



แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานกิจการยุติธรรม
พ.ศ. ๒๕๖๐



ประกาศ สำนักงานกิจการยุติธรรม

เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานกิจการยุติธรรม เห็นสมควรให้มีการกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ดังนี้

คำนิยาม

๑. “องค์กร” (Organization) หมายความว่า สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม
๒. “ผู้บังคับบัญชา” (Commander) หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานกิจการยุติธรรม
๓. “ผู้บริหารระดับสูงสุด” (Chief Executive Officer: CEO) หมายความว่า ผู้มีอำนาจสูงสุดของสำนักงานกิจการยุติธรรม ได้แก่ ผู้อำนวยการสำนักงานกิจการยุติธรรม ซึ่งมีหน้าที่รับผิดชอบในส่วนของการกำหนดนโยบาย ให้คำปรึกษา แนะนำแนวทาง ตลอดจนติดตามกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม
๔. “ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” (Chief Information Office: CIO) หมายความว่า มีอำนาจตัดสินใจในด้านเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม ได้แก่ รองผู้อำนวยการสำนักงานกิจการยุติธรรมที่ได้รับมอบหมาย ซึ่งมีหน้าที่รับผิดชอบการกำหนดนโยบายและมาตรฐานการควบคุมดูแลการใช้งานและพัฒนาระบบเทคโนโลยีสารสนเทศ
๕. “สำนักเทคโนโลยีสารสนเทศ” (Office of Information Technology) หมายความว่า สำนักเทคโนโลยีสารสนเทศและการสื่อสารกระบวนการยุติธรรม ซึ่งเป็นหน่วยงานให้บริการเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง และบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในสำนักงานกิจการยุติธรรม
๖. “ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ” (Director of Technology Bureau) หมายความว่า ผู้บังคับบัญชาสูงสุดของสำนักเทคโนโลยีสารสนเทศ รับผิดชอบกำกับดูแลการปฏิบัติงานของบุคลากร ตลอดจนทบทวน วางแผนบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ
๗. “การรักษาความมั่นคงปลอดภัย” (Security) หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม
๘. “มาตรฐาน” (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๙. “ขั้นตอนการปฏิบัติ” (Procedure) หมายความว่า รายละเอียดขั้นตอนที่ต้องปฏิบัติเป็นข้อๆ
๑๐. “แนวทางปฏิบัติ” (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
๑๑. “ผู้ใช้งาน” (User) หมายความว่า บุคลากรของสำนักงานกิจการยุติธรรม ที่ได้รับอนุญาต (Authorized user) ให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาทความรับผิดชอบ (Role) ซึ่งกำหนดไว้ดังนี้
- (๑) “ผู้บริหาร” (Administrator) หมายความว่า ผู้มีอำนาจบริหารในระดับสูงของสำนักงานกิจการยุติธรรม ได้แก่ ผู้อำนวยการสำนักงานกิจการยุติธรรม/รองผู้อำนวยการ/ผู้อำนวยการสำนัก/ผู้อำนวยการกอง และหัวหน้ากลุ่ม
 - (๒) “ผู้ดูแลระบบ” (System Administrator) หมายความว่า เจ้าหน้าที่ของสำนักงานกิจการยุติธรรมที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้รับผิดชอบในการกำกับการดูแลระบบคอมพิวเตอร์ระบบเครือข่าย
 - (๓) “เจ้าหน้าที่” (Staff) หมายความว่า ข้าราชการ พนักงานราชการ พนักงานจ้าง ลูกจ้างชั่วคราว เจ้าหน้าที่ประจำโครงการต่างๆ ของสำนักงานกิจการยุติธรรม รวมถึงบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานกิจการยุติธรรม
 - (๔) “ผู้แทนหน่วยงานในกระบวนการยุติธรรมที่ได้รับมอบหมาย ซึ่งมีสิทธิในการใช้งานฐานข้อมูลร่วมกัน” หมายความว่า ข้าราชการ พนักงานราชการ พนักงานจ้าง ลูกจ้างของหน่วยงานภาครัฐในกระบวนการยุติธรรม ซึ่งมีหน้าที่รับผิดชอบในการค้นหาข้อมูล วิเคราะห์ จัดการข้อมูลเกี่ยวกับการปฏิบัติงานในกระบวนการยุติธรรม ได้แก่ ข้อมูลประวัติอาชญากรรม ข้อมูลการกระทำผิด ข้อมูลการคุมประพฤติ เป็นต้น
๑๒. “หน่วยงานในกระบวนการยุติธรรม” หมายความว่า หน่วยงานที่ลงนามใช้ฐานข้อมูลด้านกระบวนการยุติธรรมร่วมกัน โดยมีสำนักงานกิจการยุติธรรมเป็นผู้ให้บริการฐานข้อมูล ได้แก่ สำนักงานอัยการสูงสุด สำนักงานตำรวจแห่งชาติ สำนักงานปลัดกระทรวงยุติธรรม สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ กรมคุมประพฤติ สอ.บต. สถาบันนิติวิทยาศาสตร์ กรมคุ้มครองสิทธิและเสรีภาพ กรมบังคับคดี สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานประกันสังคม กรมสอบสวนคดีพิเศษ กอ.รมน. ภาค ๔ ส่วนหน้า กรมพินิจและคุ้มครองเด็กและเยาวชน กรมการขนส่งทางบก กรมการปกครอง และกรมราชทัณฑ์
๑๓. “หน่วยงานภายนอก” (External Organization) หรือบุคคลภายนอก หมายความว่า องค์กร หรือหน่วยงาน หรือผู้มาติดต่อจากภายนอกที่สำนักงานกิจการยุติธรรมอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานระบบหรือทรัพย์สินต่างๆ ของสำนักงานกิจการยุติธรรม โดยจะได้รับสิทธิในการใช้เข้าถึงและใช้งานสารสนเทศตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ และความลับของข้อมูล

๑๔. “ข้อมูลคอมพิวเตอร์” (Data) หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือบรรดาสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สามารถประมวลผลได้ และให้รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
๑๕. “สารสนเทศ” (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการประมวลผลข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ ภาพกราฟิก เสียง ให้เป็นสิ่งที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน และการตัดสินใจ
๑๖. “ระบบคอมพิวเตอร์” (Computer System) หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง ให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
๑๗. “ระบบเครือข่าย” (Network System) หมายความว่า กลุ่มของคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่ถูกเชื่อมต่อเข้าด้วยกันเพื่อให้ผู้ใช้งานใช้ติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้ข้อมูลบนระบบเครือข่ายร่วมกันได้
๑๘. “ระบบแลน” (LAN) และระบบอินทราเน็ต (Intranet) หมายความว่า ระบบเครือข่ายที่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ เข้าด้วยกัน เพื่อใช้ติดต่อสื่อสารและแลกเปลี่ยนข้อมูล ภายในองค์กรเท่านั้น
๑๙. “ระบบอินเทอร์เน็ต” (Internet) หมายความว่า ระบบเครือข่ายที่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ ขององค์กร กับเครือข่ายอินเทอร์เน็ตทั่วโลก เพื่อใช้ติดต่อสื่อสารและแลกเปลี่ยนข้อมูลได้ทั่วโลก
๒๐. “ระบบเทคโนโลยีสารสนเทศ” (Information Technology System) หมายความว่า ระบบงานขององค์กรที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสนับสนุนการบริหาร และควบคุมการติดต่อสื่อสาร
๒๑. “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” (Information System Workspace) หมายความว่า พื้นที่ที่อนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็นพื้นที่ทำงานทั่วไป (General Working Area) คือ พื้นที่โต๊ะทำงานที่ติดตั้งเครื่องคอมพิวเตอร์เพื่อทำงาน พื้นที่สำหรับทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบ (IT Equipment or Network Area) พื้นที่สำหรับจัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่สำหรับใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)
๒๒. “สิทธิของผู้ใช้งาน” (User Permissions) หมายความว่า สิทธิทั่วไป สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม
๒๓. “สินทรัพย์” (Asset) หมายความว่า ทรัพย์สินหรือสิ่งอื่นใดก็ตามของสำนักงานกิจการยุติธรรม ทั้งที่สามารถจับต้องได้และจับต้องไม่ได้ อันมีมูลค่าหรือคุณค่าสำหรับสำนักงานกิจการยุติธรรม

๒๔. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” (Information Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบสารสนเทศหรือระบบเครือข่ายขององค์กร ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอกหรือหน่วยงานภายนอก
๒๕. “ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งานของระบบสารสนเทศ (Availability) ทั้งนี้ รวมถึงคุณสมบัติด้านความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
๒๖. “เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Incident) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๒๗. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Unexpected Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบสารสนเทศขององค์กรถูกบุกรุกโจมตี หรือความมั่นคงปลอดภัยถูกคุกคาม
๒๘. “จดหมายอิเล็กทรอนิกส์” (e-Mail) หมายความว่า ระบบที่ใช้รับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวเลข ตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข้อมูลเหล่านี้ไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งจดหมายอิเล็กทรอนิกส์ ได้แก่ SMTP, POP3 และ IMAP
๒๙. “รหัสผ่าน” (Password) หมายความว่า ตัวอักษร อักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูล
๓๐. “ชุดคำสั่งไม่พึงประสงค์” (Unwanted Software) หมายความว่า ชุดคำสั่งคอมพิวเตอร์ที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นในระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงจนขัดข้อง ประมวลผลไม่เป็นไปตามปกติที่กำหนดไว้
๓๑. “SSD” (Service Set Identifier) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยข้อมูลในเครือข่ายไร้สาย โดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าของชุดตัวเลขนี้
๓๒. “WPA” (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Equivalent Privacy)

๓๓. “MAC Address” (Media Access Control Access) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างอิงอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย หมายเลขนี้จะมากับ Ethernet Card โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ประโยชน์มีไว้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง แม่นยำ

๓๔. “แผนผังระบบเครือข่าย” (Network Diagram) หมายความว่า แผนผังแสดงถึงการเชื่อมต่อระบบเครือข่ายขององค์กร

๓๕. “SSL VPN” (Secure Sockets Layer Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนสร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำการโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นจนถึงปลายทาง

๓๖. “Intrusion Detection System (IDS)” หมายความว่า ระบบที่คอยตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี รวมไปถึงข้อมูลจำพวกไวรัสด้วย โดยสามารถทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้าออกภายในเครือข่ายว่ามีลักษณะการทำงานที่เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่ายหรือไม่ โดยระบบ IDS นี้ จะทำการแจ้งเตือนให้ผู้ดูแลระบบทราบ

๓๗. “Intrusion Prevention System (IPS)” หมายความว่า ระบบที่มีลักษณะเช่นเดียวกับระบบ IDS แต่มีความสามารถพิเศษมากกว่าระบบ IDS กล่าวคือ เมื่อตรวจพบข้อมูลที่มีลักษณะการทำงานที่เป็นความเสี่ยงต่อระบบเครือข่ายก็จะทำการป้องกันข้อมูลดังกล่าวไว้ไม่ให้เข้ามาภายในเครือข่ายได้

หมวดที่ ๑

การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อเป็นมาตรการควบคุมและป้องกันรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงระบบสารสนเทศ และการเข้าถึงพื้นที่ใช้ควบคุมระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน หน่วยงานภายนอกหรือบุคคลภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบสารสนเทศของสำนักงานกิจการยุติธรรม

ผู้รับผิดชอบ

๑. สำนักเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบ
๓. เจ้าหน้าที่สารสนเทศ
๔. ผู้ใช้งาน

ส่วนที่ ๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพ

การควบคุมทรัพย์สินสารสนเทศและการใช้งานคอมพิวเตอร์ เพื่อควบคุมและป้องกันไม่ให้สินทรัพย์สารสนเทศหรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ มีดังนี้

