สำนักงานศาลปกครอง

ICT SECURITY POLICY

นโยบายและแนวปฏิบัติใน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานศาลปกครอง (พ.ศ. 2567)

จัดทำโดย
สำนักวิทยาการสารสนเทศ
2567

นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานศาลปกครอง (พ.ศ. ๒๕๖๗)

(ICT Security Policy)

โดย

สำนักงานศาลปกครอง

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศมีบทบาทสำคัญที่เข้ามาช่วยอำนวยความสะดวกในการบริหารงานและดำเนินงานขององค์กร ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ สามารถขับเคลื่อนภารกิจตามแผนยุทธศาสตร์ขององค์กรให้มีประสิทธิภาพ และช่วยประหยัดค่าใช้จ่ายในการเดินทางเพื่อไปยังแหล่งข้อมูลหรือการประชุม เช่น การใช้อินเตอร์เน็ต การใช้ระบบเครือข่ายไร้สาย การใช้ระบบประชุมทางไกลผ่านจอภาพ การใช้ระบบสารสนเทศ เป็นต้น ระบบเทคโนโลยีสารสนเทศมีประโยชน์และสามารถช่วยอำนวยความสะดวกในด้านต่าง ๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูงที่อาจก่อให้เกิดความเสียหายของข้อมูล และการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่าง ๆ ทำให้มีโอกาสที่จะมีภัยคุกคามแฝงเข้ามาบุกรุกระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเตอร์เน็ตเพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการดักข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก ดังนั้นผู้ใช้งานและผู้ดูแลระบบด้านเทคโนโลยีสารสนเทศต้องตระหนักถึงการใช้งานและการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มากเป็นพิเศษ

สำนักงานศาลปกครองจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การปฏิบัติงานตามภารกิจด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากทุกหน่วยงานในสำนักงานศาลปกครอง และควรทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และมีการปรับปรุงเพื่อให้สอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศอย่างรวดเร็ว

สำนักงานศาลปกครองจึงหวังเป็นอย่างยิ่งว่า นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ นำไปใช้ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานศาลปกครองต่อไป

สำนักงานศาลปกครอง

กันยายน ๒๕๖๗

สารบัญ

		หน้า
บททั่วไป		
๑.	วัตถุประสงค์	๑
๒.	องค์ประกอบของนโยบาย	๒
คำนิยาม		๓
ส่วนที่ ๑	นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	๗
ส่วนที่ ๒	นโยบายการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย	๙
ส่วนที่ ๓	นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ	๑๒
ส่วนที่ ๔	นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน	๒๗
ส่วนที่ ๕	นโยบายการควบคุมการเข้าถึงเครือข่าย	๓๑
ส่วนที่ ๖	นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ	๓๔
ส่วนที่ ๗	นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ	๓๗
ส่วนที่ ๘	นโยบายการควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ต่อพ่วง	๔๑
ส่วนที่ ๙	นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา	๔๔
ส่วนที่ ๑๐	นโยบายการใช้งานระบบเครือข่ายอินเทอร์เน็ต	๔๗
ส่วนที่ ๑๑	นโยบายการใช้งานระบบเครือข่ายไร้สาย WiFi	๔๙
ส่วนที่ ๑๒	นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์	๕๑
ส่วนที่ ๑๓	นโยบายการป้องกันไวรัสคอมพิวเตอร์และซอฟต์แวร์ที่ไม่ประสงค์ดี	๕๓
ส่วนที่ ๑๔	นโยบายการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก	๕๕
ส่วนที่ ๑๕	นโยบายการใช้ระบบประชุมทางไกลผ่านจอภาพ	๕๗
ส่วนที่ ๑๖	นโยบายการสำรองและกู้คืนข้อมูล	๕๙
ส่วนที่ ๑๗	นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๖๓
ส่วนที่ ๑๘	นโยบายการกำหนดผู้รับผิดชอบ	๖๕
คณะผู้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานศาลปกครอง		๖๗

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานศาลปกครอง
(ICT Security Policy)

๑. วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานศาลปกครอง หรือต่อไปนี้เรียกว่า “องค์กร” ที่มีการก่อตั้งมานานกว่า ๒๔ ปี มีการติดตั้งใช้งานเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์รักษาความปลอดภัย ระบบงานสารสนเทศ พบปัญหาอุปสรรคที่ทำให้ระบบขัดข้อง และใช้วิธีการแก้ปัญหาที่ยังไม่ได้มีแนวปฏิบัติที่ชัดเจน ผู้ใช้งานก็ยังขาดความเข้าใจการใช้งานที่ถูกต้อง ซึ่งองค์กรได้ใช้วิธีปฏิบัติตามสากลทั่วไป และเพื่อให้มีความปลอดภัย ให้มีเสถียรภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง เชื่อถือได้ ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะรูปแบบต่าง ๆ ให้รอดพ้นจากภัยคุกคามทุกประเภท ที่จะพยายามบุกรุกเข้ามาภายในองค์กร และเป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ได้กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร จึงเห็นสมควรให้มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับใช้ภายใน โดยกำหนดให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของสำนักงานศาลปกครอง ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในสำนักงานศาลปกครองได้รับทราบและถือปฏิบัติ ตามนโยบายอย่างเคร่งครัด

๑.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ผู้ใช้งานและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานศาลปกครอง ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของสำนักงานศาลปกครอง ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละหนึ่งครั้ง

๒. องค์ประกอบของนโยบาย

คำนิยาม

ส่วนที่ ๑ นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ นโยบายการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

ส่วนที่ ๓ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๔ นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๕ นโยบายการควบคุมการเข้าถึงเครือข่าย

ส่วนที่ ๖ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๗ นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

ส่วนที่ ๘ นโยบายการควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ต่อพ่วง

ส่วนที่ ๙ นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ส่วนที่ ๑๐ นโยบายการใช้งานระบบเครือข่ายอินเทอร์เน็ต

ส่วนที่ ๑๑ นโยบายการใช้งานระบบเครือข่ายไร้สาย WiFi

ส่วนที่ ๑๒ นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๓ นโยบายการป้องกันไวรัสคอมพิวเตอร์และซอฟต์แวร์ที่ไม่ประสงค์ดี

ส่วนที่ ๑๔ นโยบายการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

ส่วนที่ ๑๕ นโยบายการใช้ระบบประชุมทางไกลผ่านจอภาพ

ส่วนที่ ๑๖ นโยบายการสำรองและกู้คืนข้อมูล

ส่วนที่ ๑๗ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑๘ นโยบายการกำหนดผู้รับผิดชอบ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานศาลปกครอง แต่ละส่วนจะประกอบด้วยวัตถุประสงค์ แนวปฏิบัติ และขั้นตอนการปฏิบัติ เพื่อที่จะทำให้สำนักงานศาลปกครองมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัยช่วยลดความเสียหายต่อการดำเนินงาน ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย การเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานศาลปกครองนี้จัดเป็นมาตรฐานด้านความปลอดภัย ซึ่งเจ้าหน้าที่ของสำนักงานศาลปกครองและบุคคลภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

องค์กร หมายถึง สำนักงานศาลปกครอง

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) หมายถึง เลขาธิการสำนักงานศาลปกครอง

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (Ministry Chief Information Officer : MCIO) หมายถึง ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ การประสานงานและให้ความร่วมมือกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง MCIO ของหน่วยงานอื่นที่เกี่ยวข้องในการจัดทำโครงการเทคโนโลยีสารสนเทศเพื่อแลกเปลี่ยนข้อมูลร่วมกัน และให้คำปรึกษาด้านระบบเทคโนโลยีสารสนเทศ

สำนักวิทยาการสารสนเทศ หมายถึง หน่วยงานภายในองค์กรที่ให้บริการด้านระบบเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบสารสนเทศขององค์กร ระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร

ผู้อำนวยการสำนักวิทยาการสารสนเทศ หมายถึง ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศของสำนักวิทยาการสารสนเทศ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในการกำหนดนโยบายแนวปฏิบัติในการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย

แนวทางปฏิบัติ หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ขั้นตอนการปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท ซึ่งองค์กรกำหนด และให้หมายความรวมถึงผู้บริหาร ผู้ดูแลระบบและเจ้าหน้าที่

ผู้บริหาร หมายถึง เลขาธิการสำนักงานศาลปกครอง รองเลขาธิการสำนักงานศาลปกครอง ที่ปรึกษาสำนักงานศาลปกครอง ผู้อำนวยการสำนักงานศาล ผู้อำนวยการสำนัก ผู้อำนวยการวิทยาลัย หัวหน้ากลุ่มขึ้นตรงต่อเลขาธิการสำนักงานศาลปกครอง และผู้อำนวยการกลุ่ม

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาของสำนักวิทยาการสารสนเทศให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ซึ่งสามารถเข้าถึงแอปพลิเคชันเครือข่ายคอมพิวเตอร์ ฐานข้อมูลสารสนเทศ และการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

เจ้าหน้าที่ หมายถึง ข้าราชการศาลปกครอง พนักงานราชการ และลูกจ้างสำนักงานศาลปกครอง

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

สินทรัพย์ (Assets) หมายถึง ข้อมูล ระบบสารสนเทศ และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตได้แก่ว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมิชอบเอาไว้ด้วย

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง ครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non- Repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ข้อมูล (Data) หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้น จะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม ภาพเคลื่อนไหว เสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่ทำการบันทึกไว้ปรากฏได้

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ

เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แม่ข่าย (Server) และรวมถึงเครื่องคอมพิวเตอร์ลูกข่าย(client) ชนิดตั้งโต๊ะ (Personal Computer) และชนิดพกพา (Notebook)

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ขององค์กรเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบแลน (LAN) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในองค์กรเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในองค์กร

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กร ได้ ได้แก่ ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet)

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหารการสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย แอปพลิเคชันข้อมูล และสารสนเทศ

ระบบสารสนเทศ (Information System) เป็นระบบพื้นฐานของการทำงานต่างๆ ในรูปแบบของการเก็บการประมวลผล เผยแพร่ และมีส่วนจัดเก็บข้อมูล

เจ้าของข้อมูล (Owner data) หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

ชื่อผู้ใช้งาน (Username) หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ โดยทั่วไปแล้วจะเป็นการพิสูจน์โดยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

ลงบันทึกเข้า (Login) หมายถึง กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

ลงบันทึกออก (Logout) หมายถึง กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

ช่องโหว่ (Vulnerability) หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การเข้ารหัส (Encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

อุปกรณ์กระจายสัญญาณ (Access Point) หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณคลื่นวิทยุด้วยความถี่ที่กำหนดไว้ในเครือข่ายไร้สาย

SSID (Service Set Identifier) หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

WEP (Wired Equivalent Privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย โดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล

WPA (Wi-fi Protected Access) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าแบบ WEP

แบนด์วิดท์ (Bandwidth) หมายถึง ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบเป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

ชุดคำสั่งไม่พึงประสงค์ (Malicious software) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

ข้อมูลจราจรทางคอมพิวเตอร์ (Log) หมายถึง ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ส่วนที่ ๑

นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. วัตถุประสงค์

เพื่อเป็นการควบคุมและการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ติดตั้งใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยจะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. สำนักบริหารทรัพย์สิน
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติการกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ ภายในองค์กรต้องมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์เป็นการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๓.๒ ต้องมีเจ้าหน้าที่รักษาความปลอดภัย ดูแลอาคารและห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตลักลอบเข้าสู่พื้นที่ปฏิบัติงาน

๓.๓ ผู้บริหาร ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว อาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป พื้นที่ทำงานของผู้ดูแลระบบ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ พื้นที่ใช้งานเครือข่ายไร้สาย

๓.๔ ผู้บริหาร ต้องกำหนดสิทธิให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเพื่อปฏิบัติหน้าที่ตามภารกิจที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

๓.๔.๑ จัดทำ “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๔.๒ ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “สมุดบันทึกการเข้า-ออกพื้นที่”

๓.๔.๓ ต้องมีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่อย่างน้อยปีละ ๑ ครั้ง

๔. แนวปฏิบัติการควบคุมการเข้า-ออก อาคาร สถานที่

๔.๑ การเข้าถึงอาคารองค์กรของบุคคลภายในต้องมีระบบควบคุมการเข้าออกอาคารสถานที่โดยระบบควบคุมการเข้าถึง (Access Control) ซึ่งบุคคลภายนอกจะได้รับอนุญาตเฉพาะรายไป

๔.๒ องค์กรต้องกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้า-ออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๔.๓ ต้องรณรงค์และออกกฎให้เจ้าหน้าที่ในองค์กรติดบัตรเพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน

๔.๔ การเข้าถึงอาคารขององค์กรของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแสดงบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ ได้แก่ บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ แล้วทำการลงบันทึกข้อมูลบัตรในระบบควบคุมการเข้าออกอาคารศาลปกครองหรือสมุดบันทึกการเข้า-ออกพร้อมให้รับบัตรผู้ติดต่อ (Visitor)

๔.๕ บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ภายในองค์กร

๔.๖ กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ ได้แก่ เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้ามาในบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในระบบควบคุมการเข้าออกอาคารศาลปกครอง หรือสมุดบันทึกการเข้า-ออก ระบุรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง

๔.๗ บุคคลภายนอกหรือผู้ติดต่อจะต้องคืนบัตรผู้ติดต่อ (Visitor) หรือ (ถ้ามี) แบบฟอร์มนำของออกให้มอบให้กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคารและเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่ระบบควบคุมการเข้าออกอาคารศาลปกครอง หรือสมุดบันทึกการเข้า-ออกให้ถูกต้อง

๔.๘ ผู้ใช้งานจะได้รับสิทธิให้เข้า-ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

ส่วนที่ ๒

นโยบายการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๑. วัตถุประสงค์

เพื่อกำหนดให้มีการควบคุม ตรวจสอบ จำกัดสิทธิบุคคลภายในและภายนอกที่ไม่มีหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ ซึ่งอาจจะทำให้เกิดความเสียหายต่อระบบสารสนเทศขององค์กร โดยกำหนดให้มีการควบคุมการเข้า-ออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. สำนักงานศาลปกครองในภูมิภาค ๑๔ แห่ง
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย (ส่วนกลาง)

๓.๑ ผู้ดูแลระบบ และเจ้าหน้าที่สำนักวิทยาการสารสนเทศ มีแนวทางปฏิบัติ ดังนี้

๓.๑.๑ ผู้ดูแลห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ต้องจัดระบบเทคโนโลยีสารสนเทศเป็นสัดส่วนชัดเจน ได้แก่ ส่วนบริหารเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๓.๑.๒ ผู้ดูแลห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้า-ออกห้อง โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และทำทะเบียน “ผู้มีสิทธิเข้า-ออกพื้นที่” ได้แก่ เจ้าหน้าที่จากบริษัทภายนอก (Outsource) และเจ้าหน้าที่ภายในสำนักวิทยาการสารสนเทศ

๓.๑.๓ เจ้าหน้าที่ทุกคนต้องใช้บัตรผ่าน (Key Card) หรือสแกนใบหน้า หรือสแกนลายนิ้วมือ เพื่อเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๓.๑.๔ ต้องจัดทำระบบเก็บบันทึกการเข้า-ออก (Access Control Log) ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๓.๑.๕ การเข้าถึงห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ให้ลงข้อมูลตามแบบฟอร์มที่ระบุไว้ใน “สมุดบันทึกการเข้า-ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า-ออก ทุกคนต้องกรอกในสมุดดังกล่าว

