ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด
- ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต
- รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต และระบบจดหมาย อิเล็กทรอนิกส์
- ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กสอ.

ภาคผนวก

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอกนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