บันทึกข้อความ

ส่วนราชการ สำนักงานบริหารกิจการ อส. สำนักเทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐ ๒๕๑๕ ๔๑๗๖
ที่ อส ๐๐๐๑.๑(ทส)/ว ๑ **วันที่** ๒๙ เมษายน ๒๕๖๒
เรื่อง ประกาศสำนักงานอัยการสูงสุด เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

เรียน รองอัยการสูงสุด ผู้ตรวจการอัยการ อธิบดีอัยการ อธิบดีอัยการภาค อัยการพิเศษฝ่าย เลขานุการอัยการสูงสุด อัยการจังหวัด ผู้อำนวยการสำนักงานกิจการและโครงการในพระดำริพระเจ้าหลานเธอพระองค์เจ้าพัชรกิติยาภา และผู้อำนวยการสำนักงาน

สำนักงานอัยการสูงสุดได้ปฏิบัติตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยมีสำนักเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) เป็นหน่วยงานที่รับผิดชอบการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานอัยการสูงสุด และได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร เสนอและได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มาตั้งแต่ปีงบประมาณ พ.ศ. ๒๕๖๑ และในปี พ.ศ. ๒๕๖๒ สำนักงานอัยการสูงสุดจึงได้เสนอขอทบทวนนโยบายและแนวปฏิบัติฯ เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ ข้อ ๓ (๔) และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) ได้มีมติเห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒ ในการประชุมครั้งที่ ๒/๒๕๖๒ เมื่อวันที่ ๒๖ มีนาคม ๒๕๖๒ แล้วนั้น

ดังนั้น เพื่อให้บุคลากรของสำนักงานอัยการสูงสุดและผู้มีส่วนเกี่ยวข้องทราบ และให้หน่วยงานภายในสังกัดสำนักงานอัยการสูงสุดปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปในทิศทางเดียวกัน จึงได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒ มาพร้อมนี้และให้ถือปฏิบัติอย่างเคร่งครัด โดยสามารถดาวน์โหลดเอกสารได้ที่เว็บไซต์ http://www.ictc.ago.go.th/new_ictc๒/ict_law.php รายละเอียดปรากฏตามประกาศแนบท้ายนี้

จึงเรียนมาเพื่อโปรดทราบ และแจ้งให้บุคลากรในสังกัดทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

(นายเชิดศักดิ์ หิรัญสิริสมบัติ)
รองอัยการสูงสุด ปฏิบัติราชการแทน
อัยการสูงสุด

ประกาศสำนักงานอัยการสูงสุด
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

.....

เพื่อให้ระบบสารสนเทศของสำนักงานอัยการสูงสุดมีความมั่นคงปลอดภัย และมิให้ผู้กระทำด้วยประการใด ๆ ให้ระบบเทคโนโลยีสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่น ในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จ หรือมีลักษณะอันลามกอนาจาร ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงานอัยการสูงสุด ซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้อง จึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และด้วยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานอัยการสูงสุดจึงได้ออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานอัยการสูงสุด เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศให้ความเห็นชอบแนวนโยบายและแนวปฏิบัติเป็นต้นไป

ข้อ ๓ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้วซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๔ คำนิยาม ประกอบด้วย

(๑) หน่วยงาน หมายความว่า สำนักงานอัยการสูงสุด ทั้งนี้ให้หมายรวมถึงหน่วยงานในสังกัด

(๒) ผู้บริหารระดับสูงสุด หมายความว่า อัยการสูงสุด

(๓) ผู้บริหารระดับสูง หมายความว่า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

(๔) ผู้บริหารเหนือขึ้นไป ๑ ระดับ หมายความว่า ผู้อำนวยการสำนักงานบริหารกิจการสำนักงานอัยการสูงสุด

(๕) ผู้อำนวยการ หมายความว่า ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

(๖) ผู้ดูแลระบบ (Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้อำนวยการให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

(๗) หัวหน้าหน่วยงาน หมายความว่า พนักงานอัยการที่เป็นหัวหน้าในท้องที่ตั้งสำนักงานอัยการจังหวัด ตามพระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ กำหนด

(๘) ผู้ใช้งาน (User) หมายความว่า บุคคลที่ได้รับอนุญาตให้เข้าถึงและมีรหัสผ่านเพื่อให้สามารถเข้าใช้งานเครือข่ายผ่านระบบการพิสูจน์ยืนยันตัวตน (Authentication) หรือระบบการดูแลรักษาระบบสารสนเทศของหน่วยงาน โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่สำนักงานอัยการสูงสุดกำหนด

(๙) บุคคลภายนอก หมายความว่า บุคคลหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล โดยปฏิบัติงานอยู่ในความดูแลของผู้ดูแลระบบ

(๑๐) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศที่สำนักงานอัยการสูงสุดกำหนดให้เข้าถึงระบบเครือข่ายนั้น

(๑๑) บัญชีผู้ใช้งาน (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

(๑๒) รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๑๓) สื่อบันทึกพกพา หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy disk เป็นต้น

(๑๔) สินทรัพย์ (Asset) หมายความว่า เครื่องคอมพิวเตอร์ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลสารสนเทศ ระบบเครือข่าย ระบบสารสนเทศหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน

(๑๕) ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสนับสนุนการปฏิบัติงานและสามารถนำข้อมูลที่ได้มาใช้ประโยชน์ในการวางแผนงาน การตัดสินใจ ควบคุมการติดต่อสื่อสาร และสนับสนุนทางการบริหาร ประกอบด้วย ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลสารสนเทศ เป็นต้น

(๑๖) ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๑๗) เครือข่าย (network) หมายความว่า กลุ่มของคอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่าง ๆ ที่นำมาเชื่อมต่อกันเพื่อให้ผู้ใช้งานในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและใช้อุปกรณ์ต่าง ๆ ร่วมกันในเครือข่ายได้ โดยช่องทางที่ใช้ในการติดต่อสื่อสารกัน เรียกว่า ช่องสัญญาณ (communication channel)

(๑๘) ระบบเครือข่ายไร้สาย (Wireless LAN : WLAN) หมายความว่า เทคโนโลยีที่ช่วยให้การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ ๒ เครื่อง เป็นการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์โดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทนการรับส่งข้อมูลระหว่างกันจะผ่านอากาศ ทำให้ไม่ต้องเดินสายสัญญาณและติดตั้งใช้งานได้สะดวกขึ้น

(๑๙) คอมพิวเตอร์แม่ข่าย หมายความว่า คอมพิวเตอร์ที่ทำหน้าที่เป็นผู้ให้บริการทรัพยากร (Resources) ต่าง ๆ ซึ่งได้แก่ หน่วยประมวลผล หน่วยความจำ หน่วยความจำสำรอง ฐานข้อมูล โปรแกรมต่าง ๆ เป็นต้น ในระบบเครือข่ายภายใน (LAN) ซึ่งทำหน้าที่เป็นตัวกลางในการเชื่อมต่อกับเครื่องลูกข่าย

(๒๐) การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าถึงระบบสารสนเทศของหน่วยงานเป็นขั้นตอนในการพิสูจน์ยืนยันตัวตนของผู้ใช้งาน จะเป็นการพิสูจน์ยืนยันตัวตนโดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ก่อนเข้าใช้งานระบบเครือข่าย

(๒๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศของหน่วยงานทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๒๒) เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๒๓) ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

ทั้งนี้ เพื่อป้องกันการสูญเสีย สูญหาย การถูกขโมย การเข้าถึงหรือการเปิดเผยโดยไม่ได้รับอนุญาต การปลอมแปลง การปฏิเสธความรับผิดหรือการกระทำใดก็ตามที่ก่อให้เกิดความเสียหายต่อความลับ (confidentiality) กล่าวคือ สินทรัพย์ของหน่วยงานจะต้องสามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น ความถูกต้องครบถ้วน (Integrity) กล่าวคือ สินทรัพย์ของหน่วยงานจะต้องมีความถูกต้องครบถ้วนและสมบูรณ์ การเปลี่ยนแปลงสามารถทำได้แต่ต้องโดยผู้ที่ได้รับอนุญาตเท่านั้น ความพร้อมใช้ (availability) กล่าวคือ สินทรัพย์ของหน่วยงานจะต้องสามารถเข้าถึงและพร้อมใช้งานได้ดีตลอดเวลา

(๒๔) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๒๕) จดหมายอิเล็กทรอนิกส์ (e-Mail) หมายความว่า ช่องทางที่ใช้ในการรับ-ส่งข้อความอิเล็กทรอนิกส์ระหว่างกันผ่านระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนได้ โดยมาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP

(๒๖) ไวรัสหรือชุดคำสั่งไม่พึงประสงค์ หมายความว่า รหัสคอมพิวเตอร์ที่ฝังตัวเองในไฟล์หรือโปรแกรมใดก็ตามที่จะแพร่กระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งผ่านทางเครือข่ายสาธารณะ หรือเข้ามาโดยไม่ได้รับอนุญาตหรือโดยไม่รู้ตัว และทำความเสียหายแก่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศต่าง ๆ อาจสร้างความรำคาญ ทำให้เครื่องคอมพิวเตอร์ทำงานช้าหรือทำงานผิดปกติหรือทำงานในลักษณะที่ไม่เป็นประโยชน์ ไม่สร้างสรรค์หรือไม่เป็นผลดีต่อเครื่องคอมพิวเตอร์นั้น ซึ่งความรุนแรงในการก่อความเสียหายอาจแตกต่างกันตามแต่ชนิดของไวรัสหรือชุดคำสั่งไม่พึงประสงค์นั้น

(๒๗) ห้องศูนย์ข้อมูล (Data Center) หมายความว่า สถานที่ติดตั้งอุปกรณ์เครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายคอมพิวเตอร์ (Server) ของหน่วยงาน

ข้อ ๕ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้มี ๒ ส่วน ดังนี้

๕.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๖.๑

๕.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๖.๒

"นโยบาย" หมายความว่า หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ที่สำนักงานอัยการสูงสุดได้จัดทำไว้ เพื่อให้บริการแก่ประชาชนผู้มีส่วนได้ส่วนเสียหรือเจ้าหน้าที่ ซึ่งได้ประกาศไว้ให้เจ้าหน้าที่และผู้ใช้งานที่เกี่ยวข้องในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุดได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน และเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

"แนวปฏิบัติ" หมายความว่า ขั้นตอนวิธีการที่สำนักงานอัยการสูงสุดได้กำหนดให้เจ้าหน้าที่และผู้ใช้งานได้พึงใช้เป็นแนวทางในการปฏิบัติงานที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมุ่งเน้นให้สำนักงานอัยการสูงสุดมีแนวทางปฏิบัติในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย และไม่ขัดต่อแนวนโยบายและแนวปฏิบัติตามประกาศนี้

ข้อ ๖ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ได้กำหนดประเด็นสำคัญดังต่อไปนี้

๖.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกทางเว็บไซต์ของสำนักงานอัยการสูงสุด

(๒) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๓) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๖.๒ ส่วนที่ว่าด้วยรายละเอียดของแนวปฏิบัติ

(๑) การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

๑.๑. การเข้าถึงระบบเทคโนโลยีสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตการเข้าถึงทุกขั้นตอนตั้งแต่การลงทะเบียนผู้ใช้งานใหม่ (User Registration) การเปลี่ยนแปลงสถานภาพต่าง ๆ ไปจนถึงการเพิกถอนสิทธิผู้ใช้งาน โดยนโยบาย ขั้นตอนการปฏิบัติงานและวิธีการปฏิบัติงานต่าง ๆ ต้องครอบคลุมและบังคับใช้กับสารสนเทศและทุกระบบที่อยู่ภายใต้ขอบเขตของสำนักงานอัยการสูงสุด เพื่อให้ผู้ใช้งานได้รับทราบ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และต้องจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑.๒. การควบคุมการเข้าถึงเครือข่าย ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ยืนยันตัวตนทุกครั้งเมื่อทำการ Log on เข้าสู่ระบบ เพื่อป้องกันการเข้าถึงเครือข่ายของสำนักงานอัยการสูงสุดโดยไม่ได้รับอนุญาต ด้วยการกำหนดสิทธิในการเข้าถึงโดยแสดงตัวตนด้วยบัญชีผู้ใช้งาน (Username) ซึ่งจะต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) ก่อนการเข้าใช้งานเครือข่าย และสำนักเทคโนโลยีสารสนเทศและการสื่อสารจะกำหนดเส้นทางการเชื่อมต่อและการเข้าถึงโดยผ่านระบบรักษาความมั่นคงปลอดภัยตามที่ได้กำหนดไว้ เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๑.๓. การควบคุมการเข้าถึงระบบงาน เพื่อป้องกันการเข้าถึงระบบงานต่าง ๆ ของสำนักงานอัยการสูงสุดโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิการเข้าถึงเมื่อทำการเข้าสู่ระบบงาน (Login) โดยแสดงตัวตนด้วยบัญชีผู้ใช้งาน (Username) และพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน (Password) ก่อนการเข้าใช้งานระบบงานต่าง ๆ และกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันไวรัสหรือชุดคำสั่งไม่พึงประสงค์

๑.๔. การควบคุมการเข้าถึงโปรแกรมประยุกต์ (Application) รวมถึงจดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบเครือข่ายภายใน (Intranet) ผู้ใช้งานจะต้องได้รับการพิสูจน์ตัวตน (Authentication) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบของหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ

(๒) มีระบบสารสนเทศและระบบสำรองข้อมูล เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุดสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ ต้องจัดทำระบบเทคโนโลยีสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา และจัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ (IT Contingency Plan) พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ และต้องทบทวนอย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือต่อเหตุฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยสำนักงานอัยการพิเศษฝ่ายประเมินผล และสำนักงานตรวจสอบภายใน หรือหน่วยงานที่ได้รับมอบหมายจากสำนักงานอัยการสูงสุด ในการตรวจสอบงบประมาณดำเนินโครงการด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

(๔) การสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ด้วยวิธีการจัดทำคู่มือ เผยแพร่นโยบายและแนวปฏิบัติฯ ผ่านทางเว็บไซต์ และจัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๗ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ให้เป็นไปตามที่กำหนดไว้ใน ***แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒***

ข้อ ๘ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๙ ให้อัยการสูงสุด ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบในการบริหารความเสี่ยง ควบคุมความเสียหายหรืออันตรายที่เกิดขึ้นในกรณีระบบเทคโนโลยีสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๐ ให้ผู้บริหารระดับสูง มีหน้าที่กำกับดูแลด้านเทคโนโลยีสารสนเทศ และผู้อำนวยการเป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด โดยมีผู้บริหารเหนือขึ้นไป ๑ ระดับ คอยกำกับและติดตาม ดูแล ควบคุม ตรวจสอบ รวมทั้งให้คำแนะนำแก่ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ข้อ ๑๑ ให้สำนักเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติฯ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ การกระทำใด ๆ ที่เกิดจากการใช้งานระบบสารสนเทศของสำนักงานอัยการสูงสุด อันมีกฎหมายกำหนดให้เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประกอบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ผู้ใช้งานจะรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๓ ให้บุคลากรของสำนักงานอัยการสูงสุดทุกหน่วยงานถือปฏิบัติในส่วนที่เกี่ยวข้องตามนโยบายฯ ฉบับดังกล่าวที่แนบท้ายประกาศฉบับนี้อย่างเคร่งครัด

ประกาศ ณ วันที่ ๒๙ เมษายน พ.ศ. ๒๕๖๒

(นายเข็มชัย ชุติวงศ์)
อัยการสูงสุด

สำนักงานอัยการสูงสุด

Electronic Transactions Commission

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานอัยการสูงสุด
พ.ศ. ๒๕๖๒

ผ่านความเห็นชอบโดย
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ส[illegible] ๒๕๖๒

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ มีความมั่นคงปลอดภัย เชื่อถือได้ สำนักงานอัยการสูงสุดจึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๐ เสนอขอรับการพิจารณาเพื่อประกาศเป็นกฎหมายของสำนักงานอัยการสูงสุด และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้เห็นชอบต่อนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด เมื่อวันที่ ๒๕ กันยายน ๒๕๖๐ (การประชุมครั้งที่ ๕/๒๕๖๐) แต่เนื่องจากตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ข้อ ๓ กำหนดให้หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวและต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง และต้องประกาศนโยบายและข้อปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึงเข้าใจและปฏิบัติตามนโยบายและข้อปฏิบัติได้

ดังนั้น เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ของสำนักงานอัยการสูงสุดมีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายกำหนดและปฏิบัติตามระเบียบปฏิบัติที่เกี่ยวข้อง อย่างไรก็ตามต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯ จากบุคลากรและผู้เกี่ยวข้องทั้งหมด มีการปรับปรุงและตรวจสอบอย่างสม่ำเสมอเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว จึงหวังเป็นอย่างยิ่งว่าประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของสำนักงานอัยการสูงสุดทุกคน ถือปฏิบัติโดยเคร่งครัดต่อไป

กลุ่มแผนงานเทคโนโลยีสารสนเทศ
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานอัยการสูงสุด

สารบัญ

เอกสารแนบท้ายประกาศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. หลักการและเหตุผล

ตามประกาศในราชกิจจานุเบกษา หน้าที่ ๘ เล่ม ๑๓๓ ตอนพิเศษ ๑๘๙ ง ลงวันที่ ๒๕ สิงหาคม ๒๕๕๙ กำหนดให้สำนักงานอัยการสูงสุดเป็นหน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ในปีงบประมาณ พ.ศ. ๒๕๖๑ สำนักงานอัยการสูงสุดได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ที่กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร และเมื่อวันที่ ๒๕ กันยายน ๒๕๖๐ (การประชุมครั้งที่ ๕/๒๕๖๐) คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๐ ตามหนังสือที่ ดศ ๐๒๐๗/๘๖๑๐ ลงวันที่ ๕ ตุลาคม ๒๕๖๐ แล้วนั้น แต่เนื่องจากตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ข้อที่ ๓ หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน และต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุดมีการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีระบบสำรองให้อยู่ในสภาพพร้อมใช้งานและมีความมั่นคงปลอดภัย รวมถึงการป้องกันปัญหาอื่นที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศที่ไม่ถูกต้องหรือจากภัยคุกคามต่าง ๆ จากผู้ไม่ประสงค์ดี จึงต้องทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒ ให้เป็นปัจจุบันตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๒. วัตถุประสงค์

๒.๑ เพื่อปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุดให้เป็นปัจจุบัน

๒.๒ เพื่อปฏิบัติตามกฎหมาย พระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ ที่เกี่ยวข้องในเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๓ เพื่อให้ผู้ใช้งานและบุคลากรของสำนักงานอัยการสูงสุดได้รับทราบและถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด

๓. คำนิยาม

หน่วยงาน หมายความว่า สำนักงานอัยการสูงสุด ทั้งนี้ให้หมายรวมถึงหน่วยงานในสังกัด

ผู้บริหารระดับสูงสุด หมายความว่า อัยการสูงสุด

ผู้บริหารระดับสูง หมายความว่า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

ผู้บริหารเหนือขึ้นไป ๑ ระดับ หมายความว่า ผู้อำนวยการสำนักงานบริหารกิจการสำนักงานอัยการสูงสุด

ผู้อำนวยการ หมายความว่า ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้ดูแลระบบ (Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้อำนวยการให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

หัวหน้าหน่วยงาน หมายความว่า พนักงานอัยการที่เป็นหัวหน้าในท้องที่ตั้งสำนักงานอัยการจังหวัดตามพระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ กำหนด

ผู้ใช้งาน (User) หมายความว่า บุคคลที่ได้รับอนุญาตให้เข้าถึงและมีรหัสผ่านเพื่อให้สามารถเข้าใช้งานเครือข่ายผ่านระบบการพิสูจน์ยืนยันตัวตน (Authentication) หรือระบบการดูแลรักษาระบบสารสนเทศของหน่วยงาน โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่สำนักงานอัยการสูงสุดกำหนด

บุคคลภายนอก หมายความว่า บุคคลหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล โดยปฏิบัติงานอยู่ในความดูแลของผู้ดูแลระบบ

สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไปสิทธิจำเพาะสิทธิพิเศษและสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศที่สำนักงานอัยการสูงสุดกำหนดให้เข้าถึงระบบเครือข่ายนั้น

บัญชีผู้ใช้งาน (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้น เพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

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

สินทรัพย์ (Asset) หมายความว่า เครื่องคอมพิวเตอร์ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลสารสนเทศ ระบบเครือข่าย ระบบสารสนเทศหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน

ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสนับสนุนการปฏิบัติงานและสามารถนำข้อมูลที่ได้มาใช้ประโยชน์ในการวางแผนงาน การตัดสินใจ ควบคุมการติดต่อสื่อสาร และสนับสนุนทางการบริหารประกอบด้วย ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลสารสนเทศ เป็นต้น

ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

เครือข่าย (network) หมายความว่า กลุ่มของคอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่าง ๆ ที่นำมาเชื่อมต่อกันเพื่อให้ผู้ใช้งานในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและใช้อุปกรณ์ต่าง ๆ ร่วมกันในเครือข่ายได้ โดยช่องทางที่ใช้ในการติดต่อสื่อสารกันเรียกว่า ช่องสัญญาณ (communication channel)

ระบบเครือข่ายไร้สาย (Wireless LAN : WLAN) หมายความว่า เทคโนโลยีที่ช่วยให้การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ ๒ เครื่อง เป็นการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์โดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทนการรับส่งข้อมูลระหว่างกันจะผ่านอากาศ ทำให้ไม่ต้องเดินสายสัญญาณและติดตั้งใช้งานได้สะดวกขึ้น

คอมพิวเตอร์แม่ข่าย หมายความว่า คอมพิวเตอร์ที่ทำหน้าที่เป็นผู้ให้บริการทรัพยากร (Resources) ต่าง ๆ ซึ่งได้แก่ หน่วยประมวลผล หน่วยความจำ หน่วยความจำสำรอง ฐานข้อมูล โปรแกรมต่าง ๆ เป็นต้น ในระบบเครือข่ายภายใน (LAN) ซึ่งทำหน้าที่เป็นตัวกลางในการเชื่อมต่อกับเครื่องลูกข่าย

การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าถึงระบบสารสนเทศของหน่วยงานเป็นขั้นตอนในการพิสูจน์ยืนยันตัวตนของผู้ใช้งาน จะเป็นการพิสูจน์ยืนยันตัวตนโดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ก่อนเข้าใช้งานระบบเครือข่าย

การเข้าถึงและควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศของหน่วยงานทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

ทั้งนี้ เพื่อป้องกันการสูญเสีย สูญหาย การถูกขโมย การเข้าถึงหรือการเปิดเผยโดยไม่ได้รับอนุญาต การปลอมแปลง การปฏิเสธความรับผิดหรือการกระทำใดก็ตามที่ก่อให้เกิดความเสียหายต่อความลับ (confidentiality) กล่าวคือ สินทรัพย์ของหน่วยงานจะต้องสามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้นความถูกต้องครบถ้วน (Integrity) กล่าวคือ สินทรัพย์ของหน่วยงานจะต้องมีความถูกต้องครบถ้วนและสมบูรณ์การเปลี่ยนแปลงสามารถทำได้แต่ต้องโดยผู้ที่ได้รับอนุญาตเท่านั้นความพร้อมใช้ (availability) กล่าวคือ สินทรัพย์ของหน่วยงานจะต้องสามารถเข้าถึงและพร้อมใช้งานได้ตลอดเวลา

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (e-Mail) หมายความว่า ช่องทางที่ใช้ในการรับ-ส่งข้อความอิเล็กทรอนิกส์ระหว่างกันผ่านระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนได้โดยมาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP

ไวรัสหรือชุดคำสั่งไม่พึงประสงค์ หมายความว่า รหัสคอมพิวเตอร์ที่ฝังตัวเองในไฟล์หรือโปรแกรมใดก็ตามที่จะแพร่กระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งผ่านทางเครือข่ายสาธารณะ หรือเข้ามาโดยไม่ได้รับอนุญาตหรือโดยไม่รู้ตัว และทำความเสียหายแก่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศต่าง ๆ อาจสร้างความรำคาญ ทำให้เครื่องคอมพิวเตอร์ทำงานช้าหรือทำงานผิดปกติหรือทำงานในลักษณะที่ไม่เป็นประโยชน์ ไม่สร้างสรรค์หรือไม่เป็นผลดีต่อเครื่องคอมพิวเตอร์นั้น ซึ่งความรุนแรงในการก่อความเสียหายอาจแตกต่างกันตามแต่ชนิดของไวรัสหรือชุดคำสั่งไม่พึงประสงค์นั้น

ห้องศูนย์ข้อมูล (Data Center) หมายความว่า สถานที่ติดตั้งอุปกรณ์เครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายคอมพิวเตอร์ (Server) ของหน่วยงาน

หมวด ๑
นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่าย จากโปรแกรมชุดคำสั่งที่ไม่ประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลสารสนเทศหรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ยืนยันตัวตนได้อย่างถูกต้อง โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ผู้ใช้งานเข้าใจและปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และให้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน จำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ บริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และบันทึกรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศให้ผู้อำนวยการทราบทันที และกำหนดขั้นตอนขอบเขตของการปฏิบัติงานเพื่อตอบสนองต่อสถานการณ์ที่เกิดขึ้นได้อย่างรวดเร็ว มีระเบียบและประสิทธิภาพ และหากขั้นตอนการดำเนินงานใดที่เกี่ยวข้องทางกฎหมายต้องรวบรวม จัดเก็บและนำเสนอหลักฐานให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

๑.๓ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูงหรือผู้อำนวยการแล้วแต่กรณี เพื่อให้ความเห็นชอบและอนุญาตก่อน โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิตามอนุญาตนั้น ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

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

๑.๔ ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศ และปฏิบัติงานตามผู้อำนวยการมอบหมาย ดังนี้

(๑) อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำได้ต่อเมื่อได้รับอนุญาตจากผู้อำนวยการเท่านั้น

(๒) กำหนดสิทธิของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิการเข้าถึงนั้นอย่างสม่ำเสมอ

(๓) จัดทำ "ทะเบียนผู้มีสิทธิเข้าออกพื้นที่" เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

(๔) ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

๑.๕ ผู้ดูแลระบบต้องควบคุมการเข้า-ออกพื้นที่ควบคุมของห้องศูนย์ข้อมูล (Data Center) ดังนี้

(๑) ทำความเข้าใจและประชาสัมพันธ์ให้แก่ผู้ใช้งาน (Users) และบุคคลภายนอกเพื่อให้เข้าใจกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ในระหว่างที่ปฏิบัติงานอยู่ในห้องศูนย์ข้อมูลและบริเวณที่มีความสำคัญ และต้องไม่นำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณห้องศูนย์ข้อมูล (Data Center)

(๒) ไม่อนุญาตให้ผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูลและบริเวณที่มีความสำคัญ เว้นแต่ได้รับการอนุญาต กรณีมีความจำเป็นให้ผู้ดูแลระบบตรวจสอบเหตุผล วัตถุประสงค์และความจำเป็นโดยละเอียดก่อนเสนอขออนุญาตจากผู้อำนวยการทุกครั้ง

(๓) การบันทึกข้อมูลการเข้า-ออกพื้นที่ห้องศูนย์ข้อมูลและบริเวณที่มีความสำคัญ เพื่อใช้ตรวจสอบในภายหลังหากมีความจำเป็น โดยจัดทำเป็นเอกสาร "บันทึกการเข้า-ออกพื้นที่" ไว้ให้ชัดเจน และให้ปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ใช้งานห้องศูนย์ข้อมูล (Data Center) อย่างน้อยปีละ ๑ ครั้ง

