เอกสารแนบท้ายประกาศ

นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) พ.ศ. ๒๕๖๓

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) หรือต่อไปนี้เรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ องค์กรจึงเห็นสมควรปรับปรุงนโยบายการรักษาความปลอดภัยด้านสารสนเทศและระบบเครือข่ายขององค์กรพร้อมรวบรวมจัดทำขึ้นใหม่ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศพร้อมการป้องกันภัยคุกคามต่าง ๆ เรียกประกาศฉบับนี้ว่า “นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) พุทธศักราช ๒๕๖๓” และ ให้ยกเลิกการบังคับใช้ “นโยบายการรักษาความปลอดภัยด้านสารสนเทศและระบบเครือข่าย สำนักงาน ป.ป.ส.” ฉบับเดิม

นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) พ.ศ. ๒๕๖๓ มีวัตถุประสงค์ ดังต่อไปนี้

๑. กำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือ เครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิ์ผล

๒. รองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๓. การกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

๔. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๕. กำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร หน่วยงานภาคเอกชน มูลนิธิ ที่มีที่ตั้งภายในองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๖. ศูนย์เทคโนโลยีสารสนเทศ ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายนี้ พร้อมปรับปรุงให้ทันสมัยและยืดหยุ่นต่อการทำงานของเจ้าหน้าที่สำนักงาน ป.ป.ส. และที่เกี่ยวข้อง ตามระยะเวลา ๑ ครั้งต่อปี

๗. ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ควบคุมดูแลให้นโยบายนี้ บังคับใช้ได้อย่างสมบูรณ์

สารบัญ

หมวดที่ ๓ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ระดับผู้ดูแลระบบ

หมวดที่ ๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ระดับผู้ใช้งานภายนอกและหน่วยงานภายนอก

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

“องค์กร” หมายถึง สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.)

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

“ผู้บริหารสูงสุดขององค์กร (Chief Executive Officer : CEO)” หมายถึง เลขาธิการคณะกรรมการป้องกันและปราบปรามยาเสพติด

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)” หมายถึง ตำแหน่งที่มีอำนาจหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารในองค์กร ซึ่งหมายรวมถึงการดูแลเกี่ยวกับมาตรฐาน กฎเกณฑ์ โครงสร้าง งบประมาณ กระบวนการให้ความรู้ บุคลากรของหน่วยงานสารสนเทศ โดย CIO เป็นผู้ให้คำแนะนำแก่ผู้บริหารสูงสุดขององค์กร (Chief Executive Officer : CEO) เกี่ยวกับการพัฒนาและนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ให้การบริหารองค์กรประสบความสำเร็จตามวิสัยทัศน์ และเป้าหมายรวมของหน่วยงานที่กำหนดไว้

“ศูนย์เทคโนโลยีสารสนเทศ” หมายถึง ศูนย์เทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ส. เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร

“ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ” หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“ผู้ใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท ซึ่งองค์กรกำหนด ได้แก่ บุคคล ดังนี้

- **“ผู้บริหาร”** หมายถึง เลขาธิการ ป.ป.ส. ที่ปรึกษาการป้องกันและปราบปรามยาเสพติด รองเลขาธิการ ป.ป.ส. ผู้อำนวยการกอง/สำนัก/ส่วนราชการที่ขึ้นตรง ผู้เชี่ยวชาญ ขององค์กร
- **“ที่ปรึกษา”** หมายถึง บุคคลที่องค์กรแต่งตั้งให้ปฏิบัติหน้าที่เป็นที่ปรึกษาองค์กรตามภารกิจที่ได้รับมอบหมาย
- **“เจ้าหน้าที่”** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานและลูกจ้างของกองทุนป้องกันและปราบปรามยาเสพติด และลูกจ้างเหมาเอกชน ในสังกัดสำนักงาน ป.ป.ส.

“ผู้ดูแลระบบ” หมายถึง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายให้ควบคุมดูแลบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

“ผู้ใช้งานภายนอก” หมายถึง บุคคลภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

“ผู้ประสานงาน” หมายถึง เจ้าหน้าที่องค์กร ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการสนับสนุนด้านการดูแลรักษาความปลอดภัย หรือด้านเทคนิคในการบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ร่วมกับผู้ดูแลระบบ (Administrator) ของศูนย์เทคโนโลยีสารสนเทศ

“เจ้าพนักงาน” หมายถึง บุคคลที่ได้รับการแต่งตั้งตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องแต่งตั้งพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

“มาตรฐาน (Standard)” หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

“วิธีการปฏิบัติ (Procedure)” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวปฏิบัติ (Guideline)” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

“การใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่องค์กรกำหนดไว้

“สิทธิ์ของผู้ใช้งาน” หมายถึง การเข้าใช้งาน การเข้าถึงระบบสารสนเทศ หรือการให้บริการข้อมูล ข้อสนเทศ รวมถึงการใช้อุปกรณ์ดิจิตอลส่วนประกอบ ตามชั้นความลับที่ได้รับอนุญาตจากเจ้าของระบบหรือเจ้าของข้อมูล

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

“หน่วยงานภายนอก” หมายถึง หน่วยงานภายนอกที่องค์กรอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ขององค์กร โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“ข้อมูล (Data)” หมายถึง ข้อเท็จจริงหรือสาระต่าง ๆ ที่เกี่ยวข้องกับงานที่ปฏิบัติ อาจเป็นตัวเลขหรือข้อความที่เกิดขึ้นจากการดำเนินงาน หรือที่ได้จากหน่วยงานอื่น ๆ ข้อมูลเหล่านี้ ยังไม่สามารถนำไปใช้ประโยชน์ในการตัดสินใจได้ทันที จะนำไปใช้ได้ก็ต่อเมื่อผ่านกระบวนการประมวลผลแล้ว

“สารสนเทศ (Information)” หมายถึง ข้อมูลที่ได้ผ่านกระบวนการประมวลผลแล้ว เช่น หาค่าเฉลี่ย เป็นต้น หรือใช้เทคนิคขั้นสูง เช่น การวิจัยดำเนินงาน เป็นต้น เปลี่ยนแปลงสภาพข้อมูลทั่วไปให้อยู่ในรูปแบบที่มีความสัมพันธ์ หรือมีความเกี่ยวข้องกัน เพื่อนำไปใช้ประโยชน์ในการตัดสินใจหรือตอบปัญหาต่าง ๆ ได้ สารสนเทศ ประกอบด้วยข้อมูล เอกสาร เสียง หรือรูปภาพต่าง ๆ แต่จัดเนื้อเรื่องให้อยู่ในรูปที่มีความหมาย สารสนเทศไม่ใช่จำกัดเฉพาะเพียงตัวเลขเพียงอย่างเดียวเท่านั้น

“ระบบสารสนเทศ” หมายถึง ระบบงานที่ใช้จัดเก็บและประมวลผลข้อมูลซึ่งทำงาน ประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผลให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสารได้

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร ได้แก่

- **“ระบบ LAN และระบบ Intranet”** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในองค์กรเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในองค์กร

- **“ระบบอินเทอร์เน็ต (Internet)”** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ขององค์กรเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานขององค์กรที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่องค์กรสามารถนำมาใช้ประโยชน์ ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง พื้นที่ที่องค์กรอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
- พื้นที่ทำงานของผู้ดูแลระบบ (Administrator Area)
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area /Data Center)
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
- พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“สินทรัพย์” หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับองค์กร ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน

“จดหมายอิเล็กทรอนิกส์ (e-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

“รหัสผ่าน (Password)” หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“ชุดคำสั่งไม่พึงประสงค์” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“เครือข่ายสังคมออนไลน์ (Social Network)” หมายถึง การใช้โปรแกรม หรือเว็บไซต์ที่มีผู้ให้บริการทั้งจากภายนอก หรือภายในองค์กร เพื่อใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารในการสื่อข้อมูลแบบออนไลน์ผ่านระบบอินเทอร์เน็ต

“สื่อสังคมออนไลน์ (Social Media)” หมายถึง สื่อที่เป็นเครื่องมือสื่อสารในการใช้งานแบบปฏิบัติ สัมพันธ์แบบออนไลน์ ตัวอย่างสื่อสังคมออนไลน์ เช่น Facebook, Hi๕, mySpace, LinkedIn, Ning, Bebo, Orkut, MSN, Twitter, YouTube, Pownce, Skype, PhpBB, Phorum, Flickr, Crowdstorm, Slideshare, Digg, Wikia, Doof, Friendfeed, CyWorld เป็นต้น โดยรวมถึงโปรแกรมและเว็บไซต์อื่น ๆ ที่มีการใช้งานในลักษณะเข้าข่ายหรือถูกจัดประเภทเป็นสื่อสังคมออนไลน์ (Social Network / Social Media Landscape)

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง มีการบริหารจัดการข้อมูลสารสนเทศในแบบ CIA คือ การรักษาความลับ (Confidentiality) ความถูกต้องแท้จริง (Integrity) และความสามารถพร้อมใช้งาน (Availability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ที่เกิดขึ้นและมีส่วนเกี่ยวข้องกับการรักษาความปลอดภัยสารสนเทศ เช่น การกู้ระบบกลับคืนเป็นปกติ การป้องกันการบุกรุกทำลายข้อมูล เป็นต้น