๓.๑.๖ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ก็ให้มีการควบคุมอย่างรัดกุม

๓.๑.๗ กรณีผู้ติดต่อจากหน่วยงานภายนอก มีความจำเป็นต้องเข้าห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เจ้าหน้าที่ผู้รับผิดชอบของสำนักวิทยาการสารสนเทศจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน และในกรณีที่เจ้าหน้าที่บริษัทที่มีหน้าที่ดูแลระบบต่าง ๆ ภายในอาคาร และระบบต่าง ๆ ในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย (Server) ที่จำเป็นต้องเข้ามาตรวจสอบการทำงานของระบบต่าง ๆ นอกเวลาราชการ ให้สำนักบริหารทรัพย์สินแจ้งรายชื่อและรูปถ่ายเจ้าหน้าที่บริษัทที่จะเข้ามาปฏิบัติงานภายในห้องควบคุมระบบฯ

๓.๒ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๓.๒.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประจำตัวประชาชนหรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงข้อมูลในสมุดบันทึกการเข้า-ออกพื้นที่

๓.๒.๒ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ที่ขออนุญาต ระบุไว้ในเอกสารด้วยทุกครั้งให้ถูกต้องชัดเจน

๓.๒.๓ ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผู้ติดต่อตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๓.๒.๔ พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอกสามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้า-ออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

๓.๒.๕ ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้า-ออก

๓.๒.๖ เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงข้อมูลไว้ในแบบฟอร์มการขออนุญาตเข้า-ออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

๓.๒.๗ เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้า-ออก กับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำ

๔. แนวปฏิบัติการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย (ส่วนภูมิภาค)

๔.๑ ผู้อำนวยการกลุ่มบริหารทั่วไป สำนักงานศาลปกครองส่วนภูมิภาค นายช่างคอมพิวเตอร์สำนักงานศาลปกครองส่วนภูมิภาค และเจ้าหน้าที่สำนักงานศาลปกครองส่วนภูมิภาค มีแนวทางปฏิบัติ ดังนี้

๔.๑.๑ ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย สำนักงานศาลปกครองส่วนภูมิภาคให้จัดระบบเทคโนโลยีสารสนเทศ ตามที่สำนักวิทยาการสารสนเทศเป็นผู้กำหนดผังการจัดวาง ได้แก่ ส่วนบริหารเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๔.๑.๒ ห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายสำนักงานศาลปกครองส่วนภูมิภาคต้องมีการกำหนดสิทธิ บุคคลในการเข้า-ออกห้อง โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการทำทะเบียน “ผู้มีสิทธิเข้า-ออกพื้นที่” ได้แก่ เจ้าหน้าที่จากบริษัทภายนอก (Outsource) และเจ้าหน้าที่สำนักงานศาลปกครองส่วนภูมิภาค

๔.๑.๓ การเข้าถึงห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายสำนักงานศาลปกครองส่วนภูมิภาคต้องให้ลงบันทึกตามแบบฟอร์มที่ระบุไว้ใน “สมุดบันทึกการเข้า-ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า-ออก ทุกคนต้องกรอกข้อมูลในสมุดดังกล่าว

๔.๑.๔ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายสำนักงานศาลปกครองส่วนภูมิภาค ต้องมีการควบคุมอย่างรัดกุม

๔.๑.๕ กรณีผู้ติดต่อจากหน่วยงานภายนอก มีความจำเป็นต้องเข้าห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เจ้าหน้าที่ผู้รับผิดชอบของสำนักงานศาลปกครองส่วนภูมิภาค จะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน

๔.๒ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๔.๒.๑ ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประจำตัวประชาชนหรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงข้อมูลในสมุดบันทึกการเข้า - ออกพื้นที่

๔.๒.๒ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ขออนุญาตที่ระบุไว้ในเอกสารทุกครั้งให้ถูกต้องชัดเจน

๔.๒.๓ ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายสำนักงานศาลปกครองส่วนภูมิภาค

๔.๒.๔ พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้า-ออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

๔.๒.๕ ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้า-ออก

๔.๒.๖ เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้า-ออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

๔.๒.๗ เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้า-ออก กับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำ

ส่วนที่ ๓

นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่ได้รับอนุญาตที่เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรและป้องกันภัยคุกคามจากผู้บุกรุกผ่านระบบเครือข่ายโดยใช้โปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงาน ทำให้ระบบเทคโนโลยีสารสนเทศเกิดปัญหาขัดข้อง หรือระบบล้มเหลว และผู้ดูแลระบบสามารถตรวจสอบติดตามบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง ช่องทางการเข้าถึง และข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control)

๓.๑ ประเภทข้อมูลขององค์กร แบ่งได้ดังนี้

๓.๑.๑ ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

๓.๑.๒ ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน ได้แก่ ข้อมูลจัดการงานคดีปกครอง ข้อมูลกฎระเบียบ กฎหมายปกครอง ข้อมูลการดำเนินการตามภารกิจ ข้อมูลติดตามการใช้จ่ายงบประมาณ ข้อมูลรายงานผลการปฏิบัติงาน

๓.๑.๓ ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลเผยแพร่คำพิพากษาคดีปกครอง ข้อมูลวิชาการและองค์ความรู้ด้านคดีปกครอง ข้อมูลสถิติคดีปกครอง ข้อมูลกฎหมายที่เกี่ยวข้องกับคดีปกครอง

๓.๒ ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญดังนี้

๓.๒.๑ การกำหนดชั้นความลับ ตามความสำคัญของข้อมูลในเอกสาร กำหนดไว้ ๓ ระดับ ได้แก่ ลับที่สุด ลับมาก ลับ และมีการกำหนดความรับผิดชอบ ให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนดระดับชั้นความลับของข้อมูล และการยกเลิกหรือปรับระดับชั้นความลับของข้อมูลตามความจำเป็น

๓.๒.๒ การเข้าถึงข้อมูล ใช้แนวทางตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งพระราชบัญญัติดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการข้อมูลอิเล็กทรอนิกส์ และเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ เอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อข้อมูลอิเล็กทรอนิกส์ และเอกสารอิเล็กทรอนิกส์

๓.๓ ระดับชั้นการเข้าถึง

๓.๓.๑ ระดับชั้นสำหรับผู้ดูแลระบบ สามารถเข้าถึงข้อมูลที่ดูแลรับผิดชอบได้ทุกส่วน

๓.๓.๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงข้อมูลทั่วไปที่เปิดเผยได้

๓.๔ เวลาที่ได้เข้าถึง

๓.๔.๑ การเข้าถึงสารสนเทศในเวลาราชการ ใช้แนวทางตามวันและเวลาทำงานตามปกติของข้าราชการศาลปกครอง พนักงานราชการ และลูกจ้างสำนักงานศาลปกครอง ตามประกาศ ก.บ.ศป. เรื่อง กำหนดวันและเวลาทำงาน และวันหยุดราชการของข้าราชการศาลปกครอง พนักงานราชการ และลูกจ้างสำนักงานศาลปกครอง

๓.๔.๒ การเข้าถึงสารสนเทศนอกเวลาราชการ

๓.๔.๓ การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ และวันหยุดนักขัตฤกษ์ที่ได้รับอนุญาต

๓.๕ ช่องทางการเข้าถึง

๓.๕.๑ ระบบแลน

๓.๕.๒ ระบบอินทราเน็ต

๓.๕.๓ ระบบอินเทอร์เน็ต

๓.๕.๔ ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

๓.๕.๕ ระบบเครือข่ายไร้สาย WiFi

๓.๕.๖ ระบบเครือข่ายเสมือน VPN

๓.๖ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ

๓.๖.๑ การควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๓.๖.๒ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบ

๔.๑ สถานที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๔.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงทุก ๑ ปีเป็นอย่างน้อย ทั้งนี้ ผู้ใช้งานระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๔.๓ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

๔.๔ ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรและตรวจการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศสำคัญ

๔.๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเก็บไว้เป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๕.๑ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบและกำหนดสิทธิในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศขององค์กร ได้แก่ ผู้ใช้งาน ในการขออนุญาตเข้าใช้ระบบงาน จะต้องมีการทำเป็นเอกสารเพื่อขอใช้สิทธิระบบสารสนเทศ และกำหนดให้มีการลงชื่อในเอกสารดังกล่าวและจัดเก็บไว้เป็นหลักฐาน

๕.๒ เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะ ในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

๕.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๖. แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตให้ปฏิบัติอย่างน้อยดังนี้

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก เรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๖.๒ ต้องมีการจัดฝึกอบรมเนื้อหาการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมาตรการเชิงป้องกันตามความเหมาะสม อย่างน้อยปีละ ๑ ครั้ง โดยการจัดฝึกอบรมอาจให้มีการแทรกเนื้อหาเข้าไปในหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมขององค์กรด้วย

๖.๓ จัดทำสื่อข้อมูลเพื่อการใช้งานระบบสารสนเทศอย่างปลอดภัยผ่านช่องทางต่าง ๆ ของหน่วยงาน

๖.๔ มีการตรวจสอบเพื่อประเมิน และจัดการความเสี่ยงทางด้านสารสนเทศ

๖.๕ การลงทะเบียนผู้ใช้งาน (User registration)

๖.๕.๑ จัดทำแบบฟอร์มการลงทะเบียน หรือทำโดยผ่านระบบอิเล็กทรอนิกส์สำหรับผู้ขอใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

๖.๕.๒ ผู้ใช้งานต้องทำการ “การพิสูจน์และยืนยันตัวตน” เพื่อพิสูจน์และยืนยันความถูกต้องของตัวบุคคล หรือผ่าน “ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล” ที่เป็นเครือข่ายทางอิเล็กทรอนิกส์ ที่เชื่อมโยงข้อมูลระหว่าง

บุคคลใด ๆ หรือหน่วยงานของรัฐเพื่อประโยชน์ในการพิสูจน์และยืนยันตัวตน และการทำธุรกรรมอื่น ๆ ที่เกี่ยวเนื่องกับการพิสูจน์และยืนยันตัวตน แนวทางตามพระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒

๖.๕.๓ ผู้ใช้งานต้องทำการขออนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะ ในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

๖.๕.๔ ผู้ใช้งานทำการขออนุญาตกรอกข้อมูลการขอใช้งานผ่านแบบฟอร์มการลงทะเบียน หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ให้ผู้ใช้งานเข้าสู่ระบบสารสนเทศ และได้รับความเห็นชอบจากผู้อำนวยการสำนักงานศาล/ ผู้อำนวยการสำนัก/ ผู้อำนวยการวิทยาลัย/ หัวหน้ากลุ่มขึ้นตรงต่อเลขาธิการสำนักงานศาลปกครอง/ ผู้อำนวยการกลุ่มหรือเทียบเท่า

๖.๕.๕ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ควบคุมข้อมูล เจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๖.๕.๖ ผู้ดูแลระบบกำหนดชื่อผู้ใช้งาน (Username) จากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น หรือทำโดยผ่านระบบอิเล็กทรอนิกส์

๖.๕.๗ ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศและให้เก็บย้อนหลังอย่างน้อย ๑ ปี

๖.๕.๘ ผู้ดูแลระบบกำหนดให้มีการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศเมื่อได้รับแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร หรือทำโดยผ่านระบบอิเล็กทรอนิกส์

๖.๕.๙ กำหนดการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๖.๕.๙.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบสารสนเทศของผู้ใช้งานทั่วไป โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๖.๕.๙.๒ ผู้ดูแลระบบต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๖.๕.๙.๓ ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศให้เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

๖.๕.๙.๔ ผู้ดูแลระบบต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานเป็นลายลักษณ์อักษร หรือระบบอิเล็กทรอนิกส์ และให้เก็บย้อนหลังอย่างน้อย ๑ ปี

๖.๕.๙.๕ ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้

๖.๕.๙.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ดูแลระบบ หรือผู้ใช้งานอื่นใดที่มีสิทธิในระดับสูงผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยกำหนดระยะเวลาการใช้งานและระงับการ

ใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๖.๕.๑๐ กำหนดการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๖.๕.๑๐.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๖.๕.๑๐.๒ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราวที่ยากต่อการคาดเดา และต้องมีความแตกต่าง

๖.๕.๑๐.๓ ผู้ดูแลระบบต้องกำหนดวันหมดอายุอย่างน้อยทุก ๖ เดือน สำหรับรหัสผ่านของผู้ใช้งานทุกคน

๖.๕.๑๐.๔ ผู้ดูแลระบบต้องส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยโดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน หรือทำโดยผ่านระบบอิเล็กทรอนิกส์

๖.๕.๑๐.๕ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

๖.๕.๑๐.๖ ผู้ดูแลระบบต้องตรวจสอบการพิสูจน์และยืนยันตัวตนให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสผ่านใหม่ หรือกระทำโดยผ่านระบบอิเล็กทรอนิกส์

๖.๕.๑๑ ข้อกำหนดการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ให้มีกระบวนการในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศโดยมีการปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง หรือเมื่อมีการเปลี่ยนแปลงอื่นใดในลักษณะเดียวกันนี้และให้มีการทบทวนสิทธิผู้ใช้งานในระดับสูง เช่น สิทธิผู้ดูแลระบบ อย่างน้อยปีละ ๒ ครั้ง พร้อมทั้งมีทำการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่ได้ทำการทบทวน เพื่อใช้ในการตรวจสอบภายหลัง

๖.๖ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผยการล่วงรู้การลักลอบทำสำเนาข้อมูลสารสนเทศหรือลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้ปฏิบัติอย่างน้อย ดังนี้

๖.๖.๑ วิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งานเพื่อให้สามารถกำหนดรหัสผ่านการใช้งานรหัสผ่านและการเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย ให้ผู้ใช้งานปฏิบัติ ดังต่อไปนี้

๖.๖.๑.๑ เปลี่ยนรหัสผ่านทันทีเมื่อ Authentication ใช้งานระบบครั้งแรก

๖.๖.๑.๒ ให้ตั้งรหัสผ่านที่ยากต่อการคาดเดา

๖.๖.๑.๓ ให้กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๖.๖.๑.๔ ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลทีมีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๖.๖.๑.๕ ไม่ตั้งรหัสผ่านโดยใช้ตัวเลขหรือตัวอักษรที่เรียงกัน หรือเหมือนกันทั้งหมด หรือกลุ่มเหมือนกัน

๖.๖.๑.๖ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๖.๖.๑.๗ เก็บรักษารหัสผ่านทั้งของตนเองและของหน่วยงานไว้เป็นความลับ

๖.๖.๑.๘ ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

๖.๖.๑.๙ ไม่ใช่รหัสผ่านของตนเองร่วมกับผู้อื่น

๖.๖.๑.๑๐ ไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบหรือใช้งานแทนตน กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๖.๖.๑.๑๑ ให้เปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๖ เดือน หรือเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้ต้องแจ้งให้สำนักวิทยาการสารสนเทศทราบทันที

๖.๖.๑.๑๒ ให้มีการเปลี่ยนรหัสผ่านสำหรับผู้ดูแลระบบ อย่างน้อยทุก ๆ ๓ เดือน

๖.๖.๑.๑๓ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

๖.๖.๑.๑๔ การเปลี่ยนรหัสผ่านให้หลีกเลี่ยงการใช้รหัสผ่านเดิม

๖.๖.๑.๑๕ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์

๖.๖.๑.๑๖ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User ID ของตน เว้นแต่พิสูจน์เป็นอย่างอื่น