(๔) ผู้ใช้งานหรือบุคคลภายนอกที่เข้ามาปฏิบัติงานในหน่วยงาน ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่ปฏิบัติงาน และต้องให้ลงชื่อขออนุญาตการเข้า-ออกในแบบฟอร์มที่กำหนดไว้ โดยมีผู้ดูแลระบบควบคุมการปฏิบัติงานของผู้ใช้งานหรือบุคคลภายนอกตลอดเวลา

(๕) ทบทวนสิทธิ หรือยกเลิกการเข้าถึงห้องศูนย์ข้อมูลและบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑.๖ จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาเข้าถึงและช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจน โดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญ ไว้ดังนี้

(๑) จัดแบ่งระดับชั้นการเข้าถึง
- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย

(๒) จัดแบ่งลำดับชั้นความลับของข้อมูล
- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงมาก

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓) จัดแบ่งประเภทของข้อมูล

๑. ข้อมูลสารสนเทศสำหรับการบริหาร คือ

- ข้อมูลนโยบาย ยุทธศาสตร์
- คำรับรองการปฏิบัติราชการ
- ข้อมูลบุคลากร
- ข้อมูลระบบสลิปเงินเดือน (สำหรับบุคลากรที่มีหน่วยเบิกจ่ายอยู่ส่วนกลาง)
- ข้อมูลระบบประเมินผลการปฏิบัติราชการ (KPI)
- ข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลระบบโปรแกรมทะเบียนคุมทรัพย์สิน
- ข้อมูลระบบงานสารสนเทศ
- ข้อมูลระบบจัดสรรครุภัณฑ์ฯ (E-Survey)
- ข้อมูลระบบสารสนเทศและการรายงานผลการดำเนินงาน สคช.
- ข้อมูลระบบลงทะเบียนขอใช้งานอินเทอร์เน็ตของสำนักงานอัยการสูงสุด
- ข้อมูลระบบงานประเมินผล
- ข้อมูลระบบงานพัฒนากฎหมาย
- ข้อมูลระบบรายงานคุณภาพชีวิตฯ
- ข้อมูลระบบรายงานการใช้ทรัพยากรสำนักงานอัยการสูงสุด

๒. ข้อมูลสารสนเทศสนับสนุนการปฏิบัติงาน คือ

- ข้อมูลสารบบคดีอิเล็กทรอนิกส์
- ข้อมูลระบบรายงานจำนวนสารบบคดีอิเล็กทรอนิกส์
- ข้อมูลระบบการเชื่อมโยงกับตำรวจ (NSW : National Single Windows)
- ข้อมูลระบบติดตามข้อมูลการดำเนินคดีค้ามนุษย์ (AGO-CAHT : Case Anti Human Trafficking)
- ข้อมูลระบบการติดตามความคืบหน้าการดำเนินคดีเพื่อการบริการภายในสำนักงานอัยการสูงสุด (AGO-CTS : Case Tracking System)
- ข้อมูลระบบติดตามข้อมูลคดีในการดำเนินการคดีค้ามนุษย์ (AGO-AHT : Anti Human Trafficking)
- ข้อมูลระบบประมวลผลข้อมูลคดีเชิงลึกและซับซ้อน (AGO-CCCS : Criminal Complicated Case System)
- ข้อมูลระบบรายงานสำนวนคดีหมิ่นพระบรมเดชานุภาพ มาตรา ๑๑๒
- ข้อมูลระบบงานสารบรรณอิเล็กทรอนิกส์สำนักงานอัยการสูงสุด
- ข้อมูลระบบจองห้องประชุม
- ข้อมูลระบบลงทะเบียนใช้งานอีเมล์ภาครัฐ

ทั้งนี้ ข้อมูลระบบงานต่าง ๆ เป็นข้อมูลส่วนบุคคลและเป็นข้อมูลคดีที่ไม่สามารถเปิดเผยให้ผู้ไม่เกี่ยวข้องได้ล่วงรู้ถึงข้อมูลดังกล่าวได้ จึงถูกจัดเก็บไว้ระบบงานภายใน (Intranet)

(๔) กำหนดช่องทางการเข้าถึง

- ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในหน่วยงาน คือ ระบบประเมินผลการปฏิบัติราชการ (KPI) ระบบสารบบคดีอิเล็กทรอนิกส์ และตามข้อ (๓) ข้างต้น
- ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอก สามารถเข้าถึงได้ตลอดเวลา ได้แก่ ระบบประชาสัมพันธ์ ระบบสอบถามปัญหากฎหมาย

๑.๗ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ

(๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของข้อมูลแต่ละระดับ

(๕) การรับ-ส่งข้อมูลด้วย SSL, VPN หรือ XML Encryption ผ่านระบบเครือข่ายต้องเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน รวมถึงการบำรุงรักษา ตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

(๕) กำหนดเวลาการเข้าถึงระบบสารสนเทศ หากมีการบันทึกแก้ไขข้อมูลสารบบคดีอิเล็กทรอนิกส์ให้เรียกรายงานได้ในเวลาเช้าวันรุ่งขึ้นในอีกวันถัดไปเท่านั้น เนื่องจากระบบจะทำการประมวลผลตอนเที่ยงคืน

(๖) การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of connection time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนด ส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

๑.๘ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) ควบคุมการเข้าถึงสารสนเทศ โดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิเกี่ยวข้องกับระบบสารสนเทศ

(๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๑.๙ การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

(๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังนี้

- ระบบรักษาความปลอดภัย (Security)
- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศและควบคุมความชื้น

(๒) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน

(๔) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอก และให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

(๕) ตรวจสอบ สอดส่อง ดูแลสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติ เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ภายในห้องศูนย์ข้อมูล (Data Center)

(๖) การเดินสายไฟ สายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิ้ลอื่น ที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้น ให้ร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันหนู นก กระรอก แมลงสาบหรือสัตว์อื่นกัดสายไฟ ป้องกันการดักจับสัญญาณ การตัดสายสัญญาณ อันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้

(๗) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน แล้วให้จัดเก็บสายสัญญาณต่าง ๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิทเพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

๑.๑๐ จัดทำโครงการบำรุงรักษาระบบคอมพิวเตอร์และระบบสารสนเทศ ดังนี้

(๑) กำหนดการบำรุงรักษาอุปกรณ์แต่ละประเภทตามรอบระยะเวลาการใช้งานไว้ในแผนการบำรุงรักษาประจำปี

(๒) บันทึกรายละเอียดการให้บริการบำรุงรักษาอุปกรณ์ทุกครั้งผ่านระบบ Support Desk และต้องบันทึกรายละเอียดข้อบกพร่องของอุปกรณ์ที่ตรวจพบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ในภายหลัง

(๓) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้รับจ้างให้เป็นไปตามข้อกำหนดของสัญญา

๑.๑๑ การควบคุมการนำสินทรัพย์ของหน่วยงานออกนอกพื้นที่ ดังนี้

(๑) บันทึกและจัดเก็บข้อมูลสินทรัพย์ของหน่วยงานที่นำออกนอกพื้นที่ เพื่อเป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกการส่งคืน

(๒) ห้ามผู้ใช้งานละทิ้งสินทรัพย์ของหน่วยงานไว้เพียงลำพังในที่สาธารณะ ให้ถือเสมือนเป็นทรัพย์สินของตนเอง

(๓) กรณีจำเป็นต้องจำหน่ายสินทรัพย์ของหน่วยงาน ให้ทำลายข้อมูลสำคัญหรือสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายอุปกรณ์นั้น

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

๒.๑ กำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)

๒.๒ จัดฝึกอบรมการใช้งานโปรแกรมระบบสารสนเทศของหน่วยงานเพื่อสนับสนุนการปฏิบัติงาน และหลักสูตรการใช้งาน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด หรือลดน้อยลง และลดผลกระทบที่อาจเกิดจากการใช้งานระบบสารสนเทศโดยรู้เท่าไม่ถึงการณ์หรือไม่ระมัดระวัง รวมถึงมีมาตรการเชิงป้องกันตามความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงโปรแกรมระบบ

๒.๓ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ให้ครอบคลุมเรื่องต่อไปนี้

(๑) จัดทำระบบกรอกแบบฟอร์มการขอใช้งานระบบสารสนเทศ โดยผู้ใช้งานสามารถตรวจสอบสิทธิและดำเนินการแจ้งความจำนงตามขั้นตอนการลงทะเบียนผ่าน application ที่สำนักเทคโนโลยีสารสนเทศและการสื่อสารพัฒนาขึ้นไว้รองรับสำหรับบางระบบที่มีความสำคัญ

(๒) การกำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ยืนยันตัวตนของผู้ใช้งานในแต่ละระดับขั้นความลับ โดยบัญชีผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สองหรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๓) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศด้วยการพิสูจน์ยืนยันตัวตน (authentication) ในการใช้งานระบบสารสนเทศและระบบอินเทอร์เน็ตของหน่วยงาน และได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๔) ตรวจสอบสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๕) กำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิดต่อเนื่อง ๓ ครั้ง จนกว่าจะยื่นความจำนงผ่านระบบหรือยื่นเรื่องพร้อมหลักฐานแสดงความเป็นตัวตนต่อสำนักเทคโนโลยีสารสนเทศและการสื่อสารเพื่อขอรับรหัสผ่านใหม่อีกครั้ง

(๖) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๗) การจัดส่งมอบรหัสผ่าน (Password) ให้กับผู้ใช้งาน (User) ต้องจัดส่งด้วยเอกสารปิดผนึก (Slip) ทางระบบไปรษณีย์หรือผ่านระบบ

๒.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบสารสนเทศและให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานทางอินทราเน็ต

(๒) ระบุชื่อ นามสกุล ตำแหน่ง หน่วยงานที่สังกัด และหมายเลขโทรศัพท์ของผู้ใช้งาน

(๓) ตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ ตามความจำเป็นในการใช้งาน และต้องสอดคล้องกับนโยบายควบคุมการเข้าถึงข้อมูลเป็นสำคัญ

(๔) บันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๒.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) มีขั้นตอนการขอมีบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

- ตรวจสอบสิทธิตามแบบฟอร์มที่กำหนดทางระบบสารสนเทศ และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
- ระบุชื่อ นามสกุล ตำแหน่ง หน่วยงานที่สังกัด และหมายเลขโทรศัพท์ติดต่อได้
- ผู้ใช้งานได้รับรหัสผ่านแล้วและเมื่อมีการเข้าใช้งานระบบสารสนเทศครั้งแรกนั้น ระบบจะกำหนดให้เปลี่ยนรหัสผ่านโดยทันที ซึ่งต้องเปลี่ยนเป็นรหัสใหม่ที่ไม่ซ้ำกับรหัส สำรที่เคยตั้งไว้ก่อนหน้า การกำหนดรหัสต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและสัญลักษณ์เข้าด้วยกัน ประกอบไปด้วยอักษร (Alphabets) ผสมตัวเลข (Numerical character) และตัวอักษรพิเศษ (Special character) ไม่น้อยกว่า ๖ ตัวอักษร

(๒) การตั้งรหัสผ่านชั่วคราวระบบจะกำหนดให้อัตโนมัติ และผู้ใช้งานต้องเปลี่ยนเป็นรหัสที่ยากต่อการเดาและต้องมีความแตกต่างกันกับรหัสผ่านชั่วคราวทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว

(๓) การส่งมอบบัญชีผู้ใช้งาน (username) และรหัสผ่าน (password) ผู้ดูแลระบบที่ได้รับมอบหมายจะดำเนินการเป็น ๒ รูปแบบ ดังนี้

๑. แจ้งการจัดสรรบัญชีผู้ใช้งานผ่านระบบสารสนเทศ

๒. ส่งมอบรหัสในรูปแบบเอกสารปิดผนึกทางไปรษณีย์ ระบุถึงผู้รับโดยตรง

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือเมื่อพ้นจากตำแหน่ง และกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง

๒.๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้าง ดังนี้

(๑) ทบทวนสิทธิการเข้าถึงผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และทบทวนสำหรับผู้ที่มีสิทธิในระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน

(๒) ทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้างงาน และบันทึกการเปลี่ยนแปลงเพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อยดังนี้

๓.๑ กำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่านและการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อ Login เข้าใช้งานระบบสารสนเทศครั้งแรก

(๒) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานต้องให้ยากต่อการเดา และส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยและให้มีอักษรจำนวนไม่น้อยกว่า ๖ ตัวอักษร โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและสัญลักษณ์เข้าด้วยกัน ซึ่งประกอบไปด้วยอักษร (Alphabets) ผสมตัวเลข (Numerical character) และตัวอักษรพิเศษ (Special character)

(๓) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุล หรือบุคคลในครอบครัว เบอร์โทรศัพท์ อักขระที่เรียงกันหรือกลุ่มเหมือนกันที่ง่ายต่อการคาดเดา หรือใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๔) ไม่ใช้รหัสผ่านส่วนบุคคลร่วมกับบุคคลอื่น และไม่จดหรือบันทึกช่วยจำไว้ในที่ที่ง่ายต่อการสังเกตเห็นได้ง่ายจากบุคคลอื่น และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ

(๕) หากมีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากความจำเป็นต้องใช้ในงาน หลังจากดำเนินการเสร็จสิ้นแล้วให้ทำการเปลี่ยนรหัสผ่านนั้นโดยทันที

(๖) ให้หลีกเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานอื่น ๆ และหลีกเลี่ยงการใช้รหัสผ่านเดิม

(๗) ผู้ใช้งานมีหน้าที่ป้องกัน ดูแลรักษาข้อมูลบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนมีบัญชีผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่านของตน

(๘) ผู้ดูแลระบบต้องทำการเปลี่ยนรหัสผ่านถี่กว่าผู้ใช้งานทั่วไป

(๙) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๙๐ วัน หรือทุกครั้งที่ระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๑) กำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่ เพื่อป้องกันการสูญหายหรือเข้าถึงโดยไม่ได้รับอนุญาต ดังนี้

- ต้องกำหนดรหัสผ่านก่อนเข้าใช้งานเครื่องคอมพิวเตอร์
- ดาวน์โหลดไฟล์จากแหล่งข้อมูลอินเทอร์เน็ตที่ไว้ใจได้เท่านั้น

(๒) ป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งานหรือปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราวในช่วงระยะเวลา ๑๕ นาที ต้องกำหนดให้เครื่องคอมพิวเตอร์ปิดหรือ Lock หน้าจอทันที เมื่อหน้าจอ Lock แล้ว ต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเข้าใช้งานผ่านหน้าจอเครื่องคอมพิวเตอร์ได้อีกครั้ง

(๓) ป้องกันการเข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศโดยใส่รหัสผ่านให้ถูกต้องก่อนการใช้งานทุกครั้ง

(๔) ออกจากระบบสารสนเทศของหน่วยงานทันทีที่เสร็จสิ้นการใช้งาน

๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศที่เป็นเอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) กำหนดมาตรการป้องกันสินทรัพย์ของหน่วยงาน และควบคุมไม่ให้ทิ้งหรือปล่อยระบบสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องการจัดบริเวณล้อมรอบ การควบคุมการเข้า-ออก การจัดบริเวณการเข้าถึง การวางอุปกรณ์ ระบบและอุปกรณ์สนับสนุนการทำงาน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันสินทรัพย์ของหน่วยงาน
- ลงชื่อออกจากระบบและล้อคเครื่องคอมพิวเตอร์ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ปิดเครื่องโทรสารเมื่อไม่ใช้งาน และป้องกันไม่ให้ผู้อื่นใช้กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร
- ป้องกันเครื่องคอมพิวเตอร์โดยใช้กลไกการพิสูจน์ตัวตนก่อนการใช้งาน
- ไม่ควรเสียบสายไฟค้างไว้ที่เต้าเสียบ อาจจะทำให้เกิดฟ้าผ่าเข้าเครื่องหรือกระแสไฟฟ้าไหลเข้าเครื่องได้

(๒) การป้องกันต้องมีความสอดคล้องกับแนวทางการจัดการสารสนเทศ และการนำเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับต้องปฏิบัติตามระเบียบการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

- ต้องแสดงหลักเกณฑ์ในการกำหนดเรื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด
- ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

(๓) การกระทำใด ๆ ที่เกิดจากการใช้บัญชีผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประกอบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ผู้ใช้งานจะรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

(๔) การทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
Hard disk หรือ Flash Drive	- ใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลาย ๆ รอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
Tape	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
CD / DVD	ใช้วิธีการหั่นด้วยเครื่องทำลายเอกสาร หรือหักให้ละเอียด
กระดาษ	ใช้วิธีการหั่นด้วยเครื่องทำลายเอกสาร (Paper Shredder)

๓.๔ ผู้ใช้งานและบุคคลภายนอกต้องทำการพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ยืนยันตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากการใช้รหัสผ่านผิดพลาดหรือใช้งานไม่ได้ก็ดี ต้องแจ้งให้สำนักเทคโนโลยีสารสนเทศและการสื่อสารทราบทันที โดยต้องปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภทที่ทำการเชื่อมต่อเข้ากับระบบเครือข่ายภายในของหน่วยงาน (LAN) ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ยืนยันตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในระบบเครือข่ายและเครือข่ายไร้สาย (Wi-fi) ผู้ใช้งานต้องทำการพิสูจน์ยืนยันตัวตนก่อนการใช้งานระบบเครือข่ายทุกครั้ง

(๓) การใช้งานเครือข่ายอินเทอร์เน็ต (Internet) ของหน่วยงาน ต้องทำการพิสูจน์ยืนยันตัวตนและต้องบันทึกข้อมูลที่บ่งบอกตัวตนของผู้ใช้งานได้

(๔) เมื่อผู้ใช้งานไม่อยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องทำการ Log out ออกจากระบบเครือข่ายหรือล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ยืนยันตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

๓.๕ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลสารสนเทศ ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงานหรือเป็นข้อมูลของบุคคลภายนอก

๓.๖ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในความดูแลของหน่วยงานห้ามไม่ให้เผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงสุดหรือผู้บริหารระดับสูง

๓.๗ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของหน่วยงาน และข้อมูลของผู้มารับบริการ หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๓.๘ ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท โปรแกรมดูหนัง เกมส์ หรือฟังเพลง เพื่อความบันเทิงที่ถือเป็นการรบกวนการทำงานของเพื่อนร่วมงานในระหว่างปฏิบัติงาน

๓.๙ ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อประโยชน์ทางการค้า

๓.๑๐ ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวน ก่อให้เกิดความเสียหายหรือใช้ในการโจรกรรมข้อมูล การเผยแพร่ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมายหรือกระทบต่อภารกิจของหน่วยงาน

๓.๑๑ ห้ามกระทำการใด ๆ ที่เป็นการรบกวน ทำลายหรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

๓.๑๒ ห้ามใช้ระบบสารสนเทศของหน่วยงานเพื่อการควบคุมคอมพิวเตอร์หรือระบบเครือข่ายภายนอกโดยไม่ได้รับอนุญาตจากผู้อำนวยการและผู้บริหารระดับสูง

๓.๑๓ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือล่วงรู้บัญชีผู้ใช้งานของผู้อื่นไม่ว่ากรณีใด ๆ เพื่อเข้าถึงข้อมูลหรือเพื่อใช้สินทรัพย์ของหน่วยงาน

๓.๑๔ ห้ามติดตั้งอุปกรณ์เครือข่ายและ Application หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้อำนวยการ

ส่วนที่ ๔ การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control : NAC)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

๔.๑ การใช้งานบริการเครือข่ายและระบบสารสนเทศของหน่วยงาน ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) กำหนดระบบงานที่ควบคุมการเข้าถึงและระบุเครือข่ายหรือบริการที่อนุญาตให้ใช้งานได้และข้อปฏิบัติของผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้เท่าที่เพียงได้รับอนุญาตเท่านั้น ได้แก่

๑. ระบบสารบบคดีอิเล็กทรอนิกส์ ซึ่งสามารถเข้าถึงข้อมูลได้ตามสิทธิที่กำหนด ไว้ดังนี้

- สิทธิผู้ใช้งาน จะสามารถบันทึกข้อมูลในส่วนงานที่ตนเองรับผิดชอบตามสิทธิที่ได้รับมอบหมายเท่านั้น
- สิทธิของนิติกร สำหรับการลงคำพิพากษา และออกรายงาน อก.๔๐ ได้เฉพาะหน่วยงานที่รับผิดชอบและได้รับมอบหมายเท่านั้น
- สิทธิของอัยการ สำหรับการลงอัยการการจัดการได้เฉพาะหน่วยงานที่รับผิดชอบและได้รับมอบหมายเท่านั้น
- สิทธิของผู้บริหารสูงสุดจะสามารถตรวจสอบผลการดำเนินคดีของสำนักงานอัยการสูงสุดได้ทั้งหมด แต่ไม่สามารถแก้ไขใด ๆ ได้

๒. ระบบประเมินผลการปฏิบัติราชการ (KPI) จะเปิดระบบให้ข้าราชการของหน่วยงานทุกคนบันทึกข้อมูลประเมินตามรอบที่กำหนดในแต่ละปี

๓. ระบบงานสารบรรณอิเล็กทรอนิกส์ ระบบจะกำหนดสิทธิให้ผู้มีหน้าที่รับผิดชอบงานสารบรรณในแต่ละหน่วยงานเท่านั้น

๔. ระบบบริหารอาคารและที่ดิน ระบบจะกำหนดสิทธิให้ผู้มีหน้าที่รับผิดชอบงานสารบรรณในแต่ละหน่วยงานเท่านั้น

๕. ระบบโปรแกรมทะเบียนคุมทรัพย์สิน ระบบจะกำหนดสิทธิให้ผู้มีหน้าที่รับผิดชอบงานสารบรรณในแต่ละหน่วยงานเท่านั้น

๖. กำหนดการใช้ระบบสารสนเทศที่สำคัญ คือ ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) ระบบเครือข่ายภายใน (intranet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้อำนวยการเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิอย่างน้อยปีละ ๑ ครั้ง

๔.๒ การพิสูจน์ยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถ เข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๑) การเข้าสู่เครือข่ายและระบบสารสนเทศของหน่วยงานด้วยวิธีการใด ๆ ที่สามารถเข้าสู่ระบบสารสนเทศของหน่วยงานต้องได้รับการอนุญาตจากผู้อำนวยการเท่านั้น โดยต้องบันทึกการเข้าใช้งาน (Login) เพื่อแสดงตัวตนด้วยบัญชีผู้ใช้งาน และการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๒) การพิสูจน์ยืนยันตัวตนมีวิธีการในการตรวจสอบเพื่อพิสูจน์ยืนยันตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานอย่างน้อย ๑ วิธี

- การเข้าระบบด้วย Username และ Password
- การใช้งาน smart card

๔.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in network) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๑) ผู้ดูแลระบบจัดเก็บบัญชีอุปกรณ์ บัญชีอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อและบัญชีการขอเชื่อมต่อเครือข่าย สถานที่ติดตั้ง

(๒) อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อเข้ากับเครือข่ายของหน่วยงานให้ระบุเลขรหัสประจำเครื่องคอมพิวเตอร์ (IP Address) ทุกครั้ง

(๓) อุปกรณ์ที่เชื่อมต่อเข้ากับเครือข่ายของหน่วยงานต้องตรวจสอบเลขรหัสประจำคอมพิวเตอร์ (IP Address) จากทั้งต้นทางและปลายทางได้

(๔) การใช้งานระบบอินเทอร์เน็ตของหน่วยงานต้องพิสูจน์ยืนยันตัวตนก่อนเข้าใช้งานทุกครั้ง

(๕) จำกัดผู้ใช้งานที่สามารถเข้าใช้งานสินทรัพย์ของหน่วยงาน และต้องควบคุมการใช้งานอย่างเหมาะสม

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตในการเข้าถึงทั้งกายภาพและทางเครือข่าย

(๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ต ที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๓) ป้องกันพอร์ตที่ใช้สำหรับการควบคุมช่องทางในการติดต่อสื่อสารระหว่างระบบสารสนเทศกับอุปกรณ์ภายนอก (Port) ที่ใช้อย่างรัดกุม

(๔) ควบคุมพอร์ตอย่างเข้มงวด และต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด และต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว โดยจะเปิดให้ใช้ได้ต่อเมื่อร้องขอเป็นลายลักษณ์อักษรเท่านั้นและได้รับอนุมัติอย่างถูกต้องจากผู้อำนวยการแล้วเท่านั้น

(๕) การควบคุมการเข้าสู่ระบบสารสนเทศจากระยะไกล (remote access) เพื่อเข้าสู่ระบบสารสนเทศและระบบอินเทอร์เน็ตของหน่วยงาน ต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบงานภายใน โดยต้องได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนทุกครั้ง

๔.๕ การแบ่งแยกเครือข่าย (segregation in network) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ ดังต่อไปนี้

(๑) ระบบเครือข่ายอินเทอร์เน็ต (Internet) เพื่อควบคุมการเข้าถึงระบบเครือข่ายจากบุคคลภายนอกโดยไม่ได้รับอนุญาต

(๒) ระบบเครือข่ายภายใน (Intranet) ผู้ใช้งานสามารถใช้งานผ่านสายสัญญาณเครือข่าย (LAN) ผ่านจุดเชื่อมต่อ (Outlets) และระบบเครือข่ายไร้สาย (Wireless LAN) ภายในหน่วยงานเท่านั้น

(๓) DMZ (Demilitarized Zone) เป็นเขตพิเศษที่เชื่อมต่อทั้งเครือข่ายภายใน (Intranet) และเครือข่ายภายนอก (Internet) สำหรับแยกเครื่องแม่ข่ายที่ให้บริการทั้งบนเครือข่ายภายนอกและเครือข่ายภายใน เพื่อป้องกันการเข้าถึงระบบเครือข่ายภายในหน่วยงานโดยไม่ได้รับอนุญาต

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๑) บุคคลภายนอกและผู้ใช้งานจะนำเครื่องคอมพิวเตอร์มาเชื่อมต่อกับระบบอินเทอร์เน็ตของหน่วยงานได้ ต้องได้รับอนุญาตจากผู้อำนวยการเท่านั้นและให้ปฏิบัติตามนโยบายนี้โดยเคร่งครัด

(๒) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานระบบสารสนเทศหรือระบบอินเทอร์เน็ตที่ได้รับอนุญาตเท่านั้น

(๓) จำกัดเส้นทางการเข้าถึงระบบสารสนเทศและระบบอินเทอร์เน็ตที่มีการใช้งานร่วมกัน

(๔) จำกัดการใช้งานระบบสารสนเทศของหน่วยงานจากคอมพิวเตอร์และระบบอินเทอร์เน็ตเพื่อป้องกันไม่ให้ผู้ใช้งานเข้าใช้งานระบบสารสนเทศที่ส่งผลกระทบต่อการทำงานได้

(๕) หากจำเป็นต้องเชื่อมต่อระบบสารสนเทศและระบบอินเทอร์เน็ตของหน่วยงานไปยังหน่วยงานภายนอก ให้เชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย (Firewall) ที่มีความสามารถในการดักจับ Malware (Malicious Software) ไวรัสหรือชุดคำสั่งไม่พึงประสงค์เท่านั้น โดยต้องพิจารณาถึงโครงสร้างพื้นฐานการใช้งานเครือข่ายของหน่วยงานนั้นเป็นสำคัญ

๑. การเชื่อมโยงกับหน่วยงานภาครัฐที่ใช้ระบบเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN : Government Information Network)

๒. การเชื่อมต่อกับหน่วยงานภาครัฐที่ใช้ระบบเครือข่ายอื่น โดย TOT, CAT

(๖) ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) ตรวจสอบการใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือระบบสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้ตามภารกิจ