ข้อ ๑ การจัดการสภาพแวดล้อมทางกายภาพ

- (๑) จำแนกพื้นที่การใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้แก่
 - (๑.๑) พื้นที่ทั่วไป เป็นพื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์เพื่อทำงาน
 - (๑.๒) พื้นที่ทำงานของผู้ดูแลระบบ ซึ่งอยู่ติดกับบริเวณพื้นที่ตามข้อ ๑ (๑.๓)
 - (๑.๓) พื้นที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบ ได้แก่ Data Centre
 - (๑.๔) พื้นที่จัดเก็บข้อมูล ได้แก่ ห้องจัดเก็บอุปกรณ์บันทึกข้อมูล
 - (๑.๕) พื้นที่ใช้งานเครือข่ายไร้สาย ได้แก่ บริเวณภายในสำนักงานกิจการยุติธรรม
- (๒) พื้นที่ระบบสารสนเทศตามข้อ ๑ (๑.๓) ให้ติดตั้งสัญญาณแจ้งเตือนเมื่อมีการบุกรุกทางกายภาพ และเมื่อเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
- (๓) มีการติดตั้งกล้องวงจรปิดในบริเวณพื้นที่ใช้งาน เพื่อบันทึกเหตุการณ์ไว้ตรวจสอบภายหลัง
- (๔) ผู้ดูแลระบบต้องตรวจสอบการปิดล็อกประตูทุกครั้งก่อนเลิกงาน
- (๕) ผู้ดูแลระบบต้องทดสอบประสิทธิภาพระบบแจ้งเตือน และระบบป้องกันการบุกรุกทางกายภาพให้มั่นใจได้ว่าใช้งานได้ตามปกติ

ข้อ ๒ การควบคุมการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- (๑) ห้ามบุคคลภายนอกและผู้ใช้งานเข้าถึงพื้นที่ปฏิบัติการระบบสารสนเทศ เว้นแต่เป็นผู้เกี่ยวข้องที่ได้รับอนุญาตจากผู้ดูแลระบบและต้องติดบัตรอนุญาตให้เห็นเด่นชัด
- (๒) ให้สแกนลายนิ้วมือบันทึกเวลาการผ่านเข้า-ออกพื้นที่ใช้งานทุกครั้ง
- (๓) มีกล้องวงจรปิดติดตั้งไว้โดยรอบพื้นที่ใช้งาน เพื่อบันทึกเหตุการณ์การเข้า-ออกตลอดเวลา
- (๔) หากผู้ใช้งานนำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์ต่อพ่วงส่วนตัวเข้ามาในพื้นที่ใช้งาน ต้องบันทึกรายละเอียดของอุปกรณ์ที่นำมาในแบบฟอร์มบันทึกการเข้า-ออกให้ครบถ้วน ประกอบด้วย ชื่ออุปกรณ์ ยี่ห้อ รุ่น สี จำนวนชิ้นที่นำมา
- (๕) หากผู้ใช้งานมีความจำเป็นต้องยืมคอมพิวเตอร์พกพาและอุปกรณ์ต่างๆ ให้บันทึกแบบฟอร์มขอยืมทรัพย์สินจากสำนักเทคโนโลยีสารสนเทศ พร้อมระบุรายละเอียดของอุปกรณ์ที่ยืมให้ครบถ้วน อันได้แก่ ชื่ออุปกรณ์ ยี่ห้อ รุ่น สี จำนวนชิ้น ระยะเวลาที่ขอยืม-คืน เลขที่ครุภัณฑ์ เป็นต้น ทั้งนี้ ผู้ใช้งานต้องปฏิบัติตามข้อ ๗ อย่างเคร่งครัด และต้องคืนสินทรัพย์ตามรายการที่ยืมให้ครบถ้วน สภาพเดิม และภายในกำหนดเวลาด้วย
- (๖) ตามข้อ ๒ (๔) (๕) ให้ผู้ดูแลระบบตรวจสอบรายละเอียดให้ถูกต้อง ครบถ้วน
- (๗) ผู้ดูแลระบบต้องยกเลิกข้อมูลสิทธิการเข้า-ออกทันที เมื่อผู้มีสิทธิใช้งานลาออกหรือทบทวนสิทธิ ทันทีเมื่อมีการปรับเปลี่ยน/โยกย้ายตำแหน่ง

ข้อ ๓ การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

- (๑) จัดพื้นที่ส่งมอบพัสดุหรือขนถ่ายผลิตภัณฑ์แยกจากพื้นที่ใช้งาน เพื่อป้องกันการเข้าถึงพื้นที่ใช้งานโดยไม่ได้รับอนุญาต
- (๒) จำกัดจำนวนบุคคลที่สามารถเข้าถึงพื้นที่ส่งมอบหรือบริเวณส่งมอบตามข้อ ๓ (๑)
- (๓) ผู้ดูแลระบบต้องตรวจนับ และตรวจสอบพัสดุหรือผลิตภัณฑ์ให้ถูกต้องครบถ้วน
- (๔) ต้องลงทะเบียนพัสดุหรือผลิตภัณฑ์ที่ส่งมอบตามระเบียบพัสดุก่อนเคลื่อนย้ายไปติดตั้งในพื้นที่ใช้งาน

ข้อ ๔ การจัดวางหรือการป้องกันอุปกรณ์และระบบสนับสนุนการทำงาน

- (๑) จัดวางอุปกรณ์ในพื้นที่หรือในบริเวณที่เหมาะสมเพื่อให้เกิดความเรียบร้อย
- (๒) ต้องแยกอุปกรณ์สำคัญเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัยสูง
- (๓) ไม่นำอาหารและเครื่องดื่มเข้ามารับประทานในพื้นที่ของระบบสารสนเทศ
- (๔) ถอดรองเท้าก่อนเข้าห้อง DataCentre เพื่อไม่ให้ฝุ่นที่ติดอยู่กับรองเท้าเข้าสู่เครื่องคอมพิวเตอร์ และเครื่องทำความเย็น
- (๖) ดำเนินการตรวจสอบ ดูแลสภาพแวดล้อม อุณหภูมิ ความชื้น ภายในพื้นที่ของระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายต่ออุปกรณ์ภายในพื้นที่ดังกล่าว
- (๕) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรอย่างเพียงพอ ได้แก่ ระบบสำรองกระแสไฟฟ้า (UPS) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย

ระบบปรับอากาศ ระบบระบายอากาศ ระบบควบคุมความชื้น ฉนวนกันความร้อน ระบบก๊าซไฟโลเจน (Pylogen) และระบบสัญญาณแจ้งเตือนอัคคีภัยและไฟฟ้าดับ

(๖) ทดสอบการทำงานของระบบสนับสนุนตามข้อ ๔ (๕) อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถทำงานได้ตามปกติ

ข้อ ๕ การเดินสายไฟ สายสัญญาณสื่อสารต่างๆ

- (๑) สายไฟฟ้า สายเคเบิล และสายสัญญาณอื่นๆ ต้องมีการร้อยท่อสายสัญญาณ เพื่อป้องกันการดักจับข้อมูล การตัดสาย รวมถึงป้องกันสัตว์กัดแทะ
- (๒) สายไฟฟ้า สายเคเบิล และสายสัญญาณอื่นๆ ต้องติดป้ายชื่อกำกับเพื่อป้องกันการตัดสายผิดเส้น
- (๓) แยกการเดินสายไฟออกจากสายสัญญาณสื่อสาร เพื่อป้องกันสัญญาณถูกรบกวน
- (๔) จัดทำแผนผังระบบเครือข่ายแสดงการเชื่อมสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วน
- (๕) จุดเชื่อมต่อสายสัญญาณ (ตู้ Rack) ต้องปิดให้สนิทป้องกันการเข้าถึงจากผู้ที่ไม่เกี่ยวข้อง

ข้อ ๖ การบำรุงรักษาอุปกรณ์

- (๑) ดำเนินการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ตามรอบระยะเวลาที่กำหนดในคู่มือผลิตภัณฑ์
- (๒) จัดเก็บข้อมูลการให้บริการบำรุงรักษาไว้ทุกครั้ง เพื่อใช้ในการตรวจประเมินภายหลัง
- (๓) จัดเก็บข้อมูลปัญหาและข้อบกพร่องที่พบ เพื่อประเมินและแก้ไขข้อบกพร่องของอุปกรณ์ดังกล่าว
- (๔) กรณีจ้างผู้รับเหมาบำรุงรักษาระบบคอมพิวเตอร์ ผู้ดูแลระบบต้องควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้รับเหมาที่มาทำการบำรุงรักษาอุปกรณ์อย่างใกล้ชิด ตลอดจนเสร็จสิ้นการบำรุงรักษา
- (๕) ผู้ดูแลระบบต้องควบคุมการส่งอุปกรณ์ไปซ่อมแซมนอกสถานที่ เพื่อป้องกันการสูญหาย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และป้องกันการสับเปลี่ยนอุปกรณ์
- (๖) ผู้รับเหมาบำรุงรักษาระบบต้องกรอกแบบฟอร์มขออนุญาตเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยให้ผู้ดูแลระบบเป็นผู้ควบคุม เพื่อป้องกันการลักลอบเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๗ การป้องกันอุปกรณ์ที่ใช้งานอยู่ภายนอกองค์กร

มาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินขององค์กรไปใช้ภายนอกบริเวณ ให้เป็นไปตามแนวปฏิบัติ ข้อ ๒ (๕) ข้อ ๙ และ

- (๑) ผู้ใช้งานต้องไม่ทิ้งอุปกรณ์หรือทรัพย์สินขององค์กรไว้ในที่สาธารณะ
- (๒) ผู้ใช้งานต้องรับผิดชอบดูแลทรัพย์สินขององค์กรประดุจเป็นทรัพย์สินของตนเอง และหากเกิดความเสียหายจากการใช้งาน พฤติกรรมการทิ้งตามข้อ ๗ (๑) จะต้องรับผิดชอบค่าใช้จ่ายเช่นเดิม

ข้อ ๘ การจำกัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่อีกครั้ง

- (๑) ให้ทำลายข้อมูลในอุปกรณ์ ได้แก่ Harddisk drive CD/DVD Blu-ray Disc Thumb drive Flash drive Memory drive เทปบันทึกข้อมูล เป็นต้น ก่อนที่จะจำหน่ายหรือทำลายอุปกรณ์
- (๒) การทำลายข้อมูลในอุปกรณ์ตามข้อ ๘ (๑) ให้ผู้ดูแลระบบดำเนินการตามมาตรฐานกระทรวงกลาโหม สหรัฐอเมริกา ว่าด้วยการลบแบบดิจิทัล DoD 5220.22-M (การ Format และเขียนทับข้อมูลเดิมหลายๆ รอบก่อนนำไปทำลายอีกครั้ง) และให้สอดคล้องกับส่วนที่ ๗ การทำลาย ในระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ ด้วย

ข้อ ๙ การนำสินทรัพย์ออกนอกองค์กร

- (๑) ไม่อนุญาตให้ผู้ใช้งานนำอุปกรณ์หรือสินทรัพย์ออกนอกบริเวณองค์กร เว้นแต่ได้รับอนุญาตตามความข้อ ๒ (๕) (๖) และต้องนำมาส่งคืนในสภาพเดิมและเก็บเข้าที่ให้เรียบร้อย
- (๒) ไม่อนุญาตให้ผู้ใช้งานที่เป็นบุคคลภายนอก ยืม หรือนำสินทรัพย์ขององค์กรไปใช้ภายนอก และใช้เพื่อการส่วนตัวโดยเด็ดขาด

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

ข้อ ๑๐ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้ตระหนักถึงภัยและผลกระทบที่เกิดจากการเข้าถึง และใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ โดยกำหนดมาตรการเชิงป้องกันไว้ ดังนี้

- (๑) จัดทำ Infographic การใช้งานระบบสารสนเทศ และโทษของการใช้งานเทคโนโลยีสารสนเทศในทางที่ผิด ให้ผู้ใช้งานได้รับทราบ
- (๒) จัดการฝึกอบรมหลักสูตรเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ รวมถึงภัยและผลกระทบจากการใช้งานเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์
- (๓) จัดทำคู่มือผู้ใช้งานระบบสารสนเทศแจกให้ผู้ใช้งานเมื่อมีการลงทะเบียน
- (๔) ให้ดำเนินการตามความหมวดที่ ๔ ส่วนที่ ๒ การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้ใช้งาน