๖.๖.๑.๑๗ ผู้ใช้งานอาจได้รับการร้องขอจากสำนักวิทยาการสารสนเทศให้ทำการเปลี่ยนรหัสผ่านใหม่ ในกรณีที่รหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัยสามารถถูกคาดเดาหรือถูกล่วงละเมิดได้ง่าย ทั้งนี้ผู้ใช้งานต้องตรวจสอบความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวง

๖.๖.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้ปฏิบัติดังนี้

๖.๖.๒.๑ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๖.๖.๒.๒ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๕ นาที โดยต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๖.๖.๒.๓ ผู้ใช้งานต้องล็อคหรือใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๖.๖.๒.๔ ผู้ใช้งานต้องทำความเข้าใจในการเข้าถึงอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๖.๖.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ให้ใช้งานปฏิบัติ ดังนี้

๖.๖.๓.๑ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย โดยห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๖.๖.๓.๒ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงในเครื่องคอมพิวเตอร์ของหน่วยงาน

๖.๖.๓.๓ ปิดเครื่องคอมพิวเตอร์ (Power off/Shutdown) ทุกครั้งหลังเลิกงานหรือไม่ใช้งาน

๖.๖.๓.๔ ออกจากระบบ (Log off) ออกจากระบบสารสนเทศหรือระบบคอมพิวเตอร์ทันทีเมื่อใช้งานเสร็จ หรือจำเป็นต้องปล่อยทิ้งโดยไม่ดูแล

๖.๖.๓.๕ การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงานไปตรวจซ่อมจะต้องดำเนินการโดยผ่านความเห็นของเจ้าหน้าที่สำนักวิทยาการสารสนเทศ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

๖.๖.๓.๖ ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

๖.๖.๓.๗ ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บนเครื่องคอมพิวเตอร์

๖.๖.๓.๘ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๖.๖.๓.๙ ให้ใช้ความระมัดระวังในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์ โดยใส่กล่องหรือห่อหุ้มด้วยวัสดุป้องกันการกระแทก เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

๖.๖.๓.๑๐ การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๖.๖.๓.๑๑ หลีกเลี่ยงการใช้ปากกา หรือวัสดุอื่นใดกดสัมผัสหน้าจอ LCD หรือ LED ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD หรือ LED ของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้

๖.๖.๓.๑๒ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๖.๖.๓.๑๓ ให้ติดตั้งหรือจัดเก็บอุปกรณ์คอมพิวเตอร์ ตู้ติดตั้งอุปกรณ์เครือข่าย กล่องใส่ CD/DVD หรือสิ่งอื่นใดที่เป็นอุปกรณ์เฉพาะสำหรับติดตั้งหรือเก็บรักษาที่มั่นคงแข็งแรง

๖.๖.๓.๑๔ เพื่อความเป็นระเบียบและปลอดภัยสำหรับอุปกรณ์คอมพิวเตอร์ที่พกพาประเภท CD/DVD หรือ Thumb Drive หรือสิ่งอื่นใดลักษณะเดียวกันนี้ ให้จัดเก็บไว้ในสถานที่หรืออุปกรณ์เฉพาะ ที่สามารถปิดล็อคได้

๖.๖.๓.๑๕ ต้องกำหนดสิทธิการเข้าใช้งาน โดยมีการตั้งรหัสผ่านการเข้าใช้งานเครื่องคอมพิวเตอร์ให้ปฏิบัติตามข้อกำหนดในวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use)

๖.๖.๓.๑๖ ตรวจสอบ สายไฟ สายเมาส์ สายแป้นพิมพ์ หรือสายสัญญาณของอุปกรณ์คอมพิวเตอร์อื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์คอมพิวเตอร์ได้รับความเสียหาย

๖.๖.๓.๑๗ ทำความสะอาดอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละออง ที่จะทำให้เครื่องคอมพิวเตอร์เกิดขัดข้อง/เสียหาย

๖.๖.๓.๑๘ ควรใช้วิธีการทางเทคนิคในการเข้ารหัสข้อมูลเพื่อเข้ารหัสข้อมูลสำคัญในเครื่องคอมพิวเตอร์

๖.๖.๓.๑๙ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันเครื่องคอมพิวเตอร์มิให้ถูกขโมยหรือสูญหาย โดยล็อคเครื่องขณะไม่ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหายให้เก็บไว้ในตู้ที่สามารถล็อคได้หรือวิธีอื่นตามเหมาะสม

๖.๖.๓.๒๐ ห้ามนำเครื่องคอมพิวเตอร์ที่ไม่ใช่ของหน่วยงานมาใช้กับเครือข่ายหน่วยงาน เว้นแต่ได้รับการตรวจสอบจากผู้ดูแลระบบที่เกี่ยวข้องก่อนการใช้งาน

๖.๖.๓.๒๑ ห้ามเปลี่ยนแปลงหมายเลขไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงาน

๖.๖.๓.๒๒ ต้องทำการสำรองข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

๖.๖.๓.๒๓ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกแบบภายนอก CD, DVD, External Hard Disk หรืออื่น ๆ ที่เหมาะสม

๖.๖.๓.๒๔ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖.๖.๔ ผู้ใช้งานต้องป้องกัน และแก้ไขไวรัสคอมพิวเตอร์ หรือซอฟต์แวร์ไม่ประสงค์ดี (Antivirus)

๖.๖.๔.๑ ตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานมีโปรแกรมป้องกันไวรัสติดตั้งอยู่ และต้องเปิดใช้งานตลอดเวลาที่ใช้งาน

๖.๖.๔.๒ ปรับปรุงฐานข้อมูลไวรัส (Update Virus Signature)

๖.๖.๔.๓ ห้ามทำการใดเพื่อขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๖.๖.๔.๔ ควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก และจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น

๖.๖.๔.๕ ทำการตรวจหาไวรัสทุกครั้งหลังจากรับไฟล์จากแหล่งใด ๆ ก็ตามมาใช้ที่เครื่องคอมพิวเตอร์

๖.๖.๔.๖ ใช้งานอินเทอร์เน็ตด้วยความระมัดระวังโดยไม่เปิดเว็บไซต์เกมออนไลน์บนอินเทอร์เน็ต เว็บไซต์ลามกอนาจาร เว็บการพนัน เว็บดูหนังออนไลน์ เว็บไซต์ที่มีเนื้อหาไม่เหมาะสม

หมิ่นประมาท เป็นภัยต่อความมั่นคง เว็บที่หมิ่นพระบรมเดชานุภาพ และเว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมหรือไฟล์ต่าง ๆ หรือพฤติการณ์อื่นใดที่มีความเสี่ยงต่อการติดไวรัส หรือมีเนื้อหาเข้าข่ายผิดกฎหมาย

๖.๖.๔.๗ ห้ามติดตั้งโปรแกรม Java, ActiveX, Extension หรือโปรแกรมประเภท Active Code อื่นใดจากแหล่งที่ไม่น่าเชื่อถือ

๖.๖.๔.๘ ไม่เปิดจดหมายอิเล็กทรอนิกส์ (E-mail) จากบุคคลที่ไม่รู้จักหรือชื่อเรื่องที่ไม่เคยติดต่อกันมาก่อน หรือสงสัยว่าไม่ปลอดภัย

๖.๖.๔.๙ ไม่เปิด Share Drive หากมีความจำเป็นให้เปิดเพียง Share Folder โดยต้องอนุญาตใช้รหัสผ่าน หรือมีระบบ Authentication และอนุญาตให้อ่านอย่างเดียว

๖.๖.๔.๑๐ ไม่คลิกเปิดหน้าต่างโฆษณาแบบป๊อบอัพ (pop-up) หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม (spam)

๖.๖.๔.๑๑ ห้ามสร้าง เก็บ หรือเผยแพร่ไวรัส (Virus), หนอนอินเทอร์เน็ต (Worms), โปรแกรมแฝง (Trojan Horses), อีเมลบอมบ์ (Email-Bomber), แอดแวร์ (Adware), สปายแวร์ (Spyware), บอท (BOT), แรนซัมแวร์ (Ransomware) มัลแวร์ (Malware) หน้าเว็บไซต์ปลอม (Phishing) โปรแกรมตรวจจับการพิมพ์ (Key Logger) หรือซอฟต์แวร์ไม่ประสงค์ดีอื่นใด

๖.๖.๔.๑๒ ให้ความสำคัญกับการแจ้งเตือนจากโปรแกรมป้องกันไวรัส หากมีข้อสงสัยหรือพบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติหรือโปรแกรมป้องกันไวรัสมีการแจ้งเตือนมากผิดปกติหรือโปรแกรมป้องกันไวรัสมีการแจ้งเตือนมากผิดปกติโปรดแจ้งสำนักวิทยาการสารสนเทศ

๖.๖.๕ การยับยั้งหรือจำกัดความเสียหาย เมื่อเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์หรือโปรแกรมประสงค์ร้ายให้ผู้ที่ทำหน้าที่ป้องกันและแก้ไขไวรัสปฏิบัติ ดังต่อไปนี้

๖.๖.๕.๑ ให้แยกเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติออกจากเครือข่ายของหน่วยงานโดยการถอดสาย LAN หรือปิดอุปกรณ์ไร้สาย (Wireless LAN)

๖.๖.๕.๒ สำรองข้อมูลสำคัญในเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติ

๖.๖.๕.๓ ให้ทำการตรวจหาไวรัสที่อาจจะฝังตัวอยู่กับข้อมูลที่สำรองไว้ก่อนนำข้อมูลไปใช้กับเครื่องคอมพิวเตอร์อื่น

๖.๖.๕.๔ ในกรณีที่พบไฟล์ที่ติดไวรัสหรือไฟล์ที่เป็นโปรแกรมประสงค์ร้าย และซอฟต์แวร์ตรวจสอบไวรัสสามารถแก้ไขไวรัสที่ติดได้ ให้ดำเนินการแก้ไขโดยใช้ซอฟต์แวร์ ตรวจสอบไวรัส หากซอฟต์แวร์ตรวจสอบไวรัสไม่สามารถแก้ไขไวรัสที่ติดได้ ให้ลบไฟล์ที่ติดไวรัสหรือไฟล์ที่เป็นโปรแกรมประสงค์ร้ายทิ้ง

๖.๖.๕.๕ ให้ติดตั้งโปรแกรมส่วนแก้ไข (Update Patch) ตามความเหมาะสม ปรับปรุงเวอร์ชันซอฟต์แวร์ตรวจสอบไวรัส และปรับปรุงฐานข้อมูลป้องกันไวรัส (Update Virus Signature) ให้เป็นปัจจุบันเพื่อเพิ่มประสิทธิภาพในการป้องกันไวรัส

๖.๖.๖ การจัดการเอกสารลับบนกระดาษหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

๖.๖.๖.๑ มีการจัดหมวดหมู่เอกสารลับไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างดีพอ

๖.๖.๖.๒ จำกัดการสำเนาเอกสารลับเท่าที่จำเป็นต้องใช้งานเท่านั้น

๖.๖.๖.๓ ระมัดระวังการกระจาย ส่ง หรือแจกจ่ายเอกสารลับไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับทราบ หรือใช้งานเอกสารนั้นเท่านั้น

๖.๖.๖.๔ ใช้วิธีการตามกฎหมายที่หน่วยงานได้ถือปฏิบัติอยู่แล้วสำหรับการจัดส่งเอกสารลับทางไปรษณีย์

๖.๖.๗ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๖.๖.๘ เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๖.๖.๙ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลายสื่อหรือข้อมูลอิเล็กทรอนิกส์ ดังนี้

๖.๖.๙.๑ Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย

๖.๖.๙.๒ กระดาษ หรือแผ่น CD/DVD ใช้วิธีหั่นด้วยเครื่องหั่นทำลายเอกสาร

๖.๖.๙.๓ เทป ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย

๖.๖.๙.๔ ฮาร์ดดิสก์ หรือ Solid State Drive (SSD) ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามแนวทางมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DoD ๕๕๒๐.๒๒ M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๖.๖.๑๐ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ให้มีการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล SSL, VPN

๖.๖.๑๑ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

๖.๖.๑๒ ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เพื่อส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมหรือจำหน่าย หรือเพื่อการอื่นให้มีการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๖.๖.๑๓ ป้องกันไม่ให้บุคคลภายนอกเข้าถึงหรือใช้งานกล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกัน โดยไม่ได้รับอนุญาต

๖.๖.๑๔ ให้นำเอกสารออกจากเครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้ทันทีที่ใช้งานเสร็จ

๖.๖.๑๕ ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ ออกจากพื้นที่ใช้งาน ต้องขออนุญาตจากผู้บังคับบัญชาก่อนทุกครั้ง

๖.๖.๑๖ ผู้ใช้งานต้องคืนทรัพย์สินทั้งหมดที่เกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า - ออก คอมพิวเตอร์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ เมื่อพ้นจากการปฏิบัติหน้าที่

๖.๖.๑๗ ผู้ดูแลระบบต้องระงับสิทธิ หรือถอดถอนสิทธิ หรือเรียกคืนสินทรัพย์ตามเห็นควร หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายว่าด้วยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๖.๗ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

๖.๗.๑ ต้องมีการพิจารณาทบทวนสิทธิอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดทุก ๆ รอบ ๑ ปี และทุกครั้งที่มีการเปลี่ยนแปลงสถานภาพ ได้แก่ การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ การเกษียณอายุ การลาออก การเลิกจ้าง

๖.๗.๒ การให้อำนาจสำหรับสิทธิการเข้าถึงพิเศษ ต้องมีการทบทวนบ่อยครั้งมากขึ้น อย่างน้อยปีละ ๒ ครั้ง

๖.๗.๓ การติดตามการจัดสรรสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

๖.๗.๔ การเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน และการติดตาม

๗. แนวปฏิบัติการควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน

๗.๑ ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ ให้แก่ผู้ใช้งานให้มีความเหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่และได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ ในกรณีมีความจำเป็นต้องใช้ user ที่มีสิทธิพิเศษต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ในการพิจารณาว่าการควบคุม user ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้น สำนักวิทยาการสารสนเทศจะพิจารณาในภาพรวม

๗.๒ ต้องได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

๗.๓ ควบคุมการใช้งาน User ที่มีสิทธิพิเศษอย่างเข้มงวด

๗.๔ ต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๗.๕ เปลี่ยนรหัสผ่านอย่างเคร่งครัด ได้แก่ ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

๗.๖ ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งาน โดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง ได้แก่ กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์

๗.๗ ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ ได้แก่ การ share files จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๘. แนวปฏิบัติการควบคุมการใช้งานบัญชีรายชื่อและรหัสผ่าน

๘.๑ ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง

๘.๒ กำหนดให้รหัสผ่านมีความยาวพอสมควร ให้มีความยาวขั้นต่ำ ๘ ตัวอักษร

๘.๓ ใช้อักขระพิเศษประกอบ

๘.๔ สำหรับผู้ใช้งานทั่วไป ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน

๘.๕ ผู้ใช้งานที่มีสิทธิพิเศษ ได้แก่ ผู้ดูแลระบบ และผู้ใช้งานที่ติดมากับระบบ (default user) ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓ เดือน

๘.๕.๑ การเปลี่ยนรหัสผ่านแต่ละครั้ง ต้องไม่กำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

๘.๕.๒ ต้องไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน ได้แก่ “abcdef” “aaaaaa” “123456” เป็นต้น