(๑) ป้องกันไม่ให้บุคคลภายนอกหรือหน่วยงานภายนอกมองเห็นเลขรหัสประจำคอมพิวเตอร์ที่ต่ออยู่บนเครือข่าย (IP Address) เพื่อป้องกันไม่ให้ล่วงรู้ข้อมูลเกี่ยวกับโครงสร้างเครือข่ายภายในของหน่วยงานได้โดยง่าย

(๒) จัดทำแผนผังเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งที่อยู่ภายใน ภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๓) การใช้เครื่องมือต่าง ๆ เพื่อตรวจสอบระบบอินเทอร์เน็ตและเครือข่ายหรือการติดตั้ง ปรับปรุงซอฟต์แวร์ระบบต้องได้รับการอนุมัติจากผู้อำนวยการก่อนทุกครั้ง และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๔) บริหารควบคุมอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบสารสนเทศในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

(๕) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อเข้ากับระบบอินเทอร์เน็ตและเครือข่ายของหน่วยงานอย่างชัดเจน และทบทวนการกำหนดค่าพารามิเตอร์ (Parameters) ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง และหากกำหนดการแก้ไขหรือเปลี่ยนแปลงค่า parameter ให้แจ้งผู้ที่เกี่ยวข้องทราบทุกครั้ง

(๖) เครือข่ายของหน่วยงานที่เชื่อมต่อไปยังหน่วยงานภายนอก ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย (Firewall) รวมทั้งความสามารถในการดักจับ Malware (Malicious Software) ไวรัสหรือชุดคำสั่งไม่พึงประสงค์ด้วย

(๗) ต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System : IPS/IDS) เพื่อตรวจสอบการใช้งานของผู้ใช้งานเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๘) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบเครือข่ายของหน่วยงานต้องได้รับการอนุมัติจากผู้อำนวยการ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๙) กำหนดให้ต้องจัดเก็บคำสั่งในการเขียนโปรแกรม (Source Code) คลังโปรแกรม (Library) และเอกสารสำหรับซอฟต์แวร์ระบบไว้ในสถานที่ที่มีความปลอดภัย

(๑๐) การติดตั้งหรือปรับปรุงเครือข่าย รวมถึงการติดตั้งอุปกรณ์เครือข่ายเพิ่มเติมภายในหน่วยงานต้องได้รับการอนุมัติจากผู้อำนวยการก่อนทุกครั้ง

(๑๑) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ซึ่งเป็นข้อมูลสำคัญที่สามารถนำมาใช้ในการสืบสวนหรือสอบสวนการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (ตามมาตรา ๒๔) เป็นระยะเวลา ๙๐ วัน แต่ไม่เกิน ๑ ปี โดยกำหนดประเภทของ Log File ที่มีความจำเป็นต้องเก็บไว้ออกเป็น ๕ ประเภท ดังนี้

๑. Personal Computer log file
๒. Network Access Server or RADIUS server log file
๓. Email Server log file (SMTP log)
๔. FTP Server log file
๕. Web Server (HTTP server) log file

๔.๘ มาตรการควบคุมการเข้า–ออกห้องศูนย์ข้อมูล (Data Center)

(๑) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นที่ใช้ในการปฏิบัติงานมากระทำการใด ๆ ในห้องศูนย์ข้อมูล (Data Center) ของหน่วยงานต้องให้ระบุจำนวน ประเภท และชนิดอุปกรณ์ไว้ในหนังสือขออนุญาตเข้าพื้นที่ให้ชัดเจน และตามแบบฟอร์มที่สำนักเทคโนโลยีสารสนเทศและการสื่อสารกำหนดไว้

(๒) ผู้ดูแลระบบทำการตรวจสอบความถูกต้องหนังสือขออนุญาตเข้าพื้นที่ โดยผู้ขออนุญาตต้องระบุอุปกรณ์และแผนการดำเนินงานมาให้ชัดเจนพร้อมระบุชื่อบุคคลในการดำเนินงาน มายังผู้อำนวยการเพื่อพิจารณาอนุญาตล่วงหน้าอย่างน้อย ๕ วันทำการ

๔.๙ การขออนุญาตใช้งานพื้นที่ Web Server ที่เป็นชื่อโดเมนย่อย (Sub Domain Name) ของหน่วยงานให้ทำหนังสือขออนุญาตต่อผู้อำนวยการ และไม่ติดตั้งโปรแกรมใด ๆ ที่จะส่งผลกระทบต่อความเสียหายของระบบและผู้ใช้งานอื่น

๔.๑๐ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือกระทำการใด ๆ ต่ออุปกรณ์ในห้องศูนย์ข้อมูล (Data Center) และสินทรัพย์ของหน่วยงาน ได้แก่ อุปกรณ์ค้นหาเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) และอุปกรณ์อื่นที่ทำหน้าที่เชื่อมต่อกับเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้อำนวยการ

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

๕.๑ ผู้ดูแลระบบ (System administrator) มีหน้าที่ดังนี้

(๑) ติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการสินทรัพย์ของหน่วยงาน

(๒) กำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน โดยกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน การลาออก หรือการเปลี่ยนตำแหน่งภายในหน่วยงาน

(๓) การกำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ต้องไม่ซ้ำกัน

(๔) ในกรณีที่จำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานคนใด ต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานเท่านั้น และให้กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และการกำหนดสิทธิพิเศษให้สามารถเข้าถึงข้อมูลของหน่วยงานในระดับใดบ้าง และกำหนดบัญชีผู้ใช้งานให้ต่างจากผู้ใช้งานปกติด้วย

(๕) ห้ามควบคุมระบบคอมพิวเตอร์และระบบสารสนเทศของหน่วยงานภายนอก โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้บริหารระดับสูง

๕.๒ ผู้ใช้งาน (User) ต้องไม่ละเมิดการปฏิบัติ ดังนี้

(๑) Software ที่หน่วยงานติดตั้งไว้ให้ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลงแก้ไขหรือทำสำเนาเพื่อนำไปใช้งานที่อื่น และห้ามติดตั้งโปรแกรมที่ไม่พึงประสงค์กับคอมพิวเตอร์ของหน่วยงาน

(๒) ห้ามใช้สินทรัพย์ทุกประเภทที่เป็นของหน่วยงานเพื่อประโยชน์ทางการค้า ห้ามนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพที่ไม่เหมาะสมหรือขัดต่อศีลธรรม

๕.๓ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการ ต้องควบคุมโดยวิธีการพิสูจน์ยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(๑) ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่จะเข้าระบบพิสูจน์ยืนยันตัวตน (authentication) เสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อกับเครื่องปลายทางได้ เมื่อพบความผิดปกติว่าพยายามคาดเดาหรือเข้าถึงจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัส

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง command line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕.๔ การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๑) ก่อนเข้าใช้งานเครือข่าย ต้องทำการพิสูจน์ยืนยันตัวตน (User Identification and Authentication) ด้วยบัญชีผู้ใช้งาน (Username) และพิสูจน์ยืนยันตัวตน ด้วยรหัสผ่าน (Password) เพื่อตรวจสอบความถูกต้องและยืนยันตัวตนก่อนเข้าใช้งานทุกครั้ง

(๒) หากมีความจำเป็นต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านเทคนิคและการปฏิบัติงาน

(๓) สามารถใช้อุปกรณ์ Smart Card ควบคุมความปลอดภัยเพิ่มเติม

๕.๕ การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๑) ผู้ดูแลระบบ (Admin) เป็นผู้กำหนดรหัสผ่านสำหรับผู้ใช้งาน

(๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ

(๓) การเข้าใช้งานต้องระบุและยืนยันการเข้าใช้งานโดยใช้ชื่อ (Username) และรหัสผ่าน (Password) ที่ผู้อำนวยการได้อนุญาตไว้แล้วเท่านั้น

(๔) ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานระบบสารสนเทศของหน่วยงานร่วมกัน

๕.๖ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์หรือจำกัดให้ผู้ใช้คำสั่งนี้ต้องเป็นผู้ดูแลระบบเท่านั้น ซึ่งต้องเข้าโหมดการจัดการก่อนถึงจะดำเนินการได้

- โปรแกรม Formatter
- Find File โปรแกรมช่วยค้นหาไฟล์ข้อมูล
- Backup and Recovery โปรแกรมช่วยทำข้อมูลสำรองและนำคืนข้อมูลสำรอง
- System Diagnostic โปรแกรมตรวจเช็คฮาร์ดแวร์และระบบปฏิบัติการ
- Resource utilization performance meter โปรแกรมตรวจสอบประสิทธิภาพการใช้งานทรัพยากร) เป็นต้น

(๒) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องการใช้งานเป็นประจำ

(๓) ถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๗ การใช้งานโปรแกรมยูทิลิตี้ (Utilities Program) เพื่อการบำรุงรักษาเครื่องคอมพิวเตอร์ที่ติดตั้งอยู่ในระบบคอมพิวเตอร์อย่างสม่ำเสมอ ผู้ใช้งานต้องหมั่นใช้โปรแกรม Scandisk เพื่อทำการตรวจสอบการทำงานของหน่วยสำรองข้อมูล ฮาร์ดดิสก์ และ Floppy Disk ว่าส่วนไหนไม่สามารถบันทึกได้ รวมถึงตรวจสอบโครงสร้างของแฟ้มข้อมูลให้มีความถูกต้อง หากพบปัญหาก็จะทำการแก้ไขให้โดยอัตโนมัติ

(๑) Disk defragmenter โปรแกรมช่วยจัดระเบียบข้อมูลในดิสก์

(๒) Disk cleanup โปรแกรมกำจัดข้อมูลที่ซ้ำซ้อนหรือไม่ได้ใช้งานในระบบ

๕.๘ หากว่างเว้นจากการใช้งานระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๑) ต้องกำหนดการยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน ให้ตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลา ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบสารสนเทศ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบอัตโนมัติ

(๓) สินทรัพย์ของหน่วยงานที่ตั้งอยู่ในพื้นที่มีความเสี่ยงสูง ต้องกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(๔) ตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน และเพื่อให้ใส่รหัสผ่าน (Password) ก่อนการใช้งานทุกครั้ง

๕.๙ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูงซึ่งหน่วยงานไม่ได้กำหนดระยะเวลาขั้นต่ำในการเชื่อมต่อแต่ละครั้งไว้ แต่กำหนดให้ดำเนินการได้เฉพาะในเวลาราชการระหว่างเวลา ๐๘.๓๐ – ๑๖.๓๐ น. เท่านั้น ได้แก่ การอัพโหลดข้อมูลขึ้นเว็บไซต์

(๒) ต้อง Logout ทันที เมื่อเลิกจากการใช้งานระบบสารสนเทศ และต้องกำหนดให้ระบบปิดหน้าจอทันทีเมื่อไม่มีการใช้งานเป็นเวลา ๑๕ นาที

(๓) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อเครือข่ายจากปลายทาง ต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งอุปกรณ์ด้วยเป็นสำคัญ โดยผู้ใช้งานเครือข่ายปลายทางที่จะเข้าดำเนินการใด ๆ กับเครือข่ายของหน่วยงานต้องแจ้งเป็นลายลักษณ์อักษรมายังผู้อำนวยการก่อนทุกครั้ง และจะอนุญาตให้ดำเนินการได้ในช่วงเวลาราชการเท่านั้น โดยไม่จำกัดระยะเวลาการเชื่อมต่อในแต่ละครั้ง เมื่อสิ้นสุดระยะเวลาที่ร้องขอแล้วผู้ดูแลระบบจะปิดการเชื่อมต่อทันที ซึ่งหากปลายทางยังดำเนินการไม่แล้วเสร็จต้องร้องขอเป็นลายลักษณ์อักษรเข้ามาอีกครั้ง

๕.๑๐ ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิของผู้ใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยต้องปฏิบัติตามแนวทาง ดังนี้

(๑) สำนักบริหารทรัพยากรบุคคลซึ่งเป็นหน่วยงานที่ทำหน้าที่เป็นผู้บริหารจัดการระบบฐานข้อมูลบุคลากรของหน่วยงาน ต้องทำการตรวจสอบข้อมูลและทบทวนบัญชีผู้ใช้งานร่วมกับผู้ดูแลระบบของสำนักเทคโนโลยีสารสนเทศและการสื่อสารอย่างต่อเนื่อง และข้อมูลต้องทันสมัยและเป็นปัจจุบันตลอดเวลา

(๒) ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามคำสั่งสำนักงานอัยการสูงสุด

(๓) สำนักบริหารทรัพยากรบุคคล ร่วมกับ ผู้ดูแลระบบของสำนักเทคโนโลยีสารสนเทศและการสื่อสารต้องดำเนินการยกเลิกสิทธิผู้ใช้งาน เมื่อมีการลาออกภายใน ๓ วัน หรือเมื่อมีการโยกย้ายเปลี่ยนตำแหน่งงานภายในหน่วยงาน โดยต้องดำเนินการภายใน ๗ วัน

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๖.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ ให้รวมถึงระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และการขอสิทธิผู้ใช้งานต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานของผู้ร้องขอเป็นลายลักษณ์อักษร ก่อนจะเสนอมายังผู้อำนวยการเพื่อพิจารณาและดำเนินการจัดสรรสิทธิเท่านั้น และผู้ดูแลระบบต้องกำหนดสิทธิเฉพาะการปฏิบัติงานในหน้าที่และให้ทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ

๖.๒ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร โดยการกำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ต้องไม่ซ้ำกัน ในกรณีที่จำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานคนใด ต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานเท่านั้น และให้กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และการกำหนดสิทธิพิเศษให้สามารถเข้าถึงข้อมูลของหน่วยงานในระดับใดบ้าง และกำหนดบัญชีผู้ใช้งานให้ต่างจากผู้ใช้งานปกติด้วย

๖.๓ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงระบบสารสนเทศและฟังก์ชั่น (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๑) ห้องที่มีสายสัญญาสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของผู้ใช้งานและบุคคลภายนอก

(๒) หลีกเลี่ยงการเดินสายสัญญาเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่เข้าถึงได้

(๓) กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานของบุคคลภายนอกโดยแบ่งสิทธิในการใช้งาน ดังนี้ ผู้ดูแลระบบ ผู้ใช้งาน

(๔) ควบคุมการเข้าออกโดยจัดทำเอกสารระบุสิทธิของผู้ใช้งานและบุคคลภายนอกในการเข้าถึงได้ดังนี้

๑. กำหนดสิทธิผู้ใช้งานที่มีสิทธิเข้าออกและลงเวลาในการเข้าออกในแต่ละพื้นที่อย่างชัดเจน

๒. การเข้าถึงพื้นที่ห้องศูนย์ข้อมูลของบุคคลภายนอกต้องให้มีการแลกบัตรประชาชนที่ใช้ระบุตัวตนของบุคคลนั้น ๆ และทำการลงบันทึกข้อมูลในสมุดการเข้าออกพร้อมรับบัตรผู้มาติดต่อ (Visitor) จากเจ้าหน้าที่รักษาความปลอดภัยภายในอาคาร และต้องติดบัตรตลอดเวลาในระหว่างการปฏิบัติงานหรือมาติดต่อ

๓. ต้องกำหนดสิทธิการเข้าออกของบุคคลภายนอกและอนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ ของหน่วยงานได้เฉพาะที่ผู้อำนวยการได้อนุญาตเท่านั้น และการควบคุมการปฏิบัติงานโดยเจ้าหน้าที่ที่ได้รับมอบหมายหรือผู้ดูแลระบบตลอด

๔. ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูลทำงานผิดปกติหรือหยุดทำงาน

๖.๔ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องดำเนินการ ดังนี้

(๑) การจำกัดการเข้าถึงระบบสารสนเทศและควบคุมการเข้าใช้งาน โดยแยกระบบที่มีความสำคัญไว้เป็นการเฉพาะออกจากระบบอื่น ๆ และต้องแสดงให้เห็นถึงผลกระทบและระดับความสำคัญของหน่วยงาน มีระบบรักษาความปลอดภัยโดยอนุญาตเฉพาะผู้มีสิทธิในการเข้าถึง

(๒) การจำกัดการเข้าถึงต้องมีการ Lock กุญแจเครื่องแม่ข่ายให้บริการ โดยต้องควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ

(๓) จำกัดการเข้าถึงโดยจำกัดสิทธิผู้ใช้งานให้สามารถเข้ามาอ่านได้เพียงอย่างเดียว และเฉพาะบุคคลที่มีส่วนเกี่ยวข้องกับโปรแกรมระบบงานดังกล่าวเท่านั้น

(๔) ต้องควบคุมอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่จากการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบ

(๕) ผู้ใช้งานไม่สามารถ Remote ผ่านการ Login มาจากเครือข่ายภายนอกองค์กรหรือเครือข่ายไร้สายที่ให้บริการสำหรับบุคคลภายนอกของหน่วยงานได้

๖.๕ การควบคุมอุปกรณ์คอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องระบบสารสนเทศของหน่วยงานจากความเสี่ยงจากการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ *(อ้างตามระเบียบสำนักงานอัยการสูงสุดว่าด้วยเครื่องคอมพิวเตอร์พกพา พ.ศ. ๒๕๕๕ ประกอบระเบียบสำนักงานอัยการสูงสุดว่าด้วยการให้ข่าวและบริการข่าวสาร พ.ศ. ๒๕๕๔)*

๖.๖ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน ต้องปฏิบัติดังนี้

(๑) ต้องได้รับอนุญาตจากผู้อำนวยการและผู้บริหารระดับสูงก่อนทุกครั้ง

(๒) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานตลอดเวลา โดยการกำหนดสิทธิการเข้าถึงให้กับหน่วยงานนั้นๆ ให้เข้าถึงได้เฉพาะบางระบบงานหรือบางส่วน และต้องดำเนินการภายในเวลาราชการเท่านั้น

(๓) หากใช้งานเรียบร้อยแล้ว ให้ปิดการใช้งานจากภายนอกหน่วยงานทันที

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๗.๑ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่การใช้งานระบบเครือข่ายไร้สายให้น้อยที่สุด

๗.๒ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSI (Service Set Identifier) ที่ถูกกำหนดเป็นค่ามาตรฐาน (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

๗.๓ ผู้ดูแลระบบกำหนดค่า Wireless Security เป็นแบบ WPA/WPA2 (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ แบบไร้สาย (Access Point)

๗.๔ ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุมบัญชีผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มีบัญชีผู้ใช้งาน และรหัสผ่านตามที่กำหนดไว้เท่านั้น เพื่อให้เข้าใช้งานระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๗.๕ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย และบันทึกเหตุการณ์ที่น่าสงสัยที่อาจเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการทราบทันที

๗.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานข้อมูลสารสนเทศผ่านระบบเครือข่ายไร้สาย และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

๗.๗ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานต้องทำการลงทะเบียนกับสำนักเทคโนโลยีสารสนเทศและการสื่อสาร และต้องได้รับอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษรและส่งมายังผู้อำนวยการเพื่อพิจารณาและดำเนินการจัดสรรสิทธิก่อนทุกครั้ง

๗.๘ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งต้องทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ และต้องได้รับอนุญาตจากผู้อำนวยการตามความจำเป็นในการใช้งาน

ส่วนที่ ๘ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

๘.๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมดของหน่วยงาน

๘.๒ การกำหนดค่าเริ่มต้นพื้นฐานของ Firewall กำหนดเป็นปฏิเสธทั้งหมด (Deny) และทำการอนุญาต (Allow) เฉพาะที่ใช้งานเท่านั้น

๘.๓ ทุกเส้นทางเชื่อมต่อและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๘.๔ ผู้ใช้งานอินเทอร์เน็ตต้องทำการบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานด้วยบัญชีผู้ใช้งาน (User account) และรหัสผ่าน (User password) ทุกครั้ง

๘.๕ การเข้าถึงอุปกรณ์ Firewall ต้องเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายจากผู้อำนวยการให้ดำเนินการเท่านั้น

๘.๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่วิ่งเข้า-ออกผ่านอุปกรณ์ Firewall ต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน และต้องสำรองข้อมูลการกำหนดค่าอุปกรณ์ไฟร์วอลล์เป็นประจำทุกเดือนหรือทุกครั้งที่เปลี่ยนแปลงค่า

๘.๗ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์แม่ข่าย ต้องเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ผู้อำนวยการอนุญาตให้ใช้งาน และหากมีความจำเป็นใช้งานพอร์ตการเชื่อมต่อนอกเหนือจากที่กำหนดต้องได้รับความยินยอมจากผู้อำนวยการก่อนทุกครั้งด้วย

๘.๘ คอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงาน ต้องไม่อนุญาตให้เชื่อมต่อเพื่อใช้งานเว็บไซต์ประเภทมัลติมีเดีย โดยกำหนดเป็นกรณีไป

๘.๙ หน่วยงานมีสิทธิที่จะระงับหรือบล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข และหากภายหลังอนุญาตให้ใช้งานแล้วยังปฏิบัติขัดต่อนโยบาย ประกาศหรือระเบียบ หรือก่อให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางสำนักเทคโนโลยีสารสนเทศและการสื่อสารต้องเสนอผู้บริหารระดับสูงและผู้บริหารระดับสูงสุดเพื่อโปรดทราบ และขอยกเลิกการให้สิทธิแก่ผู้กระทำผิดนั้นทันที

๘.๑๐ กำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย และกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการและให้ระบุข้อมูลดังนี้

(๑) หมายเลข Port ที่ต้องการขอเปิด

(๒) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(๓) วัตถุประสงค์หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้น ๆ

(๔) วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

ส่วนที่ ๙ การใช้งานเครือข่ายอินเทอร์เน็ต

๙.๑ ผู้ใช้งานมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

(๑) การลงทะเบียนบัญชีผู้ใช้งานระบบอินเทอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้งานโดยยื่นคำขอมายังสำนักเทคโนโลยีสารสนเทศและการสื่อสาร โดยผู้ใช้งานต้องเป็นบุคลากรของหน่วยงาน สำหรับบุคคลภายนอกที่ประสงค์ใช้งานต้องได้รับอนุญาตจากผู้อำนวยการหรือผู้บริหารระดับสูงก่อนทุกครั้ง

(๒) ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ขัดต่อศีลธรรมและเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

(๓) ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่ายหรือข้อมูลที่ส่งผ่านเครือข่ายของหน่วยงาน

(๔) ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานบัญชีผู้ใช้งานของตนโดยเด็ดขาด หากเกิดปัญหาการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้งานนั้นต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(๕) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

(๖) ต้องระมัดระวังการดาว์นโหลดโปรแกรมจากอินเทอร์เน็ต และการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาว์นโหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลางาน

(๗) หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ออกจากอินเทอร์เน็ตด้วยการ Logout ออกจากระบบการพิสูจน์ยืนยันตัวตน (Authentication) และปิดเว็บบราวเซอร์ที่ใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๐ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑๐.๑ ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

(๑) การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการหรือตามภารกิจของหน่วยงาน ผู้ใช้งานต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน หรือจดหมายอิเล็กทรอนิกส์ภาครัฐเท่านั้น ห้ามไม่ให้ใช้จดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ระบบจดหมายจะขัดข้อง

(๒) การใช้งานจดหมายอิเล็กทรอนิกส์ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่เป็นการปลุกปั่นยั่วยุ เสียดสี หรือส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคลหรือก่อให้เกิดความเสียหายต่อหน่วยงาน

(๓) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) จดหมายลูกโซ่ (Chain Letter) จดหมายที่มีไวรัสไปให้ผู้รับโดยเจตนา และที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

(๔) ต้องทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ (โอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงในภายหลังมายังเครื่องคอมพิวเตอร์ของตน) เพื่อป้องกันข้อมูลจดหมายอิเล็กทรอนิกส์สูญหาย หรือถูกลบจากผู้ใช้งานอื่นภายในหน่วยงาน

(๕) ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จักและเสี่ยงต่อการติดไวรัสคอมพิวเตอร์

(๖) ผู้ใช้งานต้องตรวจสอบกล่องข้อความจดหมายอิเล็กทรอนิกส์ของหน่วยงานทุกวัน และต้องลบแฟ้มจดหมายอิเล็กทรอนิกส์ที่อ่านแล้วหรือที่ไม่ต้องการออกจากระบบจดหมายอิเล็กทรอนิกส์ เพื่อลดปริมาณการใช้เนื้อที่จดหมายอิเล็กทรอนิกส์ของหน่วยงาน

(๗) การแนบไฟล์สามารถแนบไฟล์ได้ไม่เกิน ๑๐ เมกะไบท์

(๘) ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ (อีเมล์ส่วนบุคคล) สำหรับใช้รับ-ส่งข้อมูลในระบบราชการ ตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่ ๑๑ การใช้งานเครือข่ายสังคมออนไลน์ (Social network)

๑๑.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๑.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักถึงด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์และเครือข่ายอยู่เสมอ และต้องรับผิดชอบทุกกรณีหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๑๑.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งสำนักเทคโนโลยีสารสนเทศและการสื่อสารโดยเร็วที่สุด เพื่อดำเนินการแก้ไขตามความเหมาะสม

๑๑.๔ การเผยแพร่ข้อมูลสู่สาธารณะโดยผ่านระบบสารสนเทศของหน่วยงาน เจ้าของข้อมูลต้องตรวจสอบความถูกต้องข้อมูลก่อนนำออกเผยแพร่ ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาดและมีความเสียหาย

เกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดของเจ้าหน้าที่ที่นำข้อมูลดังกล่าวออกเผยแพร่

และข้อมูลที่นำออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายและแนวปฏิบัติ ต้องได้รับความเห็นชอบจากผู้บริหารระดับสูงและผู้บริหารระดับสูงสุดก่อนนำออกเผยแพร่ทุกครั้ง

๑๑.๕ การเผยแพร่ข้อมูลสู่สาธารณะโดยผ่านระบบสารสนเทศของหน่วยงาน ให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่ผู้บริหารระดับสูงและผู้บริหารระดับสูงสุดได้สั่งการหรือเห็นชอบไว้เป็นอย่างอื่น

ส่วนที่ ๑๒ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันชุดคำสั่งไม่พึงประสงค์ (Software Licensing and intellectual property and Preventing Malware)

๑๒.๑ สำนักงานอัยการสูงสุดได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟแวร์อื่นใดที่ไม่มีสิทธิ หากตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๑๒.๒ ซอฟต์แวร์ (Software) ที่สำนักงานอัยการสูงสุดได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลงแก้ไขหรือทำสำเนา เพื่อนำไปใช้งานที่อื่นยกเว้นได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบ

๑๒.๓ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่สำนักงานอัยการสูงสุดได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นใช้เพื่อการศึกษาหรือเพื่อเผยแพร่ทางกฎหมายโดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้อำนวยการแล้วแต่กรณี

๑๒.๔ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และชุดคำสั่งไม่พึงประสงค์ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๑๒.๕ ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๑๒.๖ ผู้ใช้งานต้องพึงระวังไวรัสหรือชุดคำสั่งไม่พึงประสงค์ตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่สำนักเทคโนโลยีสารสนเทศและการสื่อสารทราบทันที

๑๒.๗ เมื่อผู้ใช้งานตรวจพบว่าระบบคอมพิวเตอร์ของตัวเองติดไวรัส ต้องปลดการเชื่อมต่อระหว่างคอมพิวเตอร์กับเครือข่ายทันที และต้องแจ้งให้สำนักเทคโนโลยีสารสนเทศและการสื่อสารทราบทันที

๑๒.๘ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ระบบสารสนเทศของหน่วยงาน

๑๒.๙ การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้แต่ต้องไม่ดำเนินการ ดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองสินทรัพย์ของหน่วยงานมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย (กรณีสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์)

๑๒.๑๐ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) ต้องควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) ต้องระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพ และความถูกต้องของซอฟต์แวร์ที่จะพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ต้องตรวจสอบไวรัสหรือชุดคำสั่งไม่พึงประสงค์หรือโปรแกรมแฝงในซอฟต์แวร์ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ ทันที