ข้อ ๑๑ การลงทะเบียนผู้ใช้งาน

- (๑) กรอกข้อมูลตามแบบฟอร์มการขอใช้ระบบเทคโนโลยีสารสนเทศที่กำหนดและยื่นต่อผู้ดูแลระบบ หรือเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ
- (๒) ผู้ดูแลระบบตรวจสอบขอบเขตการอนุญาตสิทธิการใช้งาน โดยพิจารณาจากประเภทบุคลากร หน้าที่ความรับผิดชอบงานขององค์กร ตามหลักเกณฑ์การอนุญาตข้อ ๒๐ และเสนอขออนุญาตต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ
- (๓) ผู้ดูแลระบบตรวจสอบและดำเนินการตามขั้นตอนข้อ ๑๒

ข้อ ๑๒ การบริหารจัดการสิทธิของผู้ใช้งาน

- (๑) ผู้ดูแลระบบกำหนดชื่อผู้ใช้งาน รหัสผ่าน ตามข้อมูลที่ได้รับอนุญาตตามข้อ ๑๑ (๑) (๒) และกำหนดสิทธิในการเข้าถึงและใช้งานระบบสารสนเทศตามหลักเกณฑ์ในข้อ ๒๐ (๒) (๓) (๔) (๕) (๖) (๗)
- (๒) หากจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องควบคุมการใช้งานผู้ใช้งานนั้นอย่างรัดกุมเพียงพอ ได้แก่
 - (๒.๑) ต้องได้รับการอนุญาตจากผู้บริหารระดับสูง หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง แล้วแต่กรณีเท่านั้น และ
 - (๒.๒) ควบคุมการใช้งานอย่างเข้มงวด กำหนดให้ใช้งานได้เฉพาะกรณีจำเป็นเท่านั้น และกำหนดระยะเวลาในการอนุญาตสิทธิพิเศษไว้ด้วย
 - (๒.๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานสิทธิของผู้ใช้งานนั้นทันทีเมื่อพ้นระยะเวลาที่กำหนดไว้ตามความข้อ ๑๒ (๒.๒)
 - (๒.๔) กำหนดให้เปลี่ยนรหัสผ่านทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือหากมีความจำเป็นต้องใช้งานเป็นระยะเวลานานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

ข้อ ๑๓ กำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายภายใน (LAN) ระบบเครือข่ายไร้สาย (Wi-Fi) ระบบเครือข่ายอินเทอร์เน็ต (Internet) โดยใช้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และได้รับอนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร โดยให้ผู้ดูแลระบบทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๑๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

- (๑) เปลี่ยนรหัสผ่านทันทีเมื่อได้รับรหัสผ่านชั่วคราวจากการลงทะเบียนผู้ใช้งานและภายหลังการติดตั้งซอฟต์แวร์
- (๒) ไม่กำหนดรหัสผ่านจากชื่อ สกุลของตน ชื่อ สกุลของบุคคลรู้จัก ข้อมูลวันเดือนปีเกิดและคำศัพท์จากพจนานุกรม
- (๓) กำหนดรหัสผ่านอย่างน้อยที่สุด ๘ ตัวอักษร โดยต้องให้มีการผสมระหว่างตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข สัญลักษณ์ และอักขระพิเศษ
- (๔) กำหนดเวลาให้ต้องเปลี่ยนรหัสผ่านอัตโนมัติทุก ๖ เดือน โดยต้องไม่ใช่รหัสผ่านเดิมที่เคยกำหนดใช้งาน
- (๕) การส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานโดยวิธีปลอดภัย ไม่ส่งผ่านบุคคลที่สาม หรือส่งเป็นจดหมายอิเล็กทรอนิกส์ (e-Mail)

ข้อ ๑๕ การทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งาน

- (๑) ผู้ดูแลระบบต้องทบทวนความเหมาะสมของสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อย ทุกๆ ๖ เดือน หรือทันทีหากมีการปรับเปลี่ยน โยกย้ายตำแหน่ง
- (๒) ระงับสิทธิการใช้งานทันทีเมื่อผู้ใช้งานสิ้นสุดหน้าที่ความรับผิดชอบงานขององค์กร และให้คืนทรัพย์สินที่เกี่ยวข้องกับการปฏิบัติงานของตนทั้งหมดด้วย

- (๓) ส่งสรุปรายงานสิทธิการใช้งานให้ผู้บังคับบัญชาของแต่ละสำนัก/กอง/กลุ่ม ทราบ
ทุกครั้งที่มีการทบทวนสิทธิ อันได้แก่ รายละเอียดชื่อผู้ใช้งาน สิทธิที่ได้รับว่ามี
ความถูกต้องหรือไม่ พร้อมทั้งแบบตอบรับยืนยันความถูกต้อง หรือแก้ไขสิทธิ
(๔) หากมีการแก้ไขสิทธิตามข้อ ๑๕ (๓) ให้ผู้ดูแลระบบปรับดำเนินการแก้ไข

ข้อ ๑๖ กำหนดขอบเขต หน้าที่ ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ การลักลอบทำสำเนาหรือล่วงข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ดังนี้

- (๑) การใช้งานรหัสผ่าน ผู้ใช้งานมีหน้าที่
- (๑.๑) เก็บรหัสผ่านไว้เป็นความลับ
 - (๑.๒) ไม่จด ไม่บันทึกรหัสผ่านไว้ในสถานที่ซึ่งง่ายต่อการสังเกตรู้ของบุคคลอื่น
 - (๑.๓) เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบหรือสงสัยว่ารหัสผ่านอาจรั่วไหลหรือถูกเปิดเผย
 - (๑.๔) กรณีมีความจำเป็นต้องบอกรหัสผ่านแก่บุคคลอื่นในองค์กร ต้องเปลี่ยนรหัสผ่านทันทีหลังปฏิบัติงานเสร็จเรียบร้อย
 - (๑.๕) เมื่อบุคลากรในองค์กรโยกย้าย เปลี่ยนตำแหน่งหน้าที่หรือลาออก ให้แจ้งผู้ดูแลระบบทันที เพื่อเปลี่ยนหรือถอนสิทธิออกจากระบบ
 - (๑.๖) ไม่บันทึกรหัสผ่านไว้ในโปรแกรม หรือตั้งค่าให้เข้าสู่ระบบอัตโนมัติ
 - (๑.๗) กำหนดรหัสผ่านให้มีคุณภาพสูง ง่ายต่อการจำ และต้องไม่ใช่ข้อมูลพื้นฐานของตนเองที่บุคคลอื่นสามารถคาดเดาได้ง่าย ไม่เป็นคำในพจนานุกรม โดยต้องมีการผสมระหว่างอักขระพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข สัญลักษณ์และอักขระพิเศษ และต้องมีความยาวอย่างน้อย ๘ ตัวอักษร รวมถึงต้องไม่ใช่เลขหรือตัวอักษรเรียงกันซ้ำๆ
 - (๑.๘) เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยทุกๆ ๖ เดือน สำหรับผู้ใช้งานทั่วไปและทุกๆ ๓ เดือน สำหรับผู้ดูแลระบบหรือผู้ที่ได้รับสิทธิพิเศษ
- (๒) การป้องกันอุปกรณ์ขณะที่ผู้ใช้งานไม่อยู่
- (๒.๑) ผู้ใช้งานต้องล็อกหน้าจอคอมพิวเตอร์ทุกครั้งเมื่อไม่ใช้งาน หรือตั้งค่าให้มีการล็อกหน้าจออัตโนมัติหลังจากไม่ใช้งานนานเกิน ๑๕ นาที
 - (๒.๒) หลังจากมีการล็อกหน้าจอแล้ว ต้องกำหนดให้ใส่รหัสผ่านให้ถูกต้องก่อนจึงจะสามารถเข้าใช้งานคอมพิวเตอร์ได้
 - (๒.๓) ผู้ใช้งานต้องออกจากระบบ (Logout) ทันที เมื่อเลิกใช้ระบบสารสนเทศ

ส่วนที่ ๓ การควบคุมการเข้าถึงระบบสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศและอุปกรณ์ประมวลผลข้อมูลให้มีความมั่นคงปลอดภัย สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

ข้อ ๑๗ ผู้ดูแลระบบรับมอบอำนาจจากผู้บริหารระดับสูงสุด ในการอนุญาต การกำหนดสิทธิ การเข้าถึงสารสนเทศของผู้ใช้งาน โดยให้เป็นไปตามความข้อ ๑๘ และข้อ ๒๐

ข้อ ๑๘ กำหนดสิทธิผู้ใช้งาน ดังนี้

- (๑) การใช้งานครั้งแรก ต้องดำเนินการตามข้อ ๑๑ (๑) และต้องได้รับการพิจารณาจากผู้ดูแลระบบตามข้อ ๑๑ (๒) (๓) ก่อนจึงจะมีสิทธิเข้าใช้งาน
- (๒) ผู้ดูแลระบบกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน ได้แก่ สิทธิอ่านได้อย่างเดียว สิทธิการเพิ่มข้อมูล สิทธิการแก้ไขข้อมูล สิทธิการลบข้อมูล สิทธิการอนุญาต/อนุมัติ และไม่มีสิทธิใดๆ
- (๓) กำหนดการระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศของผู้ใช้งานที่กำหนดไว้ตามข้อ ๒๐
- (๔) บุคคลภายนอกที่ไม่มีส่วนเกี่ยวข้อง ไม่มีสิทธิลงทะเบียนและใช้งานระบบสารสนเทศขององค์กร

ข้อ ๑๙ กำหนดประเภทข้อมูล ลำดับชั้นความลับ ความสำคัญ เวลา และช่องทางที่เข้าถึง ดังนี้

(๑) จัดแบ่งประเภทข้อมูล ได้แก่

(๑.๑) ข้อมูลด้านการบริหาร ประกอบด้วย

- (ก) ข้อมูลด้านนโยบาย
- (ข) ข้อมูลแผนปฏิบัติการ ยุทธศาสตร์ และตัวชี้วัด
- (ค) ข้อมูลการรับรองการปฏิบัติราชการ
- (ง) ข้อมูลด้านบุคลากร
- (จ) ข้อมูลด้านงบประมาณ
- (ฉ) ข้อมูลด้านการเงินและบัญชี
- (ช) ข้อมูลด้านการพัสดุ

(๑.๒) ข้อมูลด้านการดำเนินงาน ประกอบด้วย

- (ก) การดำเนินงานตามภารกิจขององค์กร
- (ข) กฎหมาย ระเบียบ ข้อบังคับ ประกาศและคำสั่ง
- (ค) การเบิกจ่ายเงินงบประมาณ
- (ง) ผลการปฏิบัติงานและรายงานประจำปี

(๑.๓) ข้อมูลด้านการให้บริการ ประกอบด้วย

- (ก) ข้อมูลสถิติต่างๆ ของสำนักงานกิจการยุติธรรม
- (ข) ข้อมูลวิชาการ องค์ความรู้กฎหมายและงานวิจัย
- (ค) ข้อมูลการประชุมคณะกรรมการต่างๆ

(๒) จัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภทออกเป็น ๓ ชั้น ตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ได้แก่

- (๒.๑) ลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- (๒.๒) ลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- (๒.๓) ลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

(๓) จัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภท เป็น ๔ ระดับ ได้แก่

(๓.๑) สำคัญมากที่สุด

(๓.๒) สำคัญมาก

(๓.๓) สำคัญ

(๓.๔) ทั่วไป

(๔) จัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท ได้แก่

(๔.๑) เข้าถึงได้ทุกกลุ่มผู้ใช้งาน

(๔.๒) เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้อง

(๔.๓) เข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับอนุมัติสิทธิ

(๔.๔) เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบ

(๕) กำหนดช่องทางในการเข้าถึงข้อมูล ได้แก่

(๕.๑) เครือข่ายภายใน (LAN)

(๕.๒) เครือข่ายอินทราเน็ต (Intranet)

(๕.๓) เครือข่ายอินเทอร์เน็ต (Internet)

(๕.๔) จดหมายอิเล็กทรอนิกส์ (e-Mail)

(๕.๕) เครือข่ายไร้สาย (Wi-Fi)

(๖) กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล ได้แก่

(๖.๑) เวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.)