๘.๕.๓ ต้องไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด

๘.๕.๔ ต้องไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

๘.๕.๕ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปต้องไม่เกิน ๕ ครั้ง

๘.๕.๖ ต้องจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย ได้แก่ การใส่ซองปิดผนึก

๘.๕.๗ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือ ได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านโดยทันที

๘.๖ ผู้ใช้งานต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที

๘.๗ ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญ อย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ

๙. แนวปฏิบัติการเข้าถึงระบบคอมพิวเตอร์แม่ข่าย

เพื่อให้มีการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม ไม่ก่อให้เกิดความเสี่ยงในการเข้าถึงระบบสารสนเทศและเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาตและให้เครื่องคอมพิวเตอร์แม่ข่ายทำงานได้อย่างมีประสิทธิภาพ มีความถูกต้อง น่าเชื่อถือ และพร้อมใช้งานให้ปฏิบัติดังนี้

๙.๑ การควบคุมการติดตั้งซอฟแวร์ลงในระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๙.๑.๑ ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

๙.๑.๒ ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้วหรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

๙.๑.๓ การติดตั้งหรือปรับปรุงซอฟแวร์ที่อาจกระทบต่อการให้บริการของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๙.๑.๔ ไม่ติดตั้งซอร์สโค๊ต (Source Code) หรือชุดคำสั่ง ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ หรือใช้เทคนิคการป้องกันซอร์สโค๊ต (Source Code) หรือชุดคำสั่งที่อาจถูกเปิดเผยได้

๙.๑.๕ กำหนดให้มีการจัดเก็บซอร์สโค๊ต (Source Code) หรือชุดคำสั่ง และไลบรารี่ (Library) สำหรับซอฟแวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๙.๑.๖ ให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องทำการทดสอบซอฟแวร์ระบบปฏิบัติการ ซอฟแวร์ที่เป็นตัวระบบสารสนเทศ หรือซอฟแวร์หรือระบบสารสนเทศอื่นใด ตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๙.๑.๗ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๙.๑.๘ ให้มีการจัดเก็บซอฟแวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนการปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเก่าเหล่านั้นตามระยะเวลาที่เหมาะสม

๙.๑.๙ ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มพัฒนา

๙.๑.๑๐ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น

๙.๒ ข้อกำหนดในการทบทวนการทำงานของระบบสารสนเทศหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๙.๒.๑ แจ้งให้ผู้เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๙.๒.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๙.๒.๓ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๙.๒.๔ ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่ายในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๙.๒.๕ ต้องมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๙.๓ การพัฒนาซอฟแวร์โดยหน่วยงานภายนอก

๙.๓.๑ ให้มีการควบคุมโครงการพัฒนาซอฟแวร์โดยผู้รับจ้างภายนอก

๙.๓.๒ ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค๊ต (Source Code) หรือชุดคำสั่งในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๙.๓.๓ ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบคุณภาพและความถูกต้องของซอฟต์แวร์ ที่จะมีการพัฒนาโดยผู้รับจ้างให้บริการจากภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๙.๓.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

๙.๔.๑ ให้จัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังนี้

๙.๔.๑.๑ ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

๙.๔.๑.๒ สถานที่ติดตั้ง

๙.๔.๑.๓ เครื่องที่ติดตั้ง

๙.๔.๑.๔ ผู้ผลิตซอฟต์แวร์

๙.๔.๑.๕ ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๙.๔.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๙.๔.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

๙.๔.๓.๑ มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

๙.๔.๓.๒ ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน

๙.๔.๓.๓ กำหนดให้ผู้ที่เกี่ยวข้องทำการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๙.๔.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษรหรือกระทำโดยผ่านระบบอิเล็กทรอนิกส์

๙.๔.๕ ข้อกำหนดในการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) และการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ

๙.๔.๕.๑ ข้อมูลชื่อบัญชีผู้ใช้งาน

๙.๔.๕.๒ ข้อมูลวันเวลาที่เข้าถึงระบบ

๙.๔.๕.๓ ข้อมูลวันเวลาที่ออกจากระบบ

๙.๔.๕.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๙.๔.๕.๕ ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

๙.๔.๕.๖ ข้อมูลพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

๙.๔.๕.๗ ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่นของระบบ

๙.๔.๕.๘ ข้อมูลแสดงการใช้งานแอปพลิเคชัน

๙.๔.๕.๙ ข้อมูลแสดงการเปิด ปิด เขียน อ่านไฟล์ หรือลักษณะอื่นใดในการกระทำกับไฟล์

๙.๔.๕.๑๐ ข้อมูลไอพีแอดเดรสที่ใช้ และที่เข้าถึง

๙.๔.๕.๑๑ ข้อมูลโปรโตคอลเครือข่ายที่ใช้

๙.๔.๕.๑๒ ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

๙.๔.๕.๑๓ ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๙.๔.๖ ต้องดำเนินการติดตั้งอัพเดตซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ ได้แก่ Web Server

๑๐. แนวปฏิบัติการบริหารจัดการและการตรวจสอบระบบเครือข่าย

๑๐.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ Server Zone, Management Zone, DMZ Zone, Branch Zone เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๑๐.๒ ต้องมีระบบป้องกันการบุกรุก ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

๑๐.๓ ต้องมีระบบการตรวจสอบการบุกรุก (IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุก ผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๑๐.๔ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๑๐.๕ ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่าย ไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๑๐.๖ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไข หรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๑๐.๗ การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๑๐.๘ ต้องจัดทำผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของ เครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละครั้ง

๑๐.๙ IP address ภายในของระบบงานเครือข่ายภายในขององค์กรต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถทราบได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของสำนักวิทยาการสารสนเทศได้โดยง่าย

๑๐.๑๐ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุญาตจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น

๑๑. แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

๑๑.๑ ต้องกำหนดให้มีการบันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๑๑.๒ ต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๑.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๔

นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๑. วัตถุประสงค์

เพื่อเป็นการป้องกันผู้ใช้งานเข้าถึงข้อมูลสารสนเทศ หรืออุปกรณ์ประมวลผลสารสนเทศ โดยไม่ถูกต้อง ไม่ได้รับอนุญาต แอบลักลอบมาขโมยข้อมูล หรืออุปกรณ์ โดยวิธีการต่างๆ และนำไปเปิดเผย

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๓.๑ การใช้งานรหัสผ่าน (password use)

๓.๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านด้วยตนเอง ที่ง่ายต่อการจดจำ บุคคลอื่นไม่สามารถคาดเดาได้ง่าย

๓.๑.๒ ผู้ใช้งานต้องเก็บรักษารหัสผ่านที่บุคคลอื่นไม่สามารถค้นหาได้ง่าย ได้แก่ บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาอื่นๆ และให้เก็บรักษาในสถานที่ที่ปลอดภัย

๓.๑.๓ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านมีการถูกลักลอบนำไปใช้โดยบุคคลอื่นที่ไม่ได้รับอนุญาต

๓.๑.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อย ๖ เดือนต่อครั้ง และผู้ดูแลระบบอย่างน้อย ๓ เดือนต่อครั้ง หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ และหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยมีการใช้มาแล้ว

๓.๑.๕ ผู้ใช้งานต้องดำเนินการเปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

๓.๑.๖ ผู้ใช้งานต้องไม่เก็บรหัสผ่านไว้ในโปรแกรมที่จดจำรหัสผ่านแบบถาวร หรือขั้นตอนการ Login แบบอัตโนมัติ

๓.๑.๗ ผู้ใช้งานต้องไม่ใช้รหัสผ่านร่วมกับบุคคลอื่น

๓.๑.๘ ผู้ใช้งานต้องไม่ใช้รหัสผ่านเดียวกันกับหลายๆ ระบบ หรืออุปกรณ์ส่วนตัว

๓.๑.๙ กรณีมีความจำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องจดจำรหัสผ่านหลายตัว ผู้ใช้งานสามารถใช้รหัสผ่านเดียวกันได้ แต่ระบบต้องมีความปลอดภัยในระดับที่เชื่อถือได้

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๓.๒.๑ ผู้ใช้งานต้องออกจากระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพาอื่น ๆ โดยทันทีเมื่อเสร็จงาน

๓.๒.๒ ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้เป็นเวลานาน

๓.๒.๓ ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบ เทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๓.๒.๔ เครื่องคอมพิวเตอร์ทุกเครื่อง ผู้ใช้งานต้องกำหนดระยะเวลาการพักหน้าจอ (screen saver) เมื่อไม่ได้ใช้งาน ไม่เกิน ๑๕ นาที

๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy)

๓.๓.๑ การจัดทำบริเวณล้อมรอบ

๓.๓.๑.๑ ต้องมีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในองค์กร

๓.๓.๑.๒ ต้องมีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง

๓.๓.๑.๓ ผนังล้อมรอบของสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในต้องสร้างเป็นผนังทึบหรือกระจกทึบ

๓.๓.๑.๔ ประตูหรือทางเข้า-ออก สำนักงานหรืออาคาร ให้มีการออกแบบที่สามารถป้องกันการบุกรุกทางกายภาพ

๓.๓.๑.๕ ประตูหรือทางเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายต้องมีระบบที่สามารถปิดทางเข้า-ออกได้ และทางเข้า-ออก ต้องปิดตลอดเวลา เพื่อป้องกันการบุกรุกทางกายภาพ

๓.๓.๑.๖ บุคลากรที่ปฏิบัติงานภายในองค์กร ต้องปิดประตูและหน้าต่างเสมอหลังจากเลิกงานและนอกเวลาราชการ

๓.๓.๑.๗ ต้องมีการจัดระบบการรักษาความปลอดภัย โดยมีเจ้าหน้าที่รักษาความปลอดภัยและต้องมีการติดตั้งกล้องวงจรปิดที่เห็นบริเวณทางเดิน เข้า-ออก ห้องภายในสำนักงาน และภายในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เพื่อควบคุมการเข้าถึงของบุคคล

๓.๓.๑.๘ ผนังห้องต้องมีการก่อสร้างให้มีความทนทานต่อความร้อน และความชื้นได้อย่างเพียงพอ

๓.๓.๑.๙ ต้องแยกพื้นที่ของระบบเทคโนโลยีสารสนเทศในองค์กรออกจากพื้นที่ที่มีการดูแลหรือบริหารจัดการโดยผู้ให้บริการจากภายนอก

๓.๓.๒ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

๓.๓.๒.๑ จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันบุคคลทั่วไปเข้าถึงโดยไม่ได้รับอนุญาต

๓.๓.๒.๒ จำกัดบุคคลทั่วไปซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๓.๓.๒.๓ จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงบุคคลทั่วไปเข้าถึงพื้นที่อื่น ๆ ภายในองค์กร

๓.๓.๒.๔ ต้องตรวจสอบวัสดุที่อาจพบว่าเป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

๓.๓.๒.๕ ต้องมีการลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการจากภายนอกโดยให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

๓.๓.๓ การจัดวางและการป้องกันอุปกรณ์ในบริเวณพื้นที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๓.๓.๓.๑ ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในหน่วยงานหรือสำนักงานให้น้อยที่สุด

๓.๓.๓.๒ ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอก โดยการหันหน้าจอเข้ามาด้านในโดยไม่ให้บุคคลผู้ซึ่งไม่มีสิทธิสามารถมองเห็นหน้าจอนั้นได้

๓.๓.๓.๓ ต้องแยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่งเพื่อดูแลความมั่นคงปลอดภัย

๓.๓.๓.๔ ห้ามนำอาหาร เครื่องดื่ม เข้ามาในบริเวณหรือพื้นที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๓.๓.๓.๕ ดำเนินการตรวจสอบ สอดส่อง ระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

๓.๓.๓.๖ ต้องมีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่เสถียร ได้แก่ ไฟฟ้าตก ไฟฟ้าดับ ไฟฟ้าเกิน

๓.๓.๔ ระบบและอุปกรณ์สนับสนุนการทำงาน

๓.๓.๔.๑ ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรที่เพียงพอต่อความต้องการใช้งาน ได้แก่ ระบบปรับอากาศ ระบบระบายอากาศ ระบบกระแสไฟฟ้าสำรอง และต้องมีการตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบสามารถทำงานได้ตามปกติ และลดปัญหาความเสี่ยงที่จะทำให้ระบบสารสนเทศหยุดทำงาน

๓.๓.๔.๒ ต้องมีการใช้ระบบ UPS กับระบบเทคโนโลยีสารสนเทศเพื่อป้องกันอุปกรณ์อิเล็กทรอนิกส์เสียหายจากความไม่เสถียรของกระแสไฟฟ้า และต้องมีการตรวจสอบระบบ UPS อย่างสม่ำเสมอ โดยตรวจสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

๓.๓.๕ การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่น ๆ

๓.๓.๕.๑ เจ้าหน้าที่ทุกคนต้องปฏิบัติการป้องกันทรัพย์สินของทางราชการ

๓.๓.๕.๒ เจ้าหน้าที่ต้องออกจากระบบสารสนเทศที่ใช้งานทันที เมื่อจำเป็นต้องปล่อยทิ้งไว้ว่างเว้นจากการใช้งานโดยไม่มีผู้ดูแล

๓.๓.๕.๓ ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ปลอดภัย ได้แก่ ในตู้เอกสารที่มีกุญแจล็อคและไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะทำงาน เพื่อความปลอดภัยของทรัพย์สินของราชการ

๓.๓.๕.๔ ต้องป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน และป้องกันตู้เอกสารหรือบริเวณที่ใช้ในการรับ-ส่ง เอกสาร เพื่อความปลอดภัยของข้อมูล

๓.๓.๕.๕ ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่าง ๆ ได้แก่เครื่องคอมพิวเตอร์ กล้องดิจิตอล โทรศัพท์มือถือที่มีกล้อง เครื่องพิมพ์ เครื่องถ่ายเอกสาร เครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต

๓.๓.๕.๖ ให้นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๓.๖ มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

๓.๓.๖.๑ ต้องทำการเคลียข้อมูลที่บันทึกอยู่ในอุปกรณ์สื่อบันทึกข้อมูลได้แก่ ฮาร์ดดิสก์ และ Flash drive ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

๓.๓.๖.๒ ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์สื่อบันทึกข้อมูลได้แก่ ฮาร์ดดิสก์ และ Flash drive ก่อนทำการทำลายด้วยการทุบหรือบดให้เสียหาย

๓.๓.๖.๓ อุปกรณ์สื่อบันทึกข้อมูลได้แก่ ฮาร์ดดิสก์ และ Flash drive ต้องทำการฟอร์แมต (Format) ฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยการใช้วิธีแบบเขียนทับซ้ำจำนวน ๑ ครั้ง ตามมาตรฐาน NIST ๘๐๐-๘๘ สำหรับข้อมูลที่มีความลับ หรือแบบเขียนทับซ้ำจำนวน ๓ ครั้ง ตามมาตรฐาน DoD ๕๒๒๐.๒๒-M สำหรับข้อมูลที่มีความลับมาก หรือแบบเขียนทับซ้ำจำนวน ๗ ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีความลับมากที่สุด

๓.๓.๖.๔ ต้องมีการเปลี่ยนฮาร์ดดิสก์หรือลบข้อมูลออกจากฐานข้อมูลที่มีอายุตั้งแต่ ๕ ปีขึ้นไป และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๓.๓.๖.๕ อุปกรณ์สื่อบันทึกข้อมูล ได้แก่ แผ่น CD/DVD และกระดาษ วิธีการทำลายให้ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร

๓.๓.๖.๖ อุปกรณ์สื่อบันทึกข้อมูล ได้แก่ เทป วิธีการทำลายให้ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย

๓.๓.๖.๗ ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายอุปกรณ์ สื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

๓.๔ การจัดการการเข้าถึงข้อมูลชั้นความลับ

ผู้ดูแลระบบต้องจัดการการเข้าถึงข้อมูลชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ระยะเวลาในการเข้าถึง ช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูล ตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังต่อไปนี้

๓.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

๓.๔.๒ ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๔.๓ กำหนดวัน เวลา เริ่มต้นใช้งาน และวัน เวลาสิ้นสุดการใช้งาน

๓.๔.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ การใช้ TLS VPN หรือเทคโนโลยีอื่นใดที่ดีกว่า

๓.๔.๕ กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๓.๔.๖ กรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ได้แก่ ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องปฏิบัติการสำรองและลบข้อมูลที่เก็บในฮาร์ดดิสก์เสียก่อน

๓.๔.๗ ต้องมีการทบทวนสิทธิในการเข้าถึงข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ใช้อย่างถูกต้องและมีความเหมาะสม

๓.๔.๘ ผู้ใช้สามารถนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ส่วนที่ ๕

นโยบายการควบคุมการเข้าถึงเครือข่าย

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมการเข้าถึงระบบเครือข่าย ให้ผู้ใช้งานใช้ประโยชน์จากระบบเครือข่ายในการเข้าถึงเครือข่ายได้อย่างถูกต้อง ป้องกันมิให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง แก้ไขเปลี่ยนแปลงระบบเครือข่าย ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศขององค์กรโดยมีการกำหนดแนวปฏิบัติควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกัน

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย

๓.๑ การใช้งานบริการเครือข่าย

๓.๑.๑ ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลผ่านระบบเครือข่ายที่เป็นการขัดต่อความดีงาม ศีลธรรม กฎหมาย โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว องค์กรไม่มีส่วนร่วมรับผิดชอบใดๆ ทั้งสิ้น

๓.๑.๒ องค์กรไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายเพื่อการค้าแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และระบบเครือข่าย ได้แก่ การประกาศแจ้งการซื้อขายสินค้า การให้บริการโฆษณาสินค้า หรือการ download ไฟล์เพื่อการค้าแสวงหาผลกำไร

๓.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อบุคคลอื่นใด คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การเจาะระบบ (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของบุคคลอื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่บุคคลอื่น การใช้ภาษาไม่สุภาพ หรือการเขียนข้อความที่ทำให้บุคคลอื่นเสียหาย ถือเป็นการละเมิดสิทธิของบุคคลอื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์กรไม่มีส่วนร่วมรับผิดชอบใดๆ ทั้งสิ้น

๓.๑.๔ ห้ามมิให้บุคคลใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบเครือข่าย เพื่อดักข้อมูล ล้วงข้อมูลรหัสผ่าน หรือข้อมูลที่สำคัญชั้นความลับ

๓.๑.๕ องค์กรได้มอบบัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานห้ามโอนหรือแจกจ่ายสิทธินี้ให้กับบุคคลอื่นนำไปใช้โดยพลการ

๓.๑.๖ บัญชีผู้ใช้งาน (User Account) ที่องค์กรให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ ที่อาจเกิดขึ้นและมีความเสียหาย ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของบุคคลอื่น

๓.๑.๗ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (user authentication for external connections)

๓.๒.๑ ผู้ใช้งานต้องแจ้งความประสงค์ขอใช้บริการระบบเครือข่ายภายในองค์กร โดยมีการเข้าถึงจากภายนอกองค์กร ตามแบบฟอร์มการขอใช้บริการ โดยต้องผ่านความเห็นชอบจากผู้บังคับบัญชาตามลำดับชั้น

๓.๒.๒ ผู้ใช้งานที่จะเข้าใช้งานระบบการเข้าถึงจากภายนอกองค์กรต้องมีการแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และรหัสผู้ใช้งาน (password) ทุกครั้ง

๓.๒.๓ ต้องมีระบบการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศภายใน โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง ได้แก่ การใช้รหัสผ่าน (Password)

๓.๒.๔ ต้องมีการผ่านวิธีตรวจสอบชั้นความปลอดภัยอีกระดับเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน ได้แก่ ฐานข้อมูลผู้ใช้งานระบบ Active Directory (AD)

๓.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

๓.๓.๑ ผู้ใช้งานต้องแจ้งความประสงค์จะขอใช้บริการอุปกรณ์บนระบบเครือข่ายภายในองค์กร ตามแบบฟอร์มการขอใช้บริการ โดยต้องผ่านความเห็นชอบจากผู้บังคับบัญชาตามลำดับชั้น

๓.๓.๒ ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ หมายเลข IP Address และสถานที่ใช้งาน

๓.๓.๓ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการกำหนดระบุอุปกรณ์ว่าให้สามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้

๓.๓.๔ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบหมายเลข IP Address ของอุปกรณ์ต้นทางและอุปกรณ์ปลายทางได้

๓.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

๓.๔.๑ ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงพอร์ตหมายเลขต่างๆ ของอุปกรณ์เครือข่าย โดยจะปิดพอร์ตที่ไม่จำเป็นต้องใช้งาน และพอร์ตที่เสี่ยงจะเป็นช่องโหว่ของการบุกรุกสร้างความเสียหายต่อระบบเครือข่าย

๓.๔.๒ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายจะต้องลงชื่อเข้า-ออกใน “สมุดบันทึกการเข้า-ออกพื้นที่” ให้ถูกต้อง และได้รับการอนุญาตจากผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่ายก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๓.๔.๓ ต้องมีการตรวจสอบการโจมตีระบบเครือข่ายโดยผ่านพอร์ตต่าง ๆ และนำพอร์ตที่ถูกการโจมตีมากำหนดการปิด เพื่อป้องกันการบุกรุกของภัยคุกคามทีแฝงตัวมากับข้อมูลที่ใช้งานในระบบเครือข่าย

๓.๕ การแบ่งแยกเครือข่าย (segregation in networks)

๓.๕.๑ องค์กรต้องจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

๓.๕.๒ องค์กรต้องแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ในอาคารที่ส่วนกลางและอาคารส่วนภูมิภาค เพื่อควบคุมการเข้าถึงระบบเครือข่าย

๓.๕.๓ องค์กรต้องติดตั้งอุปกรณ์ Firewall เพื่อป้องกันเครือข่ายตามการแบ่งโซนกลุ่มผู้ใช้งานและกลุ่มระบบสารสนเทศอื่น ๆ

๓.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๓.๖.๑ ต้องมีการตรวจสอบการเชื่อมต่อในระบบเครือข่าย LAN และ WAN

๓.๖.๒ ต้องมีระบบควบคุมระดับ Bandwidth ของระบบสารสนเทศต่าง ๆ ที่วิ่งผ่านวงจรการเชื่อมต่อระบบเครือข่ายที่ใช้งานเชื่อมระหว่างส่วนกลางและภูมิภาค

๓.๖.๓ จำกัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

๓.๖.๔ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๓.๖.๕ มีระบบการตรวจจับผู้บุกรุกในระดับเครือข่าย

๓.๖.๖ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๓.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๓.๗.๑ ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลข IP Address ในเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย

๓.๗.๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓.๗.๓ กำหนดการบังคับใช้เส้นทางเครือข่าย โดยกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

ส่วนที่ ๖

นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงการใช้ระบบปฏิบัติการ ทำความเข้าใจ และมีความรับผิดชอบต่อเหตุการณ์ที่ได้ปฏิบัติตามภารกิจ ซึ่งจะช่วยให้การเข้าถึงทรัพยากรและข้อมูลของหน่วยงาน มีความปลอดภัยและพร้อมใช้งานอยู่เสมอ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติเพื่อการควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๓.๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓.๑.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อล็อคหน้าจอภาพเมื่อไม่มีการใช้งานเป็นระยะเวลาสั้นๆ และให้ใส่รหัสผ่าน (Password) เพื่อเปิดเข้าใช้หน้าจอภาพ

๓.๑.๓ การเข้าใช้ระบบปฏิบัติการต้องกำหนดให้มีการใส่ Username และ Password ทุกครั้ง

๓.๑.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานระบบปฏิบัติการร่วมกัน

๓.๑.๕ ผู้ใช้งานต้องออกจากระบบบัญชีผู้ใช้งาน (sign out) ทันที ที่ไม่ได้ใช้งานเป็นระยะเวลานาน

๓.๑.๖ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓.๑.๗ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (password) ในทันทีที่ได้รับสิทธิการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓.๑.๘ ซอฟต์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อไปใช้งานที่อื่น

๓.๑.๙ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นขององค์กรเพื่อประโยชน์ทางการค้า

๓.๑.๑๐ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมกรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๓.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication)

๓.๒.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๓.๒.๒ ให้มีระบบจัดเก็บข้อมูลผู้ใช้งานเป็นฐานข้อมูลซึ่งใช้เป็นกระบวนการในการอ้างอิงตรวจสอบความถูกต้องข้อมูลของผู้ใช้งานในการเข้าถึงระบบปฏิบัติการซึ่งต้องมีการยืนยันการใส่ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

๓.๒.๓ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศเพื่อยืนยันสิทธิและเป็นการป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งาน มีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๒.๔ ผู้ใช้งานที่เป็นเจ้าของชื่อผู้ใช้งาน (Username) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้งาน เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของบุคคลอื่น

๓.๒.๕ ผู้ใช้งานต้องลงชื่อเข้าใช้ (Login) โดยใช้ชื่อผู้ใช้งาน (Username) ของตนเอง และทำการลงชื่อออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๓.๓ การบริหารจัดการรหัสผ่าน (password management system)

๓.๓.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนเอง

๓.๓.๒ ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการติดตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย โดยกำหนดให้รหัสผ่านมีความยาวไม่ต่ำกว่า ๘ ตัวอักษร

๓.๓.๒.๑ สำหรับผู้ใช้งานทั่วไป ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน

๓.๓.๒.๒ ผู้ใช้งานที่มีสิทธิพิเศษ ได้แก่ ผู้บริหารระบบ (system administrator) และผู้ใช้งานที่ติดมากับระบบ (default user) ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๓ เดือน

๓.๓.๒.๓ ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ต้องไม่กำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

๓.๓.๒.๔ ต้องไม่กำหนดรหัสผ่านซ้ำอักษรเดียวกันหรือเรียงลำดับอักษร

๓.๓.๒.๕ ต้องไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้ใช้งาน ได้แก่ ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่

๓.๓.๒.๖ ต้องไม่กำหนดรหัสผ่านเป็นคำสแลง คำศัพท์ และคำอื่นๆ ที่เป็นที่รู้จักกันโดยทั่วไป

๓.๓.๓ ผู้ดูแลระบบจะต้องดำเนินการกำหนดรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๓.๓.๔ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ ได้แก่ ทุก ๆ ๖ เดือน

๓.๓.๕ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการล็อกอินเข้าใช้งานระบบงานเป็นครั้งแรก

๓.๓.๖ ระบบบริหารจัดการรหัสผ่านต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน

๓.๓.๗ ระบบบริหารจัดการรหัสผ่านต้องป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ หรือที่จำเป็น ต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๓.๘ มีระบบการจัดเก็บรหัสผ่าน ที่ผู้ใช้งานสามารถเข้าไปในระบบทำการแก้ไข เปลี่ยนรหัสผ่านเชิงโต้ตอบด้วยตนเองได้

๓.๓.๙ ระบบการจัดเก็บรหัสผ่าน สามารถนำไปใช้เชื่อมโยงเพื่อตรวจสอบสิทธ์ก่อนเข้าใช้งานระบบสารสนเทศได้

๓.๔ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities)

ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางประเภทสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

๓.๔.๑ ผู้ดูแลระบบของสำนักวิทยาการสารสนเทศเป็นผู้กำหนดโปรแกรมอรรถประโยชน์ที่จะติดตั้งและเป็นผู้ดำเนินการติดตั้งโปรแกรมลงในเครื่องคอมพิวเตอร์ทุกเครื่อง

๓.๔.๒ ไม่อนุญาตผู้ใช้งานติดตั้งโปรแกรมอรรถประโยชน์ลงในเครื่องคอมพิวเตอร์เพิ่มเติม เว้นแต่มีความจำเป็นต้องขออนุญาตจากผู้บังคับบัญชาและแจ้งให้ผู้ดูแลระบบพิจารณา

๓.๔.๓ กำหนดสิทธิและจำกัดการใช้โปรแกรมอรรถประโยชน์สำหรับผู้ใช้งานที่เกี่ยวข้อง

๓.๔.๔ ต้องยกเลิกสิทธิการใช้หรือลบทิ้งโปรแกรมอรรถประโยชน์กรณีหมดภารกิจหรือความจำเป็นที่ต้องใช้งาน

๓.๕ การเว้นว่างจากการใช้งานในระยะเวลาหนึ่ง (session time-out)

๓.๕.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบงาน อุปกรณ์เครือข่าย ต้องให้มีการตัดและหมดเวลาการใช้งานรวมถึงปิดการใช้งาน หลังจากที่ไม่มีการใช้งานช่วงระยะเวลา ๑๐ นาที

๓.๕.๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศต้องให้มีการล้างข้อความ รูปภาพ บนหน้าจอกรณีที่ไม่มีการใช้งาน ช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันบุคคลอื่นที่เข้ามาใช้งานเห็นข้อมูลเดิมที่ค้างอยู่บนหน้าจอ

๓.๕.๓ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศต้องให้มีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)

๓.๖.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศต้องมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๒ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

๓.๖.๒ ต้องกำหนดให้ระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง ต้องมีการจำกัดระยะเวลาในการใช้งานหรือเชื่อมต่อในแต่ละครั้ง โดยกำหนดช่วงระยะเวลา ๑ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

๓.๖.๓ ต้องกำหนดให้มีการ disconnect ระบบสารสนเทศ โดยผ่านระบบเทคโนโลยีสารสนเทศได้แก่ อุปกรณ์เครือข่ายได้ทันที กรณีเกิดเหตุการณ์ผิดปกติจากการใช้งานหรือเกิดการบุกรุกจากภัยคุกคาม

ส่วนที่ ๗

นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการจำกัดการใช้งานระบบสารสนเทศ การใช้อุปกรณ์คอมพิวเตอร์ให้สามารถปกป้องระบบจากปัจจัยความเสี่ยงต่าง ๆ ที่จะเข้ามารบกวนหรือทำลายข้อมูลสารสนเทศจากหลายช่องทางที่มีการเจาะจงการเข้าถึงโดยเฉพาะจากภายในและภายนอกองค์กร

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรม

๓.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction)

๓.๑.๑ ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร กำหนดการปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งการยกเลิกสิทธิการใช้งาน

๓.๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบสารสนเทศต่าง ๆ ที่สำคัญ ได้แก่ ระบบโปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต (Internet) ระบบอินทราเน็ต (Intranet) ระบบเครือข่ายไร้สาย (WiFi) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๑.๓ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๓.๑.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบ ลาออก พ้นจากตำแหน่ง เกษียณอายุ หรือยกเลิกการใช้งาน

๓.๑.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ต้องหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๓.๑.๓.๓ ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๑.๓.๔ กำหนดชื่อผู้ใช้งานหรือรหัสผ่านต้องไม่ซ้ำกัน