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด” หมายถึง เหตุการณ์ที่เกิดขึ้นโดยไม่ได้กำหนดให้เกิดขึ้น แล้วมีผลเสียต่อการให้บริการ หรือทำให้การบริการระบบสารสนเทศติดขัด/ขัดข้อง

“SSL” หมายถึง Secure Socket Layer คือ เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน เพื่อให้ข้อมูลปลอดภัยจากการเข้าถึงข้อมูลจากแฮกเกอร์ โดยวิธีการเรียกใช้งาน จะเรียกผ่านโปรโตคอล HTTPS หรือโปรโตคอลความปลอดภัยอื่น ๆ ตามแต่วิธีการใช้งาน

“VPN” หมายถึง Virtual Private Network คือ เป็นฟังก์ชั่นหนึ่งในระบบเน็ตเวิร์ค สร้างขึ้นมาทำให้สามารถรับส่งข้อมูลได้ปลอดภัยมากขึ้น และสามารถเชื่อมตรงกับเซิร์ฟเวอร์/อุปกรณ์ที่อยู่ใน VPN เดียวกันได้สะดวกขึ้น ซึ่งทำงานโดยใช้โครงสร้างของอินเทอร์เน็ตเป็นตัวส่งผ่านข้อมูล มีการเข้ารหัสข้อมูลทั้งหมด และจะมี Gateway เฉพาะในการส่งข้อมูล มีการ login ผู้ใช้/พาสเวิร์ดสำหรับบุคคลที่ได้รับอนุญาต และแต่ละอุปกรณ์ที่เชื่อมเข้ามาใน VPN จะมี IP เฉพาะ ทำให้สะดวกขึ้น เชื่อมต่อข้อมูลได้ง่ายมากขึ้น

“SLA” หมายถึง Service Level Agreement คือ ข้อตกลงในการให้บริการว่าจะทำการรักษาระดับคุณภาพการให้บริการแก่ผู้ใช้งาน ตามข้อตกลงที่ศูนย์เทคโนโลยีสารสนเทศให้ไว้กับผู้ใช้งาน

“OLA” หมายถึง Operational Level Agreement คือ ข้อตกลงในการให้บริการระหว่างหน่วยงานภายในศูนย์เทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อสามารถให้บริการผู้ใช้งานได้อย่างมีประสิทธิภาพ

หมวดที่ ๑
นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ
สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.)
พ.ศ. ๒๕๖๓

๑. การกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ต้องกำหนดตำแหน่งด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดความรับผิดชอบให้เหมาะสม พร้อมทั้งควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

๑.๓ ผู้บริหาร ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

๑.๔ ศูนย์เทคโนโลยีสารสนเทศ มีภารกิจ ดังนี้

๑.๔.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ร่วมกับกลุ่มงานตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

๑.๔.๒ จัดโครงสร้างองค์กรให้มีกลุ่มงาน หรือคณะทำงานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

๑.๔.๓ จัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นลายลักษณ์อักษร เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อ สารข้อมูล โดยนโยบายดังกล่าวจะต้องได้รับการอนุมัติจาก เลขาธิการ ป.ป.ส. เพื่อการนำไปใช้

๑.๔.๔ จัดให้มีการเผยแพร่เอกสารนโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ ให้กับผู้ใช้งาน และผู้ใช้งานภายนอกรับทราบ

๑.๔.๕ ติดตามประเมินผลการปฏิบัติตามแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

๑.๔.๖ ทบทวนและจัดทำแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และจัดหาระบบสารสนเทศสำรอง รวมทั้งสินทรัพย์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ขององค์กร ดังนี้

๑) พิจารณาคัดเลือกและจัดทำระบบสารสนเทศระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๒) จัดหาอุปกรณ์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๓) กำหนดหน้าที่ความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง

๔) จัดทำแผนต่าง ๆ ทดสอบสภาพความพร้อมใช้งานระบบสารสนเทศ ระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติต่อเนื่องและเหมาะสม สอดคล้องกับการใช้งานตามภารกิจ

๕) ฝึกซ้อมตามแผนต่าง ๆ ที่ได้กำหนดและทดสอบสภาพความพร้อมใช้งานระบบสารสนเทศ ระบบสำรอง ไว้อย่างน้อยปีละ ๑ ครั้ง