(๖.๒) นอกเวลาราชการ

(๖.๓) ช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

(๖.๔) ช่วงเวลาพิเศษตามที่กำหนดเป็นรายครั้ง

ข้อ ๒๐ กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศไว้ดังนี้

(๑) ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นต่อการใช้งานระบบสารสนเทศ โดยเป็นไปตามข้อ ๑๒ (๑) ข้อ ๑๓ ข้อ ๑๘ และข้อ ๒๐ (๒)

(๒) ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานมีสิทธิเข้าใช้งานระบบได้เฉพาะในระบบที่จำเป็นและมีส่วนเกี่ยวข้องกับอำนาจหน้าที่และตำแหน่งงาน ดังต่อไปนี้

(๒.๑) บุคลากรของสำนักงานกิจการยุติธรรมทุกคน มีสิทธิในการใช้งานระบบดังต่อไปนี้

(ก) ระบบอินเทอร์เน็ต (Internet)

(ข) ระบบอินทราเน็ต (Intranet)

(ค) ระบบเครือข่ายไร้สาย (Wi-Fi)

(ง) ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)

(จ) ระบบสารบรรณอิเล็กทรอนิกส์ (e-Sarabun)

(ฉ) ระบบลาราชการ (e-Absent)

(ช) ระบบจองห้องประชุม/รถราชการ (e-Meetingroom&Cars)

(ซ) ระบบสนับสนุนงานวิจัย (e-Research)

(ณ) ระบบจัดฝึกอบรม (e-Hr)

(ญ) ระบบบริหารจัดการงบประมาณ (e-Budget)

- (ฎ) ระบบวัสดุ/ครุภัณฑ์ (e-Asset)
- (ฉ) ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ (e-Doc)
- (ฐ) ระบบงานสถิติข้อมูล (e-Data)
- (ฑ) ระบบจัดการเรื่องร้องเรียน (e-News)
- (ฒ) ระบบ VPN SSL

(๒.๒) ผู้บริหาร อันได้แก่ ผู้อำนวยการสำนักงานกิจการยุติธรรม รองผู้อำนวยการ ผู้อำนวยการสถานบัน/สำนัก/กอง หัวหน้ากลุ่ม จะได้รับสิทธิพิเศษเพิ่มเติมจากบุคลากร ในการเข้าถึงระบบสารสนเทศ ดังนี้

- (ก) ระบบ DPIS
- (ข) ระบบติดตามงาน (e-Tracking)
- (ค) ข้อมูลลับตามข้อ ๑๙ (๒)

(๒.๓) ผู้ดูแลระบบมีสิทธิเพิ่มเติมจากสิทธิบุคลากรของสำนักงานกิจการยุติธรรม ในการเข้าถึงระบบสารสนเทศ ดังนี้

- (ก) ระบบบริหารจัดการบัญชีผู้ใช้งาน (Account Management)
- (ข) ระบบบริหารจัดการจดหมายอิเล็กทรอนิกส์ (e-Mail)
- (ค) ระบบบริหารจัดการเครือข่าย (Network Management)
- (ง) ระบบบริหารจัดการเซิร์ฟเวอร์ (Server Management)
- (จ) ระบบสำรองและกู้คืนข้อมูล (Backup&Recovery)
- (ฉ) ระบบเฝ้าระวังและเตือนภัยการโจมตี (Watching&Warning)
- (ช) ระบบบริหารจัดการฐานข้อมูลระบบ ตามข้อ ๒๐ (๒.๑) (๒.๒)

(๒.๔) บุคคลภายนอกที่ได้รับสิทธิ มีสิทธิในการเข้าถึงระบบ ดังนี้

- (ก) ระบบอินเทอร์เน็ต (Internet)
- (ข) ระบบเครือข่ายไร้สาย (Wi-Fi)

(๓) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานระบบ ใช้ระบบสารสนเทศได้ตามที่ได้รับอนุญาตเท่านั้น

(๔) กรณีผู้ใช้งานมีความจำเป็นต้องใช้งานระบบสารสนเทศที่อยู่นอกเหนือจากตำแหน่งงานและหน้าที่ความรับผิดชอบของตนเอง ตาม (๒) ข้างต้น ให้เป็นไปตามข้อ ๑๒ (๒) และ

(๔.๑) สิทธิในระดับการจัดการระบบ (System) และสิทธิพิเศษอื่นๆ ให้กำหนดชื่อผู้ใช้งานแยกจากผู้ใช้งานตามข้อ ๒๐ (๒.๑) (๒.๒) ข้างต้น

(๔.๒) ต้องกำหนดระยะเวลาการใช้งานและต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาที่ได้รับสิทธิพิเศษ หรือพ้นจากตำแหน่ง

(๕) ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีผู้ใช้งานซ้ำซ้อนกัน และถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวบุคคลของผู้ใช้งาน

(๖) ให้ผู้ดูแลระบบจำกัดการใช้งานบัญชีชื่อผู้ใช้งานแบบกลุ่มซึ่งมีการใช้งานร่วมกัน กล่าวคือ อนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้น และบัญชีผู้ใช้งานแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน

- (๗) ผู้ดูแลระบบต้องไม่อนุญาตให้ผู้ร้องขอใช้ระบบสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุญาตครบขั้นตอนตามข้อ ๑๑ และข้อ ๑๒ (๑) แล้วเท่านั้น
- (๘) ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบสารสนเทศ และต้องปฏิบัติตามอย่างเคร่งครัด
- (๙) ผู้ดูแลระบบต้องทบทวนการอนุญาตให้เข้าถึงและใช้งานสารสนเทศทุกครั้งที่มีการปรับเปลี่ยน โยกย้ายตำแหน่ง หรือถอนถอนสิทธิการใช้งานหากผู้ใช้งานลาออก

ข้อ ๒๑ การรักษาความลับของข้อมูล

- (๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับตามข้อ ๑๙ (๒) ทั้งการเข้าถึงโดยตรงและผ่านระบบงานสารสนเทศ
- (๒) การรับส่งข้อมูลที่เป็นความลับหรือข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL VPN และ XML Encryption
- (๓) กำหนดรหัสผ่านในการเข้าถึงไฟล์ข้อมูลลับอย่างรัดกุม เพื่อป้องกันการเข้าถึงไฟล์ข้อมูลลับที่จัดเก็บไว้ในคอมพิวเตอร์ที่ใช้งาน
- (๔) ไม่เผยแพร่ข้อมูลลับบนเครือข่าย (Share) เพื่อให้ผู้อื่นเข้าถึงได้
- (๕) ตรวจสอบการทำงานของซอฟต์แวร์ป้องกันไวรัส ติดตั้งซอฟต์แวร์แก้ไขช่องโหว่ของระบบปฏิบัติการคอมพิวเตอร์อย่างสม่ำเสมอ
- (๖) ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ เว้นแต่ได้ประกาศไว้เป็นอย่างอื่น

ข้อ ๒๒ การควบคุมสินทรัพย์สารสนเทศและการใช้งาน

- (๑) ผู้ดูแลระบบจัดทำบัญชีสินทรัพย์สารสนเทศ โดยระบุผู้ครอบครองสินทรัพย์สารสนเทศนั้นๆ อย่างชัดเจน และตรวจสอบความถูกต้องอยู่เสมอ
- (๒) การยืม-คืนสินทรัพย์สารสนเทศ ให้เป็นไปตามความข้อ ๒ (๕) และข้อ ๗
- (๓) ผู้ใช้งานต้องเก็บสินทรัพย์ที่ตนใช้งานเสร็จในที่ที่กำหนดไว้ให้เรียบร้อย หากเป็นการใช้งานระบบสารสนเทศจะต้องทำการออกจากระบบ (Logout) ทุกครั้ง
- (๔) ในกรณีที่สินทรัพย์อยู่ในรูปแบบอิเล็กทรอนิกส์และถูกระบุชั้นความลับ หากมีการส่งสารสนเทศนั้นผ่านระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ต้องเปิดฟังก์ชันห้ามการส่งต่อ
- (๕) การทำลายข้อมูลในสื่อบันทึกที่เป็นรูปแบบอิเล็กทรอนิกส์ ให้เป็นไปตามความข้อ ๘ (๑) (๒)

ส่วนที่ ๔ การควบคุมการเข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย

ข้อ ๒๓ การปฏิบัติสำหรับผู้ดูแลระบบและเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ มีดังนี้

- (๑) ผู้ดูแลระบบต้องดูแลตรวจสอบบุคคลที่มาติดต่อและผู้ที่ได้รับอนุญาตให้เข้ามาภายในห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายอย่างเคร่งครัด ตลอดเวลาที่มาติดต่อจนเสร็จภารกิจ

- (๒) ผู้ดูแลระบบต้องจัดทำทะเบียนผู้มีสิทธิเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย และกำหนดสิทธิในการเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องและบุคคลที่ได้รับอนุญาตตามความข้อ ๒๔ (๑) เท่านั้น
- (๓) เจ้าหน้าที่สารสนเทศ และผู้ที่เกี่ยวข้องทุกคนต้องบันทึกข้อมูลยืนยันตัวบุคคล ได้แก่ บันทึกลายนิ้วมือ ทำบัตรเข้าออก เพื่อใช้ในการผ่านเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย
- (๔) ผู้ดูแลระบบต้องตรวจสอบว่าผู้มาติดต่อนำอุปกรณ์เข้า-ออกสถานที่หรือไม่ หากมีอุปกรณ์ส่วนตัวนำมา ให้จดบันทึกในแบบฟอร์มการเข้าออกสถานที่ตามข้อ ๒ (๔)
- (๖) ผู้ที่เข้าไปปฏิบัติหน้าที่ในห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายต้องบันทึกรายการปฏิบัติงานในแบบฟอร์มบันทึกการปฏิบัติงานในห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายหลังเสร็จสิ้นการปฏิบัติงานทุกครั้ง
- (๗) ผู้ดูแลระบบต้องหมั่นตรวจเช็คกล้องวงจรปิดในพื้นที่ใช้งานและรายงานให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทราบ อย่างน้อยที่สุดเดือนละ ๑ ครั้ง และรายงานทันทีหากมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
- (๘) การเพิกถอนสิทธิในการเข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย ให้เป็นไปตามข้อ ๒ (๗)
- (๙) ไม่อนุญาตให้นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ส่วนบุคคลมาใช้ภายในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย และเชื่อมต่อกับคอมพิวเตอร์แม่ข่าย โดยไม่ได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข้อ ๒๔ การปฏิบัติสำหรับบุคคลภายนอก มีดังนี้

- (๑) บุคคลภายนอกต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อน จึงจะมีสิทธิเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย
- (๒) ไม่อนุญาตให้นำเครื่องคอมพิวเตอร์และอุปกรณ์ของบุคคลภายนอกเข้ามาในห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายอย่างเด็ดขาด
- (๓) บุคคลภายนอกต้องลงบันทึกในแบบฟอร์มการเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายให้ชัดเจน ถูกต้อง ทุกครั้ง
- (๔) ห้ามบุคคลภายนอกนำอุปกรณ์ใดๆ ออกจากห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายอย่างเด็ดขาด โดยให้ผู้ดูแลระบบตรวจสอบด้วยทุกครั้ง

ส่วนที่ ๕ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

ข้อ ๒๕ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย ให้เป็นไปตามแนวปฏิบัติหมวดที่ ๑ การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน ส่วนที่ ๓ การควบคุมการเข้าถึงระบบสารสนเทศ ส่วนที่ ๔ การควบคุมการเข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันสารสนเทศ ส่วนที่ ๑๐ การควบคุมการตรวจจับการบุกรุก และส่วนที่ ๑๑ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ข้อ ๒๖ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายทางด้านกายภาพ ให้เป็นไปตามแนวปฏิบัติหมวดที่ ๑ ส่วนที่ ๑ การรักษาความมั่นคงปลอดภัยด้านกายภาพ