ส่วนที่ ๑๓ การบริหารจัดการสินทรัพย์ (Assets Management)

๑๓.๑ สำนักเทคโนโลยีสารสนเทศและการสื่อสารจัดทำและเก็บทะเบียนสินทรัพย์ และต้องตรวจสอบสินทรัพย์ (Inventory Check) ทุกประเภทตามระยะเวลาที่กำหนดไว้ปีละ ๑ ครั้ง หรือภายใน ๑ เดือน เมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ของหน่วยงาน

๑๓.๒ ผู้ใช้งานที่ไม่มีส่วนเกี่ยวข้องต้องไม่เข้าไปในห้องศูนย์ข้อมูล (Data Center) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการ

๑๓.๓ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือเครื่องมืออื่นใดเชื่อมต่อเข้ากับระบบเครือข่ายของหน่วยงานเพื่อการประกอบธุรกิจส่วนบุคคล

๑๓.๔ ผู้ใช้งานต้องไม่ทำการคัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานของหน่วยงานก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

๑๓.๕ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่สำนักงานอัยการสูงสุดมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยต้องรับผิดชอบการรับ/คืนสินทรัพย์ ซึ่งจะถูกบันทึกและตรวจสอบทุกครั้งจากผู้ดูแลระบบหรือผู้อำนวยการ

๑๓.๖ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมอุปกรณ์เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (PC) หรือคอมพิวเตอร์แบบพกพา (Notebook) ไม่ว่ากรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงานหรือผู้อำนวยการ แล้วแต่กรณี

๑๓.๗ ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อปฏิบัติงานในหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อหน่วยงาน และความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อนี้ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๑๔ การบริหารจัดการระบบการเชื่อมโยงข้อมูลกับหน่วยงานภายนอก

๑๔.๑ ระบบสารสนเทศที่เชื่อมโยงแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก (Data Exchange System : DXS) ให้หัวหน้าหน่วยงานที่มีส่วนเกี่ยวข้องและผู้บริหารระดับสูงพิจารณาประเด็นทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่าง ๆ ก่อนตัดสินใจให้ใช้ข้อมูลร่วมกันในระบบสารสนเทศที่ตกลงเชื่อมโยงกันกับหน่วยงานในกระบวนการยุติธรรม ๑๐ หน่วยงาน

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกันและบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒) จำกัดหรือไม่อนุญาตการเข้าถึงข้อมูล

(๓) พิจารณาว่าบุคคลใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

(๔) กำหนดวิธีการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้ใช้งานข้อมูลสำคัญหรือข้อมูลที่เป็นความลับร่วมกัน ในกรณีที่ระบบไม่มีมาตรการป้องกันที่ดีเพียงพอ

๑๔.๒ กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมายและต้องชดใช้ค่าเสียหายกรณีสินทรัพย์นั้นเกิดการชำรุด สูญหายตามมูลค่าหรือเกิดความเสียหายอันเกิดจากความประมาทของผู้ใช้งาน และทุกกรณีโดยไม่มีข้อโต้แย้งใด ๆ

ส่วนที่ ๑๕ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ให้ปฏิบัติดังต่อไปนี้

๑๕.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง ต้องระบุตัวบุคคลที่เข้าถึงสื่อได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๑๕.๒ ห้ามผู้ดูแลระบบทำการแก้ไขข้อมูลที่ได้ทำการเก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงานหรือบุคคลที่หน่วยงานมอบหมาย

๑๕.๓ บันทึกการทำงานของระบบสารสนเทศ บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบสารสนเทศเพื่อป้องกันการบุกรุก บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ โดยต้องทำการจัดเก็บข้อมูล log ไว้ใช้ในการตรวจสอบอย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานนั้นสิ้นสุดลง

๑๕.๔ ป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล log ต่าง ๆ และจำกัดสิทธิการเข้าถึงข้อมูล log เหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวด ๒
นโยบายระบบสารสนเทศและระบบสำรองข้อมูล

วัตถุประสงค์

เพื่อจัดให้มีระบบสารสนเทศ ระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องให้บริการได้อย่างต่อเนื่อง มีมาตรการในการสำรองข้อมูลที่เป็นมาตรฐาน แนวทางปฏิบัติของผู้ดูแลระบบ และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินหรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

แนวปฏิบัติ

ส่วนที่ ๑ ระบบสำรองข้อมูลสารสนเทศและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

๑.๑ สำนักเทคโนโลยีสารสนเทศและการสื่อสารกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูลเมื่อมีระบบงานใหม่ เกิดข้อมูลใหม่หรือข้อมูลที่เปลี่ยนแปลงใหม่ ไว้ดังนี้

(๑) คัดเลือกประเภทข้อมูล ระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้ และความถี่ในการสำรองข้อมูล และระบบงานที่เปลี่ยนแปลงบ่อยให้มีความถี่ในการสำรองข้อมูลมากขึ้น ได้แก่

- โปรแกรมงานสารบบคดีอิเล็กทรอนิกส์
- ระบบประเมินผลการปฏิบัติราชการ
- ระบบบริหารอาคารและที่ดิน
- ระบบงานสารบรรณอิเล็กทรอนิกส์
- ระบบจัดสรรครุภัณฑ์ e-Survey

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง ซึ่งหมายถึง การสำรองข้อมูลแบบเต็ม (Full Backup) และกำหนดผู้รับผิดชอบในการสำรองข้อมูลให้ชัดเจน ซึ่งได้ดำเนินการกับโปรแกรมระบบสารบบคดีอิเล็กทรอนิกส์และทำการสำรองข้อมูล (Backup) เป็น ๒ แบบ ดังนี้

๑. แบบ Full Backup โดยใช้ฟังก์ชั่นการ backup ของ Oracle Database ที่เรียกว่า RMAN ซึ่งกำหนดให้เริ่มการ backup เวลา ๑๖.๓๐ น. ของทุกวัน โดยทำการจัดเก็บ File ที่สำรองไว้บน Tape

๒. แบบ Full Backup โดยใช้ฟังก์ชั่นการ export datapump ของ Oracle Database ซึ่งกำหนดให้เริ่มการ backup เวลา ๐๔.๐๐ น. ของทุกวัน โดยทำการจัดเก็บ File ที่สำรองไว้บน Disk

๓. แบบ Full Backup โดยใช้ฟังก์ชั่นการ export datapump ของ Oracle Database ซึ่งกำหนดให้เริ่มการ backup เวลา ๐๘.๐๐ น. ทุกวันเสาร์ โดยทำการจัดเก็บ File ที่สำรองไว้บน Tape

<u>หมายเหตุ</u> การสำรองข้อมูลแบบ Full Backup เป็นการสำรองข้อมูลทั้งหมดที่มีในฐานข้อมูล ทั้งข้อมูลเดิมและข้อมูลที่เปลี่ยนแปลง

(๓) จัดทำขั้นตอนปฏิบัติสำหรับการสำรองข้อมูล การกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ให้ชัดเจน รวมทั้งซอฟต์แวร์ที่ใช้ในการสำรองข้อมูล

(๔) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องทำการทบทวนและปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง รายละเอียดตามหนังสือด่วนที่สุด ของสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ที่ อส ๐๐๐๑.๑ (ทส)/๑๖๕๙ ลงวันที่ ๓๐ ตุลาคม ๒๕๖๑ และแผนฯ ดังกล่าวได้ถูกประกาศไว้ทางเว็บไซต์ http://www.ictc.ago.go.th/new_ictc๒/Files/RiskPlanICT๒๕๖๒.pdf

(๕) ผู้ดูแลระบบบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ต้องบันทึกข้อมูลผู้ดำเนินการ วัน/เวลา ชื่อฐานข้อมูลหรือข้อมูลที่ทำการสำรอง สำเร็จ/ไม่สำเร็จ

(๖) จัดเก็บข้อมูลที่สำรองไว้ในสื่อเก็บข้อมูล โดยต้องพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่/เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ต้องใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้ และต้องทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้นเป็นสำคัญ

(๗) ตรวจสอบและทดสอบประสิทธิภาพ ประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ บันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และต้องสำรองซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการตั้งค่า (Configuration) ข้อมูลในฐานข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม

(๘) จัดเก็บข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด ระยะทางระหว่างสถานที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันประมาณ ๒๐ กิโลเมตร เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่ในกรณีที่เกิดภัยพิบัติไฟไหม้ เหตุการณ์จลาจลทางการเมืองกับหน่วยงาน หรือเหตุอื่น

(๙) กำหนดให้ต้องทบทวนแผนการดำเนินงานระบบสารสนเทศ ระบบสำรองข้อมูลและแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๒ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

๒.๑ การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย

(๑) ให้ผู้ใช้งานต้องแจ้งไปยังสำนักเทคโนโลยีสารสนเทศและการสื่อสารทันทีที่มีเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบสนเทศของหน่วยงาน ดังนี้

(ก) มีไวรัสหรือชุดคำสั่งไม่พึงประสงค์เข้ามาในระบบ
(ข) มีการบุกรุกเข้ามาในเครือข่าย
(ค) ข้อมูลสำคัญมีการเปลี่ยนแปลงหรือสูญหาย
(ง) มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
(จ) มีการนำข้อมูลที่สำคัญไปใช้ผิดวัตถุประสงค์
(ฉ) มีการใช้ระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์
(ช) พบจุดอ่อนในระบบงาน ซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้งาน
(ซ) มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้
(ฌ) ระบบสารสนเทศชำรุดหรือสูญหาย
(ญ) บุคคลภายนอกเข้าใช้ระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

(ฎ) มีการติดตั้งซอฟต์แวร์เพื่อขโมยข้อมูล เข้าถึงข้อมูลหรือเหตุการณ์อื่นที่เป็นการละเมิดต่อความมั่นคงปลอดภัยของหน่วยงาน

๒.๒ ผู้อำนวยการเมื่อได้รับแจ้งเหตุตามข้อ ๒.๑ จากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติดังนี้

(๑) ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้น ว่ามีผลกระทบระดับใด

(๒) แจ้งผู้บริหารระดับสูง และผู้บริหารระดับสูงสุดทราบทันที

(๓) ต้องทำการวิเคราะห์ปัญหาและแก้ไขปัญหาตามความจำเป็น โดยดำเนินการร่วมกับทีมที่ปรึกษาด้านเทคโนโลยีสารสนเทศ แล้วแต่กรณี

(๔) กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ มีผู้เชี่ยวชาญหรือผู้ที่ผ่านการอบรมหรือได้รับการฝึกฝนเป็นผู้ดำเนินการ เพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัยและจำกัดการเข้าถึงหลักฐานนั้น

(๕) จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลางขึ้นไป และแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีรายละเอียดข้อมูลดังนี้

- รายละเอียดเหตุการณ์
- วันเวลา สถานที่เกิดเหตุ
- ชื่อผู้แจ้ง/หน่วยงาน
- สถานะของเหตุการณ์ในแต่ละช่วงเวลา
- ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา
- สาเหตุและวิธีการแก้ไข
- ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

๒.๓ ความรับผิดชอบของผู้อำนวยการกรณีที่มีการละเมิดการปฏิบัติ ต้องปฏิบัติดังนี้

(๑) ให้รายงานต่อผู้บริหารระดับสูง และผู้บริหารระดับสูงสุดทราบ

(๒) สั่งการสอบสวนหาตัวผู้กระทำความผิดและผู้รับผิดชอบให้เร็วที่สุด

(๓) พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เกิดเหตุการณ์ซ้ำได้อีก

(๔) ต้องพิจารณาบทลงโทษ เสนอผู้บริหารระดับสูงและผู้บริหารระดับสูงสุด เพื่อสั่งการลงโทษทางวินัย หรือดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ต่อผู้ละเมิด ผู้เกี่ยวข้องและผู้รับผิดชอบเมื่อมีการละเมิดตามระเบียบนี้จะโดยเจตนาหรือไม่เจตนาก็ดี และการละเมิดนั้นจะเกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อราชการก็ตาม

๒.๔ ความรับผิดชอบของผู้ดูแลระบบ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ดำเนินการ ดังนี้

(๑) พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่าง ๆ หรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศ มีผลกระทบหรือสร้างความเสียหายต่อราชการอย่างไรบ้าง

(๒) ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดทันที ในการนี้ต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติพร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร

๒.๕ ความรับผิดชอบของผู้ใช้งานต่อประกาศ

(๑) ปฏิบัติตามประกาศนี้อย่างเคร่งครัด และต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

(๒) ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไขหรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบสารสนเทศและเครือข่ายของหน่วยงาน

(๓) ไม่รบกวน หรือแทรกแซงการสื่อสารข้อมูลในระบบอินเทอร์เน็ตและเครือข่ายของหน่วยงาน

(๔) รายงานความเสี่ยง จุดอ่อน จุดแข็ง หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังสำนักเทคโนโลยีสารสนเทศและการสื่อสารโดยเร็วที่สุด

หมวด ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศหรือสถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

๑.๑ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยสำนักงานตรวจสอบภายในของสำนักงานอัยการสูงสุด (Internal Auditor) ปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๓ จัดลำดับความสำคัญของความเสี่ยง และระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของสำนักงานอัยการสูงสุด เพื่อประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศที่ได้รับความเสียหายจากผู้ใช้งาน (Human error) ไวรัสคอมพิวเตอร์ (Computer Virus) ระบบไฟฟ้าขัดข้อง ความเสียหายจากเพลิงไหม้ การโจรกรรมและการขโมยอุปกรณ์คอมพิวเตอร์

๑.๔ กำหนดวิธีการตรวจสอบและการประเมินความเสี่ยง และความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๑.๕ การตรวจสอบและการประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ อย่างน้อยดังนี้

(๑) การระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๒) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบเทคโนโลยีสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีระบบจัดเก็บเครื่องมือจากการเข้าถึงโดยไม่ได้รับอนุญาต และกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๓) กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ต้องสร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือจัดเก็บไว้โดยต้องป้องกันอย่างดี

(๔) ต้องเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log แสดงการเข้าถึง รวมถึงวัน และเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

(๖) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

(๗) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๑.๖ กำหนดมาตรการจัดการความเสี่ยง

(๑) ต้องทบทวนแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) เป็นประจำทุกปี

(๒) จัดทำคู่มือมาตรฐานการให้บริการ (Service Level Agreement : SLA) ด้านเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด เพื่อใช้เป็นแนวทางในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยจะทำการทบทวนอีกครั้งเมื่อมีการปรับเปลี่ยนกระบวนการปฏิบัติงาน

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศ

๒.๑ ความเสี่ยงจากการติดตามตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบสารสนเทศสามารถแยกออกได้ ๕ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่ บุคลากร (Human error) เนื่องจากขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบสารสนเทศเกิดความเสียหาย ชะงักงันหรือหยุดการทำงาน ส่งผลให้การทำงานของระบบไม่เต็มประสิทธิภาพ จึงกำหนดแนวทางการปฏิบัติเพื่อลดความเสี่ยงไว้ ดังนี้

(๑) จัดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness training) แก่ผู้ใช้งานของหน่วยงาน และหลักสูตรการสร้างความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ในเบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุดหรือลดน้อยลง

(๒) จัดทำหนังสือเวียนแจ้งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ให้ทุกหน่วยงานในสังกัดสำนักงานอัยการสูงสุดทราบ

ประเภทที่ ๒ ภัยที่เกิดจาก Software ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) ที่สร้างความเสียหายให้กับสินทรัพย์ของหน่วยงาน เหล่านี้อาจก่อให้เกิดความเสียหายแก่ระบบสารสนเทศได้จึงกำหนดแนวปฏิบัติไว้ ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้ง Antivirus Software เพื่อดักจับไวรัสที่เข้ามาในระบบเครือข่าย และต้องตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบสารสนเทศของหน่วยงาน

ประเภทที่ ๓ ภัยจากระบบไฟฟ้าขัดข้อง ความเสียหายจากเพลิงไหม้ จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบสารสนเทศ จึงกำหนดแนวปฏิบัติไว้ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับอุปกรณ์คอมพิวเตอร์แม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบสารสนเทศและเครือข่ายจะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดกระแสไฟฟ้าลัดวงจรหรือเกิดเหตุการณ์กระแสไฟฟ้าขัดข้อง หรือมีควันไฟเกิดขึ้นภายในห้องศูนย์ข้อมูล (Data Center) ซึ่งอุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนไปยังผู้รับผิดชอบ และรีบเข้ามาระงับเหตุฉุกเฉินได้ทันท่วงที และต้องตรวจสอบและทดสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องศูนย์ข้อมูล (Data Center) เพื่อใช้ในกรณีเหตุไฟไหม้ โดยต้องตรวจสอบถังก๊าซอย่างสม่ำเสมอ

<u>ประเภทที่ ๔</u> ภัยจากธรรมชาติ ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบสารสนเทศ จึงกำหนดแนวปฏิบัติไว้ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลาในกรณีที่อยู่ในภาวะเสี่ยงต่อการเกิดน้ำท่วม

(๒) ถอดเทป Backup ข้อมูลทั้งหมดไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องศูนย์ข้อมูล (Data Center) โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

(๔) ช่วยกันเคลื่อนย้ายอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดแล้ว ต้องให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องศูนย์ข้อมูล (Data Center) ให้ใช้การได้ดี และเตรียมความพร้อมห้องศูนย์ข้อมูล (Data Center) ในการติดตั้งอุปกรณ์และเครือข่าย

(๖) ติดตั้งอุปกรณ์และเครือข่าย พร้อมทำการทดสอบการใช้งานเครือข่ายให้สามารถใช้งานได้ปกติ และเชื่อมต่อเครือข่าย (Network) เข้ากับอุปกรณ์คอมพิวเตอร์ลูกข่ายได้อย่างมีประสิทธิภาพ

(๗) เมื่อตรวจสอบการทำงานของอุปกรณ์และเครือข่ายสามารถใช้งานได้ดีแล้ว ให้แจ้งหน่วยงานที่เกี่ยวข้องทราบ เพื่อให้ใช้งานได้ตามปกติ

<u>ประเภทที่ ๕</u> การโจรกรรมและการขโมยอุปกรณ์คอมพิวเตอร์ ความเสี่ยงนี้จัดเป็นภัยที่อาจเกิดขึ้นได้ ซึ่งผู้ดูแลระบบต้องมีมาตรการในการควบคุมการเข้า-ออก ห้องศูนย์ข้อมูล (Data Center) อย่างเป็นระบบ ต้องบันทึกข้อมูลการเข้า-ออก และมีหนังสือขออนุญาตจากผู้อำนวยการ

<u>ประเภทที่ ๖</u> ภัยที่เกิดจากการมุ่งร้ายต่อองค์กร ได้แก่ การประท้วง การจราจล การก่อวินาศกรรม อาจทำให้ระบบสารสนเทศเกิดความเสียหาย ชะงักงันหรือหยุดการทำงาน ส่งผลให้การทำงานของระบบไม่เต็มประสิทธิภาพ จึงกำหนดแนวทางการปฏิบัติเพื่อลดความเสี่ยงไว้ ดังนี้

(๑) จัดทำศูนย์สำรองระบบสารสนเทศ (Disaster Recovery Site) และจัดทำระบบสำรองข้อมูล (Backup System) ห่างจาก main site ประมาณ ๑๖๐ กิโลเมตร หรือพิจารณาจากภัยพิบัติรอบข้าง เพื่อสร้างความปลอดภัยของข้อมูลและสามารถนำข้อมูลที่ได้สำรองไว้กลับมาใช้งานผ่านระบบสารสนเทศได้อย่างเต็มรูปแบบ กรณี main site เกิดความเสียหายจากภัยพิบัติธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม ความเสียหายจากเหตุการณ์พื้นที่เสี่ยง เช่น ไฟไหม้ ไฟดับ network ไม่สามารถใช้งานได้เป็นเวลานาน และเหตุการณ์ทางการเมือง หรือความเสียหายจากอุปกรณ์ IT การดำเนินงานที่ผิดพลาด หรืออื่น ๆ ที่ทำให้เกิด downtime <u>ทั้งนี้ โครงการดังกล่าวสำนักเทคโนโลยีสารสนเทศและการสื่อสารได้เสนอขออนุมัติมาอย่างต่อเนื่องตั้งแต่ปี พ.ศ. 2557 แต่ยังไม่ได้รับงบประมาณสนับสนุนแต่อย่างใด</u>

(๒) เก็บข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันประมาณ ๒๐ กิโลเมตร เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่

(๓) ติดตั้งระบบเตือนเพลิงไหม้ อุณหภูมิสูงเกินกำหนด น้ำรั่วซึม พร้อมระบบ SMS

(๔) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับอุปกรณ์

หมวด ๔
นโยบายการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

วัตถุประสงค์

เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศให้กับผู้ใช้งานของหน่วยงาน ป้องกันการกระทำความผิดทางคอมพิวเตอร์อันอาจเกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน และเพื่อให้การใช้งานเครือข่ายและระบบสารสนเทศมีความมั่นคงปลอดภัย

แนวปฏิบัติ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

๑. จัดทำหลักสูตรฝึกอบรม และจัดทำคู่มือการใช้งานระบบสารสนเทศและเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๒. จัดประชุมสัมมนา อบรมหรือมีหนังสือเวียนแจ้งหน่วยงาน ในการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งานได้ทราบ โดยสอดแทรกเนื้อหาไปกับหลักสูตรอื่น ๆ ของหน่วยงานที่จัดอยู่ได้ และอาจเชิญวิทยากรจากหน่วยงานภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดองค์ความรู้

๓. ติดประกาศ ประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวนโยบายและแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย และต้องปรับปรุงความรู้ให้ทันสมัยและง่ายต่อการจดจำอยู่เสมอ โดยต้องทบทวน ปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุดให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

๔. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผลและสำรวจความต้องการของผู้ใช้งาน

๕. สร้างความตระหนักเกี่ยวกับไวรัสหรือชุดคำสั่งไม่พึงประสงค์ เพื่อให้บุคลากรของหน่วยงานมีความรู้ความเข้าใจ ป้องกันตนเองได้ และรับทราบขั้นตอนปฏิบัติเมื่อพบเหตุว่าต้องดำเนินการในเบื้องต้นอย่างไร

๖. สร้างความเข้าใจให้แก่ผู้ใช้งาน ให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรืออาจเกิดขึ้นอย่างไม่คาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของสำนักงานอัยการสูงสุด

๗. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบต่าง ๆ ของหน่วยงานอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด ๕
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้บริหารระดับสูงสุด ผู้อำนวยการ หัวหน้ากลุ่มงานและบุคคลภายนอกที่ได้รับมอบหมาย ให้ดำเนินการหรือดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศในแต่ละระดับ ดังนี้

แนวปฏิบัติ

๑. ระดับนโยบาย ผู้รับผิดชอบ คือ

- ผู้บริหารระดับสูงสุด หมายความว่า อัยการสูงสุด
- ผู้บริหารระดับสูง หมายความว่า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)
- ผู้บริหารเหนือขึ้นไป ๑ ระดับ หมายความว่า ผู้อำนวยการสำนักงานบริหารกิจการสำนักงานอัยการสูงสุด
- ผู้อำนวยการ หมายความว่า ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

(๑) มีหน้าที่ความรับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับบริหารและระดับปฏิบัติ

(๒) บริหารความเสี่ยง ควบคุมความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) ตรวจสอบและมีข้อสั่งการในการดำเนินการทางวินัย ในกรณีกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ตามระเบียบสำนักงานอัยการสูงสุดว่าด้วยการให้ข่าวและบริการข่าวสาร พ.ศ. ๒๕๕๔ ประกอบตามระเบียบคณะกรรมการอัยการเกี่ยวกับการดำเนินทางวินัยของธุรการ พ.ศ. ๒๕๕๔ และตามพระราชบัญญัติระเบียบข้าราชการฝ่ายอัยการ พ.ศ. ๒๕๕๓

๒. ระดับบริหาร ผู้รับผิดชอบ คือ หัวหน้ากลุ่มงาน มีหน้าที่ความรับผิดชอบ ดังนี้

(๑) กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) ควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล และบำรุงรักษาระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและระบบคอมพิวเตอร์

(๓) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศ จากสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบสารสนเทศ

(๔) ป้องกันการเข้าถึงเครือข่ายของหน่วยงานจากผู้ไม่ประสงค์ดี และแก้ไขปัญหาการเข้าถึงระบบจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๕) ป้องกันการรักษาความปลอดภัยระบบอินเทอร์เน็ต

๓. ระดับปฏิบัติ ผู้รับผิดชอบ คือ นักวิชาการคอมพิวเตอร์ และบุคคลภายนอกที่ได้รับมอบหมาย มีหน้าที่ความรับผิดชอบ ดังนี้

(๑) ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) สำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(๓) ปฏิบัติงานตามที่ได้รับมอบหมาย

ทั้งนี้ บุคลากรที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ชื่อ – สกุล	ตำแหน่ง	เบอร์ที่ทำงาน	มือถือ
นายรัชต์เทพ ดีประหลาด	ผู้อำนวยการสำนักงานบริหารกิจการสำนักงานอัยการสูงสุด	๐๒-๑๔๒๑๕๔๕	๐๘๕-๖๖๑๙๕๙๖
กลุ่มอำนวยการ			
นางณฐนน แก้วกระจ่าง	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร	๐๒-๕๑๕๔๑๘๙	๐๙๘-๘๒๙๐๕๙๖
นายนพพล พิเศษพงษา	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๘๐	๐๘๑-๔๔๕๐๖๑๙
น.ส.ณัฐสุดา วังแก้ว	นักจัดการงานทั่วไปปฏิบัติการ	๐๒-๕๑๕๔๑๗๙	๐๙๒-๕๓๙๘๙๒๖
น.ส.สุกัญญา ไชยพงษ์	เจ้าพนักงานธุรการปฏิบัติงาน	๐๒-๕๑๕๔๑๘๔	๐๘๑-๘๖๖๔๙๔๑
นายชาญวิทย์ หงษ์ทอง	เจ้าพนักงานธุรการปฏิบัติงาน	๐๒-๕๑๕๔๑๘๒	๐๖๔-๗๙๑๕๕๗๕
นายวีรยุทธ สวนพรม	เจ้าพนักงานธุรการปฏิบัติงาน	๐๒-๕๑๕๔๑๘๔	๐๙๑-๐๓๙๐๒๓๓
กลุ่มแผนงานเทคโนโลยีสารสนเทศ			
น.ส.ภูริดา จันต๊ะพรมมา	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๗๖	๐๘๑-๐๓๓๕๗๙๘
น.ส.อุษา สิริปรีดากุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๗๗	๐๘๔-๗๒๐๗๓๙๐
น.ส.เบญญาภา ดีชานนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๗๗	๐๘๐-๑๐๘๕๐๙๑
กลุ่มระบบเครื่องคอมพิวเตอร์และแม่ข่ายระบบเครือข่ายและความมั่นคงปลอดภัยของระบบคอมพิวเตอร์			
น.ส.ชุติภัค เงินเจือ	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๘๓	๐๙๑-๗๓๔๙๗๕๕
นายพนธ์พิวัชร์ ชมสุรินทร์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๓	๐๘๑-๔๐๓๔๔๙๔
นายอนวัช ทินเลย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๗	๐๘๗-๗๗๔๔๘๒๒
นายเกริกเกียรติ สุขเนาว์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๗	๐๘๐-๒๘๑๕๙๓๘
กลุ่มสนับสนุน และบริหารงานเทคโนโลยีสารสนเทศ			
น.ส.สุรีพร ศิริภักดี	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๘๘	๐๘๙-๑๒๙๔๘๑๒
น.ส.อัจฉรา ภู่ระย้า	นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๒-๕๑๕๔๑๘๑	๐๘๔-๕๕๑๓๔๔๐
น.ส.เล็ก เบาราญ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๑	๐๘๔-๗๗๑๕๓๗๓
นายปรีชา กันหล้า	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๑	๐๘๑-๐๒๖๘๘๐๐
กลุ่มพัฒนาระบบงานคอมพิวเตอร์และฐานข้อมูล			
น.ส.ชฎาวัลย์ สิงห์อินทร์	นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๒-๕๑๕๔๑๘๖	๐๘๙-๖๖๐๓๘๓๐
นายพงศ์เดช โอวาสิทธิ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๗๘	๐๘๖-๘๑๒๘๘๑๐