๓.๑.๓.๕ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง

๓.๑.๔ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๓.๑.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๓.๑.๔.๒ ต้องกำหนดรายชื่อผู้ใช้งาน และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๑.๔.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา

๓.๑.๔.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๓.๑.๕ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน

๓.๒ ระบบซึ่งไวต่อการรบกวน

๓.๒.๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ได้แก่ ระบบ GFMIS (ระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์) ระบบ EGP (ระบบการจัดซื้อจัดจ้างภาครัฐ) ระบบ FORMULA (ระบบการเงินการบัญชี) ระบบดังกล่าวเป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณการบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร และระบบทะเบียนราษฎร์ซึ่งจะได้รับการแยกออกจากระบบงานอื่น ๆ ขององค์กร

๓.๒.๒ ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะโดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมหรือจัดการระบบเชื่อมต่อในอุปกรณ์การรักษาความปลอดภัย Firewall เพื่อควบคุมเครื่องคอมพิวเตอร์ รวมถึงให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร กรณีต้องใช้งานจากภายนอก ให้ผู้ใช้แจ้งคำขอใช้มาที่ผู้ดูแลระบบ เพื่อผู้ดูแลระบบจะได้ดำเนินการอนุญาตให้มีการใช้งานต่อไป ซึ่งใช้งานกับระบบที่ต้องเชื่อมไปยังกรมบัญชีกลาง และสำนักทะเบียนราษฎร์ กรมการปกครอง ที่ต้องเชื่อมโยงผ่านเครือข่าย GIN

๓.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๓.๓.๑ ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๓.๓.๒ ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๓.๓.๓ เมื่อหมดความจำเป็นที่ต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

๓.๓.๔ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

๓.๓.๕ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดขึ้นจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๓.๔ การปฏิบัติงานจากภายนอกสำนักงาน (teleworking)

๓.๔.๑ ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อนซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานระยะไกล

๓.๔.๒ ต้องมีการกำหนดมาตรการความปลอดภัยสำหรับระบบเครือข่ายระหว่างสถานที่ที่จะมีการปฏิบัติงาน และระบบงานต่าง ๆ ภายในองค์กรก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานระยะไกล

๓.๔.๓ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อระบบเครือข่าย โดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

๓.๔.๔ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อระบบเครือข่าย โดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

๓.๔.๕ องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงาน และบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๓.๔.๖ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกลมีการป้องกันไวรัสคอมพิวเตอร์และการใช้งาน Firewall ตามที่องค์กรต้องการ

๓.๔.๗ ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน

๓.๕ แนวทางการปฏิบัติการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

๓.๕.๑ ต้องมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

๓.๕.๒ ต้องมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

๓.๕.๓ จัดให้มีคณะกรรมการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๓.๕.๔ พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๓.๕.๕ พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๓.๕.๖ ให้มีการตรวจสอบโปรแกรมที่ไม่พึงประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๓.๕.๗ หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

ส่วนที่ ๘

นโยบายการควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ต่อพ่วง

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานทราบถึงข้อกำหนดและมาตรฐานการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงโดยผู้ใช้งานมีหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงการบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงเพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง มีประสิทธิภาพ และมีความพร้อมใช้งานอยู่เสมอ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติทั่วไป

๓.๑ องค์กรต้องจัดให้มีเจ้าหน้าที่ผู้ดูแลรับผิดชอบและเป็นผู้ประสานงานจัดทำทะเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงรวมถึงการติดตามปรับปรุงและแก้ไขทะเบียนครุภัณฑ์อย่างต่อเนื่อง

๓.๒ คอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่องค์กรอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง อย่างมีประสิทธิภาพเพื่องานขององค์กร

๓.๓ เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงขององค์กรห้ามนำไปใช้นอกสถานที่เว้นแต่จะนำไปใช้งานในภารกิจขององค์กร โดยจะต้องได้รับอนุญาตจากผู้บังคับบัญชาภายในหน่วยงานที่ผู้ใช้งานสังกัด

๓.๔ ผู้ใช้งานต้องจัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงไว้ในสถานที่ปลอดภัย ห้ามจัดการแก้ไขเปลี่ยนแปลงชิ้นส่วนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง เว้นแต่เป็นการดำเนินการเพื่อซ่อมแซมบำรุงรักษาโดยเจ้าหน้าที่สำนักงานวิทยาการสารสนเทศ

๓.๕ กรณีมีการย้ายจุดติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ผู้ใช้งานต้องได้รับความเห็นชอบจากผู้บังคับบัญชาหน่วยงานภายในองค์กรในแต่ละสังกัดและต้องแจ้งให้เจ้าหน้าที่สำนักวิทยาการสารสนเทศทราบเป็นหนังสือไว้เป็นหลักฐาน

๓.๖ การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของสำนักวิทยาการสารสนเทศเท่านั้นเว้นแต่จะได้รับอนุญาตจากเจ้าหน้าที่ของสำนักวิทยาการสารสนเทศเป็นรายไป

๓.๗ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓.๘ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนขององค์กร

๓.๙ ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์

๓.๑๐ ไม่เก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ขององค์กรที่ท่านใช้งานอยู่

๓.๑๑ ไม่สร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร

๓.๑๒ รักษาความสะอาดโดยไม่กินอาหารและเครื่องดื่มบริเวณเครื่องคอมพิวเตอร์

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๑ ต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการ

๔.๒ ไม่อนุญาตให้บุคคลอื่นใช้ชื่อผู้ใช้งาน และรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๔.๓ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานต้อง Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver

๔.๔ ไม่อนุญาตให้ผู้ใช้งานทำการ แก้ไข เปลี่ยนแปลง หรือปรับค่าต่างๆที่กำหนดไว้ในเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ได้แก่ ค่าทางระบบเครือข่าย (Network configuration) หมายเลขประจำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงในระบบเครือข่าย (IP Address)

๕. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๕.๑ ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๕.๒ กรณีที่เครื่องคอมพิวเตอร์ไม่ Update ฐานข้อมูลไวรัสคอมพิวเตอร์ ผู้ใช้งานสามารถดำเนินการเองหรือแจ้งเจ้าหน้าที่สำนักวิทยาการสารสนเทศเพื่อดำเนินการ ทั้งนี้เพื่อป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๕.๓ ผู้ใช้งานต้องตรวจสอบหาไวรัสคอมพิวเตอร์จากสื่อบันทึกข้อมูลต่าง ๆ ได้แก่ Flash Drive และ Data Storage อื่น ๆ ด้วยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนใช้งาน

๕.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนใช้งาน

๕.๕ ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

๖.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลอื่น ๆ ได้แก่ CD DVD External Hard Disk หรือแจ้งผ่านโปรแกรมระบบงานแจ้งซ่อมภายในของสำนักวิทยาการสารสนเทศให้ทราบเพื่อดำเนินการตามเหตุการณ์

๖.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖.๓ ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ต้องไม่เป็นข้อมูลสำคัญที่เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็จะไม่กระทบต่อการดำเนินการขององค์กร

ส่วนที่ ๙

นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานทราบถึงข้อกำหนดและมาตรฐานการใช้งานเครื่องคอมพิวเตอร์แบบพกพา การนำไปปฏิบัติงานภายในและภายนอกองค์กร โดยผู้ใช้งานมีหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์แบบพกพา การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กรให้มีความลับ ความถูกต้อง มีประสิทธิภาพและมีความพร้อมใช้งานอยู่เสมอ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติทั่วไป

๓.๑ องค์กรต้องจัดให้มีเจ้าหน้าที่ผู้ดูแลรับผิดชอบและเป็นผู้ประสานงานจัดทำทะเบียนครุภัณฑ์เครื่องคอมพิวเตอร์แบบพกพารวมถึงการติดตามปรับปรุงและแก้ไขทะเบียนครุภัณฑ์อย่างต่อเนื่อง

๓.๒ คอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

๓.๓ เครื่องคอมพิวเตอร์แบบพกพาขององค์กรห้ามนำไปใช้นอกสถานที่เว้นแต่จะนำไปใช้งานในภารกิจขององค์กร โดยจะต้องได้รับอนุญาตจากผู้บังคับบัญชาภายในหน่วยงานที่ผู้ใช้งานสังกัด

๓.๔ ผู้ใช้งานต้องจัดวางเครื่องคอมพิวเตอร์แบบพกพาไว้ในสถานที่ปลอดภัย ห้ามจัดการแก้ไข เปลี่ยนแปลงชิ้นส่วนเครื่องคอมพิวเตอร์แบบพกพา เว้นแต่เป็นการดำเนินการเพื่อซ่อมแซมบำรุงรักษาโดยเจ้าหน้าที่ของสำนักวิทยาการสารสนเทศ

๓.๕ การส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของสำนักวิทยาการสารสนเทศเท่านั้นเว้นแต่จะได้รับอนุญาตจากเจ้าหน้าที่ของสำนักวิทยาการสารสนเทศเป็นรายไป

๓.๖ ผู้ใช้งานสามารถนำเครื่องคอมพิวเตอร์แบบพกพามาใช้ในองค์กรได้ แต่ต้องขออนุญาตผู้บังคับบัญชาที่สังกัด และถ้าประสงค์จะนำมาใช้เชื่อมต่อเข้ากับระบบเครือข่ายในองค์กรต้องขออนุญาต ผอ.สำนักวิทยาการสารสนเทศ

๓.๗ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓.๘ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน ได้แก่ การตกจากโต๊ะทำงานหรือหลุดมือ

๓.๙ ต้องไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่องหรืออาจถูกจับโยนได้

๓.๑๐ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๓.๑๑ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง ได้แก่ ปลายปากกากดสัมผัสหน้าจอให้เป็นรอยขีดข่วน หรือทำให้จอของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๓.๑๒ การเช็ดทำความสะอาดหน้าจอภาพเช็ดอย่างเบามือที่สุด และเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๓.๑๓ ต้องไม่เคลื่อนย้ายเครื่องในขณะ Hard disk กำลังทำงาน

๔. แนวปฏิบัติการป้องกันความปลอดภัยทางด้านกายภาพ

๔.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ได้แก่ ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๔.๒ ผู้ใช้งานต้องไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๔.๓ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อยที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการ

๕.๒ ไม่อนุญาตให้บุคคลอื่นใช้ชื่อผู้ใช้งาน และรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๕.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบพกพาขององค์กร

๕.๔ ไม่อนุญาตให้ผู้ใช้งานทำการ แก้ไข เปลี่ยนแปลง หรือปรับค่าต่าง ๆ ที่กำหนดไว้ในเครื่องคอมพิวเตอร์แบบพกพา ได้แก่ ค่าทางระบบเครือข่าย หมายเลขประจำเครื่องคอมพิวเตอร์แบบพกพาในระบบเครือข่าย (IP Address)

๖. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคาสั่งไม่พึงประสงค์ (Malware)

๖.๑ กรณีที่เครื่องคอมพิวเตอร์ไม่ Update ฐานข้อมูลไวรัสคอมพิวเตอร์ ผู้ใช้งานสามารถดำเนินการเองหรือแจ้งเจ้าหน้าที่สำนักวิทยาการสารสนเทศเพื่อดำเนินการ ทั้งนี้เพื่อป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๖.๒ ผู้ใช้งานต้องตรวจสอบหาไวรัสคอมพิวเตอร์จากสื่อบันทึกข้อมูลต่าง ๆ ได้แก่ Flash Drive และ Data Storage อื่น ๆ ด้วยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนใช้งาน

๖.๓ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนใช้งาน

๗. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

๗.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD DVD External Hard Disk หรือแจ้งเจ้าหน้าที่สำนักวิทยาการสารสนเทศเพื่อดำเนินการ

๗.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๓ ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ต้องไม่เป็นข้อมูลสำคัญที่เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

ส่วนที่ ๑๐

นโยบายการใช้งานระบบเครือข่ายอินเทอร์เน็ต

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต ผู้ใช้งานจะต้องทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ไม่ละเมิดสิทธิกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

๓.๑ ต้องลงทะเบียนบัญชีผู้ใช้งานเครือข่ายอินเทอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตขององค์กร โดยผู้ใช้งานภายในองค์กรยื่นคำขอกับเจ้าหน้าที่สำนักวิทยาการสารสนเทศขององค์กร สำหรับผู้ใช้งานภายนอกจะต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่ายหรือผู้ที่ได้รับมอบหมาย

๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์

๓.๓ ไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับองค์กร

๓.๔ ผู้ใช้งานเครือข่ายอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการและต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์แบบพกพา หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๓.๕ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๓.๖ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๓.๗ ในการใช้งานสื่อ Social Media ต่าง ๆ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงต่อบุคคลหรือองค์กร การทำลายความสัมพันธ์กับบุคลากรขององค์กรอื่น ๆ

๓.๘ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้งาน

๓.๙ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๓.๑๐ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๓.๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการอัพเดท Software ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๓.๑๒ เส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นโดยใช้โปรแกรมที่ไม่ผ่านระบบรักษาความปลอดภัยของสำนักงานศาลปกครอง

๓.๑๓ หลังจากใช้งานเครือข่ายอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บบราวเซอร์ที่ใช้งานและออกจากการใช้เครือข่ายอินเทอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๑

นโยบายการใช้งานระบบเครือข่ายไร้สาย WiFi

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานระบบเครือข่ายไร้สายขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานระบบเครือข่ายไร้สาย ผู้ใช้งานจะต้องทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานระบบเครือข่ายไร้สายอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ไม่ละเมิดสิทธิกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด จะทำให้การใช้งานระบบเครือข่ายไร้สายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติในการใช้งานระบบเครือข่ายไร้สาย

๓.๑ ต้องลงทะเบียนบัญชีผู้ใช้งานระบบเครือข่ายไร้สาย ทำการกรอกข้อมูลคำขอใช้บริการระบบเครือข่ายไร้สายขององค์กร โดยผู้ใช้งานภายในองค์กรยื่นคำขอกับเจ้าหน้าที่สำนักวิทยาการสารสนเทศขององค์กร สำหรับผู้ใช้งานภายนอกจะต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่ายหรือผู้ที่ได้รับมอบหมาย

๓.๒ กำหนดการใช้งานสำหรับเจ้าหน้าที่ภายในองค์กร จะควบคุมเป็นแบบ MAC Address (Media Access Control Address) ของอุปกรณ์ Smart Phone / Tablet / computer โดยการลงทะเบียนกับตัวอุปกรณ์

๓.๓ กำหนดการใช้งานสำหรับบุคคลผู้มาติดต่อที่องค์กร ได้แก่ ผู้สื่อข่าว ผู้มาอบรม ศึกษาดูงาน ประชาชนที่มาติดต่อ จะกำหนดการควบคุมเป็นแบบ User Authentication โดยไม่ต้องมีการลงทะเบียนกับตัวอุปกรณ์ สามารถใช้งานโดยกรอกใส่ username และ password ที่ผู้ดูแลระบบขององค์กรได้จัดเตรียมไว้ให้

๓.๔ กำหนดการติดตั้งจุด Access Point ติดครอบคลุมพื้นที่บริเวณที่มีเจ้าหน้าที่ปฏิบัติงานภายในอาคารขององค์กรในส่วนกลางและภูมิภาค และห่างจากบริเวณที่มีอุปกรณ์ที่ปล่อยคลื่นความถี่ที่มีสนามแม่เหล็กรบกวน ได้แก่ เตาไมโครเวฟ

๓.๕ SSID (Service Set Identifier) ต้องมีอย่างน้อย ๒ SSID แบ่งการใช้งานสำหรับเจ้าหน้าที่ในองค์กรและบุคคลภายนอก แยกจากกันให้ชัดเจน