ข้อ ๒๗ การพัฒนาระบบสารสนเทศโดยผู้รับจ้างจากภายนอก

- (๑) ผู้ดูแลระบบต้องควบคุม สอดส่อง ติดตาม กำกับดูแลโครงการพัฒนาระบบสารสนเทศทุกโครงการอย่างรัดกุม ตั้งแต่เริ่มต้นจนเสร็จสิ้นการพัฒนา
- (๒) สำหรับ Source Code จากการพัฒนาระบบทุกระบบต้องระบุสิทธิในทรัพย์สินทางปัญญาเป็นของสำนักงานกิจการยุติธรรม
- (๓) ผู้ดูแลระบบต้องตรวจสอบโปรแกรมคำสั่งไม่พึงประสงค์ ความถูกต้องต้องของลิขสิทธิ์ในซอฟต์แวร์ต่างๆ จากผู้รับจ้างจากภายนอกก่อนติดตั้งในเครื่องคอมพิวเตอร์แม่ข่าย

ข้อ ๒๘ การควบคุมช่องโหว่ทางเทคนิค

- (๑) ผู้ดูแลระบบต้องปรับปรุงโปรแกรมจัดการช่องโหว่ต่างๆ (Patch) อย่างสม่ำเสมอ
- (๒) การควบคุมพอร์ตที่ใช้ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย ให้เป็นไปตามข้อ ๓๓

ข้อ ๒๙ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) จัดให้บันทึกพฤติกรรมการใช้งาน (Log) จากการเข้าถึงระบบสารสนเทศ มีรายละเอียดดังนี้

- (๑) ข้อมูลชื่อบัญชีผู้ใช้
- (๒) ข้อมูลวัน เวลา ที่เข้าถึงระบบ
- (๓) ข้อมูลวัน เวลา ที่ออกจากระบบ
- (๔) ข้อมูลเหตุการณ์ที่สำคัญที่เกิดขึ้น
- (๕) ข้อมูลการเข้าสู่ระบบ (Login) ทั้งที่สำเร็จและไม่สำเร็จ
- (๖) ข้อมูลการพยายามเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- (๗) ข้อมูลการเปลี่ยนค่าระบบ (Configuration)
- (๘) ข้อมูลการใช้งานแอปพลิเคชัน
- (๙) ข้อมูลแสดงการเข้าถึงไฟล์ การกระทำกับไฟล์ ได้แก่ ระยะเวลาเปิด อ่านไฟล์
- (๑๐) ข้อมูลหมายเลขอุปกรณ์ (IP Address)
- (๑๑) ข้อมูลโปรโตคอลที่ใช้งาน (Protocol)

ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย

ข้อ ๓๐ การใช้บริการเครือข่ายของผู้ใช้งาน

- (๑) ให้ผู้ใช้งานสามารถเข้าถึงได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น และ
- (๒) การใช้งานระบบอินเทอร์เน็ต
 - (๒.๑) ผู้ดูแลระบบกำหนดให้ผู้ใช้งานทุกคนมีชื่อผู้ใช้และรหัสผ่านสำหรับเข้าใช้งานอินเทอร์เน็ต จัดให้มีระบบบันทึกข้อมูลการใช้งานอินเทอร์เน็ตเพื่อเก็บไว้ตรวจสอบภายหลัง และตรวจสอบการอนุญาตใช้งานตามความจำเป็นต่อการปฏิบัติงานเท่านั้น

- (๒.๒) ผู้ดูแลระบบต้องกำหนดข้อปฏิบัติหรือกฎการเข้าถึงข้อมูลบนระบบอินเทอร์เน็ต ได้แก่ ห้ามเข้าถึงสื่อหรือเว็บไซต์หมิ่นสถาบัน เว็บไซต์เกมออนไลน์ เว็บไซต์การพนัน เว็บไซต์ลามกอนาจาร เว็บไซต์ซื้อขายออนไลน์ เป็นต้น
- (๒.๓) ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ต เพื่อหาประโยชน์ในทางธุรกิจส่วนตัว หรือใช้กระทำการใดๆ ที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน
- (๒.๔) ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น ได้แก่ เผยแพร่สื่อใดๆ ที่ก่อให้เกิดความเสื่อมเสียแก่ผู้อื่น โดยผู้ดูแลระบบต้องคอยเฝ้าระวังการละเมิดสิทธิการใช้งานของผู้อื่นและละเมิดนโยบายด้านความปลอดภัยด้วย
- (๒.๕) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานและรหัสผ่านเป็นการเฉพาะบุคคลเท่านั้น จะโอนหรือจ่ายแจกสิทธิให้แก่ผู้อื่นไม่ได้ และผู้ใช้งานต้องรับผิดชอบผลต่างๆ ที่อาจเกิดขึ้นจากบัญชีผู้ใช้งานนั้น เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของบุคคลอื่น
- (๒.๖) ต้องจัดเก็บข้อมูลการใช้งานอินเทอร์เน็ตของผู้ใช้งานตามข้อ ๓๐ (๒) (๓) ให้เป็นไปตามข้อ ๒๙ ข้อ ๖๑ ข้อ ๖๒ และข้อ ๖๓
- (๒.๗) ผู้ใช้งานต้องตระหนักและปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐ อย่างเคร่งครัด
- (๓) การใช้บริการระบบเครือข่ายไร้สาย
- (๓.๑) การกำหนดชื่อ รหัสผ่าน สำหรับเข้าใช้งานเครือข่ายไร้สายให้เป็นไปตามแนวปฏิบัติข้อ ๓๐ (๑) (๒)
- (๓.๒) ผู้ดูแลระบบต้องจัดทำบัญชีข้อมูลเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชนิดที่ใช้ระบบเครือข่ายไร้สาย ได้แก่ ชื่อผู้ใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์หรืออุปกรณ์ IP Address MAC Address สถานที่ติดต่อ เบอร์โทรศัพท์ที่ติดต่อได้
- (๓.๓) ผู้ดูแลระบบต้องเปลี่ยนค่ารหัสผู้ใช้งานและรหัสผ่านในการตั้งค่าการทำงานของอุปกรณ์ไร้สายที่ติดตั้งมาจากผู้ผลิต เพื่อป้องกันการถูกโจมตี
- (๓.๔) ต้องใช้การเข้ารหัสข้อมูลระบบเครือข่ายไร้สาย เพื่อให้ข้อมูลมีความปลอดภัย
- (๓.๕) ต้องใช้ MAC Address ตามที่กำหนดไว้ ตรวจสอบอุปกรณ์ที่มีสิทธิเข้าถึงระบบเครือข่ายไร้สาย และใช้รหัสผู้ใช้และรหัสผ่านเพื่อยืนยันตัวบุคคลในการใช้งาน

ข้อ ๓๑ การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร

- (๑) กำหนดให้ผู้ใช้งานสามารถเข้าถึงสารสนเทศและแอปพลิเคชันขององค์กรได้ ๒ ช่องทาง ได้แก่ การเข้าถึงจากเว็บไซต์ของสำนักงานกิจการยุติธรรม และการเข้าถึงโดยตรงผ่านระบบ VPN SSL
- (๒) การใช้งานระบบสารสนเทศและแอปพลิเคชันขององค์กรจากภายนอก จะต้องเป็นผู้ได้รับสิทธิในการใช้งานที่กำหนดตามแนวปฏิบัติหมวดที่ ๑ ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน ข้อ ๑๑ และข้อ ๑๒
- (๓) กรณีผู้ใช้งานจากภายนอกเป็นผู้รับจ้างออกแบบและพัฒนาระบบ (Outsource) หรือหน่วยงานภายนอก ต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งานซึ่งสามารถเข้าใช้งานโดยการใช้ชื่อผู้ใช้และรหัสผ่านที่กำหนดให้ และต้องใช้ Protocol ที่มีการเข้ารหัสข้อมูล ได้แก่ SSL
- (๔) ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบสารสนเทศและแอปพลิเคชันให้ผู้ใช้งานเข้าถึงได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น
- (๕) อุปกรณ์ที่เข้าใช้ระบบสารสนเทศและแอปพลิเคชันจากภายนอกองค์กร ต้องได้รับการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่ได้อัปเดตอย่างสม่ำเสมอ และมีการอัปเดตระบบปฏิบัติการอย่างสม่ำเสมอ
- (๖) กำหนดให้จัดเก็บข้อมูลการเข้าถึงสารสนเทศจากภายนอก เป็นไปตามหมวดที่ ๑ ส่วนที่ ๑๑ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ข้อ ๓๒ การระบุอุปกรณ์บนระบบเครือข่าย

- (๑) ผู้ดูแลระบบจัดทำบัญชีอุปกรณ์ของเครื่องคอมพิวเตอร์และอุปกรณ์ที่เชื่อมกับเครือข่าย ประกอบไปด้วย ชื่อผู้ใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์หรืออุปกรณ์ IP Address MAC Address สถานที่ติดตั้ง เบอร์โทรศัพท์ เป็นต้น
- (๒) การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายเพิ่มเติมจะต้องได้รับอนุญาตจากผู้ดูแลระบบและได้รับความเห็นชอบจากสำนักเทคโนโลยีสารสนเทศก่อน
- (๓) ใช้ไฟร์วอลล์ (Firewall) กำหนดหมายเลขอุปกรณ์ (IP Address) ในการเข้าถึงเครือข่ายขององค์กร กรณีมีอุปกรณ์ที่มีการเชื่อมต่อเครือข่ายจากภายนอกต้องระบุหมายเลขอุปกรณ์ (IP Address) ว่าสามารถเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

ข้อ ๓๓ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

- (๑) ติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงค่าระบบโดยบุคคลที่ไม่มีสิทธิ
- (๒) ต้องป้องกัน IP Address ภายในระบบเครือข่ายขององค์กรจากการมองเห็นโดยบุคคลภายนอก เพื่อป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องรู้ถึงโครงสร้างระบบเครือข่ายภายใน
- (๓) การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ซึ่งเป็นช่องทางที่มีความเสี่ยงสูงต่อความมั่นคงปลอดภัย ต้องได้รับอนุญาตสิทธิ

จากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อนทุกครั้ง พร้อมทั้งมีการควบคุมอย่างเข้มงวดโดยระบุหมายเลขอุปกรณ์ที่ใช้ในการเข้าระบบ และเมื่อเลิกใช้งานแล้วต้องยกเลิกสิทธิดังกล่าวทันที

- (๔) การเปิดพอร์ตใดๆ ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่เปิดพอร์ตทิ้งไว้โดยไม่จำเป็น
- (๕) ต้องควบคุมพอร์ตที่ใช้ในการเข้าสู่ระบบเครือข่ายอย่างรอบคอบรัดกุมและสม่ำเสมอ

ข้อ ๓๔ การแบ่งแยกเครือข่าย

- (๑) มีการแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย (VLAN) ตามอาคารต่างๆ เพื่อความสะดวกในการควบคุมและบริหารจัดการ
- (๒) มีการแบ่งแยกเครือข่ายภายใน เครือข่ายภายนอก และ Demilitarized Zone เพื่อความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ

ข้อ ๓๕ การควบคุมการเชื่อมต่อเครือข่าย

- (๑) ระบบเครือข่ายทั้งหมดต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือทำ Packet Filtering ได้แก่ Firewall
- (๒) ผู้ดูแลระบบต้องจำกัดสิทธิของผู้ใช้งานในการเข้าสู่ระบบเครือข่ายตามข้อ ๑๒ (๑) ข้อ ๑๓ ข้อ ๓๐ (๑) (๒) และการทบทวนสิทธิการเข้าถึงตามข้อ ๑๕
- (๓) การเข้าสู่ระบบเครือข่ายภายในผ่านอินเทอร์เน็ตต้องพิสูจน์ตัวตนผ่านช่องทางที่ปลอดภัยทุกครั้ง
- (๔) การเข้าสู่ระบบเครือข่ายไร้สาย ให้เป็นไปตามความข้อ ๓๐ (๓)
- (๕) กำหนดให้ยุติการเข้าถึง หรือยุติการเชื่อมต่อกับระบบเมื่อเว้นว่างจากการใช้งานตามข้อ ๔๑