๑.๔.๗ สร้างการรับรู้ให้แก่ผู้ใช้งานระบบสารสนเทศขององค์กร ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การใช้งานระบบสารสนเทศขององค์กร

๒. การจัดการบุคลากร

๒.๑ สำนักงานเลขานุการกรมชี้แจงนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้แก่เจ้าหน้าที่ทราบ รวมถึงทัณฑ์ทางวินัยและโทษตามกฎหมายในการเปิดเผยความลับของทางราชการแก่บุคคลผู้ไม่มีหน้าที่เกี่ยวข้อง และการไม่ปฏิบัติตามนโยบายและแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้แก่เจ้าหน้าที่ขององค์กรทราบ

๒.๒ ศูนย์เทคโนโลยีสารสนเทศ ต้องจัดให้ลงนามในข้อตกลงกับเจ้าหน้าที่ทุกคน ลงในแบบฟอร์ม ITC๐๓๖ ว่าจะไม่เปิดเผย**ข้อมูลคอมพิวเตอร์ ข้อมูลและสารสนเทศขององค์กร** โดยการลงนามนี้จะมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า ๑ ปี ภายหลังจากที่สิ้นสุดอายุราชการหรือสิ้นสุดการว่าจ้างแล้ว

๒.๓ กรณีเกิดการเปลี่ยนแปลงสถานะของเจ้าหน้าที่ขององค์กร เพื่อให้การบริหารจัดการบัญชีผู้ใช้ เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด เจ้าหน้าที่ที่ดูแลทรัพยากรบุคคลส่วนกลาง ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศ ทราบทันทีเมื่อมีเหตุ ดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่
- การออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างปฏิบัติงานด้านยาเสพติด หรือการถึงแก่กรรม

๓. การจัดการสินทรัพย์

ให้ศูนย์เทคโนโลยีสารสนเทศ ดำเนินการ ดังนี้

๓.๑ ต้องจัดทำและเก็บทะเบียนสินทรัพย์ เพื่อเป็นข้อมูลสำหรับการนำไปวิเคราะห์และประเมินความเสี่ยง และบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

๓.๒ ต้องตรวจสอบสินทรัพย์ตามระยะเวลาที่กำหนด เช่น ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เป็นต้น

๓.๓ สินทรัพย์ในทะเบียนสินทรัพย์ต้องกำหนดผู้รับผิดชอบให้ชัดเจน

๓.๔ การอนุญาตให้ใช้สินทรัพย์ให้เป็นไปตามแนวปฏิบัติ ดังนี้

๑) แนวปฏิบัติการใช้งานเครือข่าย

๒) ข้อกำหนดการใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์

๓) แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๓.๕ การคืน เจ้าหน้าที่ที่เกษียณ สิ้นสุดการจ้างงาน หรือสิ้นสุดโครงการต้องคืนสินทรัพย์ที่รับผิดชอบทั้งหมดรวมทั้งกุญแจ บัตรประจำตัวของเจ้าหน้าที่ บัตรผ่านเข้าออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือและอุปกรณ์ต่าง ๆ

๔. การจัดการพื้นที่ด้านความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

๔.๑ กอง/สำนัก/กลุ่มขึ้นตรง ต้องแบ่งพื้นที่อย่างชัดเจน และกำหนดระดับการควบคุมเพื่อป้องกันการเข้าถึงสินทรัพย์ที่มีความสำคัญ

๔.๒ ต้องจัดทำแผนผังแสดงตำแหน่งและพื้นที่แต่ละชนิดและประกาศให้ผู้เกี่ยวข้องทราบ

๔.๓ ต้องดูแลรักษาสภาพแวดล้อมของพื้นที่ให้เป็นไปตาม **แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ หรือห้องปฏิบัติการเครื่องคอมพิวเตอร์ (Data Centre : DC)**

๔.๔ ต้องควบคุมให้เฉพาะผู้ที่มีสิทธิ์ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่

๔.๕ ต้องกำหนดสิทธิ์ และช่วงเวลาในการผ่านเข้าออกพื้นที่

๔.๖ ต้องบันทึกการผ่านเข้าออกในพื้นที่ที่สำคัญ

๔.๗ ต้องไม่เปิดประตูทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่องค์กรโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่องค์กรและพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๔.๘ ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับองค์กร ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออกของบุคคลเป็นจำนวนมาก เป็นต้น

๔.๙ เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงานเพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๔.๑๐ ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงานในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๔.๑๑ ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม โดยให้เป็นไปตาม**แนวปฏิบัติการทำลายสื่อบันทึกข้อมูล หรือการทำลายไฟล์ข้อมูลที่มีระดับลับขึ้นไป**