ภาคผนวก

หนังสือแจ้งผลการพิจารณา

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของสำนักงานอัยการสูงสุด (ฉบับทบทวน)

จากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เมื่อวันที่ ๒๖ มีนาคม ๒๕๖๒ (การประชุมครั้งที่ ๒/๒๕๖๒)

ที่ ดศ ๐๒๐๗.๔/ ๓๒๑๕

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๒ เมษายน ๒๕๖๒

เรื่อง แจ้งผลการพิจารณานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด (ฉบับทบทวน)

กราบเรียน อัยการสูงสุด

อ้างถึง หนังสือสำนักงานอัยการสูงสุด ที่ อส๐๐๐๓.๑(ทส)/๒๖๗๔ ลงวันที่ ๖ มีนาคม ๒๕๖๒

ตามหนังสือที่อ้างถึง สำนักงานอัยการสูงสุดได้นำส่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวน) และแบบแสดงรายการทบทวนนโยบายและแนวปฏิบัติฯ พร้อมเอกสารอ้างอิง เพื่อให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณาให้ความเห็นชอบ ความละเอียดแจ้งแล้ว นั้น

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ขอกราบเรียนให้ทราบว่าคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีมติในการประชุม ครั้งที่ ๒/๒๕๖๒ เมื่อวันที่ ๒๖ มีนาคม ๒๕๖๒ เห็นชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด (ฉบับทบทวน) พร้อมแจ้งเพิ่มเติมว่าการพิจารณาให้ความเห็นชอบดังกล่าวเป็นมาตรการขั้นต่ำในการลดความเสี่ยงจากภัยคุกคามของระบบสารสนเทศ เพื่อก่อให้เกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ หน่วยงานจะต้องให้ความสำคัญ โดยประกาศนโยบายและแนวปฏิบัติฯ ให้ผู้เกี่ยวข้องทราบ และควรมีการซักซ้อม รวมถึงจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอเพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยในทางปฏิบัติ และอาจปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

จึงกราบเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถืออย่างยิ่ง

(นางคนึงนิจ คชศิลา)
ผู้ตรวจราชการกระทรวง ปฏิบัติราชการแทน
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เรียน ผอ.สทส.
☐ เพื่อโปรดพิจารณา
☐ เพื่อโปรดทราบ
☐ เพื่อควรเวียนให้ทราบทั่วกัน
☑ เห็นควรมอบให้ กลุ่มงาน... ดำเนินการ

(นายนพพล พิเศษพรชัย)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
- ๔ เม.ย. ๒๕๖๒

☐ ทราบ
☐ ดำเนินการตามเสนอ
☑ มอบให้ กลุ่มงาน... ดำเนินการ

(นางณฐนน แก้วกระจ่าง)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
- ๔ เม.ย. ๒๕๖๒

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๘ ๐ ๒๑๔๓ ๖๕๙๔
โทรสาร ๐ ๒๑๔๓ ๘๐๓๖ ๐ ๒๑๔๓ ๘๐๓๗

ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ สำนักงานบริหารกิจการ อส. สำนักเทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐ ๒๕๑๕ ๔๑๗๖

ที่ อส ๐๐๐๑.๑(ทส)/๔๓๙ **วันที่** ๑๗ เมษายน ๒๕๖๒

เรื่อง ผลการพิจารณานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด (ฉบับทบทวน)

กราบเรียน อัยการสูงสุด (ผ่าน ผอ.สบกส)

๑. เรื่องเดิม

ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด (ฉบับทบทวน) ตามหนังสือที่ ดศ ๐๒๐๗/๓๒๑๕ ลงวันที่ ๒ เมษายน ๒๕๖๒

๒. ข้อเท็จจริง

๒.๑ สำนักงานอัยการสูงสุดได้ปฏิบัติตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยสำนักเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) ในฐานะเป็นหน่วยงานผู้ดูแลและปรับปรุงพัฒนาระบบสารสนเทศของสำนักงานอัยการสูงสุด ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษรเสนอและได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มาตั้งแต่ปีงบประมาณ พ.ศ. ๒๕๖๑

อนึ่ง ความในมาตรา ๖ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูลหรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ต้องจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย ซึ่ง สทส. ได้จัดทำร่างนโยบายและแนวปฏิบัติฯ และมีหนังสือกราบเรียนท่านอัยการสูงสุดเพื่อโปรดพิจารณา (รายละเอียดปรากฏตามหนังสือของสำนักงานบริหารกิจการ อส. สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ที่ อส ๐๐๐๑.๑(ทส)/๑๑๓ ลว. ๒๘ มกราคม ๒๕๖๒) มาแล้วนั้น

๒.๒ ต่อมาในปีงบประมาณ พ.ศ. ๒๕๖๒ สำนักงานอัยการสูงสุดได้เสนอขอทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ไปยังคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้มีหนังสือแจ้งมติที่ประชุมคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ ครั้งที่ ๒/๒๕๖๒ เมื่อวันที่ ๒๖ มีนาคม ๒๕๖๒ เห็นชอบนโยบายและแนวปฏิบัติในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด (ฉบับทบทวน) โดยการพิจารณาให้ความเห็นชอบดังกล่าวเป็นเพียงมาตรการขั้นต่ำในการความเสี่ยงจากภัยคุกคามของระบบสารสนเทศ เพื่อให้เกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ของสำนักงานอัยการสูงสุด และหน่วยงานต้องให้ความสำคัญโดยต้องประกาศนโยบายและแนวปฏิบัติฯ ให้ผู้ที่เกี่ยวข้องทราบ และต้องมีการซักซ้อม รวมถึงต้องตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อให้

ระบบ...

ระบบสารสนเทศมีความมั่นคงปลอดภัยในทางปฏิบัติ และควรมีการปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม รายละเอียดปรากฏตามเอกสารแนบท้าย

ทั้งนี้ นโยบายและแนวปฏิบัติฯ ที่คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ได้ให้ความเห็นชอบแล้วนั้นไม่อาจเปลี่ยนแปลงข้อความใด ๆ ได้อีก และหน่วยงานต้องให้ผู้บริหารระดับสูงสุด (อัยการสูงสุด) เป็นผู้ลงนามในประกาศให้ครบถ้วนก่อนประกาศไว้ที่หน้าเว็บไซต์ของสำนักงานอัยการสูงสุด www.ago.go.th โดยเร่งด่วนภายหลังจากที่ได้รับหนังสือแจ้งผลการพิจารณานโยบายและแนวปฏิบัติฯ และหน่วยงานต้องสแกนเอกสารและที่เกี่ยวข้องทั้งหมดที่ได้ประกาศ ส่งกลับไปยังสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อยืนยันความครบถ้วนถูกต้องตามที่คณะกรรมการตามกฎหมายได้ให้ความเห็นชอบไว้ โดยนางสาวภูริดา จันต๊ะพรมมา นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ สทส. จะเป็นผู้ประสานงานกับฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทางจดหมายอิเล็กทรอนิกส์ (e-Mail) และทางโทรศัพท์ หรือช่องทางการติดต่ออื่น

๒.๓ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของสำนักงานอัยการสูงสุดเป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๒ และประกาศนโยบายและแนวปฏิบัติฯ ให้บุคลากรของสำนักงานอัยการสูงสุดและผู้ที่เกี่ยวข้องทราบ เพื่อให้ถือปฏิบัติตามนโยบายและแนวปฏิบัติฯ อย่างเคร่งครัด จึงได้เสนอท่านอัยการสูงสุดเพื่อโปรดลงนามในประกาศและหนังสือที่เสนอมาพร้อมนี้

๓. ข้อพิจารณาและข้อเสนอแนะ

เพื่อให้สำนักงานอัยการสูงสุดปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยที่ได้แสดงไว้ จึงเห็นควรกราบเรียนท่านอัยการสูงสุดเพื่อโปรดพิจาณาดำเนินการ ดังนี้

๑) โปรดทราบการดำเนินการ ตามข้อ ๒.๑ และข้อ ๒.๒

๒) โปรดกราบเรียนอัยการสูงสุดเพื่อลงนามในประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๒ ตามข้อ ๒.๓

๓) มอบหมายให้รองอัยการสูงสุดลงนามในหนังสือเวียนแจ้งประกาศนโยบายและแนวปฏิบัติฯ ตามข้อ ๒.๓

จึงเรียนมาเพื่อโปรดทราบ และกราบเรียนท่านอัยการสูงสุดเพื่อโปรดทราบ ตามข้อ ๑) และโปรดลงนาม ตามข้อ ๒) และข้อ ๓) ที่เสนอมาพร้อมนี้

(นางสาวภูริดา จันต๊ะพรมมา)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

(นางณฐนน แก้วกระจ่าง)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

(นายรัชต์เทพ ดีประหลาด)
ผู้อำนวยการสำนักงานบริหารกิจการสำนักงานอัยการสูงสุด
๒๔ เม.ย. ๒๕๖๒

เสนอ รอสส.
เลขรับที่ ๔๖ (สทส)
วันที่ ๒๔ เม.ย. ๒๕๖๒
เวลา 14.35

สบกส.
เลขรับที่ ๒๔๒๗
วันที่ ๒๒ เม.ย. ๒๕๖๒

กราบเรียน อัยการสูงสุด

พิจารณาแล้ว เห็นควรมีคำสั่ง ดังนี้

๑. ทราบ ตามข้อ ๑

๒. ลงนามตามข้อ ๒

อนึ่ง ได้ลงนามในหนังสือเวียนแจ้งประกาศ ตามข้อ ๓ แล้ว

เพื่อโปรดพิจารณา

(นายเชิดศักดิ์ หิรัญสิริสมบัติ)
รองอัยการสูงสุด
๒๕ เม.ย. ๒๕๖๒

ทราบ
ลงนามแล้ว

(นายเข็มชัย ชุติวงศ์)
อัยการสูงสุด
๒๙ เม.ย. ๒๕๖๒

ทราบ

(นางเณฐนัน แก้วกระจาง)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
๒๙ เม.ย. ๒๕๖๒

อสส. ๑๙๖
เลขรับที่.....
วันที่ ๒๖ เม.ย. ๒๕๖๒
เวลา ๑๑.๐๐ น.

เอกสาร/หนังสือที่เกี่ยวข้อง
ในการจัดทำนโยบายและแนวปฏิบัติฯ

บันทึกข้อความ

ส่วนราชการ สำนักงานบริหารกิจการ อส. สำนักเทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐ ๒๕๑๕ ๔๑๗๗

ที่ อส ๐๐๐๑.๑(ทส)/ ๒๔๓ **วันที่** ๒๓ กุมภาพันธ์ ๒๕๖๒

เรื่อง การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

กราบเรียน อัยการสูงสุด (ผ่าน ผอ.สบกส)

๑. เรื่องเดิม

ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด (ตามหนังสือของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เลขที่ ดศ ๐๒๐๗/๘๖๑๐ ลงวันที่ ๕ ตุลาคม ๒๕๖๐) และข้อ ๓ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และความในมาตรา ๗ วรรค ๒ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และทบทวนปรับปรุงให้เป็นปัจจุบันอยู่เสมอ นั้น

๒. ข้อเท็จจริง

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) ในฐานะเป็นหน่วยงานผู้ดูแลและปรับปรุงพัฒนาระบบงานด้านเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด โดยกลุ่มแผนงานเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบตามภารกิจในการดำเนินการตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ มาตั้งแต่ต้น จึงได้ดำเนินการทบทวนปรับปรุงนโยบายและข้อปฏิบัติข้างต้น ให้ควบคุมการเข้าถึงสารสนเทศ และปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ทั้งนี้ กระบวนการเสนอขอทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ต้องดำเนินการตามขั้นตอนที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด โดยจัดทำร่างนโยบายและแนวปฏิบัติฯ พร้อมแบบแสดงรายการทบทวน และเอกสารทบทวน เสนอขอความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายตามมาตรา ๗ วรรค ๑ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ก่อนบังคับใช้

การขอทบทวนครั้งนี้ กลุ่มแผนงานเทคโนโลยีสารสนเทศ สทส. ได้รับการประสานกับฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ให้จัดทำร่างทบทวนนโยบายและแนวปฏิบัติฯ ของสำนักงานอัยการสูงสุดจัดส่งไปทางจดหมายอิเล็กทรอนิกส์ (e-Mail) เพื่อช่วยพิจารณาปรับแก้ไขในเบื้องต้นให้ถูกต้องตรงตามข้อกำหนดของกฎหมาย เป็นการลดภาระการพิจารณาปรับแก้ในชั้นของคณะกรรมการตามกฎหมาย เนื่องจากปัจจุบันมีการพิจารณาหน่วยงานของรัฐจำนวนมากและอาจทำให้เกิดความล่าช้าในการพิจารณาตามกระบวนการได้ และหากสำนักงานอัยการสูงสุดได้มีการปรับแก้ตามข้อสังเกตและข้อเสนอแนะของฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ครบถ้วนแล้ว และเห็นชอบการพิจารณาในเบื้องต้นกลับมาทางจดหมายอิเล็กทรอนิกส์ให้กับเจ้าหน้าที่ของกลุ่มแผนงานเทคโนโลยีสารสนเทศ สทส. เพื่อยืนยันเป็นหลักฐานการพิจารณา

ร่างทบทวน...

ร่างทบทวนนโยบายและแนวปฏิบัติฯ ในเบื้องต้นเรียบร้อยแล้ว สำนักงานอัยการสูงสุดจะต้องเสนอแบบแสดงรายการทบทวนฯ พร้อมเอกสารทบทวนทั้งหมดตามที่ฝ่ายเลขานุการฯ ได้เห็นชอบไว้ทั้งหมด เพื่อให้ผู้บริหารระดับสูงสุดหรือผู้บริหารระดับสูงของหน่วยงาน หรือผู้ได้รับมอบหมาย ลงนามในแบบแสดงรายการทบทวนฯ และทราบผลการดำเนินการของหน่วยงาน และลงนามในหนังสือถึงปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) จัดส่งสำเนาเอกสารจำนวน ๕ ชุด พร้อมแผ่นซีดี (CD) ไฟล์อิเล็กทรอนิกส์ เพื่อนำเข้าที่ประชุมคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณาให้ความเห็นชอบตามกระบวนการทางกฎหมายกำหนด ก่อนบังคับใช้ ต่อไป

บัดนี้ ฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้เห็นชอบการพิจารณาร่างทบทวนนโยบายและแนวปฏิบัติฯ ของสำนักงานอัยการสูงสุด ในเบื้องต้นกลับมาทางจดหมายอิเล็กทรอนิกส์แล้ว ซึ่งสำนักงานอัยการสูงสุดต้องเร่งดำเนินการเสนอผู้บริหารระดับสูงสุดหรือผู้บริหารระดับสูงของหน่วยงาน หรือผู้ได้รับมอบหมาย ลงนามในแบบแสดงรายการทบทวนฯ และลงนามในหนังสือถึงปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) เพื่อจัดส่งสำเนาเอกสาร จำนวน ๕ ชุด พร้อมไฟล์อิเล็กทรอนิกส์บันทึกลงในแผ่นซีดีรอม (CD-Rom)

อนึ่ง การจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา ๖ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ สทส. ได้จัดทำร่างดังกล่าวเสนออัยการสูงสุดเพื่อโปรดพิจารณาตามหนังสือที่ อส ๐๐๐๑.๑(ทส)/๑๑๓ ลงวันที่ ๒๘ มกราคม ๒๕๖๒ แล้วนั้น และได้ประสานจัดส่งร่างให้กับสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณาในเบื้องต้นอีกทางหนึ่งแล้ว

๓. ข้อพิจารณาและข้อเสนอแนะ

เพื่อให้สำนักงานอัยการสูงสุดมีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด ครบถ้วนตามมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และสามารถนำมาใช้บังคับตามกฎหมายธุรกรรมอิเล็กทรอนิกส์ ให้ระบบสารสนเทศของหน่วยงานมีความมั่นคงปลอดภัย เชื่อถือได้ จึงเห็นควรกราบเรียนท่านอัยการสูงสุดเพื่อโปรดพิจารณา ดังนี้

๓.๑ โปรดทราบการดำเนินงาน ตามข้อเท็จจริง

๓.๒ โปรดลงนามในแบบแสดงรายการทบทวนฯ

๓.๓ โปรดลงนามในหนังสือถึงบลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบโปรดกราบเรียนท่านอัยการสูงสุดเพื่อโปรดทราบตามข้อ ๓.๑ และโปรดลงนาม ตามข้อ ๓.๒ และข้อ ๓.๓ ที่เสนอมาพร้อมนี้

อุษา สิริบริดากุล

(นางสาวอุษา สิริบริดากุล)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(นางสาวภูริดา จันต๊ะพรมมา)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

(นายรัชต์เทพ ดีประหลาด)
ผู้อำนวยการ

นางณฐนน แก้วกระจ่าง
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

กราบเรียน อัยการสูงสุด

- เพื่อโปรดทราบตามข้อ ๓.๑
- โปรดลงนามตาม ข้อ ๓.๓ ตามที่ ผอ.สบกส.เสนอ

(นายเชิดศักดิ์ หิรัญสิริสมบัติ)
รองอัยการสูงสุด
- ๑ มี.ค. ๒๕๖๒

ทราบ
ลงนามแล้ว

(นายเข็มชัย ชุติวงศ์)
อัยการสูงสุด
- ๖ มี.ค. ๒๕๖๒

ทราบ

(นางณฐนน แก้วกระจ่าง)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

อสส.
เลขรับที่ ๑๑๙
วันที่ - ๕ มี.ค. ๒๕๖๒
เวลา ๐๙ ๔๐ น.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

พ.ศ. ๒๕๕๓

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย จึงเห็นความสำคัญที่จะนำกฎหมาย ข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๘ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอย่างน้อยต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

(๑) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๔ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕ - ๑๕

ข้อ ๕ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนดรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้ดำเนินการตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี

อาศัยอำนาจตามความในมาตรา ๖ วรรคสอง แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่มีรายชื่อแนบท้ายประกาศฉบับนี้ ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ประกาศ ณ วันที่ ๒๘ กรกฎาคม พ.ศ. ๒๕๕๙
อุตตม สาวนายน
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๑๘.ส่วนราชการไม่สังกัดสำนักนายกรัฐมนตรี กระทรวงหรือทบวง เฉพาะ

(๑) สำนักงานตำรวจแห่งชาติ

องค์กรตามรัฐธรรมนูญ

๑. สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ

๒. สำนักงานอัยการสูงสุด

รัฐวิสาหกิจ

๑. การเคหะแห่งชาติ

๒. การท่าอากาศยานแห่งประเทศไทย

๓. การท่าเรือแห่งประเทศไทย

๔. การประปาส่วนภูมิภาค

๕. การประปานครหลวง

๖. การไฟฟ้านครหลวง

๗. การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย

๘. การไฟฟ้าส่วนภูมิภาค

๙. การยางแห่งประเทศไทย

๑๐. การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

๑๑. การรถไฟแห่งประเทศไทย

๑๒. ธนาคารกรุงไทย จำกัด (มหาชน)

๑๓. ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย

๑๔. ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

๑๕. ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

๑๖. ธนาคารออมสิน

๑๗. ธนาคารอาคารสงเคราะห์

๑๘. ธนาคารอิสลามแห่งประเทศไทย

๑๙. บรรษัทตลาดรองสินเชื่อที่อยู่อาศัย

๒๐. บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม

๒๑. บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

๒๒. บริษัท การบินไทย จำกัด (มหาชน)

๒๓. บริษัท ขนส่ง จำกัด

สำเนาคู่ฉบับ

ที่ อส๐๐๐๑.๑(ทส)/ ๒๖๗๔

สำนักงานอัยการสูงสุด
อาคารราชบุรีดิเรกฤทธิ์
ศูนย์ราชการเฉลิมพระเกียรติฯ
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๖ มีนาคม ๒๕๖๒

เรื่อง ขอจัดส่งร่างแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๒

เรียน ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สิ่งที่ส่งมาด้วย (๑) ร่างประกาศฯ แนวนโยบายและแนวปฏิบัติ จำนวน ๑ ฉบับ
(๒) ร่างแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด จำนวน ๑ ชุด
(๓) แผ่น CD-ROM จำนวน ๑ ชุด

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนำเสนอต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) พิจารณาให้ความเห็นชอบก่อนจึงจะมีผลใช้บังคับตามกฎหมายธุรกรรมอิเล็กทรอนิกส์

สำนักงานอัยการสูงสุดได้มีการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ให้คำแนะนำและเห็นชอบร่างแนวนโยบายและแนวปฏิบัติฯ ในเบื้องต้นให้แล้ว ดังนั้น สำนักงานอัยการสูงสุดจึงขอส่งร่างแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๒ มาให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อนำเข้าที่ประชุมคณะกรรมการตามกฎหมายกำหนดพิจารณาให้ความเห็นชอบร่างดังกล่าว ก่อนมีผลบังคับใช้ตามกฎหมาย ตามสิ่งที่ส่งมาด้วย ๑ และ ๒

ทั้งนี้ เพื่อให้การจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๒ มีความครบถ้วน ถูกต้อง เป็นไปตามที่กฎหมายกำหนด โดยมอบหมายให้ นางสาวภูริดา จันตีะพรมมา นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐๘ ๑๐๓๓ ๕๗๔๘ โทรสาร. ๐๒ ๕๑๕ ๔๑๗๖ e-Mail : purida.j@ago.mail.go.th เป็นผู้ประสานงานของสำนักงานอัยการสูงสุด

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายเข็มชัย ชุติวงศ์)
อัยการสูงสุด

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานอัยการสูงสุด
โทร. ๐ ๒๕๑๕ ๔๑๗๖
โทรสาร ๐ ๒๕๑๕ ๔๑๘๙
E-mail : ictc@ago.go.th

...../ตรวจ
...../ร่าง/ทาน
...../พิมพ์

แบบแสดงรายการทบทวนนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยของหน่วยงานของรัฐ
(ครั้งที่ ๑ /ประจำปี พ.ศ. ๒๕๖๒) (นับตามปีงบประมาณ)

ชื่อหน่วยงาน สำนักงานอัยการสูงสุด

ระบุเอกสารประกอบการพิจารณา

๑. (ร่าง) ประกาศสำนักงานอัยการสูงสุด เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒

๒. แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๒

๓. แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) พ.ศ. ๒๕๖๒ **(สามารถแนบเพิ่มเติมได้)**

คำชี้แจง ให้ระบุ "มี" หากหน่วยงานมีการทบทวนและปรับแก้ไข และให้ระบุ "ไม่มี" หากไม่มีการทบทวนและปรับแก้ไข

ข้อ	ประเด็นการทบทวนนโยบาย / และแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หน่วยงานทบทวนเอกสาร (ระบุการปรับแก้ไข)	
		มี/ไม่มี	อ้างอิงหน้า... / ระบุรายละเอียดการปรับแก้ไข
๑	**กำหนดคำนิยาม**		
	(๑) ผู้ใช้งาน	ไม่มี	คำนิยาม หน้า ๒
	(๒) สิทธิของผู้ใช้งาน	ไม่มี	คำนิยาม หน้า ๒
	(๓) สินทรัพย์	ไม่มี	คำนิยาม หน้า ๒
	(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	ไม่มี	คำนิยาม หน้า ๓
	(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ	ไม่มี	คำนิยาม หน้า ๓
	(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย	ไม่มี	คำนิยาม หน้า ๓
	(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	ไม่มี	คำนิยาม หน้า ๓
	(๘) คำนิยามอื่น ๆ ตามความต้องการขององค์กร	ไม่มี	คำนิยาม หน้า ๒ - ๔
๒	**หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้**		เอกสารแนบท้ายประกาศ หน้า ๑ - ๓๙
	(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	มี	- หมวด ๑ หน้า ๗ - ๘
	(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง	มี	- หมวด ๒ หน้า ๓๐
	(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ	ไม่มี	- หมวด ๓ หน้า ๓๖
๓	**หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้**		เอกสารแนบท้ายประกาศ
	(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	มี	- ปรับปรุงหลักการและเหตุผล และวัตถุประสงค์ หน้า ๑ - เพิ่มคำนิยาม หน้า ๒ และในประกาศฯ ข้อ ๔(๔) (ผบ.เหนือขึ้นไป ๑ ระดับ)
	(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้	มี	ร่างประกาศสำนักงานอัยการสูงสุด - เพิ่มข้อ ๔ (๔) หน้า ๑ - เพิ่มข้อ ๑๒ หน้า ๖ - ประกาศฯ ข้อ ๒

ข้อ	ประเด็นการทบทวนนโยบาย / และแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หน่วยงานทบทวนเอกสาร (ระบุการปรับแก้ไข)	
		มี/ไม่มี	อ้างอิงหน้า... / ระบุรายละเอียดการปรับแก้ไข
	(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน	มี	- หมวด ๕ หน้า ๓๘ เพิ่ม ผบ.เหนือขึ้นไป ๑ ระดับ - ปรับปรุงหน้า ๓๘ - ๓๙
	(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ	ไม่มี	หมวด ๔ หน้า ๓๗
๔	**ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕ – ๑๕**	มี	เอกสารแนบท้ายประกาศหน้า ๑ – ๓๙ (ปรากฏตามรายละเอียดการปรับปรุงในแต่ละข้อ)
๕	**ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้**		หมวด ๑ หน้า ๕ – ๒๙
	(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย	มี	- แก้ไขหมวด ๑ หน้า ๗ - ๘
	(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ	ไม่มี	หมวด ๑ ส่วนที่ ๑ (๑.๓) หน้า ๕
	(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับ - ประเภทของข้อมูล - ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล - รวมทั้งระดับชั้นการเข้าถึง - เวลาที่ได้เข้าถึง - และช่องทางการเข้าถึง	มี	หมวด ๑ หน้า ๕ – ๘ - แก้ไขหมวด ๑ หน้า ๗ - ๘
๖	**ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย**	ไม่มี	หมวด ๑ หน้า ๘
๗	**ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ไม่มี	- หมวด ๑ สวนที่ ๒ หน้า ๑๐–๑๑ - หมวด ๔ หน้า ๓๗
	(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม	ไม่มี	หมวด ๔ หน้า ๓๗
	(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว	ไม่มี	หมวด ๑ ส่วนที่ ๒ (๒.๓) หน้า ๑๐