ข้อ ๓๖ การควบคุมการจัดเส้นทางบนเครือข่าย

- (๑) ผู้ดูแลระบบต้องกำหนดตารางการใช้เส้นทางบนเครือข่าย (Network Routing Table) บนอุปกรณ์จัดเส้นทางหรืออุปกรณ์กระจายสัญญาณข้อมูล เพื่อควบคุมผู้ใช้งานให้ใช้งานเฉพาะเส้นทางเครือข่ายที่ได้รับอนุญาตเท่านั้น
- (๒) ผู้ดูแลระบบต้องจำกัดเส้นทางการเข้าถึงเครือข่ายของผู้ใช้งานไปยังคอมพิวเตอร์แม่ข่ายที่ให้บริการต่างๆ โดยกำหนดให้ใช้เส้นทางที่ต้องผ่าน Demilitarized Zone
- (๓) ผู้ดูแลระบบต้องจำกัดเส้นทางบนระบบเครือข่ายจากคอมพิวเตอร์ของผู้ใช้งานไปยังคอมพิวเตอร์แม่ข่ายที่ให้บริการต่างๆ โดยเชื่อมต่อเข้าสู่คอมพิวเตอร์แม่ข่ายที่ให้บริการ เพื่อการบริหารจัดการระบบและให้กำหนด IP Address เฉพาะชุดของผู้ดูแลระบบเท่านั้นที่จะสามารถเข้าถึงคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นได้
- (๔) มีอุปกรณ์ Firewall ควบคุมเส้นทางบนระบบเครือข่าย

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๓๗ การควบคุมการเข้าใช้งานระบบปฏิบัติการ

- (๑) ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพสูงในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ ตามข้อ ๑๖ (๑.๗)
- (๒) ผู้ใช้งานต้องทำการล็อกหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ และเมื่อกลับมาใช้งานต้องใส่รหัสผ่านอีกครั้งเพื่อเข้าใช้งาน
- (๓) ผู้ใช้งานต้องออกจากระบบปฏิบัติการ (Logoff) หรือปิดเครื่อง (Shutdown) ทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่เครื่องคอมพิวเตอร์เป็นเวลานาน
- (๔) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้งานโดยลงชื่อเข้าใช้ระบบด้วยชื่อผู้ใช้และรหัสผ่านของตน
- (๕) ซอฟต์แวร์ที่องค์กรใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความรับผิดชอบ ห้ามผู้ดูแลระบบติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากตรวจพบถือเป็นความผิดส่วนบุคคล ผู้นั้นต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- (๖) ซอฟต์แวร์ที่สำนักเทคโนโลยีสารสนเทศติดตั้งไว้ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไขปรับปรุง หากมีความจำเป็นต้องดำเนินการตามที่กล่าว ให้ติดต่อผู้ดูแลระบบหรือเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศที่รับผิดชอบ ช่องทางการติดต่อปรากฏตามรายละเอียดในเอกสารภาคผนวก ข.

ข้อ ๓๘ การระบุและยืนยันตัวตนบุคคลของผู้ใช้งาน

- (๑) ให้นำความข้อ ๓๑ (๑) (๒) (๓) มาใช้สำหรับการยืนยันตัวตนของผู้ใช้งาน ซึ่งหากการระบุและยืนยันตัวตนบุคคลของผู้ใช้งานมีปัญหา ให้แจ้งไปยังผู้ดูแลระบบเพื่อดำเนินการตรวจสอบและแก้ไข
- (๒) ผู้ใช้งานที่เป็นเจ้าของชื่อผู้ใช้และรหัสผ่าน ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันอาจเกิดจากการใช้งานชื่อผู้ใช้ระบบสารสนเทศ เว้นแต่จะพิสูจน์ได้ว่าผลเสียนั้นเกิดจากการกระทำของผู้อื่น
- (๓) กำหนดจำนวนครั้งในการพิสูจน์ตัวตนผิดพลาด หากใส่ชื่อผู้ใช้หรือรหัสผ่านผิดติดต่อกันเกิน ๓ ครั้ง แล้วไม่สามารถเข้าสู่ระบบสารสนเทศได้ให้ติดต่อผู้ดูแลระบบ

ข้อ ๓๙ การบริหารจัดการรหัสผ่าน ให้เป็นไปตามข้อ ๑๔

ข้อ ๔๐ การควบคุมการใช้งานโปรแกรมมัลแวร์

- (๑) การติดตั้งโปรแกรมมัลแวร์ใดๆ ผู้ดูแลระบบจะเป็นผู้ดำเนินการติดตั้งตามความจำเป็น ซึ่งต้องได้รับความเห็นชอบจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อน ผู้ใช้งานไม่มีสิทธิในการติดตั้งซอฟต์แวร์เอง
- (๒) ต้องจัดเก็บโปรแกรมมัลแวร์แยกจากซอฟต์แวร์ระบบสารสนเทศ
- (๓) จำกัดผู้ได้รับอนุญาตและจำกัดสิทธิการใช้งานโปรแกรมมัลแวร์
- (๔) ต้องยกเลิกหรือถอดถอนโปรแกรมมัลแวร์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบที่ไม่มีความจำเป็นสำหรับผู้ใช้งาน รวมถึงป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงและใช้งานโปรแกรมเหล่านั้นได้

- (๕) ตรวจสอบซอฟต์แวร์ในระบบสารสนเทศอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์พ่วงโดยไม่ได้รับอนุญาต
- (๖) ซอฟต์แวร์ที่ติดตั้งต้องเป็นซอฟต์แวร์ลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ดูแลระบบนำซอฟต์แวร์ผิดกฎหมาย ไม่ได้รับอนุญาต ซอฟต์แวร์ไม่มีลิขสิทธิ์หรือซอฟต์แวร์คัดลอกต่างๆ มาติดตั้ง แก้ไขเปลี่ยนแปลง หรือแทนที่โดยเด็ดขาด หากตรวจพบถือเป็นความผิดส่วนบุคคล ผู้นั้นต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

ข้อ ๔๑ การกำหนดเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน

- (๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบงาน อุปกรณ์เครือข่ายตัดสัญญาณหรือปิดการใช้เครือข่าย (Session Time Out) หากไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที
- (๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีกำหนดเวลาในการตัดสัญญาณหรือปิดการใช้เครือข่าย (Session Time Out) ที่สั้นขึ้น สำหรับระบบสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบสารสนเทศด้านการเงินและบัญชี ระบบงานบุคลากร ระบบประเมินผลและเลื่อนเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๔๒ การจำกัดเวลาการเชื่อมต่อระบบสารสนเทศ

- (๑) กำหนดให้จำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานระบบสารสนเทศแต่ละครั้งไม่เกิน ๔ ชั่วโมง โดยจะต้องพิสูจน์ตัวตน เพื่อเข้าใช้งานใหม่ และเมื่อไม่มีการใช้งานนานเกิน ๑๕ นาที ต้องยกเลิกการเชื่อมต่อระบบ
- (๒) กำหนดให้จำกัดระยะเวลาเชื่อมต่อที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงสูง (ในที่สาธารณะหรือภายนอกองค์กร)

ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันสารสนเทศ

ข้อ ๔๓ การจำกัดการเข้าถึงสารสนเทศ

- (๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานขององค์กร ตามข้อ ๑๑
- (๒) ต้องกำหนดเวลายุติการใช้งานตามข้อ ๔๑ และจำกัดเวลาการเชื่อมต่อระบบสารสนเทศต่างๆ ตามข้อ ๔๒
- (๓) ต้องจัดการการเข้าถึงตามประเภทชั้นความลับ ตามข้อ ๑๙ (๒) การบริหารจัดการสิทธิของผู้ใช้งานตามข้อ ๑๒ ข้อ ๑๓ การทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานตามข้อ ๑๕ และข้อ ๑๖
- (๔) ให้ผู้ดูแลระบบควบคุมสิทธิการเข้าถึงและใช้งานโปรแกรมประยุกต์หรือแอปพลิเคชันสารสนเทศของผู้ใช้งาน โดยให้นำความตามข้อ ๑๘ ข้อ ๒๑ มาเป็นข้อปฏิบัติ การทบทวนสิทธิการเข้าถึงให้เป็นไปตามความข้อ ๑๕
- (๖) ผู้รับจ้างพัฒนาระบบ โปรแกรมประยุกต์ หรือสารสนเทศ (Outsource) ให้เป็นไปตามข้อ ๒๗ และต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร

- (๗) ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้รับจ้างพัฒนาระบบ ให้มีสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้า-ออกจากระบบสารสนเทศทุกครั้ง

ข้อ ๔๔ การบริหารจัดการระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและสำคัญสูงต่อองค์กร

- (๑) ต้องระบุระดับความสำคัญของระบบซึ่งไวต่อการรบกวน และแยกระบบดังกล่าวไว้ในสภาพแวดล้อมของตนเองโดยเฉพาะ
- (๒) การสำรองและการกู้คืนระบบซึ่งไวต่อการรบกวน ให้เป็นไปตามหมวดที่ ๒ ส่วนที่ ๒ การสำรองข้อมูล
- (๓) การประเมินความเสี่ยงตามด้านสารสนเทศให้เป็นไปตามข้อปฏิบัติในหมวดที่ ๓ ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง
- (๔) ควบคุมการเข้าถึงด้านกายภาพและใช้งานระบบสารสนเทศดังกล่าว ตามข้อ ๑ ข้อ ๒ ข้อ ๕ ข้อ ๑๑ ข้อ ๑๒ ข้อ ๑๓ ข้อ ๑๕ และข้อ ๑๖

ข้อ ๔๕ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อดูแลรักษาความมั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศ

(๑) ข้อปฏิบัติทั่วไป

- (๑.๑) เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่เป็นทรัพย์สินขององค์กร ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานขององค์กรเท่านั้น
- (๑.๒) โปรแกรมหรือซอฟต์แวร์ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ขององค์กร ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น ห้ามผู้ดูแลระบบนำซอฟต์แวร์ผิดกฎหมาย ไม่ได้รับอนุญาต ซอฟต์แวร์ไม่มีลิขสิทธิ์หรือซอฟต์แวร์คัดลอกต่างๆ มาติดตั้ง แก้ไขเปลี่ยนแปลง หรือแทนที่โดยเด็ดขาด หากตรวจพบถือเป็นความผิดส่วนบุคคล ผู้นั้นต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- (๑.๓) ผู้ใช้งานต้องศึกษาคู่มือการใช้งานอย่างละเอียดและปฏิบัติตามอย่างเคร่งครัด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- (๑.๔) ไม่ดัดแปลง แก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง และดูแลรักษาให้คงสภาพเดิมอยู่เสมอ
- (๑.๕) กรณีต้องยืม เคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาและสื่อสารเคลื่อนที่ต้องดำเนินการตามข้อ ๒ (๕) โดยต้องได้รับอนุญาตจากผู้ดูแลระบบ และต้องนำอุปกรณ์ใส่กระเป๋าให้เรียบร้อย เพื่อป้องกันอันตรายที่อาจเกิดจากการกระทบกระเทือน