๓.๖ ต้องมีการจัดเก็บ Log ข้อมูลการใช้ระบบเครือข่ายไร้สายตาม พ.ร.บ. คอมพิวเตอร์ฯ

๓.๗ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายและในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้บริหารสำนักวิทยาการสารสนเทศทราบทันที

๓.๘ ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๓.๙ ผู้ใช้งานต้องไม่นำอุปกรณ์เครือข่ายไร้สาย (Wireless) มาติดตั้งหรือเปิดใช้งานเองในองค์กร ไม่ว่าจะเป็น Access point หรือ Wireless Router หรืออื่นๆ

๓.๑๐ ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ - ส่ง สัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๓.๑๑ ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

๓.๑๒ ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีการคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

ส่วนที่ ๑๒

นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์

๑. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่าย อินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๓.๑ กำหนดให้มีการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องทำการกรอกข้อมูลคำขอใช้งานจดหมายอิเล็กทรอนิกส์ขององค์กร โดยผู้ใช้งานภายในองค์กรยื่นคำขอกับเจ้าหน้าที่สำนักวิทยาการสารสนเทศ

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

๓.๓ สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๓.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ได้แก่ เปลี่ยนรหัสผ่านทุก ๖ เดือน

๓.๕ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

๓.๖ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๓.๗ ผู้ใช้งานต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๓.๘ การส่งจดหมายอิเล็กทรอนิกส์จะต้องเป็นไปตามภารกิจของงานขององค์กรเท่านั้น ห้ามไม่ให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อการอื่น ได้แก่ การรับหรือส่งข้อมูลมีลักษณะเป็นจดหมายลูกโซ่ ประกาศ หรือแสดง

ความคิดเห็นในเรื่องที่เกี่ยวข้องกับการดำเนินการขององค์กรในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนจากความเป็นจริง และก่อให้เกิดความเสียหายกับบุคคลอื่นทั้งภายในและภายนอกองค์กร

๓.๙ ห้ามใช้จดหมายอิเล็กทรอนิกส์ เพื่อแสวงหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับองค์กร

๓.๑๐ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ พึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ

๓.๑๑ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์ ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๓.๑๒ ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กรที่ยังไม่ได้ประกาศอย่างเป็นทางการ

๓.๑๓ ผู้ใช้งานต้องไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๑๔ ไม่ส่งจดหมายอิเล็กทรอนิกส์ เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร ไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงต่อบุคคลหรือองค์กร การทำลายความสัมพันธ์กับบุคลากรขององค์กรอื่นๆ

๓.๑๕ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสคอมพิวเตอร์ เพื่อป้องกันภัยคุกคามข้อมูลคอมพิวเตอร์

๓.๑๖ ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๓.๑๗ หลังจากใช้งานจดหมายอิเล็กทรอนิกส์ เสร็จแล้วให้ออกจากระบบด้วยการ Logout เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๓.๑๘ กรณีมีการกำหนดบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ให้กับบุคคลภายนอกได้แก่ ประชาชนผู้มาติดต่อฟ้องคดีปกครองที่องค์กร เพื่อใช้ในการรับ-ส่งข้อมูลข่าวสารติดตามคดีของตนเองนั้น ผู้ดูแลระบบจะต้องทำการลงทะเบียนผู้ใช้งานเข้าเป็นกลุ่มเพิ่มขึ้นมาเพื่อสะดวกกับการบริหารจัดการบัญชีผู้ใช้งานของบุคคลภายนอก

ส่วนที่ ๑๓

นโยบายการป้องกันไวรัสคอมพิวเตอร์และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑. วัตถุประสงค์

เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กรจากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์ไม่ให้เข้ามาบุกรุกในเครื่องคอมพิวเตอร์และระบบเครือข่ายในองค์กร

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติในการป้องกันไวรัสคอมพิวเตอร์และซอฟต์แวร์ที่ไม่ประสงค์ดี

๓.๑ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชั่นการทำงานที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้นเพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่าย

๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ได้รับการอนุมัติจากสำนักวิทยาการสารสนเทศ และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

๓.๓ ห้ามผู้ใช้งานนำโปรแกรมป้องกันไวรัสคอมพิวเตอร์จากภายนอกมาใช้งานภายในองค์กร นอกจากโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ได้รับอนุญาตการใช้งานจากสำนักวิทยาการสารสนเทศ

๓.๔ ห้ามผู้ใช้งาน ลบ แก้ไข เปลี่ยนแปลง หรือตั้งค่า (configuration) ใด ๆ กับโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ในเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา โดยไม่ได้รับการอนุญาตจากผู้ดูแลระบบของสำนักวิทยาการสารสนเทศ

๓.๕ ผู้ใช้งานที่จำเป็นต้องนำซอฟต์แวร์จากภายนอกมาใช้งานภายในองค์กร ต้องทำการตรวจสอบซอฟแวร์โดยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนนำไปใช้งาน

๓.๖ ห้ามผู้ใช้งานทำการดาวน์โหลดซอฟต์แวร์หรือโปรแกรมใด ๆ โดยตรงจากอินเทอร์เน็ตโดยไม่ได้รับอนุญาตจากสำนักวิทยาการสารสนเทศ หลังจากการอนุญาตแล้วเจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนการใช้งาน

๓.๗ ห้ามผู้ใช้งานดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนา เผยแพร่ ไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของในองค์กร

๓.๘ ในกรณีที่มีการนำสื่อบันทึกข้อมูลส่วนตัวหรือจากหน่วยงานภายนอกองค์กรมาใช้ ผู้ใช้งานสื่อข้อมูลนั้นต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

ส่วนที่ ๑๔

นโยบายการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๑. วัตถุประสงค์

เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในขององค์กรให้มีความมั่นคงปลอดภัยจากการบุกรุกจากภัยคุกคามจากภายในและภายนอกที่แฝงตัวเข้ามากับการใช้งานข้อมูลสารสนเทศและอินเทอร์เน็ต

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติในการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๓.๑ อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งาน บริการเครือข่ายอื่น ๆ ที่เหลือให้ปิดหมด

๓.๒ ผู้ดูแลระบบมีการตรวจสอบนโยบาย (Policy) ที่กำหนดไว้บน Firewall เพื่อความมั่นคงปลอดภัยของระบบเครือข่าย รวมถึงตรวจสอบและติดตั้งโปรแกรมอุดชองโหว่สาหรับระบบปฏิบัติการของ Firewall อย่างสม่ำเสมอ รวมถึงปิดบริการซอฟต์แวร์ที่ไม่จำเป็นบน Firewall

๓.๓ ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท Network Scanning Tools

๓.๔ ปิดบริการรวมทั้งซอฟต์แวร์ที่ไม่จำเป็นบน Firewall

๓.๕ จำกัดชื่อผู้ใช้งานบนเครื่อง Firewall ให้มีน้อยที่สุด และไม่รัน Firewall โดยใช้ชื่อผู้ใช้งาน ที่เป็น Root หรือ Administrator

๓.๖ หมั่นตรวจสอบกฎของ Firewall เพื่อลบกฎที่ไม่มีความจำเป็นทิ้งไป เพื่อเพิ่มประสิทธิภาพของการประมวลผลกฎที่กำหนดไว้ของ Firewall

๓.๗ เมื่อเพิ่มกฎข้อใหม่เข้าไปใน Firewall ตรวจสอบว่ากฎที่ใส่เขาไปนั้นไม่ขัดแย้งกับกฎที่มีอยู่แต่เดิม รวมทั้งทดสอบด้วยว่า Firewall สามารถป้องกันได้จริงตามกฎข้อใหม่นั้น

๓.๘ ไม่อนุญาตให้เข้าถึง Firewall จากทางไกลโดยโปรแกรมประเภท Telnet หรือผ่าน VPN

๓.๙ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบการตรวจจับการบุกรุกการโจมตีระบบ ได้แก่ IPS (Intrusion Prevention Systems) WAF (Web App Firewall)

๓.๑๐ ต้องมีการใช้ระบบอื่นทำงานร่วมกับ Firewall ได้แก่ระบบป้องกันการบุกรุก (IPS) Firewall ส่วนตัว (Personal Firewall) อุปกรณ์กรองอีเมล์ (Mail security) อุปกรณ์กรองเว็บ (Web security) อุปกรณ์ตรวจจับการ

โจมตีจากมัลแวร์ (Antimalware) และโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมได้สูงขึ้น

๓.๑๑ ต้องมีระบบการบันทึก log เหตุการณ์พฤติกรรมการใช้งาน กิจกรรม ปริมาณข้อมูลเข้าใช้งานเครือข่าย โดยแยกในแต่ละเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ระบบเครือข่าย ซึ่งผู้ดูแลระบบมีการตรวจสอบอย่างสม่ำเสมอ

๓.๑๒ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ผู้ดูแลระบบจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๓.๑๓ ผู้ดูแลระบบจะยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ การโจมตีระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๓.๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบเทคโนโลยีสารสนเทศขององค์กรไม่ว่าจะเป็นการกระทำของหน่วยงานหรือบุคคลจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๓.๑๕ มีอุปกรณ์ตรวจสอบและป้องกันภัยคุกคามและการโจมตีแบบต่างๆ โดยอ้างอิงตาม OWASP Top ๑๐ ได้แก่ การโจมตีแบบ Injection แบบ Broken Authentication and Session Management แบบ Cross-Site Scripting แบบ Insecure Direct Object Reference แบบ Security Misconfiguration แบบ Sensitive Data Exposure แบบ Missing Function Level Access Control แบบ Cross-Site Request Forgery (CSRF) แบบ Using Components with known Vulnerabilities และแบบ Unvalidated Redirects and Forwards ได้

๓.๑๖ มีอุปกรณ์ป้องกันภัยคุกคามที่ไม่รู้จักมาก่อน (zero-day) ที่จะเข้ามาก่อให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของสำนักงาน หากตรวจพบจะมีการปิดกั้นไม่ให้ลุกลามสู่ระบบเครือข่ายภายในได้

๓.๑๗ มีอุปกรณ์ที่คอยตรวจสอบการทำงานของระบบเครือข่ายแต่ละโซน หากมีการใช้งานที่ผิดปกติสามารถแจ้งเตือนผู้ดูแลระบบให้สามารถแก้ไขปัญหาได้โดยเร็ว

ส่วนที่ ๑๕

นโยบายการใช้ระบบประชุมทางไกลผ่านจอภาพ

๑. วัตถุประสงค์

กำหนดมาตรการการใช้ระบบประชุมทางไกลผ่านจอภาพผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงการใช้บริการบนเครือข่าย ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานระบบประชุมทางไกลผ่านจอภาพผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. ผู้ใช้งาน

๓. แนวปฏิบัติในการใช้ระบบประชุมทางไกลผ่านจอภาพ

๓.๑ กำหนดให้สำนักวิทยาการสารสนเทศเป็นผู้ควบคุม ติดตั้ง และดำเนินการถ่ายทอดระบบประชุมทางไกลผ่านจอภาพ

๓.๒ กำหนดให้ผู้ใช้งานที่ประสงค์จะใช้ระบบประชุมทางไกลผ่านจอภาพ ต้องขอใช้ห้องประชุมให้เรียบร้อยก่อน แล้วตรวจสอบว่าระบบประชุมทางไกลผ่านจอภาพว่างพร้อมสำหรับใช้งานในวันที่ต้องการประชุมหรือไม่ ผ่านระบบการประชุมออนไลน์ในอินทราเน็ตสำนักงานศาลปกครอง กรณีต้องการใช้ระบบประชุมทางไกลผ่านจอภาพในวันและเวลาที่มีผู้อื่นขอใช้ก่อนแล้ว และอุปกรณ์ที่ใช้ถ่ายทอดไม่เพียงพอ ผู้ใช้งานต้องประสานงานผู้ที่ขอใช้ระบบประชุมทางไกลผ่านจอภาพก่อน ให้เปลี่ยนแปลงวันและเวลา พร้อมยืนยันการเปลี่ยนแปลงดังกล่าว โดยบันทึกผ่านระบบการประชุมออนไลน์ในอินทราเน็ตสำนักงานศาลปกครอง หรือจัดทำหนังสือยกเลิกการขอใช้บริการระบบประชุมทางไกลผ่านจอภาพแจ้งมายังสำนักวิทยาการสารสนเทศ

๓.๓ เมื่อตรวจสอบความพร้อมของระบบประชุมทางไกลผ่านจอภาพแล้ว ให้ผู้ใช้งานบันทึกรายละเอียดการขอใช้บริการระบบประชุมทางไกลผ่านจอภาพ ผ่านระบบการประชุมออนไลน์ในอินทราเน็ตสำนักงานศาลปกครอง ให้ครบถ้วน หรือจัดทำหนังสือขอใช้ระบบประชุมทางไกลผ่านจอภาพ โดยระบุห้องประชุม สถานที่ศาลปกครอง ส่งให้สำนักวิทยาการสารสนเทศ และสำนักวิทยาการสารสนเทศจะมอบหมายผู้ดูแลระบบ ติดตั้งและทดสอบเชื่อมโยงสัญญาณระบบประชุมทางไกลผ่านจอภาพ ไปสถานที่ปลายทางตามที่กำหนด ให้พร้อมใช้ก่อนการประชุมตลอดจนอยู่ควบคุมระบบ ตั้งแต่เริ่มประชุมจนเสร็จสิ้น

๓.๔ ผู้ดูแลระบบที่ปฏิบัติการถ่ายทอดระบบประชุมทางไกลผ่านจอภาพ ต้องรายงานสรุปผลการใช้งาน ปัญหาและการแก้ไข ให้ผู้บังคับบัญชาทราบทุกครั้ง

๓.๕ กรณีที่มีการขอใช้งานประชุมเรื่องความลับ ผู้ขอใช้บริการต้องเป็นผู้ควบคุมแจ้งเตือนในที่ประชุม มิให้มีการใช้โทรศัพท์มือถือ หรือนำอุปกรณ์สื่อบันทึกต่างๆ ที่ผู้เข้าร่วมประชุมนำติดตัวเข้ามาใช้ถ่ายภาพนิ่ง ภาพเคลื่อนไหว อัดเสียง

๓.๖ ผู้ดูแลระบบอุปกรณ์ประชุมทางไกลผ่านจอภาพ ต้องมีการตรวจสอบ ทดสอบ อุปกรณ์และจุดเชื่อมต่อเครือข่ายในห้องประชุมให้มีความพร้อมในการใช้งานอยู่เสมอ

๓.๗ ผู้ควบคุมการถ่ายทอดระบบประชุมทางไกลผ่านจอภาพต้องเปิดระบบรักษาความปลอดภัยในการถ่ายทอดสัญญาณทุกครั้ง เพื่อป้องกันข้อมูลที่ส่งผ่านในระบบเครือข่าย

๓.๘ ผู้ควบคุมการถ่ายทอดระบบประชุมทางไกลผ่านจอภาพต้องจัดการประชุมให้เป็นไปตามพระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓

ส่วนที่ ๑๖

นโยบายการสำรองและกู้คืนข้อมูล

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการในการสำรองข้อมูลระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่าย กรณีเกิดเหตุฉุกเฉินกับการใช้งานงานทางอิเล็กทรอนิกส์ สามารถใช้งานข้อมูล จากการกู้ข้อมูลกลับคืนมาได้โดยเร็วที่สุด

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติในการคัดเลือกการสำรองข้อมูล