ข้อ	ประเด็นการทบทวนนโยบาย / และแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หน่วยงานทบทวนเอกสาร (ระบุการปรับแก้ไข)	
		มี/ไม่มี	อ้างอิงหน้า... / ระบุรายละเอียดการปรับแก้ไข
	(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง	ไม่มี	หมวด ๑ ส่วนที่ ๒ (๒.๔) หน้า ๑๐
	(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม	ไม่มี	หมวด ๑ ส่วนที่ ๒ (๒.๕) หน้า ๑๑
	(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้	ไม่มี	หมวด ๑ ส่วนที่ ๒ (๒.๖) หน้า ๑๑
๘	**ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ไม่มี	หมวด ๑ ส่วนที่ ๓ หน้า ๑๑ - ๑๔
	(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ	ไม่มี	หมวด ๑ ส่วนที่ ๓ (๓.๑) หน้า ๑๑ - ๑๒
	(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล	ไม่มี	หมวด ๑ ส่วนที่ ๓ (๓.๒) หน้า ๑๒
	(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน	ไม่มี	หมวด ๑ ส่วนที่ ๓ (๓.๓) หน้า ๑๒ - ๑๓
	(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔	ไม่มี	หมวด ๑ ส่วนที่ ๓ (๓.๔) หน้า ๑๔
๙	**ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ไม่มี	หมวด ๑ ส่วนที่ ๔ หน้า ๑๕ - ๑๘
	(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น	ไม่มี	หมวด ๑ ส่วนที่ ๔ (๔.๑(๑)) หน้า ๑๕
	(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้	ไม่มี	หมวด ๑ ส่วนที่ ๔ (๔.๒) หน้า ๑๕ - ๑๖

ข้อ	ประเด็นการทบทวนนโยบาย / และแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หน่วยงานทบทวนเอกสาร (ระบุการปรับแก้ไข)	
		มี/ไม่มี	อ้างอิงหน้า... / ระบุรายละเอียดการปรับแก้ไข
	(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน	ไม่มี	หมวด ๑ ส่วนที่ ๔ (๔.๓) หน้า ๑๖
	(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย	ไม่มี	หมวด ๑ ส่วนที่ ๔ (๔.๔) หน้า ๑๖
	(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ	ไม่มี	หมวด ๑ ส่วนที่ ๔ (๔.๕) หน้า ๑๖
	(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง	ไม่มี	หมวด ๑ ส่วนที่ ๔ (๔.๖) หน้า ๑๗
	(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ	ไม่มี	หมวด ๑ ส่วนที่ ๔ (๔.๗) หน้า ๑๗ -๑๘
๑๐	**ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**		หมวด ๑ ส่วนที่ ๕ หน้า ๑๙ - ๒๑
	(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย	ไม่มี	หมวด ๑ ส่วนที่ ๕ หน้า ๑๙ - ๒๑
	(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง	ไม่มี	หมวด ๑ ส่วนที่ ๕ (๕.๔) หน้า ๑๙ - ๒๐
	(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ	ไม่มี	หมวด ๑ ส่วนที่ ๕ (๕.๕) หน้า ๒๐
	(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว	ไม่มี	หมวด ๑ ส่วนที่ ๕ (๕.๖) หน้า ๒๐
	(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)	ไม่มี	หมวด ๑ ส่วนที่ ๕ (๕.๘) หน้า ๒๐ - ๒๑

ข้อ	ประเด็นการทบทวนนโยบาย / และแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หน่วยงานทบทวนเอกสาร (ระบุการปรับแก้ไข)	
		มี/ไม่มี	อ้างอิงหน้า... / ระบุรายละเอียดการปรับแก้ไข
	(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง	ไม่มี	หมวด ๑ ส่วนที่ ๕ (๕.๙) หน้า ๒๑
๑๑	**ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้**	ไม่มี	หมวด ๑ ส่วนที่ ๖ หน้า ๒๒ - ๒๓
	(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้	ไม่มี	หมวด ๑ ส่วนที่ ๖ (๖.๓) หน้า ๒๒
	(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)	ไม่มี	หมวด ๑ ส่วนที่ ๖ (๖.๔) หน้า ๒๓
	(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่	ไม่มี	หมวด ๑ ส่วนที่ ๖ (๖.๕) หน้า ๒๓
	(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน	ไม่มี	หมวด ๑ ส่วนที่ ๖ (๖.๖) หน้า ๒๓
๑๒	**หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรองตามแนวทางต่อไปนี้**		หมวด ๒ หน้า ๓๐ – ๓๓
	(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม	มี	หมวด ๒ ส่วนที่ ๑(๑.๑) หน้า ๓๐ – ๓๑ - มีเพิ่มเติมส่วนที่ ๑ (๒) ข้อ ๓
	(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ	มี	หมวด ๒ ส่วนที่ ๑ (๑.๑(๔)) หน้า ๓๑
	(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์	มี	หมวด ๒ หน้า ๓๐ – ๓๓ - เพิ่มเติมส่วนที่ ๑ (๒) ข้อ ๓ - ปรับปรุงหมวด ๕ หน้า ๓๘ – ๓๙

ข้อ	ประเด็นการทบทวนนโยบาย / และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หน่วยงานตอบพร้อมอธิบาย (ระบุการปรับแก้ไข)	
		มี/ไม่มี	อ้างอิงหน้า... / ระบุรายละเอียดการปรับแก้ไข
	(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ (โปรดระบุความถี่)	ไม่มี	หมวด ๒ ส่วนที่ ๑ (๑.๑(๖)) หน้า ๓๑
	(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน	ไม่มี	หมวด ๒ ส่วนที่ ๓ (๑.๑) หน้า ๓๐ - ๓๑
๑๓	**หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ไม่มี	หมวด ๓ หน้า ๓๔ - ๓๖
	(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง	ไม่มี	หมวด ๓ ส่วนที่ ๑ (๑.๑) หน้า ๓๔
	(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน	ไม่มี	หมวด ๓ ส่วนที่ ๑ (๑.๒) หน้า ๓๔
๑๔	**หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น**	มี	- ประกาศฯ ข้อ ๙ - ปรับปรุงประกาศฯ ข้อ ๑๐ - เพิ่มเติมหมวด ๕ หน้า ๓๘ – ปรับปรุงหมวด ๕ หน้า ๓๙

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ ตามมาตรา ๗ ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ลงชื่อ ..... (ผู้บริหารสูงสุด/ผู้ที่ได้รับมอบอำนาจ)

(นายเชิดศักดิ์ หิรัญสิริสมบัติ)

ตำแหน่ง รองอัยการสูงสุด (CIO)

ลงวันที่ ๑ มิ.ค. ๒๕๖๒

หมายเหตุ : โปรดระบุชื่อผู้ประสานงาน หมายเลขติดต่อ และ อีเมล์

นางสาวภูริตา จันต๊ะพรมมา นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานบริหารกิจการสำนักงานอัยการสูงสุด

โทร. ๐๒ ๕๑๕ ๔๑๗๖ มือถือ. ๐๘๑ ๐๓๓ ๕๗๙๘, ๐๖๓ ๓๑๙๗ ๔๐๖๑

e-Mail : punida.j@aeo.go.th, punida.n@hotmail.com

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ
อันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ
(IT Contingency Plan)
พ.ศ. ๒๕๖๒

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ

อันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan)

ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. 2562

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ อันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

กลุ่มแผนงานเทคโนโลยีสารสนเทศ

สำนักงานอัยการสูงสุด

๖ พฤศจิกายน ๒๕๖๑

คำนำ

ด้วยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) ได้มีมติในการประชุมครั้งที่ ๕/๒๕๖๐ เมื่อวันจันทร์ที่ ๒๕ กันยายน ๒๕๖๐ เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด และได้ประกาศใช้เพื่อเป็นเครื่องมือสำหรับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด ดังนั้น จึงจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติฯ เพื่อให้มีความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุดเป็นไปอย่างยั่งยืน ตามรายละเอียดในข้อ ๖ ประกาศสำนักงานอัยการสูงสุด เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๐ โดยสำนักงานอัยการสูงสุดต้องมีระบบสารสนเทศและระบบสำรองข้อมูลเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ และต้องจัดทำระบบเทคโนโลยีสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา และจัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ (IT Contingency Plan) พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ และต้องทบทวนอย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือต่อเหตุฉุกเฉินหรือ ภัยพิบัติที่อาจเกิดขึ้น และเป็นกรอบแนวทางในการดูแลรักษาระบบและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและสารสนเทศของสำนักงานอัยการสูงสุดได้

เพื่อให้สำนักงานอัยการสูงสุดมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยมีความพร้อมใช้ข้อมูลได้อย่างเต็มประสิทธิภาพตลอดเวลา และนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กร ตลอดจนเลือกใช้วิธีการที่เหมาะสมในการบริหารจัดการความเสี่ยงที่ได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและให้การดำเนินงานของสำนักงานอัยการสูงสุดอยู่ในระดับที่สามารถรองรับได้ จึงจำเป็นจะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) เป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงที่อาจนำไปสู่ผลเสียหรือความเสียหายได้ทั้งทางตรงและทางอ้อม

กลุ่มแผนงานเทคโนโลยีสารสนเทศ
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
พฤศจิกายน ๒๕๖๑

สารบัญ

สารบัญแผนภูมิ/ตาราง

เรื่อง **หน้า**

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ
อันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan)
ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

๑. หลักการและเหตุผล

ด้วยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) ได้มีมติในการประชุมครั้งที่ ๕/๒๕๖๐ เมื่อวันจันทร์ที่ ๒๕ กันยายน ๒๕๖๐ เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด และได้ประกาศใช้เพื่อเป็นเครื่องมือสำหรับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด ดังนั้น จึงจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติฯ เพื่อให้มีความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุดเป็นไปอย่างยั่งยืน ตามรายละเอียดในข้อ ๖ ประกาศสำนักงานอัยการสูงสุด เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๐ โดยสำนักงานอัยการสูงสุดต้องมีระบบสารสนเทศและระบบสำรองข้อมูลเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ และต้องจัดทำระบบเทคโนโลยีสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา และจัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ (IT Contingency Plan) พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ และต้องทบทวนอย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือต่อเหตุฉุกเฉินหรือ ภัยพิบัติที่อาจเกิดขึ้น และเป็นกรอบแนวทางในการดูแลรักษาระบบและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและสารสนเทศของสำนักงานอัยการสูงสุดได้

เพื่อให้สามารถนำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) ของสำนักงานอัยการสูงสุดมาช่วยในการบริหารงานและการตัดสินใจด้านต่าง ๆ ตลอดจนมีการใช้ทรัพยากรอย่างเหมาะสมและมีประสิทธิภาพ ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งโปรแกรมระบบสารบบคดีอิเล็กทรอนิกส์ซึ่งเป็นโปรแกรมหลักในการปฏิบัติงาน และระบบงานอื่น ๆ ที่ได้พัฒนาขึ้นมาเพื่อช่วยเพิ่มประสิทธิภาพในการปฏิบัติงาน และบริการประชาชนให้ได้รับความสะดวกมากยิ่งขึ้น ภายใต้สภาวการณ์ดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินการหรือเป้าหมายขององค์กร ขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตีจากบุคคล จากไวรัสคอมพิวเตอร์ เครื่องของบุคลากร ปัญหาไฟฟ้า อัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการปฏิบัติงานของสำนักงานอัยการสูงสุด และเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ว่าด้วยการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ จึงจำเป็นต้องมีการปรับปรุงแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

๒. วัตถุประสงค์

๒.๑ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานอัยการสูงสุด

๒.๒ เพื่อใช้เป็นแนวทางในการดำเนินการ การกำกับดูแล การตรวจสอบการบริหารจัดการ และดูแลรักษาระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้มีความเสถียรภาพ มีความพร้อมสำหรับการใช้งาน และเฝ้าระวังความเสี่ยงใหม่ๆ ที่อาจเกิดขึ้นได้ตลอดเวลา

๒.๓ ระบบเทคโนโลยีสารสนเทศดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๔ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับการดำเนินงานของสำนักเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) ให้ได้รับการยอมรับและมีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบ และมีความต่อเนื่อง

๒.๕ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๒.๖ สร้างกรอบและแนวทางในการดำเนินงานให้แก่บุคลากรในองค์กร เพื่อให้สามารถบริหาร จัดการความไม่แน่นอนที่จะเกิดขึ้นกับองค์กรได้อย่างเป็นระบบและมีประสิทธิภาพ

๒.๗ เพิ่มมูลค่าให้ผู้มีส่วนได้ส่วนเสียองค์กร

๓. การประเมินสถานการณ์ความเสี่ยง

เนื่องจากสำนักงานอัยการสูงสุดมีภารกิจหลักในการอำนวยความยุติธรรม การรักษาผลประโยชน์ของรัฐและการคุ้มครองสิทธิเสรีภาพและผลประโยชน์ของประชาชน และได้พัฒนาระบบงานต่าง ๆ ขึ้นมาเพื่อรองรับการปฏิบัติงานทั้งด้านคดีอาญาและคดีแพ่งทั้งปวงซึ่งมีความหลากหลายระบบเทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานที่จำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อรองรับและแก้ไขปัญหาจากสถานการณ์ฉุกเฉิน ลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุดให้เป็นไปอย่างเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย และนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติราชการให้เกิดประโยชน์สูงสุด

สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด ประกอบด้วย

๓.๑ ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น เว็บไซต์ของสำนักงานอัยการสูงสุด (www.ago.go.th)

๓.๒ ระบบฐานข้อมูลบริหารงานภายใน (Back Office) ได้แก่ ระบบสารบบคดีอิเล็กทรอนิกส์ ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ ฐานข้อมูลครุภัณฑ์คอมพิวเตอร์ เป็นต้น

๓.๓ ระบบให้บริการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์สำนักงานอัยการสูงสุด (Web Application Program) เป็นต้น

๓.๔ อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเน็ตเวิร์ค (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์สำนักงานอัยการสูงสุด (Web Server) เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่าง ๆ ในระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศมีดังนี้

(๑) **เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน** (Human Error) คือ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผนการตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด การถ่ายทอดความรู้ในคุณลักษณะของงานที่ชัดเจนให้ผู้รับผิดชอบงานรายใหม่ เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการใช้งานที่ถูกต้อง รวมถึงการดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น ดังนี้

๑) ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงันหรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

๒) ความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดลำดับความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้งานอาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่าง ๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

เพื่อเป็นการเสริมสร้างความรู้ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศเบื้องต้นจึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนาให้มีความรู้ความเข้าใจในด้านการใช้งานเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด

(๒) **เกิดจากระบบเครือข่าย** มีการเชื่อมโยงเครือข่ายล้มเหลวที่อาจเกิดจากสายเคเบิ้ลขาด มีการกัดแทะของหนู เกิดความขัดข้องของอุปกรณ์ ความเข้ากันได้ระหว่างอุปกรณ์เครือข่าย การตั้งค่าไม่ถูกต้อง ฮาร์ดแวร์ทำงานผิดพลาดหรือปัญหาเกี่ยวกับโปรแกรมควบคุม อาการบางอย่างเชื่อมต่อขาดตอนและไม่ชัดเจน ซึ่งกลุ่มระบบเครื่องคอมพิวเตอร์แม่ข่ายฯ หรือบุคลากรอื่นตามสัญญาจ้างบุคลากรร่วมทำงานกับ สทส. ในการบริหารจัดการห้องศูนย์ข้อมูล (Data Center) และงานอื่น ๆ ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศจะต้องทำการตรวจสอบเครือข่ายด้วยคำสั่ง Ping เพื่อตรวจสอบการเชื่อมต่อระบบเครือข่าย แยกปัญหาฮาร์ดแวร์เครือข่าย และการตั้งค่า Config ต่าง ๆ ให้กับอุปกรณ์ที่ไม่เข้ากัน ตรวจหาการสูญเสียแพ็กเกจ เมื่อทราบถึงปัญหาที่แน่นอนแล้วจึงได้ประสานผู้ให้บริการเครือข่าย (CAT และ GIN) และบริษัท ผู้รับจ้างเข้าทำ**การแก้ไขปัญหาภายใน ๔ ชั่วโมงให้แล้วเสร็จ** เพื่อไม่ให้กระทบการปฏิบัติงานของสำนักงานอัยการสูงสุด

(๓) **ความเสี่ยงด้านเทคนิค** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ความเสี่ยงที่เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) และสร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ถึงขั้นใช้งานไม่ได้ มีการดำเนินการเชิงป้องกันไว้ดังนี้

๑) ติดตั้ง Firewall เพื่อป้องกันไม่ให้บุคคลอื่นที่ไม่ได้รับอนุญาตเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักงานอัยการสูงสุดได้

๒) ติดตั้งระบบ IPS เพื่อตรวจจับภัยคุกคามต่าง ๆ ที่อาจเกิดภายในระบบเครือข่าย

๓) ติดตั้งระบบป้องกันไวรัส เพื่อป้องกันไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์แม่ข่ายและมีการติดตั้งซอฟแวร์ (Software) ป้องกันไวรัสที่เครื่องให้บริการ (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสต่าง ๆ ให้ผู้ใช้งานได้ศึกษาสามารถดำเนินการได้อย่างถูกวิธี และเพื่อตระหนักถึงความเสียหายที่จะเกิดขึ้น รวมถึงการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

(๔) **เกิดจากระบบไฟฟ้าขัดข้องหรือความเสียหายจากเพลิงไหม้** โดยได้ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) เพื่อสำรองไฟฟ้าและจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) กรณีเกิดกระแสไฟฟ้าขัดข้อง จะทำให้ระบบเครือข่ายสามารถ**ให้บริการได้ต่อเนื่องในระยะเวลาประมาณ ๘ ชั่วโมง** ที่จะสามารถทำการจัดเก็บข้อมูลและสำรองข้อมูล (Backup) ไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงไหม้นั้น ฝ่ายบริหารทั่วไป อาคารถนนรัชดาภิเษก จัดให้มีระบบควบคุมป้องกันเพลิงไหม้ไว้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่าง ๆ ภายในอาคารและทำป้ายบอกจุดติดตั้งเครื่องดับเพลิงแล้ว และได้มีข้อกำหนดการซักซ้อมแผนป้องกันอัคคีภัยให้กับบุคคลากรที่มีส่วนเกี่ยวข้อง ปีละ ๑ ครั้ง

(๕) **เกิดจากภัยหรือสถานการณ์อื่น** อันอาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความสูญเสียหรือเสียหายกับข้อมูลสารสนเทศ เช่น น้ำท่วม การชุมนุมประท้วงหรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น ซึ่ง สทส. ได้จัดเก็บข้อมูลสำรองไว้นอกสถานที่ (Backup Site) ซึ่ง**สำนักงานอัยการสูงสุดควรจะมีศูนย์สำรองระบบสารสนเทศ (Disaster Recovery Site) และจัดทำระบบสำรองข้อมูล (Backup System) ซึ่งจะต้องอยู่ห่างจากห้องศูนย์ข้อมูล (Data Center) ประมาณ ๓๐ กิโลเมตรตามกฎหมายกำหนด** แต่เนื่องจาก สทส. ได้เสนอโครงการจัดทำ DR Site และ Backup System มาตั้งแต่ปี พ.ศ. ๒๕๕๘ เรื่อยมาจนถึงปัจจุบันแต่ไม่เคยได้รับการอนุมัติงบประมาณในการดำเนินการจากสำนักงานอัยการสูงสุดแต่อย่างใด

(๖) **เกิดจากการโจรกรรม** การขโมยอุปกรณ์คอมพิวเตอร์และข้อมูลในส่วนของห้องศูนย์ข้อมูล (Data Center) จึงได้มีข้อกำหนดห้ามไม่ให้เจ้าหน้าที่และบุคลากรภายนอกที่ไม่มีส่วนเกี่ยวข้องเข้าไปในบริเวณห้องศูนย์ข้อมูล (Data Center) ยกเว้นหากมีความจำเป็นที่ต้องเข้าไปปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center) จะต้องมีเจ้าหน้าที่กลุ่มระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายและความมั่นคงปลอดภัย เป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ติดตั้งเครื่องอ่านบัตรแบบแม่เหล็ก (Access Control) เพื่อป้องกันไม่ให้บุคคลภายนอก และเจ้าหน้าที่ที่ไม่ได้มีส่วนเกี่ยวข้องเข้ามาในห้องศูนย์ข้อมูล (Data Center) โดยไม่ได้รับอนุญาต และมีการติดตั้งกล้องวงจรปิดไว้ภายในบริเวณห้องศูนย์ข้อมูล (Data Center) เพื่อป้องกันการโจรกรรม โดยมีเจ้าหน้าที่ทำการตรวจสอบระบบการบันทึกข้อมูลรายการความเคลื่อนไหวการ เข้า – ออก เพื่อตรวจสอบความผิดปกติเป็นระยะ ๆ

๔. แนวทางการจัดการภัยพิบัติ

๔.๑ **การสำรองข้อมูล (Backup)** เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล ให้สามารถนำข้อมูลกลับมาใช้งานได้ทันที โดยมีแนวทางดำเนินการที่ชัดเจน ซึ่งปัจจุบัน สทส. ได้นำเอาการสำรองข้อมูลทั้งหมดในทีเดียว (Full backup) มาใช้เพื่อเพิ่มประสิทธิภาพการทำงานให้สามารถใช้งานต่อเนื่อง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลแบบอัตโนมัติด้วยโปรแกรม Symantec net backup โดยทำการกำหนดค่า วัน เวลา และไฟล์ที่ต้องการจะทำการสำรองข้อมูล (Policies) โดยสำรองไว้ที่อุปกรณ์จัดเก็บ เช่น อุปกรณ์เทปบันทึกข้อมูล (tape) และอุปกรณ์จัดเก็บข้อมูลขนาดใหญ่ (SAN Storage) สามารถแบ่งการสำรองข้อมูลออกเป็น ๒ ประเภท คือ (๑) การสำรองฐานข้อมูล (Database) (๒) การสำรองโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการ (OS) มีรายละเอียดดังนี้

(๑) การสำรองฐานข้อมูล (Database)

การสำรองฐานข้อมูลหลักที่มีความสำคัญมาก จะทำการสำรองข้อมูล**ทุกวัน** เริ่มต้นตั้งแต่เวลา ๑๖.๓๐ น. โดยจะทำการสำรองโครงสร้างข้อมูล Source Code ลงในอุปกรณ์จัดเก็บข้อมูลขนาดใหญ่ (SAN Storage) และเทปบันทึกข้อมูล (tape) เช่น ระบบสารบบคดีอิเล็กทรอนิกส์ และระบบงาน NSW : National Single Windows โดยมีการตรวจสอบความสมบูรณ์และพร้อมใช้ของข้อมูลที่ทำการสำรองไว้ไปใช้กับโปรแกรมระบบงานที่พัฒนาต่อยอดจากฐานข้อมูลเดิมเป็นประจำทุกวัน เช่น ระบบติดตามข้อมูลการดำเนินคดีค้ามนุษย์ สำนักงานอัยการสูงสุด (ระยะที่ ๑) (CAHT) เป็นต้น

(๒) การสำรองโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการ (OS)

การสำรองฐานข้อมูลและระบบปฏิบัติการ (OS) จะทำการสำรองข้อมูล**ทุก ๆ วันเสาร์ - อาทิตย์**ที่ ๒ และ/หรือ ๔ เป็นประจำ**ทุกเดือน** โดยจะเริ่มต้นในเวลา ๐๐.๐๐ น. ของวันเสาร์ ซึ่งจัดเก็บลงในอุปกรณ์จัดเก็บข้อมูลขนาดใหญ่ (SAN Storage) เช่น ระบบบริหารอาคารและที่ดิน ระบบทะเบียนคุมทรัพย์สิน โดยมีการกำหนดระยะเวลาตรวจสอบความสมบูรณ์และพร้อมใช้ของข้อมูลที่ได้ทำการสำรองไว้ด้วยวิธีการตรวจสอบสถานะข้อผิดพลาดของข้อมูลที่ได้ทำการ backup ทุกครั้งหลังการ backup

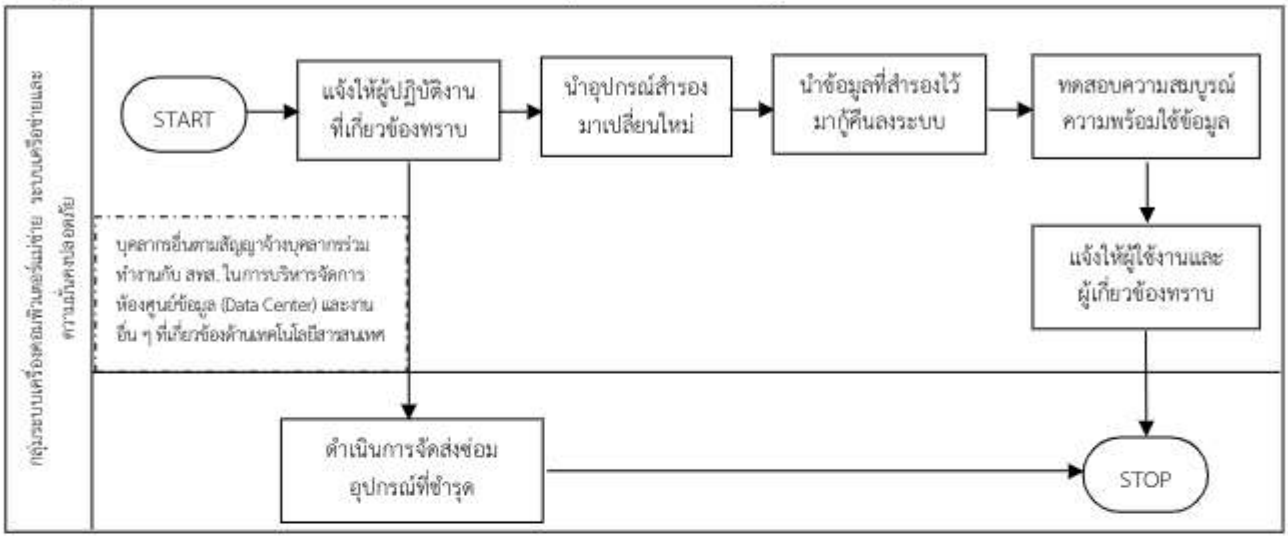
๔.๒ **ทำการทดสอบ** Recovery ฐานข้อมูล (Database) และโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการ (OS) ของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหายซึ่งมีแผนดำเนินการทุกสิ้นปี

๔.๓ **จัดหาเจ้าหน้าที่** บำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์จัดเก็บข้อมูลขนาดใหญ่ เพื่อลดความเสียหายของข้อมูล

กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย มีวิธีการดำเนินการคือ

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- จัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่สำรองไว้มากู้คืนลงระบบโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งผู้ใช้งานและผู้เกี่ยวข้องทราบ

แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



๔.๔ **การป้องกันไวรัสคอมพิวเตอร์** มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย ซึ่งผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ตเพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ มีวิธีการดังนี้

๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ โดยเครื่องคอมพิวเตอร์แม่ข่าย (server) จะทำหน้าที่โหลด patch โปรแกรมที่มีความทันสมัยและมีความสามารถในการป้องกันไวรัสที่มีประสิทธิภาพไว้ที่เครื่อง server ก่อนแล้วจึงส่ง patch การอัพเดทไปยังเครื่องคอมพิวเตอร์ลูกข่าย (client) ที่เชื่อมต่อกับระบบเครือข่ายและมีการเปิดใช้งานอยู่อีกครั้ง

๒) ใช้ความระมัดระวังในการเปิด E-mail ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มาและควรลบทิ้งทันที

๓) ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จาก Internet ไม่ดาวน์โหลดจากเว็บไซต์ที่ไม่น่าเชื่อถือและหลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น มีการติดตามข้อมูลการแจ้งการโจมตีของไวรัสต่าง ๆ อย่างสม่ำเสมอ

๔) วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด มีการตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