- (๑.๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็งกดสัมผัสหน้าจอ LCD ได้แก่ ปากกา ไม้บรรทัด เป็นต้น ซึ่งอาจทำให้เป็นรอยขีดข่วนหรือแตกเสียหาย
- (๑.๗) การเช็ดทำความสะอาดหน้าจอต้องใช้อุปกรณ์เฉพาะ เช็ดอย่างเบามือ และไปในทางเดียวกัน ห้ามเช็ดหมุนวน เนื่องจากจะทำให้หน้าจอเป็นรอยขีดข่วนได้
- (๑.๘) การนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ส่วนบุคคลมาใช้งานกับระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศ ซึ่งให้ดำเนินการตามข้อ ๒ (๔) และให้ถือปฏิบัติตามนโยบายและแนวปฏิบัติขององค์กรอย่างเคร่งครัด
- (๑.๙) หากมีความจำเป็นต้องเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ ให้ติดต่อแจ้งความเหตุผลความจำเป็นกับผู้ดูแลระบบ
- (๒) การป้องกันความปลอดภัยด้านกายภาพ
- (๒.๑) ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบในการป้องกันการสูญหาย โดยการล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องคอมพิวเตอร์แบบพกพาทิ้งไว้ในสถานที่สาธารณะหรือบริเวณที่เสี่ยงต่อการสูญหาย
- (๒.๒) ไม่เก็บ ไม่ใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละออง สูง และต้องระมัดระวังป้องกันการตกกระแทก
- (๒.๓) ไม่นำอาหารมารับประทาน และไม่สูบบุหรี่ในพื้นที่ตามข้อ ๑
- (๓) การควบคุมการเข้าถึงระบบปฏิบัติการ ให้เป็นไปตามข้อ ๓๗
- (๔) การใช้งานรหัสผ่าน ให้เป็นไปตามข้อ ๑๖ (๑)
- (๕) การป้องกันโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)
- (๕.๑) ผู้ดูแลระบบต้องปรับปรุง (Update) ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมมัลแวร์ป้องกันต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ในการโจมตีจากภัยคุกคามต่างๆ ที่เกิดขึ้นจากชุดคำสั่งไม่พึงประสงค์
- (๕.๒) ห้ามผู้ใช้งานปิดหรือยกเลิกระบบป้องกันไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์
- (๕.๓) หากผู้ใช้งานพบเห็นหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัสหรือมีโปรแกรมชุดคำสั่งไม่พึงประสงค์ ห้ามเชื่อมต่อเครื่องต้องสงสัยนั้นกับเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ไปยังเครื่องคอมพิวเตอร์อื่น และให้รีบแจ้งผู้ดูแลระบบทราบเพื่อดำเนินการแก้ไขโดยเร็ว
- (๖) การสำรองข้อมูลและกู้คืนระบบ ให้เป็นไปตามข้อปฏิบัติหมวดที่ ๒ ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๔๖ การปฏิบัติงานภายนอกองค์กร

- (๑) การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ให้เป็นไปตามข้อ ๓๓ (๓)
- (๒) ผู้ใช้งานจากระยะไกล (Remote Access) ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งานตามข้อ ๓๑ (๑) (๒) (๔)
- (๓) ไม่อนุญาตให้ครอบครัว เครือญาติ เพื่อน คนสนิท หรือคนรู้จักของผู้ใช้งานจากระยะไกลเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลขององค์กร
- (๔) เครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการเชื่อมต่อเข้าถึงระบบสารสนเทศขององค์กรจากระยะไกล ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสหรือโปรแกรมชุดคำสั่งไม่พึงประสงค์ และให้เป็นไปตามข้อ ๓๑ (๑) (๓) (๕)
- (๕) จัดเก็บข้อมูลการเข้าถึงสารสนเทศจากภายนอก ตามหมวดที่ ๑ ส่วนที่ ๑๑ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ส่วนที่ ๙ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

ข้อ ๔๗ การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail) สำหรับผู้ใช้งาน

- (๑) ผู้ดูแลระบบลงทะเบียนใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail) ให้เป็นไปตามข้อ ๑๑
- (๒) เมื่อผู้ใช้งานเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ครั้งแรก ต้องเปลี่ยนรหัสผ่านทันที โดยกำหนดรหัสผ่านใหม่ที่มีคุณภาพ ตามข้อ ๑๖ (๑.๗)
- (๓) การใช้งานรหัสผ่านจดหมายอิเล็กทรอนิกส์ ให้เป็นไปตามข้อ ๑๖ (๑)
- (๔) ห้ามใช้จดหมายอิเล็กทรอนิกส์ (e-Mail) ขององค์กร เผยแพร่ข้อมูล ข้อความ รูปภาพ เสียง หรือสื่ออื่นใดซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย กระทบต่อการดำเนินงานขององค์กร และรบกวนผู้ใช้งานอื่น
- (๕) ห้ามใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้งานอื่น เพื่ออ่าน รับ-ส่งข้อความ ข้อมูล ยกเว้นกรณีจำเป็นเร่งด่วนและได้รับความยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์นั้น และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบการใช้งานต่างๆ จากจดหมายอิเล็กทรอนิกส์ของตน
- (๖) ใช้งานจดหมายอิเล็กทรอนิกส์ขององค์กรเพื่อติดต่อกับราชการเท่านั้น ห้ามใช้เพื่อประโยชน์ส่วนตัว ธุรกิจ หรือในเชิงพาณิชย์
- (๗) ผู้ใช้งานต้องตรวจสอบไฟล์แนบในจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส เพื่อป้องกันการเปิดไฟล์ Executable (.EXE)
- (๘) ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่จำเป็นออกจากระบบ เพื่อรักษาเนื้อที่ความจุในระบบตามที่ได้จำกัดไว้
- (๙) ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) จดหมายลูกโซ่ (Chain Mail) และจดหมายอิเล็กทรอนิกส์ที่มีไวรัสให้กับบุคคลอื่นโดยเจตนา
- (๑๐) หลังจากใช้งานเสร็จต้องออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นถือโอกาสเข้ามาใช้งาน

ส่วนที่ ๑๐ การควบคุมตรวจจัดการบุกรุก

ข้อ ๔๘ IDS/IPS ต้องครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายขององค์กรและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๔๙ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ต ต้องผ่านการตรวจสอบจาก IDS/IPS ขององค์กร

ข้อ ๕๐ ระบบทั้งหมดใน Demilitarized Zone (DMZ) ตามข้อ ๓๔ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนติดตั้งและเปิดให้บริการ

ข้อ ๕๑ โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งข้อมูลผ่าน IDS/IPS จะต้องจัดให้มีการบันทึกผลการตรวจสอบ

ข้อ ๕๒ ผู้ดูแลระบบจะต้องตรวจสอบ IDS/IPS และ Update Patch/Signature อยู่เสมอ

ข้อ ๕๓ ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรมและบันทึกปริมาณข้อมูลการใช้งานเครือข่ายเป็นประจำทุกวัน

ข้อ ๕๔ IDS/IPS จะต้องทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายระบบสารสนเทศตามปกติ

ข้อ ๕๕ เครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้ง Host-based IDS ผู้ดูแลระบบจะต้องตรวจสอบข้อมูลเป็นประจำทุกวัน

ข้อ ๕๖ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การถูกโจมตี พฤติกรรมที่น่าสงสัยว่ามีการพยายามเข้าสู่ระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องรายงานให้ผู้อำนวยความสะดวกเทคโนโลยีสารสนเทศทราบทันที

ข้อ ๕๗ ต้องเก็บบันทึกข้อมูลผลการตรวจสอบการบุกรุกทั้งหมดไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๕๘ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์น่าสงสัยต่างๆ ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดขึ้นในอนาคต เป็นต้น

ข้อ ๕๙ สำนักงานกิจการยุติธรรม มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุก โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

ข้อ ๖๐ ผู้ที่ถูกตรวจสอบว่าพยายามจะกระทำการใดที่เป็นการละเมิดนโยบายของสำนักงานกิจการยุติธรรม การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมที่น่าสงสัยซึ่งเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรของระบบของสำนักงานกิจการยุติธรรม จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๑ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ข้อ ๖๑ กำหนดให้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามข้อ ๒๙ ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง เป็นจริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ ๖๒ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามข้อ ๖๑ ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เพื่อประโยชน์ในการตรวจสอบย้อนหลัง

ข้อ ๖๓ ต้องป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลจราจรคอมพิวเตอร์ และจำกัดสิทธิการเข้าถึงไว้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ ๒

การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง
๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย
๓. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๖๔ จัดทำบัญชีฐานข้อมูลระบบสารสนเทศ จำแนกตามกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

ข้อ ๖๕ กำหนดรายละเอียดของการสำรองข้อมูลเก็บไว้อย่างน้อยดังนี้

- (๑) ข้อมูลของระบบสารสนเทศ (Database)
- (๒) ข้อมูลการตั้งค่าต่างๆ ของระบบสารสนเทศ (Configuration)
- (๓) ระบบปฏิบัติการ (Operation System)
- (๔) ซอฟต์แวร์ต่างๆ ที่เกี่ยวกับระบบสารสนเทศ

ข้อ ๖๖ ในกรณีมีการใช้งานฐานข้อมูลร่วมกันระหว่างองค์กร หรือแลกเปลี่ยนข้อมูลจากองค์กร ให้จัดทำเป็นข้อตกลงการใช้ข้อมูลหรือแลกเปลี่ยนสารสนเทศระหว่างองค์กรกับหน่วยงานภายนอกดังต่อไปนี้

- (๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังสถานที่อื่น
- (๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูลระหว่างกัน
- (๓) กำหนดหน้าที่และความรับผิดชอบในการป้องกันข้อมูลร่วมกัน
- (๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าผู้ใดส่งข้อมูลและผู้ใดรับข้อมูลเพื่อป้องกันการถูกปฏิเสธ
- (๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการเสียหายหรือสูญหาย หรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูล
- (๖) กำหนดสิทธิการเข้าถึงอย่างรัดกุม
- (๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์ร่วมกัน

- (๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ที่มีความสำคัญ ได้แก่ กุญแจที่ใช้ในการเข้ารหัส เป็นต้น
- (๙) การบริหารจัดการการเข้าถึง รวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ให้เป็นไปตามความใน ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน ข้อ ๑๐ ข้อ ๑๒ ข้อ ๑๓ ข้อ ๑๔ ข้อ ๑๕ และ ข้อ ๑๖
- (๑๐) การสำรองข้อมูลข้อมูลที่ใช้ร่วมกัน ให้ทำความตกลงกันระหว่างหน่วยงาน
- (๑๑) บรรดาข้อกำหนดอื่นๆ นอกเหนือจากที่กล่าวมาข้างต้น การแก้ไข ปรับปรุงแนวปฏิบัติในการใช้งานฐานข้อมูลร่วมกันระหว่างองค์กร ให้ทำความตกลงกันระหว่างหน่วยงานนั้นๆ โดยไม่ขัดหรือแย้งกับแนวปฏิบัตินี้

ส่วนที่ ๒ การสำรองข้อมูล

- ข้อ ๖๗ จัดทำระบบสำรองข้อมูลระบบสารสนเทศที่สำคัญให้อยู่ในสภาพพร้อมใช้งานได้ตลอดเวลา ได้แก่ ระบบสารสนเทศอิเล็กทรอนิกส์ ระบบบริหารจัดการงบประมาณ ระบบสนับสนุนการตัดสินใจของผู้บริหาร (MIS) ระบบจอร์นการ/จองห้องประชุม ระบบลาการ ระบบวัสดุ/ครุภัณฑ์ เป็นต้น
- ข้อ ๖๘ จัดทำบัญชีระบบสารสนเทศทั้งหมดขององค์กรตามลำดับความสำคัญ และกำหนดระยะเวลาการสำรองข้อมูลที่เหมาะสม รวมทั้งจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง
- ข้อ ๖๙ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองและกู้คืนข้อมูลอย่างชัดเจน ตามรายละเอียดในเอกสารภาคผนวก ข. ข้อ ๖ และให้ทบทวนหน้าที่เมื่อมีการสับเปลี่ยน โยกย้ายตำแหน่งหรือลาออก
- ข้อ ๗๐ กำหนดความถี่ในการสำรองข้อมูลระบบสารสนเทศตามข้อ ๖๗ และข้อ ๖๘ หากระบบใดที่มีการเปลี่ยนแปลงบ่อยให้มีความถี่ในการสำรองมากขึ้น โดยวิธีกำหนดการสำรองข้อมูลดังนี้
 - (๑) กำหนดประเภทข้อมูลที่ต้องการทำสำรองข้อมูล และความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงโดยผู้ดูแลระบบ
 - (๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง
 - (๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินงาน วัน เวลา ขนาดของข้อมูลที่สำรอง สถานะการสำรอง (สำเร็จ/ผิดพลาด) เป็นต้น
 - (๔) ตรวจสอบค่า Configuration ต่างๆ ของระบบการสำรองข้อมูลอยู่เสมอ
 - (๕) จัดเก็บข้อมูลที่สำรองไว้ในสื่อเก็บข้อมูล โดยให้มีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น เพื่อแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบสำรองข้อมูลไว้อย่างชัดเจน
 - (๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ที่มีระยะทางระหว่างสถานที่จัดเก็บข้อมูลสำรองกับองค์กรต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับองค์กร
 - (๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