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพ พร้อมใช้งานตามแนวทางต่อไปนี้

๓.๑ ต้องสำรองข้อมูลระบบงานที่มีความสำคัญได้แก่ระบบงานคดีปกครอง ระบบงานสารบรรณ เว็บไซต์สำนักงานศาลปกครอง ระบบอินทราเน็ต โปรแกรมระบบปฏิบัติการ ระบบงานสารสนเทศ และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

๓.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ ผู้ปฏิบัติงานโดยอย่างน้อยมีรายละเอียด ดังนี้

๓.๒.๑ ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง

๓.๒.๒ ประเภทสื่อบันทึกข้อมูล

๓.๒.๓ จำนวนข้อมูลที่ต้องสำรอง

๓.๒.๔ ขั้นตอนและวิธีการสำรองข้อมูลโดยละเอียด

๓.๒.๕ สถานที่จัดเก็บและวิธีการเก็บรักษาสื่อบันทึกข้อมูล

๓.๓ ต้องมีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๓.๔ ต้องมีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อย กำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๓.๔.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๓.๔.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง ได้แก่ การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๓.๕ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ

๓.๖ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูล Configuration ข้อมูลในฐานข้อมูล

๓.๗ จัดเก็บข้อมูลที่สำรองนั้นในสื่อบันทึกข้อมูล โดยมีการพิมพ์ชื่อบนสื่อบันทึกข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๓.๘ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับองค์กร

๓.๙ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๓.๑๐ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๓.๑๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๔. แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน ตามภารกิจตามแนวทางต่อไปนี้

๔.๑ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๔.๑.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๔.๑.๒ ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับระยะเวลานาน ไฟไหม้ แผ่นดินไหว ชุมนุมประท้วง

๔.๑.๓ กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๔.๑.๔ กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๔.๑.๕ กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๔.๑.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๔.๒ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔.๓ ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๔.๔ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔.๕ ต้องทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๕. แนวปฏิบัติในการสำรองและกู้คืนข้อมูลเครื่องคอมพิวเตอร์ส่วนบุคคล

เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ฮาร์ดดิสก์เสียหาย ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยผู้ใช้งานเอง โดยมีมาตรการ ดังนี้

๕.๑ การสำรองข้อมูล

๕.๑.๑ ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๕.๑.๒ ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๕.๑.๓ เมื่อองค์กรประกาศให้มีการสำรองข้อมูลเนื่องจากจะได้มีการดำเนินการที่อาจส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ผู้ใช้งานจะต้องทำการสำรองข้อมูลดังกล่าวภายในระยะเวลาที่กำหนด

๕.๑.๔ หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ออกมาเก็บสำรองไว้ในรูปของเอกสารอิเล็กทรอนิกส์

๕.๑.๕ ผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบบนระบบทดสอบ

๕.๑.๖ ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร และเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย

๕.๒ การกู้คืนข้อมูล

เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ หรือการประมวลผลของคอมพิวเตอร์หยุดทำงานอย่างกะทันหัน หรือเปลี่ยนการทำงานไปจากเดิม ทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลาหรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติ มีมาตรการในการกู้คืนข้อมูล ดังนี้

๕.๒.๑ ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

๕.๒.๒ ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย

๕.๒.๓ ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

ส่วนที่ ๑๗

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรได้มีการนำไปประกาศเผยแพร่ให้ทุกคนในองค์กรได้ทราบและนำไปใช้ปฏิบัติตามหน้าที่ความรับผิดชอบโดยมอบหมายให้ผู้ตรวจสอบภายในเป็นผู้ตรวจสอบและมีการรายงานความสำเร็จและความเสี่ยงที่ยังมีอยู่

๒. ผู้รับผิดชอบ

๑. สำนักวิทยาการสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

๓. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงขององค์กรเพื่อการตรวจสอบ และประเมินความเสี่ยงนั้นดังต่อไปนี้

๓.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต

๓.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๓.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดขัดข้องระหว่างการใช้งาน

๓.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่า ๑ จุด

๓.๑.๕ ความเสี่ยงที่เกิดขึ้นจากการลักลอบการใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๓.๑.๖ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๓.๒ กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๓.๓ การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๓.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๓.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๓.๓.๔ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงาน เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ ความเสียหายหรืออันตรายที่จะเกิดขึ้นของหน่วยงาน

ส่วนที่ ๑๘

นโยบายการกำหนดผู้รับผิดชอบ

๑. วัตถุประสงค์

การกำหนดผู้รับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

๒. ผู้รับผิดชอบ

๑. ผู้บริหารระดับสูง
๒. ผู้อำนวยการสำนักวิทยาการสารสนเทศ
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติระดับนโยบาย

๓.๑ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น

๓.๒ รองเลขาธิการ ที่กำกับสำนักวิทยาการสารสนเทศ ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ และผู้อำนวยการสำนักวิทยาการสารสนเทศ เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัย ด้านสารสนเทศ ติดตามและกำกับดูแลควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๓.๓ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (Ministry Chief Information Officer: MCIO) ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ การประสานงานและให้ความร่วมมือกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง MCIO ของหน่วยงานอื่นที่เกี่ยวข้องในการจัดทำโครงการเทคโนโลยีสารสนเทศเพื่อแลกเปลี่ยนข้อมูลร่วมกัน และให้คำปรึกษาด้านระบบเทคโนโลยีสารสนเทศ

๔. แนวปฏิบัติของระดับผู้บริหาร

๔.๑ ผู้อำนวยการสำนักวิทยาการสารสนเทศ รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางการแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยง และตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการรวมทั้งรับผิดชอบดังนี้

๔.๑.๑ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ตามปกติ

๔.๑.๒ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลและสารสนเทศ และระบบเครือข่ายขององค์กร

๔.๑.๓ กำกับดูแลเกี่ยวกับงานสารสนเทศ และงานต่าง ๆ ของสำนักวิทยาการสารสนเทศ

๔.๑.๔ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่าย ระบบฐานข้อมูลและสารสนเทศให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ

๕. แนวปฏิบัติระดับผู้ปฏิบัติ

๕.๑ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้อำนวยการสำนักวิทยาการสารสนเทศ ได้แก่ นักวิชาการคอมพิวเตอร์ นายช่างเทคนิคคอมพิวเตอร์ นายช่างคอมพิวเตอร์ มีหน้าที่ ดังนี้

๕.๑.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

๕.๑.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติและการรักษาความปลอดภัย

๕.๑.๓ รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๕.๑.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล ตามรอบระยะเวลาที่กำหนด

๕.๑.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบจากบุคคลภายนอก โดยไม่ได้รับอนุญาต

๕.๑.๖ รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต ระบบเครือข่ายไร้สาย

๕.๑.๗ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลปกครอง

คณะผู้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานศาลปกครอง

๑. นายประพัฒน์ ตันสุวรรณนนท์	เลขาธิการสำนักงานศาลปกครอง
๒. นายชำนาญ ทิพยชนวงศ์	รองเลขาธิการสำนักงานศาลปกครอง
๓. นายทศพล ทองเทือก	ผู้อำนวยการสำนักวิทยาการสารสนเทศ
๔. นายพงศธร นาคตระกูล	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ รักษาการในตำแหน่งผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่าย สำนักวิทยาการสารสนเทศ
๕. นายวัชรพล ราชโรจน์	นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักวิทยาการสารสนเทศ

นโยบายและแนวปฏิบัติใน

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานศาลปกครอง

จัดทำโดย สำนักวิทยาการสารสนเทศ สำนักงานศาลปกครอง

ประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับที่ ๒) ลงวันที่ ๑๗ กันยายน ๒๕๖๗

ประกาศสำนักงานศาลปกครอง

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับที่ ๒)

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๕ เพื่อให้มีความเหมาะสมยิ่งขึ้น

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ ของพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ สำนักงานศาลปกครอง โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกความในบทนิยามคำว่า “ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” ในข้อ ๒ ของประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๕ และให้ใช้ความต่อไปนี้แทน

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง” (Ministry Chief Information Officer : MCIO) หมายความว่า ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ การประสานงานและให้ความร่วมมือกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง MCIO ของหน่วยงานอื่นที่เกี่ยวข้องในการจัดทำโครงการเทคโนโลยีสารสนเทศ เพื่อแลกเปลี่ยนข้อมูลร่วมกัน และให้คำปรึกษาด้านระบบเทคโนโลยีสารสนเทศ”

ข้อ ๒ ให้ยกเลิกความในข้อ ๕ (๑) (ก) ของประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๕ และให้ใช้ความต่อไปนี้แทน

“(ก) กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (Ministry Chief Information Officer : MCIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลปกครอง”

/ข้อ ๓...

ข้อ ๓ ให้ยกเลิกความในข้อ ๙ ของประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๕ และให้ใช้ความต่อไปนี้แทน

"นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานศาลปกครอง (พ.ศ. ๒๕๖๗) (ICT Security Policy) ตามปรากฏในเอกสารแนบท้ายประกาศนี้ถือเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยและเป็นไปตามกฎระเบียบที่เกี่ยวข้อง ซึ่งผู้ใช้งานและบุคคลภายนอกที่ปฏิบัติงานให้กับศาลปกครองต้องถือปฏิบัติตามอย่างเคร่งครัด"

ข้อ ๔ ให้ยกเลิกเอกสารแนบท้ายประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๕ และให้ใช้เอกสารแนบท้ายประกาศนี้แทน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๗ กันยายน พ.ศ. ๒๕๖๗

(นายประพัฒน์ ตันสุวรรณนนท์)
เลขาธิการสำนักงานศาลปกครอง

ประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๒๕ ตุลาคม ๒๕๖๕

ประกาศสำนักงานศาลปกครอง
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โดยที่เป็นการสมควรปรับปรุงการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเพิ่มประสิทธิภาพเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงการตรวจสอบการปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าว

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ ของพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ สำนักงานศาลปกครองโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๒๗ กันยายน พ.ศ. ๒๕๕๙

ข้อ ๒ ในประกาศนี้

"องค์กร" หมายความว่า สำนักงานศาลปกครอง

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

"ผู้บริหารระดับสูงสุด" (Chief Executive Officer : CEO) หมายความว่า เลขาธิการสำนักงานศาลปกครอง

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" (Chief Information Officer : CIO) หมายความว่า ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ การประสานงานและให้ความร่วมมือกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO ของหน่วยงานอื่นที่เกี่ยวข้องในการจัดทำโครงการเทคโนโลยีสารสนเทศเพื่อแลกเปลี่ยนข้อมูลร่วมกัน และให้คำปรึกษาด้านระบบเทคโนโลยีสารสนเทศ

"ผู้อำนวยการสำนักวิทยาการสารสนเทศ" หมายความว่า ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศของสำนักวิทยาการสารสนเทศ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในการกำหนดนโยบายแนวปฏิบัติในการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

"ผู้ใช้งาน" หมายความว่า บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาทตามที่องค์กรกำหนด และให้หมายความรวมถึงผู้บริหาร ผู้ดูแลระบบ และเจ้าหน้าที่

/"ผู้บริหาร"...

"ผู้บริหาร" หมายความว่า เลขาธิการสำนักงานศาลปกครอง รองเลขาธิการสำนักงานศาลปกครอง ที่ปรึกษาสำนักงานศาลปกครอง ผู้อำนวยการสำนักงานศาล ผู้อำนวยการสำนัก ผู้อำนวยการวิทยาลัย หัวหน้ากลุ่มขึ้นตรงต่อเลขาธิการสำนักงานศาลปกครอง และผู้อำนวยการกลุ่ม

"ผู้ดูแลระบบ" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้อำนวยการสำนักวิทยาการสารสนเทศ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเทคโนโลยีสารสนเทศซึ่งสามารถเข้าถึงแอปพลิเคชัน เครือข่ายคอมพิวเตอร์ ฐานข้อมูลสารสนเทศ และการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

"เจ้าหน้าที่" หมายความว่า ข้าราชการศาลปกครอง พนักงานราชการ และลูกจ้างสำนักงานศาลปกครอง

"ระบบเทคโนโลยีสารสนเทศ" (Information Technology System) หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย แอปพลิเคชัน ข้อมูล และสารสนเทศ

ข้อ ๓ บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดในส่วนที่มีการกำหนดไว้แล้วในประกาศนี้ หรือซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๔ วัตถุประสงค์ของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีดังต่อไปนี้

(๑) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของสำนักงานศาลปกครอง ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

(๒) เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในสำนักงานศาลปกครองได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

(๓) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ผู้ใช้งานและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานศาลปกครอง ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของสำนักงานศาลปกครอง ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๕ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลปกครองให้เป็นไปตามเอกสารแนบท้ายประกาศนี้ ซึ่งต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) ส่วนที่ว่าด้วยการจัดทำนโยบาย

(ก) กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลปกครอง

(ข) กำหนดให้ผู้อำนวยการสำนักวิทยาการสารสนเทศเป็นผู้รับผิดชอบติดตามกำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะและคำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

/(ค) ผู้บริหาร...

(ค) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบายและกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(ง) จัดทำนโยบายเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางระบบอินทราเน็ตของสำนักงานศาลปกครอง

(จ) จัดให้มีการทบทวนและปรับปรุงอย่างน้อยปีละหนึ่งครั้ง

(๒) ส่วนที่ว่าด้วยรายละเอียดของแนวปฏิบัติ

(ก) การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับอนุญาตให้เข้าถึง กำหนดสิทธิ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิเท่านั้นที่สามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิการใช้งาน ตรวจสอบการละเมิดความปลอดภัย และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตเสมอ

(ค) การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิในการเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ตโดยผ่านระบบรักษาความปลอดภัยตามที่สำนักงานศาลปกครองจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

(ง) การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งานและจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์ และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

(จ) การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (WiFi) ระบบอินเตอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

/ข้อ ๖ จัดทำ...

ข้อ ๖ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์

(๓) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์ เพื่อให้สามารถดำเนินงานได้ตามปกติอย่างต่อเนื่องโดยต้องปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการงานตามภารกิจ

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ โดยอย่างน้อยปีละหนึ่งครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรอง ปีละหนึ่งครั้ง

ข้อ ๗ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละหนึ่งครั้ง โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๘ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ด้วยวิธีการดังต่อไปนี้

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์ของสำนักงานศาลปกครอง ให้กับผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(๒ จัดอบรมหรือจัดให้มีคู่มือที่ให้ความรู้ความเข้าใจแก่ผู้ใช้งานเกี่ยวกับเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๙ นโยบายและแนวปฏิบัติตามปรากฏในเอกสารแนบท้ายประกาศนี้ถือเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยและเป็นไปตามกฎระเบียบที่เกี่ยวข้อง ซึ่งผู้ใช้งานและบุคคลภายนอกที่ปฏิบัติงานให้กับศาลปกครองต้องถือปฏิบัติตามอย่างเคร่งครัด

ข้อ ๑๐ ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

/ข้อ ๑๑ ให้สำนัก...

ข้อ ๑๑ ให้สำนักวิทยาการสารสนเทศเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนแนวปฏิบัติตามประกาศนี้อย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๒ ผู้ใช้งานผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามประกาศนี้ ผู้บังคับบัญชาอาจพิจารณาดำเนินการตามกฎหมายและระเบียบที่เกี่ยวข้องต่อไป

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๕

(นางสมฤดี ธัญญสิริ)
เลขาธิการสำนักงานศาลปกครอง