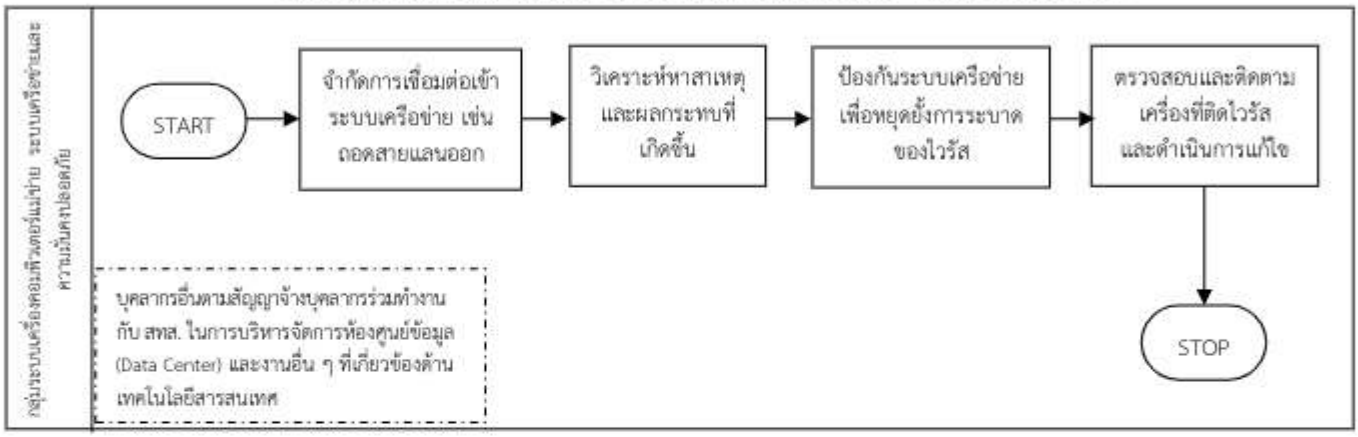
๕) กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งเหตุให้ สทส. ทราบ หรือกรณีมีเหตุอันทำให้อุปกรณ์คอมพิวเตอร์ไม่สามารถให้บริการเครือข่ายได้ สทส. จะต้องประกาศให้หน่วยงานในสังกัดสำนักงานอัยการสูงสุดทราบ

กรณีการป้องกันไวรัสล้มเหลว มีวิธีการดำเนินการคือ

- กรณีถูกไวรัสหรือผู้บุกรุกเพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งเหตุให้เจ้าหน้าที่ สทส. ทราบทันที หรือกรณีมีเหตุอันทำให้ สทส. ไม่สามารถให้บริการด้านเครือข่ายได้จะต้องประกาศให้ผู้ใช้งานในสังกัดสำนักงานอัยการสูงสุดทราบ

- **แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีการป้องกันไวรัสล้มเหลว**



๔.๕ **การป้องกันและแก้ไขที่เกิดจากกระแสไฟฟ้าขัดข้อง/ไฟดับ** เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ

๑) ติดตั้ง**เครื่องกำเนิดไฟฟ้า** (Generator) สำรองไฟฟ้าเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) เป็นการควบคุมการจ่ายกระแสไฟฟ้าให้กับเครื่องแม่ข่ายในกรณีเกิดกระแสไฟฟ้าขัดข้องซึ่งจะทำให้ระบบเครือข่ายคอมพิวเตอร์สามารถให้บริการได้ในระยะเวลาใน**การสำรองไฟฟ้าได้ประมาณ ๘ ชั่วโมง**

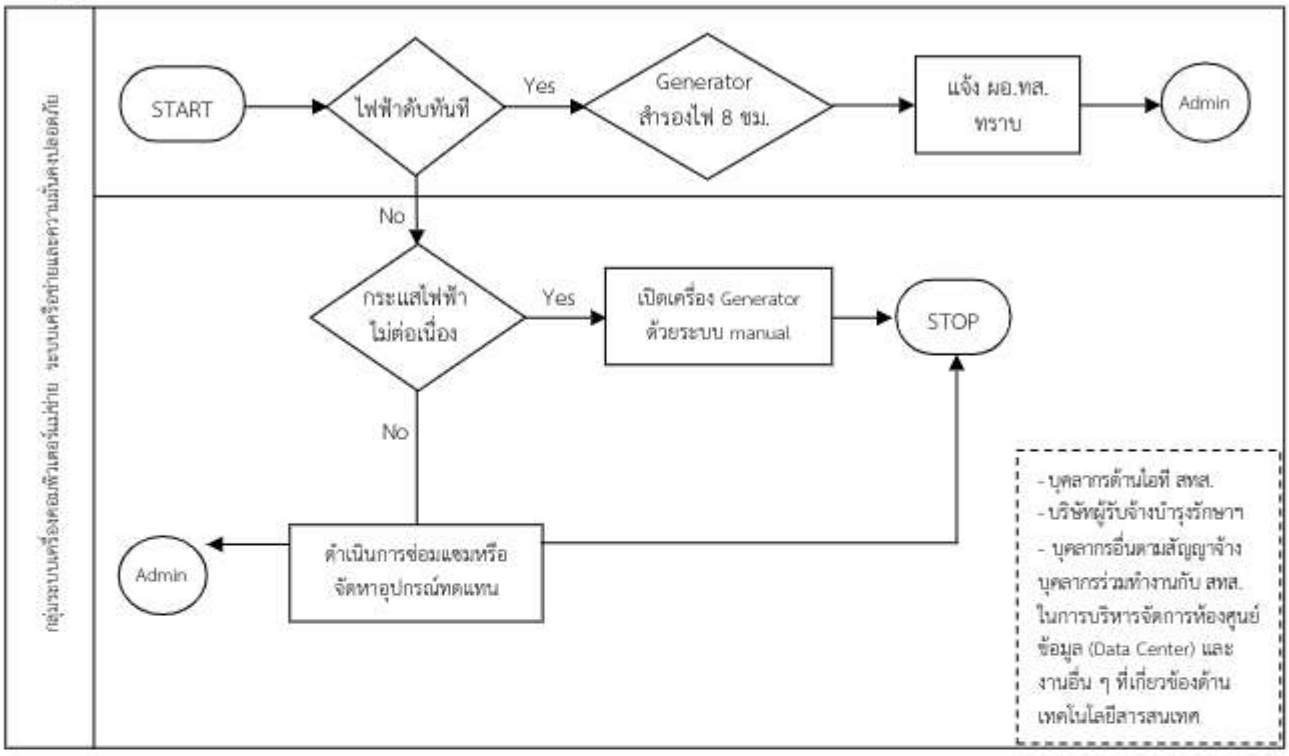
๒) เครื่องกำเนิดไฟฟ้า (Generator) ทำงานทันทีเมื่อไฟฟ้าอาคารขัดข้องหรือดับและมีการบำรุงรักษาเครื่องกำเนิดไฟฟ้าให้มีสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้งานเร่งทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ เพื่อป้องกันการสูญหายในระดับหนึ่ง

กรณีไฟฟ้าขัดข้อง มีวิธีการดำเนินการคือ

- หากไฟฟ้าดับทันทีจะมีระบบ SMS แจ้งเตือนไปยังผู้ดูแลระบบและส่งคำสั่งให้เครื่อง Generator ทำงานในระยะเวลาในการสำรองไฟฟ้าได้ประมาณ ๘ ชั่วโมง
- หากกระแสไฟฟ้าไม่สม่ำเสมอ ผู้ดูแลระบบต้องดำเนินการเปิดเครื่อง Generator ด้วยมือ
- หากเครื่อง Generator มีปัญหา แจ้ง ผอ.ทส. และบริษัทผู้รับจ้างเพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้นหรือจัดหาอุปกรณ์มาทดแทนทันที

แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีไฟฟ้าขัดข้อง

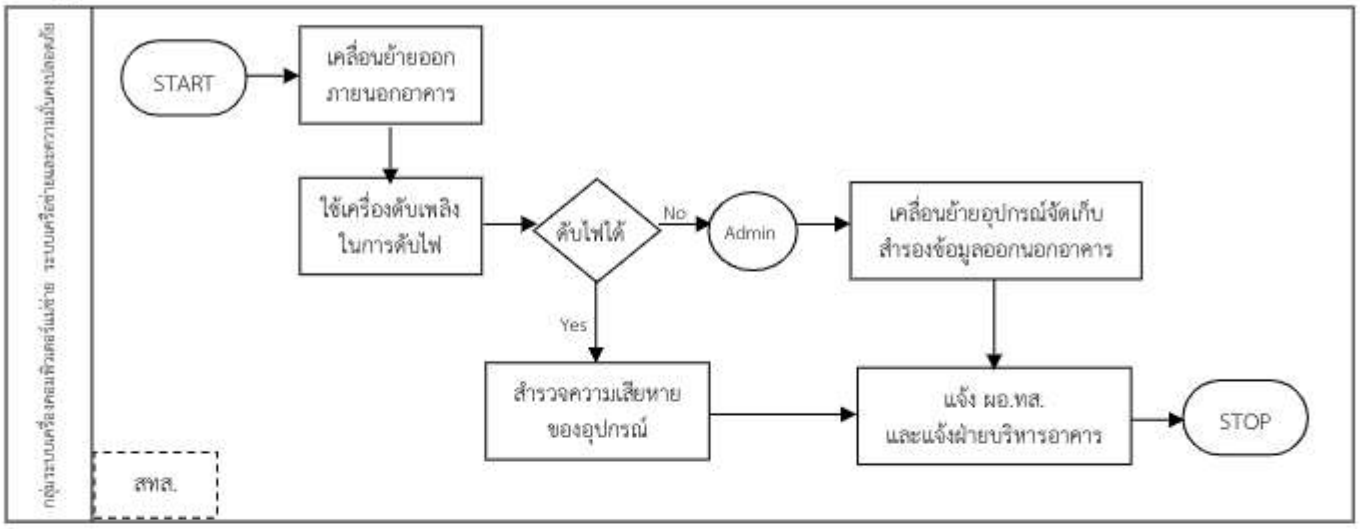


๔.๖ **มีระบบป้องกันไฟไหม้** ติดตั้งเครื่องตรวจจับควันเตือนภัยเมื่อมีควันไฟ Carbon Monoxide Detector ไว้ในห้องคอมพิวเตอร์แม่ข่าย พร้อมเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์ มีการจัดทำเครื่องหมายระบุความสำคัญของอุปกรณ์ตามลำดับเพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน ซึ่งในพื้นที่ควบคุมจะมีอุปกรณ์ดับเพลิงติดตั้งในทุกอาคารเพื่อทำการควบคุมเพลิงในเบื้องต้น

กรณีไฟไหม้ มีวิธีการดำเนินการคือ

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้รีบเคลื่อนย้ายออกไปภายนอกอาคารและให้ใช้ผู้ที่สามารถใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บสำรองข้อมูลออกภายนอกอาคารและแจ้งฝ่ายบริหารอาคารถนนรัชดาภิเษก ที่เบอร์ ๐๒ ๕๑๕ ๔๐๗๗ หรือเจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ๐๒ ๕๑๕ ๔๐๓๙
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน และอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟและดับไฟอัตโนมัติ

แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีไฟไหม้



๔.๗ **การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย** ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

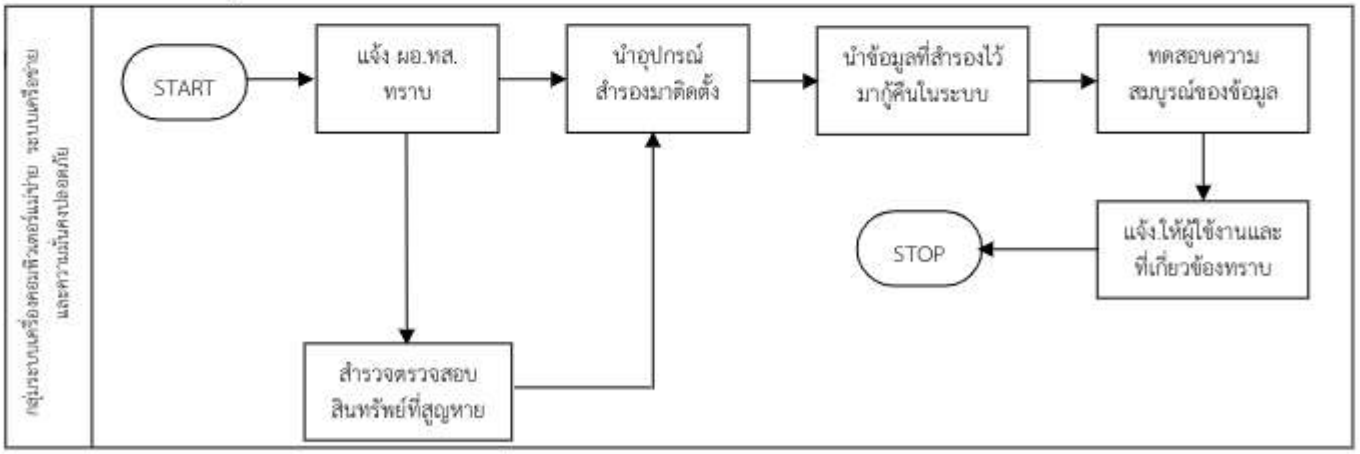
๑) มีการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่ของฝ่ายคอมพิวเตอร์และเครือข่ายเป็นผู้รับผิดชอบนำพาเข้าไป

๒) จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ติดตั้งเครื่องอ่านบัตรแบบแม่เหล็ก (Access Control) เพื่อป้องกันไม่ให้บุคคลภายนอกเข้ามาในหน่วยงานโดยไม่ได้รับอนุญาต

๓) มีการติดตั้งกล้องวงจรปิดเพื่อสามารถตรวจสอบการโจรกรรมในภายหลังได้

กรณีโจรกรรม มีวิธีการดำเนินการคือ

- ผู้ดูแลระบบแจ้งผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารทราบโดยด่วน
- สำรวจตรวจสอบรายการสินทรัพย์ที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์มาติดตั้งทดแทน และนำข้อมูลที่ได้สำรองไว้กู้คืนในระบบ เพื่อให้ผู้ใช้งานสามารถใช้ระบบงานได้โดยเร็ว

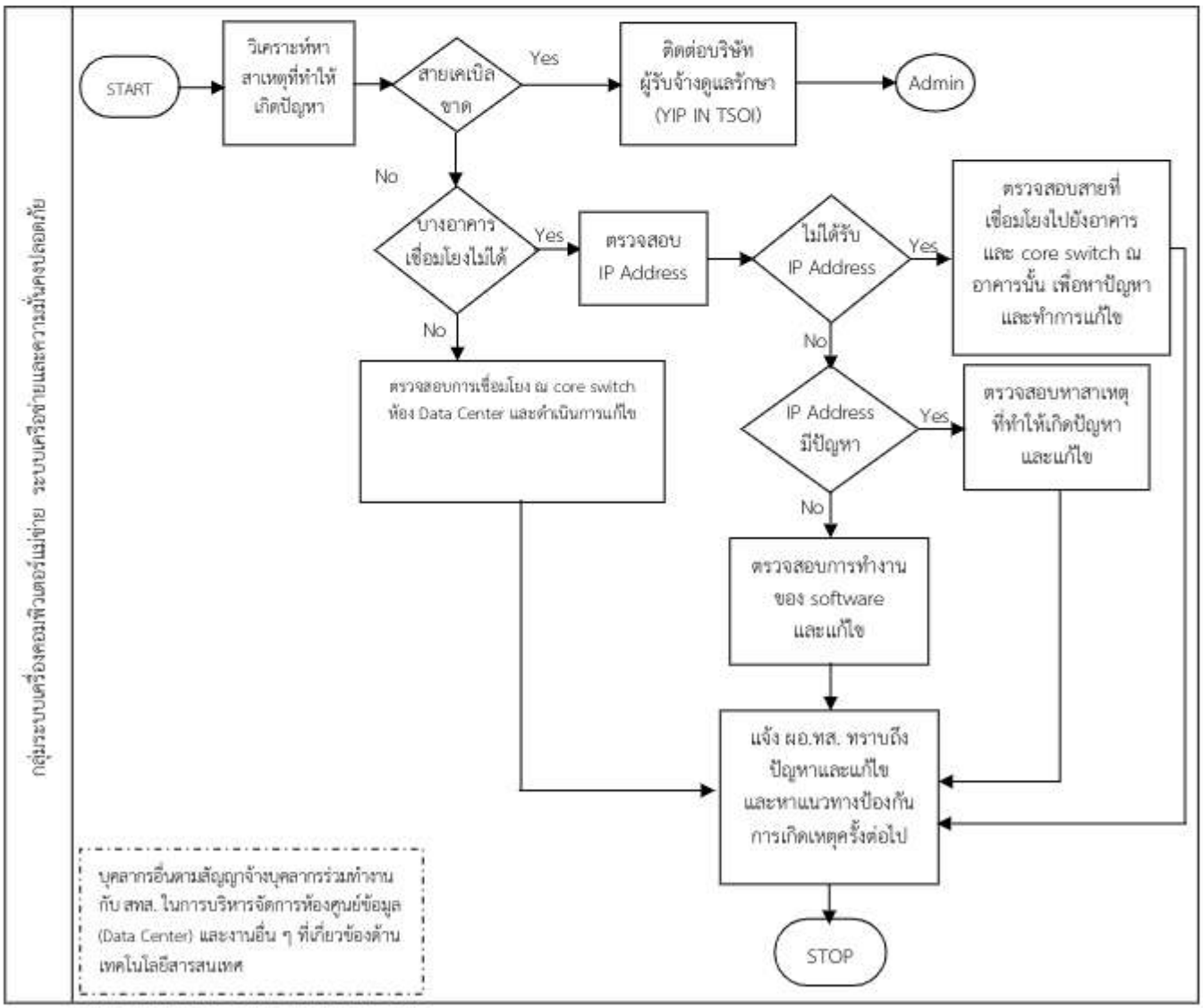


๔.๘ **ระบบการสื่อสารของเครื่องแม่ข่าย** ที่เชื่อมต่อระบบอินเทอร์เน็ตเกิดความขัดข้อง ซึ่งสำนักงานอัยการสูงสุดใช้บริการและเชื่อมโยงวงจรเครือข่ายสัญญาณ CAT MPLS จากบริษัท กสท โทรคมนาคม จำกัด (มหาชน) โดยให้สำนักงานอัยการสูงสุด ร่วมกับ กสท โทรคมนาคม จำกัด (มหาชน) ดำเนินการตรวจสอบวงจรเครือข่าย วิเคราะห์และแก้ไขปัญหาให้วงจรเครือข่ายคืนดี**พร้อมใช้งานภายใน ๔ ชั่วโมง** และรายงานการดำเนินงานให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารทราบโดยทันที

กรณีการเชื่อมโยงเครือข่ายล้มเหลว มีวิธีการดำเนินการคือ

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบติดต่อบริษัทผู้รับจ้างบำรุงรักษาฯ ทำการซ่อมแซมสายเคเบิ้ลให้เสร็จโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีการเชื่อมโยงเครือข่ายล้มเหลว



๔.๙ **การบุกรุกหรือการโจมตีจากภายนอก** เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล ดำเนินการดังนี้

๑) สแกนหาจุดอ่อนและ Update Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยการใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๒) ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักงานอัยการสูงสุดได้

๓) ติดตั้งระบบ IPS เพื่อตรวจจับภัยคุกคามต่าง ๆ ที่อาจเกิดภายในระบบเครือข่าย

๔) จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตของสำนักงานอัยการสูงสุด เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕) ติดตั้งระบบป้องกันไวรัสให้ทันสมัยและมีการอัพเดทอย่างสม่ำเสมอ และปิด Port ที่ไม่ใช้บริการทั้งหมด

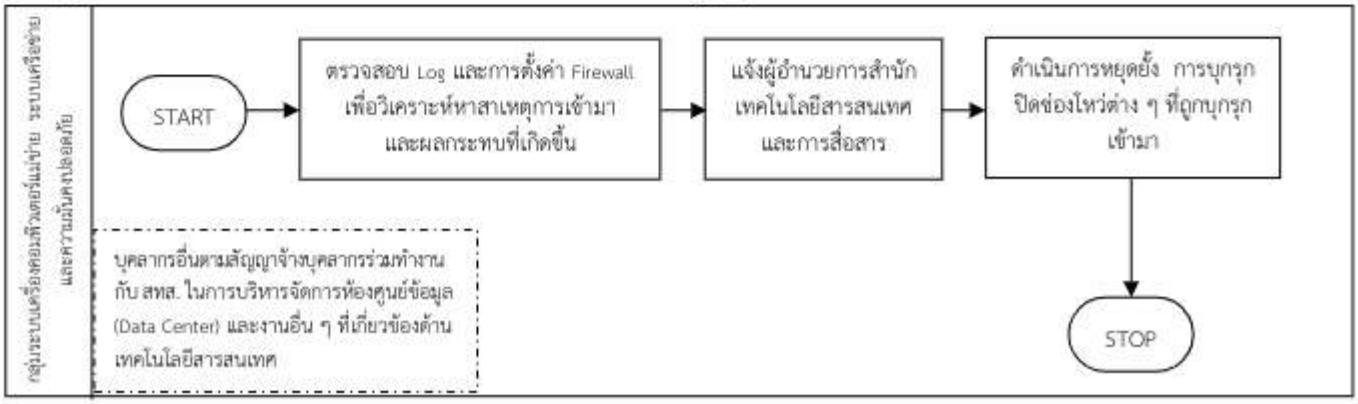
๖) การใช้งานระบบสารสนเทศจากหน่วยงานต่าง ๆ ทั้งในส่วนกลางและส่วนภูมิภาค ระบบเครือข่ายภายใน (Intranet) ผู้ใช้งานจะต้อง มีการบันทึกชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) เพื่อระบุตัวตนก่อนเข้าใช้งานได้ตามสิทธิ และอำนาจหน้าที่ที่รับผิดชอบ โดยมีการกำหนดรหัสผ่านไม่น้อยกว่า ๘ ตัวอักษรพร้อมทั้งมีอักขระพิเศษอย่างน้อย ๒ ตัวอักษร และไม่ควรกำหนดรหัสผ่านเดียวกันทุกระบบ และให้มีการ**เปลี่ยนรหัสผ่านทุก ๓ เดือน**

๗) การดำเนินการตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

กรณีการป้องกันผู้บุกรุกล้มเหลว มีวิธีการดำเนินการคือ

- กรณีที่มีผู้บุกรุก กลุ่มระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายและความมั่นคงปลอดภัย และนักวิชาการคอมพิวเตอร์ทุกคน รวมถึงเจ้าหน้าที่อื่นที่เกี่ยวข้องจะต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบของผู้บุกรุกและความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall และจากแหล่งอื่น ๆ
- ผู้ดูแลระบบต้องแจ้งผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ด้วยการปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีการป้องกันผู้บุกรุกล้มเหลว



๔๑๐ **เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจ**ในการใช้อุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน

๑) ให้ความรู้แก่บุคลากรและหน่วยงานผ่านเว็บไซต์ของสำนักงานอัยการสูงสุดที่ www.ago.go.th เว็บไซต์ของ สทส. ที่ www.ictc.ago.go.th จดหมายอิเล็กทรอนิกส์ (e-Mail) และผ่านทาง Social Network คลับไอทีของ สทส. ที่ www.facebook.com/clubitagoหรือช่องทาง Group Line ของ สทส. ที่ได้จัดทำขึ้นโดยจัดทำในรูปแบบจดหมายข่าวของ สทส.

๒) จัดจ้างบริษัทที่มีบุคลากรซึ่งมีความรู้ความชำนาญทำหน้าที่ดูแล ให้คำปรึกษา ตรวจสอบและบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ทั้งทางด้าน Hardware และ Software โดยมีเจ้าหน้าที่ผู้ชำนาญการร่วมปฏิบัติงานกับ สทส. เป็นประจำทุกวันทำการ

๔๑๑ **การจัดเตรียมอุปกรณ์ที่จำเป็น** เป็นการเตรียมความพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบสารสนเทศของสำนักงานอัยการสูงสุด กลุ่มระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายและความมั่นคงปลอดภัย รวมถึงกลุ่มงานสนับสนุนอื่นซึ่งมีหน้าที่ดูแลตามภารกิจของ สทส. ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้โดยมีการเตรียมอุปกรณ์ดังนี้

๑) แผ่น Boot Disk
๒) แผ่นติดตั้งระบบปฏิบัติการ ระบบเครือข่าย แผ่นติดตั้งระบบงานที่สำคัญ
๓) แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
๔) แผ่นโปรแกรม Anti-Virus
๕) แผ่น Driver อุปกรณ์ต่าง ๆ
๖) Hard Disk สำรอง
๗) ระบบสำรองไฟฟ้าฉุกเฉิน
๘) สำเนารายละเอียดการบันทึกค่าต่าง ๆ ในการติดตั้งอุปกรณ์ที่จำเป็น และอุปกรณ์อื่นที่เกี่ยวข้อง

๕. มาตรการความปลอดภัยด้วยรหัสผ่าน

การสร้างความปลอดภัยให้กับระบบสารสนเทศมีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศไม่สามารถเข้าถึงข้อมูล แก้ไข เปลี่ยนแปลงหรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิใช่อำนาจหน้าที่เกี่ยวข้องของตนได้ โดย

๑) กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีการลำดับชั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละดับดังนี้

- ผู้ดูแลระบบเครือข่ายหรือผู้ดูแลเครื่องแม่ข่ายจะต้องเป็นผู้ควบคุมรหัสผู้ใช้งานทั้งหมด โดยกำหนดรหัสผู้ใช้งานให้แก่บุคคลที่รับผิดชอบโดยตรงในแต่ละงานให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบเครือข่าย
- การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ FTP Server จะต้องระบุถึง IP Address ของผู้ใช้งานและแฟ้มข้อมูลที่ต้องการเข้าถึง
- การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ Database Server จะต้องกำหนดแยกเป็นรายฐานข้อมูลที่ต้องการใช้งานและเข้าถึง

๒) กำหนดระยะเวลาการใช้งานระบบสารสนเทศของผู้ใช้งาน โดยผู้ใช้งานจะไม่สามารถใช้งานระบบสารสนเทศได้เมื่อพ้นระยะเวลาที่กำหนดไว้

๓) การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๘ ตัวอักษร และควรใช้ตัวเลขผสมอักขระพิเศษประกอบ และสำหรับผู้ใช้งานระบบสารสนเทศควรมีการ**เปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๓ เดือน** โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

๔) มีการจัดทำระบบ Dot1x หรือมีชื่อเต็มว่า IEEE 802.1x ในการตรวจสอบและรับรองผู้เข้าใช้งาน (Authentication) ผ่านทาง RADIUS Server (Authentication server) โดยจะให้ผู้ใช้ทำการเข้าสู่ระบบโดยการใช้ Username และ Password ที่ถูกกำหนด โดยที่ผู้ใช้งานต้องยืนยันตัวตนทุกครั้งที่เข้าใช้งานระบบเพื่อเป็นหลักฐานว่าได้เข้าใช้ระบบด้วย IP Address ใด เวลาใด เป็นการป้องกันการเชื่อมต่อโดยเจ้าหน้าที่หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

๖. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๖.๑ กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการและประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) รีบขนย้ายอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายไปไว้ในที่ปลอดภัย

๕) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖) กรณีที่อุปกรณ์ด้าน Hardware เสีย ให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (Maintenance) นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗) ผู้ดูแลระบบต้องรีบแจ้งให้หัวหน้าหรือผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารรับทราบถึงปัญหาโดยเร็ว

๖.๒ กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้ผู้ใช้งานแจ้งเหตุนั้นให้ สทส. รับทราบ หรือกรณีมีเหตุอันทำให้ สทส. ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการถอดสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องนั้นโดยเร็ว