- (๘) ทดสอบระบบและข้อมูลที่สามารถสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- (๙) จัดทำขั้นตอนการสำรองและกู้คืนข้อมูลที่เสียหายจากที่ได้สำรองไว้อย่างถูกต้อง ครอบคลุมทั้งฮาร์ดแวร์และซอฟต์แวร์
- (๑๐) ทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม โดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น
- (๑๑) การสำรองและการกู้คืนข้อมูลทุกระบบ ต้องบันทึกไว้เป็นเอกสารและมีการตรวจสอบความถูกต้องเป็นระยะๆ
- (๑๒) ต้องตรวจสอบการจัดเก็บสื่อบันทึกข้อมูล ณ สถานที่จัดเก็บข้อมูลสำรองเป็นประจำทุกปี อย่างน้อยปีละ ๑ ครั้ง
- (๑๓) กำหนดให้เข้ารหัสกับข้อมูลลับที่ได้สำรองไว้ (Encryption)
- (๑๔) สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนตามอายุการใช้งาน ตามประเภทของสื่อ
- (๑๕) ต้องจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ให้สามารถกู้คืนระบบกลับคืนมาได้ภายในระยะเวลาที่กำหนด

ข้อ ๗๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ ตามรายละเอียดในภาคผนวก ข. ข้อ ๓ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติและต่อเนื่อง โดยต้องปรับปรุงแผนดังกล่าวให้สอดคล้องกับสถานการณ์และการใช้งานตามภารกิจ ซึ่งครอบคลุมหัวข้อดังนี้

- (๑) หน้าที่ความรับผิดชอบ การติดต่อสื่อสารกับผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบสารสนเทศ ให้เป็นไปตามภาคผนวก ข. ข้อ ๖
- (๒) ประเมินความเสี่ยงระบบสารสนเทศที่มีความสำคัญ และกำหนดมาตรการลดความเสี่ยงเหล่านั้น ได้แก่ ความเสี่ยงเมื่อเกิดกระแสไฟฟ้าดับเป็นเวลานาน อักขัยฮาร์ดแวร์ การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้งานระบบได้
- (๓) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และการกู้คืนข้อมูลที่สำรองไว้
- (๔) กำหนดขั้นตอนทดสอบการเข้าถึงข้อมูลที่สำรองไว้ชัดเจน
- (๕) กำหนดช่องทางติดต่อกับผู้ให้บริการภายนอกเมื่อเกิดเหตุจำเป็นที่ต้องติดต่อ ได้แก่ ผู้ให้บริการเครือข่าย ผู้ให้บริการด้านฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น
- (๖) สร้างความรู้ ความตระหนักแก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ รวมถึงสิ่งที่ต้องทำเมื่อเกิดเหตุฉุกเฉิน

ข้อ ๗๒ มีการทบทวน ปรับปรุง แผนเตรียมความพร้อมกรณีฉุกเฉิน ตามข้อ ๗๐ และข้อ ๗๑ ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับสถานการณ์และการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗๓ กำหนดให้ทดสอบสภาพความพร้อมของระบบสารสนเทศ ระบบสำรอง และระบบเตรียมความพร้อมฉุกเฉิน เพื่อประเมินความเสี่ยงที่ยอมรับได้ของแต่ละสถาบัน/สำนัก/กอง อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ
๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักเทคโนโลยีสารสนเทศ
๒. ผู้ตรวจสอบภายในขององค์กร
๓. ผู้ตรวจสอบอิสระจากภายนอก
๔. ผู้ดูแลระบบ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ข้อ ๗๔ สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบสารสนเทศ ร่วมกับกลุ่มตรวจสอบภายในขององค์กร (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง และโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอกองค์กร (External Auditor) อย่างน้อย ๒ ปี/ครั้ง เพื่อให้องค์กรได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

- (๑) ทบทวนกระบวนการบริหารจัดการความเสี่ยง
- (๒) ทบทวนนโยบายและแนวปฏิบัติ และมาตรการในการรักษาความมั่นคงปลอดภัยสารสนเทศ
- (๓) ศึกษาข้อมูล รวมถึงข้อดี ข้อเสีย และหาวิธีดำเนินการลดความเสี่ยง
- (๔) สรุปผล เสนอแนะแนวทางเพื่อลดความเสี่ยงที่ตรวจพบ

ข้อ ๗๕ ผู้ตรวจสอบจัดทำรายงานความเสี่ยงที่ตรวจพบ พร้อมข้อเสนอแนะรายงานต่อผู้บริหารระดับสูงสุดทราบ

ข้อ ๗๖ มาตรการในการตรวจประเมินระบบสารสนเทศต้องมียังน้อย ดังนี้

- (๑) กำหนดสิทธิผู้ตรวจสอบให้สามารถเข้าถึงข้อมูลที่เป็นต้องตรวจสอบได้ตามข้อ ๑๘ (๒) แบบอ่านอย่างเดียว แต่สามารถเข้าถึงข้อมูลตามข้อ ๑๙ (๑) (๓) (๔) ได้
- (๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในรูปแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบข้อมูลนั้นโดยทันทีที่ตรวจสอบเสร็จสิ้น
- (๓) ให้จัดสรรทรัพยากรที่จำเป็นที่ต้องใช้ในการตรวจสอบระบบ

- (๔) ในกรณีที่มีเครื่องมือสำหรับตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งออกจากระบบสารสนเทศที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและให้มีการจัดเก็บ ป้องกันเครื่องมือนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวดที่ ๔

การสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้บุคลากรขององค์กรได้รับทราบ เข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง เหมาะสม
๒. เพื่อป้องกันและลดการกระทำผิดที่เกิดขึ้นจากการใช้งานระบบสารสนเทศโดยไม่คาดคิด

ผู้รับผิดชอบ

๑. สำนักเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบ
๓. ผู้ใช้งาน

ส่วนที่ ๑ การทบทวนนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๗๗ สำนักเทคโนโลยีสารสนเทศต้องดำเนินการเสนอให้ทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้เป็นปัจจุบัน ทันเหตุการณ์อยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๒ การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้ใช้งาน

ข้อ ๗๘ ให้สำนักเทคโนโลยีสารสนเทศ จัดการให้ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้ใช้งาน โดยจัดหลักสูตรการฝึกอบรม สัมมนา โดยเสริมเนื้อหาตามแนวปฏิบัติเข้ากับหลักสูตรการฝึกอบรม อย่างน้อยปีละ ๑ ครั้ง ให้มีการรับรองบุคคลผู้ผ่านการผ่านหลักสูตรการฝึกอบรมดังกล่าวด้วย

ข้อ ๗๙ จัดทำและเผยแพร่ประชาสัมพันธ์ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ข้อควรระมัดระวัง วิธีการใช้งานสารสนเทศอย่างถูกวิธี ในลักษณะเกร็ดความรู้ อินโฟกราฟิก (Info graphic) หรือรูปแบบอื่นที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย และมีการเปลี่ยนเกร็ดความรู้ใหม่ๆ อยู่เสมอ

ข้อ ๘๐ จัดทำคู่มือการให้บริการระบบเทคโนโลยีสารสนเทศอย่างปลอดภัยสำหรับผู้ใช้งาน คู่มือสำหรับผู้ดูแลระบบ แจกจ่ายและเผยแพร่ทางระบบอินทราเน็ตขององค์กร

ข้อ ๘๑ สำนักเทคโนโลยีสารสนเทศต้องสร้างการมีส่วนร่วมไปสู่ภาคปฏิบัติ วิธีการกำกับติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน อย่างน้อยที่สุดปีละ ๑ ครั้ง พร้อมสรุปรายงานผู้บริหารระดับสูงสุด เพื่อหาแนวทางพัฒนาปรับปรุงระบบต่อไป

ข้อ ๘๒ ผู้ดูแลระบบต้องสร้างความความรู้ความเข้าใจเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ เพื่อให้ผู้ใช้งานตระหนักและสามารถดำเนินการป้องกันด้วยตนเองได้ รวมถึงจัดทำและเผยแพร่ขั้นตอนปฏิบัติเมื่อพบโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์

ข้อ ๘๓ นอกจากแนวปฏิบัตินี้ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งระเบียบ ประกาศ ของสำนักงานกิจการยุติธรรม และข้อตกลงระหว่างประเทศอย่างเคร่งครัด (ถ้ามี) ทั้งนี้ หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายที่เกี่ยวข้องถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งหากเกิดความเสียหาย ผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นนั่นเอง

หมวดที่ ๕

หน้าที่ความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ เจ้าหน้าที่ ผู้ใช้งาน ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศให้ชัดเจน

ผู้รับผิดชอบ

๑. ผู้บริหารระดับสูงสุด
๒. ผู้ดูแลระบบ
๓. ผู้ใช้งาน

ข้อ ๘๔ การกำหนดนโยบายและแนวปฏิบัติเพิ่มเติม การแก้ไข การให้ข้อเสนอแนะ การให้คำปรึกษา การติดตามกำกับดูแล การควบคุมการปฏิบัติงาน ตลอดจนความเสี่ยง ความเสียหาย และอันตรายที่เกิดขึ้นกับระบบสารสนเทศของสำนักงานกิจการยุติธรรม กำหนดให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบทั้งหมด

ข้อ ๘๕ ผู้ดูแลระบบต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติที่ผู้บริหารระดับสูงสุดกำหนดหรือแก้ไขเพิ่มเติม ซึ่งต้องไม่ขัดต่อกฎหมายและศีลธรรมอันดีของประเทศ

ข้อ ๘๖ ผู้ใช้งานต้องรับผิดชอบในการพิทักษ์ รักษา สินทรัพย์ขององค์กรประดุจเป็นของตนเอง และดำรงไว้ซึ่งสภาพพร้อมใช้งานอยู่เสมอ ไม่กระทำการใดๆ ที่ผิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

ข้อ ๘๗ เมื่อเกิดปัญหาหรือข้อขัดแย้งในการปฏิบัติตามนโยบายและแนวปฏิบัตินี้ ให้ผู้บริหารระดับสูงสุดวินิจฉัยชี้ขาด และให้ถือคำวินิจฉัยนั้นเป็นแนวปฏิบัติต่อไป

หมวดที่ ๖

บทกำหนดโทษ

วัตถุประสงค์

เพื่อกำหนดบทลงโทษแก่เจ้าหน้าที่ผู้ใช้งานระบบสารสนเทศในทางที่ก่อให้เกิดความเสียหายแก่ระบบสารสนเทศขององค์กร

ข้อ ๘๘ หากพบว่าบุคลากรของสำนักงานกิจการยุติธรรมผู้ใดฝ่าฝืน ละเว้น ไม่ปฏิบัติตามนโยบายและแนวทางปฏิบัติข้างต้น จะต้องถูกลงโทษ ดังนี้

(๑) ตักเตือน

(๒) ภาคทัณฑ์

ข้อ ๘๙ ข้าราชการมีโทษทางวินัยร้ายแรง พนักงานราชการและลูกจ้างชั่วคราวมีโทษทางวินัยสูงสุดถึงขั้นเลิกจ้าง

ข้อ ๙๐ บุคคลภายนอกผู้ใดกระทำการ อันได้แก่ เปิดเผยข้อมูล เปิดเผยมาตรการป้องกัน ดักจับข้อมูล กระทำต่อโครงสร้างสำคัญของข้อมูล แก้ไขเปลี่ยนแปลง ซะลอ หรือขัดขวางการทำงานของระบบ ไม่ว่าจะกระทำโดยเจตนาหรือไม่ก็ตาม รวมถึงการกระทำละเมิดอื่นใดกับระบบสารสนเทศและทรัพย์สินของสำนักงานกิจการยุติธรรม จะต้องถูกดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้อง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานกิจการยุติธรรมฉบับนี้ ได้ผ่านการพิจารณาจากผู้อำนวยการสำนักงานกิจการยุติธรรม เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ให้เจ้าหน้าที่ทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

ประกาศ ณ วันที่ ๒๕ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๑

(นายวัลลภ นาคบัว)

ผู้อำนวยการสำนักงานกิจการยุติธรรม