๓) ในกรณีที่เกรงว่าเหตุที่จะเกิดเป็นอันตรายต่อหน่วยงานภายในอาคารที่ตั้งของเครื่องคอมพิวเตอร์ที่พบความขัดข้อง ให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๔) กรณีที่อุปกรณ์เสีย เช่น Main Board, Hard disk, ระบบปฏิบัติการและระบบเครือข่าย ให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทผู้รับจ้างการบำรุงรักษาฯ (Maintenance) เพื่อนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุดและทำการ Recovery เพื่อนำข้อมูลเดิมกลับมาใช้โดยเร็ว

๕) ให้ผู้ดูแลระบบแจ้งเหตุขัดข้องนั้น ให้หัวหน้างานหรือผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารรับทราบโดยเร็วที่สุด

๖.๓ **กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์**

๑) ผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์ เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๒) ทำการ Scan Virus และฆ่าไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมต้านไวรัสที่มีอยู่ในเครื่อง

๓) แจ้ง สทส. เพื่อตรวจสอบให้ละเอียดอีกครั้ง

๗. หลักปฏิบัติในการป้องกันอัคคีภัย

เพื่อป้องกันมิให้เกิดอัคคีภัยภายในอาคารและบุคลากรสามารถปฏิบัติตนได้อย่างถูกต้องเมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติของบุคลากรภายใน สทส. ดังนี้

๗.๑ ไม่กระทำการใด ๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๗.๒ ควรศึกษาเรื่องตำแหน่งเส้นทางหนีไฟออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

๗.๓ ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉินไม่ให้ปิดตายหรือมีสิ่งกีดขวางและสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเองไปยังทางออกฉุกเฉินทั้งสองทางเพื่อให้สามารถไปถึงทางหนีไฟได้ถึงแม้จะมืดและมีควันปกคลุม

๗.๔ เมื่อเกิดเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพื่อเปิดสัญญาณเตือนเพลิงไหม้ จากนั้นหนีออกจากอาคารแล้วรีบโทรศัพท์แจ้งเจ้าหน้าที่รักษาความปลอดภัย (รปภ.) โทร ๐๒ ๕๑๕ ๔๐๓๙ ทันที

๗.๕ ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันที และให้รีบแจ้งฝ่ายบริหารทั่วไปอาคารถนนรัชดาภิเษกเพื่อแจ้งหน่วยดับเพลิงต่อไป

๗.๖ ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตูก่อนหากประตูมีความเย็นอยู่ให้ค่อย ๆ ปิดประตูแล้วหนีไปทางหนีไฟฉุกเฉินที่อยู่ใกล้ที่สุด

๗.๗ ถ้าเพลิงไหม้อยู่บริเวณใกล้ ๆ ประตูจะมีความร้อน ห้ามเปิดประตูเด็ดขาดให้รีบโทรศัพท์เรียกเจ้าหน้าที่รักษาความปลอดภัยและแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารที่ถูกเพลิงไหม้ หาผ้าเช็ดตัวเปียก ๆ ปิดทางเข้าของควันปิดพัดลมและเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๗.๘ ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

๘. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

๘.๑ **ระดับนโยบาย** รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามกำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ ได้แก่

๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

๒) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

๘.๒ **ระดับปฏิบัติ** รับผิดชอบในการกำกับดูแลการปฏิบัติงาน ศึกษา ทบทวนวางแผนติดตามการบริหารความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ได้แก่

๘.๒.๑ **ผู้ดูแลระบบ** คือ กลุ่มระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายและความมั่นคงปลอดภัย

๘.๒.๒ **กลุ่มงานสนับสนุนอื่น** ประกอบด้วย

๑) กลุ่มแผนงานเทคโนโลยีสารสนเทศ

๒) กลุ่มสนับสนุนงานบริการงานเทคโนโลยีสารสนเทศ

๓) กลุ่มพัฒนาระบบงานคอมพิวเตอร์และฐานข้อมูล

๔) บุคลากรอื่นตามสัญญาจ้างบุคลากรร่วมทำงานกับ สทส. ในการบริหารจัดการห้องศูนย์ข้อมูล (Data Center) และงานอื่น ๆ ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ

บุคลากรของ สทส. ที่ดูแลรับผิดชอบระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด ระบบสำรองและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ชื่อ – สกุล	ตำแหน่ง	เบอร์ที่ทำงาน	มือถือ
กลุ่มอำนวยการ (บริหารงานทั่วไป)			
นางณฐนน แก้วกระจ่าง	ผู้อำนวยการสำนักอำนวยการ	๐๒-๕๑๕๔๑๘๕	๐๙๘-๘๒๙๐๕๙๖
นายนพพล พิเศษพงษา	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๘๐	๐๖๓-๒๑๗๘๕๑๓
กลุ่มแผนงานเทคโนโลยีสารสนเทศ			
น.ส.ภูริดา จันต๊ะพรมมา	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๗๖	๐๘๑-๐๓๓๕๗๙๘
น.ส.อุษา สิริปรีดากุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๗๗	๐๘๔-๗๒๐๗๓๙๐
น.ส.เบญญาภา ดีชานนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๗๗	๐๘๐-๑๐๘๕๐๙๑
กลุ่มระบบเครื่องคอมพิวเตอร์และแม่ข่ายระบบเครือข่ายและความมั่นคงปลอดภัย			
น.ส.ชุติภัค เงินเจือ	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๘๓	๐๖๒-๖๐๒๑๖๙๘
นายพนธ์พิวัชร์ ชมสุรินทร์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๓	๐๘๑-๔๐๓๔๔๙๔
นายอนวัช ทินเลย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๗	๐๘๗-๗๗๔๔๘๒๒
นายเกริกเกียรติ สุขเนาว์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๗	๐๘๐-๒๘๑๕๙๓๘
กลุ่มสนับสนุนและบริการงานเทคโนโลยีสารสนเทศ			
น.ส.สุรีพร สิริภักดี	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๒-๕๑๕๔๑๘๘	๐๘๙-๘๙๒๘๑๔๔
น.ส.อัจฉรา ภู่ระย้า	นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๒-๕๑๕๔๑๘๑	๐๘๔-๕๕๑๓๔๔๐
น.ส.เล็ก เบาราญ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๑	๐๘๔-๗๗๑๕๓๗๓
นายปรีชา กันหล้า	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๘๑	๐๘๑-๐๒๖๘๘๐๐
กลุ่มพัฒนาระบบงานคอมพิวเตอร์และฐานข้อมูล (สารบบคดี)			
น.ส.ชฎาวัลย์ สิงห์อินทร์	นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๒-๕๑๕๔๑๘๖	๐๘๙-๖๖๐๓๘๓๐
นายพงศ์เดช โอวาสิทธิ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๗๘	๐๘๖-๘๑๒๘๘๑๐
นายชาญณรงค์ ศรีดวงโชติ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒-๕๑๕๔๑๗๘	๐๙๗-๒๙๕๔๔๕๖

๙. แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม

การกู้คืนข้อมูลเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการดังนี้

๙.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๙.๒ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียให้แล้วเสร็จภายใน ๔๘ ชั่วโมง

๙.๓ ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๙.๔ นำอุปกรณ์ Backup Tape, Hard disk ที่จัดเก็บข้อมูลที่สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบ (ผู้ดูแลระบบ เจ้าหน้าที่ สทส. และบริษัทผู้รับจ้างการบำรุงรักษาระบบสารสนเทศ) ร่วมกันกู้ระบบกลับมาโดยเร็ว ภายใน ๔๘ ชั่วโมง

๙.๕ ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศหน่วยงาน จึงมีแผนจัดทำการสำรองข้อมูลเพื่อนำไปไว้อีกที่หนึ่งเพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ

๑๐. การติดตามและรายงานผล

เพื่อให้เป็นระบบบริหารความเสี่ยงที่สมบูรณ์จำเป็นจะต้องติดตามผลหลังดำเนินการตามแผน และทำการสอบทานดูว่าแผนจัดการความเสี่ยงใดมีประสิทธิภาพดีให้คงดำเนินการต่อไปหรือแผนใดควรปรับเปลี่ยน โดยอาจกำหนดข้อมูลที่ต้องติดตาม จัดทำ Check sheet และกำหนดความถี่เพื่อสอบทานรายวัน รายเดือน ทุก ๓ เดือน หรือทุกปี เป็นต้น ทั้งนี้ขึ้นอยู่กับสภาพปัญหาที่เกิดขึ้น นอกจากนี้ยังได้กำหนดให้มีการประเมินและทบทวนแผนความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง เพื่อดูว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้วหรือมีความเสี่ยงใหม่เพิ่มขึ้นมาอีกหรือไม่ โดยอาจกำหนดเป็นแผนดำเนินงานรวมทั้งปี และต้องกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบทำการรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้

แผนการจัดทำระบบบริหารความเสี่ยง

ขั้นตอนการดำเนินงาน	ปี พ.ศ. ๒๕๖๒											
	ตค. ๖๑	พย. ๖๑	ธค. ๖๑	มค. ๖๒	กพ. ๖๒	มีค. ๖๒	เมย. ๖๒	พค. ๖๒	มิย. ๖๒	กค. ๖๒	สค. ๖๒	กย. ๖๒
กำหนดวัตถุประสงค์												
ระบุความเสี่ยง												
ประเมินความเสี่ยง (ครั้งที่ ๑)												
ดำเนินการตามแผน												
รายงานผลการดำเนินงาน												
ประเมินความเสี่ยง (ครั้งที่ ๒)												
ทบทวนและปรับเปลี่ยนแผน												

ทั้งนี้ การจัดทำระบบบริหารความเสี่ยงนั้นจะต้องกระทำอย่างต่อเนื่องและสม่ำเสมอ มีการตรวจสอบและติดตามเป็นระยะ ๆ จึงจะเกิดประโยชน์อย่างแท้จริง

แบบฟอร์มติดตามความเสี่ยง

ประเด็นความเสี่ยง	กิจกรรมแนวทางการจัดการความเสี่ยง	ระดับความเสี่ยง			ผลสำเร็จของการจัดการความเสี่ยง	ระยะเวลาการดำเนินการ	งบประมาณที่ใช้	ข้อเสนอแนะการแก้ไข
		ผลกระทบ	โอกาสเกิด	โอกาส X ผลกระทบ				

แผนการควบคุมการเข้าถึงระบบเครือข่าย

จากการติดตามตรวจสอบความเสี่ยงในระบบสารสนเทศของสำนักงานอัยการสูงสุดพบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเครือข่ายคอมพิวเตอร์ซึ่งเป็นองค์ประกอบหลักในระบบสารสนเทศคือ ปัญหาระบบเครือข่ายล้มเหลว เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของสำนักงานอัยการสูงสุด หรือการทำงานหยุดชะงักและทำให้สามารถตรวจสอบ ติดตาม การพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุดได้อย่างถูกต้อง จึงได้จัดทำแผนการควบคุมปัญหาไว้ดังนี้

๑. การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย (Access Control)

๑.๑ สถานที่ตั้งห้อง Data Center ซึ่งมีการเก็บข้อมูลสารสนเทศที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น และระบบควบคุมประตูปิดเปิดอัตโนมัติต้องเป็นระบบที่ได้มาตรฐาน

๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิในการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและสอดคล้องกับหน้าที่ความรับผิดชอบ รวมทั้งให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๑.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น (Administrator) ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลสารสนเทศได้

๑.๔ ผู้ดูแลระบบ จัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเครือข่ายของสำนักงานอัยการสูงสุด และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญอย่างสม่ำเสมอ

๑.๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งระบบเครือข่ายทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

วัตถุประสงค์เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของสำนักงานอัยการสูงสุด โดยจัดให้มีการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสม รวมถึงได้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะต้องผ่านการพิสูจน์ตัวตน (Authentication) ก่อนใช้งานระบบเสมอ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย โดยมีแนวปฏิบัติดังนี้

๒.๑ ผู้ใช้งาน (User) ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของสำนักงานอัยการสูงสุดจะต้องได้ทำบันทึกเสนอหัวหน้าหน่วยงานของผู้ใช้งานเองเพื่อขอความเห็นชอบและพิจารณาอนุญาตเป็นลายลักษณ์อักษรและจัดส่งบันทึกความประสงค์การเข้าใช้งานดังกล่าวไปยัง สทส. ต่อไป

๒.๒ ผู้ดูแลระบบ (Admin) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมก่อนเข้าใช้งานระบบ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ การกำหนดสิทธิจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สายไว้เป็นหลักฐาน

๒.๔ กำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๕ ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๒.๖ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๒.๗ ผู้ดูแลระบบควรเปลี่ยนค่า ชื่อ login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรเลือกใช้ชื่อ login และรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒.๘ ต้องกำหนดค่าใช้ WPA2 ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

๒.๙ ควรมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สาย กับเครือข่ายภายใน

๒.๑๐ ควรใช้ Software หรือ Hardware ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

๓. การบริหารจัดการการเข้าถึงเครือข่าย

๓.๑ มีการออกแบบระบบเครือข่าย ซึ่งจำเป็นต้องมีการป้องกันและมีการจัดแบ่งระบบเครือข่ายเป็นโซนเพื่อให้เกิดความสะดวกในการควบคุมและจัดการโดยเฉพาะการติดตั้ง Firewall ทั้งนี้เพื่อให้เกิดความปลอดภัย โดยแบ่งตาม Zoning ของ Network คือ

๑) Internal zone หมายถึง ระบบเครือข่ายภายในองค์กร ซึ่งถือเป็น zone ที่มีความปลอดภัยและน่าเชื่อถือสูงสุด

๒) External zone หมายถึง ระบบเครือข่ายภายนอก ซึ่งถือเป็น zone ที่มีความปลอดภัยต่ำมาก ดังนั้น จึงจำเป็นต้องมีการควบคุมในเรื่องการสื่อสารที่ต้องติดต่อกับเครือข่ายภายนอกให้มีประสิทธิภาพ

๓) Demilitarized Zone (DMZ) เป็น zone พิเศษที่จะติดต่อโดยตรงทั้ง Internal และ External เช่น Mail Server, Web Server เป็นต้น

๓.๒ จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๓.๓ ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๓.๔ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นได้

๓.๕ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๓.๖ ระบบเครือข่ายทั้งหมดของสำนักงานอัยการสูงสุดที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอกองค์กร ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall และ IPS หรือฮาร์ดแวร์อื่น รวมทั้งต้องมีความสามารถในการตรวจจับ Malware ด้วย

๓.๗ การเข้าสู่ระบบงานเครือข่ายภายในสำนักงานอัยการสูงสุดโดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๓.๘ IP Address ระบบเครือข่ายภายในสำนักงานอัยการสูงสุดจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อป้องกันไม่ให้บุคคลภายนอกล่วงรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายของสำนักงานอัยการสูงสุดได้โดยง่าย

๓.๙ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๑๐ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุญาตจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๑๑ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดย สทส. เท่านั้น

๔. การบริหารจัดการระบบคอมพิวเตอร์

๔.๑ กำหนดกลุ่มงานหรือบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๔.๒ มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารทันที

๔.๓ เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๔.๔ ติดตั้งตัว Update ระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างเหมาะสม เช่น web server เป็นต้น

๔.๕ มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากแก้ไขหรือบำรุงรักษา

๔.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ สทส. เท่านั้น

๕. การบริหารจัดการการบันทึกและตรวจสอบ

๕.๑ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้**อย่างน้อย ๓ เดือน**

๕.๒ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๕.๓ มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๖. การควบคุมการใช้งานระบบจากภายนอกสำนักงานอัยการสูงสุด

ต้องกำหนดให้มีการควบคุมการใช้งานระบบ เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก ดังนี้

๖.๑ การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายของสำนักงานอัยการสูงสุดต้องควบคุมบุคคลที่จะเข้าสู่ระบบของหน่วยงานจากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๖.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของสำนักงานอัยการสูงสุดในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๖.๓ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๖.๔ มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๖.๕ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นและไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๗. การพิสูจน์ตัวตน

การพิสูจน์ตัวตน (Authentication) ถือเป็นกระบวนการที่มีความสำคัญและเป็นการยืนยันความถูกต้องตัวบุคคล (Identity) ของผู้ใช้งาน ซึ่งการใช้งานระบบเครือข่ายของสำนักงานอัยการสูงสุดนั้น ผู้ใช้งานทุกคนจะต้องผ่านการพิสูจน์ตัวตนจากระบบ Authentication โดยวิธีการแสดงชื่อผู้ใช้งาน (Username) และใส่รหัสผ่าน (Password) ก่อนการเข้าใช้งานในระบบเครือข่ายทุกครั้ง

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒ ฉบับนี้ได้ผ่านการพิจารณาให้ความเห็นชอบจากผู้บริหารที่เกี่ยวข้องแล้ว เพื่อให้เจ้าหน้าที่ของ สทส. ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๘. รับผิดชอบการจัดทำแผน

กลุ่มแผนงานเทคโนโลยีสารสนเทศ

๑. นางสาวภูริดา จันต๊ะพรมมา	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๒. นางสาวอุษา สิริปรีดากุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๓. นางสาวเบญญาภา ดีชานนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ผู้เสนอแผน

(นางสาวภูริดา จันต๊ะพรมมา)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

ผู้ตรวจทานแผน

(นางณฐนน แก้วกระจ่าง)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้เห็นชอบแผน

(นายเชิดศักดิ์ หิรัญสิริสมบัติ)
อธิบดีอัยการ สถาบันพัฒนาข้าราชการฝ่ายอัยการ
รักษาการในตำแหน่ง รองอัยการสูงสุด

ผู้อนุมัติแผน

(นายเข็มชัย ชุติวงศ์)
อัยการสูงสุด

ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ สำนักงานบริหารกิจการ อส. สำนักเทคโนโลยีสารสนเทศและการสื่อสาร โทร ๐ ๒๕๑๕ ๔๑๗๗

ที่ อส ๐๐๐๑.๑ (ทส)/๑๖๕๙ **วันที่** ๓๐ ตุลาคม ๒๕๖๑

เรื่อง ขออนุมัติแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

เรียน ผอ.สบกส. (ผ่าน ผอ.ทส)

ข้อเท็จจริง

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้นั้น และเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถให้บริการได้อย่างต่อเนื่อง และมีระบบสำรองข้อมูลที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา รับมือต่อเหตุฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น ลดการสูญเสียโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร เกิดความมั่นคงปลอดภัยและมีความพร้อมใช้งานได้อย่างมีประสิทธิภาพ เป็นเครื่องมือสำหรับผู้ใช้บริการ ผู้ดูแลระบบงาน และ ผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด จึงได้จัดแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) และได้มีการทบทวนปรับปรุงแผนเพื่อเสนอท่านอัยการสูงสุดและประกาศใช้แผนฯ เป็นประจำทุกปี

ข้อพิจารณา

สำนักเทคโนโลยีสารสนเทศและการสื่อสารในฐานะผู้ดูแลระบบเครือข่ายสารสนเทศและการสื่อสาร มีหน้าที่รับผิดชอบในการดูแลบำรุงรักษาเครือข่ายสารสนเทศและการสื่อสารของสำนักงานอัยการสูงสุดให้สามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ ระบบการสื่อสารข้อมูล ระบบสารสนเทศและการสื่อสารของหน่วยงาน นอกเหนือจากนั้นยังรับผิดชอบการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพราะหากมีการวางแผนและมีการจัดการความเสี่ยงที่ดีแล้วจะลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่อาจเกิดขึ้นได้ตามสภาวการณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ

ตามประกาศในราชกิจจานุเบกษา หน้าที่ ๘ เล่ม ๑๓๓ ตอนพิเศษ ๑๘๙ ง ลงวันที่ ๒๕ สิงหาคม ๒๕๕๙ กำหนดให้สำนักงานอัยการสูงสุดเป็นหน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ และมติที่ประชุมคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ครั้งที่ ๕/๒๕๖๐ เมื่อวันที่ ๒๕ กันยายน ๒๕๖๐ ได้เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและร่างประกาศของสำนักงานอัยการสูงสุด โดยสำนักงานอัยการสูงสุดต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยในทางปฏิบัติ และปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง จึงจำเป็นที่สำนักงานอัยการสูงสุดจะต้องตระหนักถึงความเสี่ยงที่เผชิญอยู่เพื่อจะได้เลือกใช้วิธีการป้องกันที่เหมาะสม และจำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้ตลอดเวลาและบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพ และต้องปฏิบัติตามนโยบายและแนวปฏิบัติฯ ที่กำหนดไว้อย่างเคร่งครัด ซึ่งหากไม่มีแผนรองรับสถานการณ์ที่

อาจเกิดขึ้นแล้ว...

อาจเกิดขึ้นแล้วระบบเทคโนโลยีสารสนเทศหรือข้อมูลสารสนเทศได้รับความเสียหายจากการถูกโจมตีจากผู้ไม่ประสงค์ดีจากไวรัสคอมพิวเตอร์ จากปัญหาไฟฟ้า อัคคีภัยหรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ อาจทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศและส่งผลกระทบต่อการปฏิบัติราชการของสำนักงานอัยการสูงสุดได้ เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความเสียหายได้ทั้งทางตรงและทางอ้อม

และตามมาตรา ๗ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องเป็นลายลักษณ์อักษร โดยมีผู้บริหารระดับสูงสุด และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้ลงนามในแผนฯ ให้เป็นไปตามหลักเกณฑ์ของกฎหมายด้านไอซีทีของประเทศไทย และสำนักงานอัยการสูงสุดจะได้ทบทวนแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) เป็นประจำทุกปี เพื่อให้สอดคล้องกับมาตรา ๕(๒) ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ข้อเสนอแนะ

จึงเห็นควรกราบเรียนท่านอัยการสูงสุดเพื่อโปรดพิจารณา ดังนี้

๑. กราบเรียนท่าน CIO เพื่อโปรดเห็นชอบแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

๒. กราบเรียนท่านอัยการสูงสุดเพื่อโปรดพิจารณาอนุมัติ และลงนามในแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

๓. เห็นชอบให้ สทส. ประชาสัมพันธ์ให้ผู้ที่มีส่วนเกี่ยวข้องได้ทราบและถือปฏิบัติต่อไป

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบโปรดกราบเรียนท่าน CIO เพื่อโปรดเห็นชอบตามข้อ ๑. และข้อ ๓. โปรดกราบเรียนท่านอัยการสูงสุดเพื่อโปรดพิจารณาอนุมัติแผนฯ และลงนาม ตามข้อ ๒. ที่เสนอมาพร้อมนี้

เบญ ดี

(นางสาวเบญญาภา ดีชานนท์)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(นางสาวภูริดา จันต๊ะพรมมา)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

(นางณฐนน แก้วกระจ่าง)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

๖๗๘๖
รับที่ ๕ พ.ย. ๒๕๖๒

เรียน อธิบดีอัยการ สถาบันพัฒนาข้าราชการฝ่ายอัยการ รักษาการในตำแหน่ง รองอัยการสูงสุด
(นายเชิดศักดิ์ หิรัญสิริสมบัติ) ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

พิจารณาแล้ว เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการปฏิบัติงานของสำนักงานอัยการสูงสุดเกิดความมั่นคงปลอดภัย และมีความพร้อมใช้งานได้อย่างมีประสิทธิภาพ เห็นควรนำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ประจำปีงบประมาณ พ.ศ. ๒๕๖๒ ไปใช้ในการปฏิบัติงาน ตามที่ สทส. เสนอ

จึงเรียนมาเพื่อโปรดพิจารณา

๑. เห็นชอบแผนรองรับสถานการณ์ฉุกเฉินฯ ตามที่ สทส. เสนอ

๒. ลงนามแผนรองรับสถานการณ์ฉุกเฉินฯ ที่เสนอมาพร้อมนี้

๓. เห็นชอบให้ สทส. ประชาสัมพันธ์ให้ผู้ที่มีส่วนเกี่ยวข้องได้ทราบและถือปฏิบัติต่อไป

๔. โปรดนำกราบเรียนอัยการสูงสุดเพื่อโปรดพิจารณาอนุมัติ พร้อมลงนามแผนรองรับสถานการณ์ฉุกเฉินฯ ตามที่ สทส. เสนอ

(นายรัชต์เทพ ดีประหลาด)
ผู้อำนวยการ
สำนักงานบริหารกิจการสำนักงานอัยการสูงสุด

กราบเรียน อัยการสูงสุด

เพื่อโปรดพิจารณา เห็นชอบตามข้อ ๑, ข้อ ๓ และอนุมัติพร้อมลงนามตามข้อ ๒, ข้อ ๔ ตามที่ ผอ.สบกส.เสนอ

(นายเชิดศักดิ์ หิรัญสิริสมบัติ)
อธิบดีอัยการ สถาบันพัฒนาข้าราชการฝ่ายอัยการ รักษาการในตำแหน่ง
รองอัยการสูงสุด
๑๒ พ.ย. ๒๕๖๑

- เห็นชอบตามข้อ ๑ และข้อ ๓
- อนุมัติตามข้อ ๔
- ลงนามแล้วตามข้อ ๒

(นายเข็มชัย ชุติวงศ์)
อัยการสูงสุด
๒๐ พ.ย. ๒๕๖๑

แผนการพัฒนาศักยภาพบุคลากร
ในการดำเนินงานระบบเทคโนโลยีสารสนเทศ
ของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

แผนการพัฒนาศักยภาพบุคลากรในการดำเนินงานระบบเทคโนโลยีสารสนเทศของสำนักงานอัยการสูงสุด ประจำปี พ.ศ. ๒๕๖๒

ลำดับที่	ชื่อหลักสูตร	จำนวนคน	กำหนดการ												หมายเหตุ
			ต.ค	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค	เม.ย	พ.ค	มิ.ย	ก.ค	ส.ค	ก.ย	
๑.	การนำเทคโนโลยีสารสนเทศไปใช้ในการปฏิบัติงาน ๑. การใช้งานสารบบคดีคดีค้ามนุษย์และคดีเร่งด่วนตามข้อสั่งการ ๒. การใช้งานระบบสารสนเทศเพื่อรองรับการเชื่อมต่อกระบวนการยุติธรรม AGO-NSW	๗๒๐		×	×	×	×	×	×	×	×	×	×	×	ดำเนินการให้กับ - ส่วนกลาง ๓ รุ่นๆ ๖๐ คน - ส่วนต่างจังหวัด ๙ ภาค ๆ ละ ๖๐ คน
๒.	การออกแบบและสร้างเว็บไซต์ตามมาตรฐานของสำนักงานอัยการสูงสุด	๕๐๐	×	×	×	×	×	×	×	×	×	×	×	×	ดำเนินการทั่วประเทศ --รอรับการจัดสรรงบประมาณ--
๓.	การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ	๕๐๐	×	×	×	×	×	×	×	×	×	×	×	×	ดำเนินการทั่วประเทศ --รอรับการจัดสรรงบประมาณ--
๔.	การใช้งาน Hardware Software และการแก้ไขปัญหาเบื้องต้น	๕๐๐	×	×	×	×	×	×	×	×	×	×	×	×	ดำเนินการทั่วประเทศ --รอรับการจัดสรรงบประมาณ--
๕.	การพัฒนาและเพิ่มขีดสมรรถนะบุคลากรของสำนักเทคโนโลยีสารสนเทศและการสื่อสาร" สำหรับบุคลากรผู้ปฏิบัติงานและผู้ดูแลระบบสารสนเทศ	๑๔	×	×	×	×	×	×	×	×	×	×	×	×	บุคลากรของสำนักเทคโนโลยีสารสนเทศและการสื่อสาร --รอรับการจัดสรรงบประมาณ--

ผู้จัดทำ	ผู้อนุมัติ
ลงชื่อ..นางสาวฐิรดา จันต๊ะพรมมา..... ตำแหน่ง.นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ วันที่.....	ลงชื่อ..นางณฐนน แก้วกระจ่าง..... ตำแหน่ง.ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร วันที่.....