๔.๑๒ เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่ บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๔.๑๓ หากพบสิ่งผิดปรกติ หรือการละเมิดความมั่นคงปลอดภัย จะต้องแจ้งให้ผู้บังคับบัญชาทราบ

๔.๑๔ ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น “ห้ามเข้าก่อนได้รับอนุญาต”

๔.๑๕ ต้องแยกจุดที่รับส่งสิ่งของ ออกจากพื้นที่ที่มีอุปกรณ์ประมวลผลสารสนเทศ และดำเนินการ แกะหีบห่อหรือตรวจสอบให้เสร็จสิ้น ก่อนนำเข้าสู่พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

๕. การจัดการและการควบคุมการเข้าถึงระบบสารสนเทศ

๕.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

๕.๓ การบริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติ และกำหนดรหัสผ่านการได้ลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศและต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์ การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๔ การเข้าถึงข้อมูลตามระดับชั้นความลับ ต้องมีการจัดลำดับชั้นความลับ มีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการจำหน่ายหรือการนำอุปกรณ์กลับมาใช้ใหม่

๖. การจัดการและการควบคุมการเข้าถึงระบบเครือข่าย

๖.๑ กำหนดสิทธิ์และควบคุมการเข้าถึงระบบเครือข่าย ระบบสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูลให้แก่ผู้ใช้งาน ตลอดจนการเข้ารหัสและการจัดการกุญแจรหัสให้มีความถูกต้องและเป็นความลับ โดยต้องจัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อการเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๖.๒ กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงระบบเครือข่าย ระบบสารสนเทศและอุปกรณ์สารสนเทศ ตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ

๖.๓ กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้น การเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๖.๔ จากข้อ ๖.๑ และ ๖.๒ ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว เช่น ลาออก เกษียณ หรือพ้นจากตำแหน่ง เป็นต้น โดยต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศเป็นประจำทุก ๆ ๓ เดือน

๖.๕ ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๖ ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

๖.๗ ต้องระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๖.๘ ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและเครือข่าย

๖.๙ ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๖.๑๐ ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

๖.๑๑ ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

๖.๑๒ ไม่อนุญาตให้เชื่อมต่อระบบเครือข่ายองค์กรแบบไร้สาย เช่น Wireless LAN, Wi-Fi และการเชื่อมต่อระบบเครือข่ายไร้สายรูปแบบอื่น ๆ ที่เป็นการเชื่อมต่อระบบสารสนเทศขององค์กร

๖.๑๓ ให้บันทึก เฝ้าสังเกต ตรวจสอบการรายงานการเข้าถึงระบบเครือข่าย และกิจกรรมอื่นใดเพื่อความมั่นคงปลอดภัยระบบสารสนเทศ ทั้งระบบเครือข่ายคอมพิวเตอร์และระบบสื่อสารข้อมูลอื่น ๆ เป็นประจำทุกห้วงเวลา เช่น ทุก ๆ ๑ เดือน และ ๓ เดือน เป็นต้น

๗. การจัดการและการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๗.๑ ระบบเครือข่ายไร้สาย (WiFi) ที่เปิดให้บริการในนามขององค์กร จัดเป็นเครือข่ายภายนอกให้บริการสำหรับเข้าใช้งานอินเทอร์เน็ต โดยใช้ชื่อ SSID สำหรับเจ้าหน้าที่ขององค์กร คือ ONCB@OFFICER และสำหรับบุคคลทั่วไป หรือผู้มาติดต่อ คือ ONCB@Guest โดย ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้ควบคุมดูแลระบบ

๗.๒ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร ต้องผ่านระบบลงทะเบียน โดยใช้รหัสบัญชีผู้ใช้ ที่ออกโดยศูนย์เทคโนโลยีสารสนเทศ หรือส่วนยุทธศาสตร์และอำนวยการของกอง/สำนัก/กลุ่มขึ้นตรง

๗.๓ องค์กรอนุญาตให้นำอุปกรณ์เชื่อมต่อ WiFi เพื่อใช้งาน ดังนี้

๗.๓.๑ เครื่องคอมพิวเตอร์ หรืออุปกรณ์โมบาย ที่เป็นทรัพย์สินทางราชการ

๗.๓.๒ เครื่องคอมพิวเตอร์ หรืออุปกรณ์โมบาย ที่เป็นของส่วนตัว

๗.๔ องค์กรให้ความสำคัญกับเครื่องคอมพิวเตอร์ หรืออุปกรณ์โมบาย ที่เป็นทรัพย์สินทางราชการเป็นอันดับแรกในการให้บริการ

๘. การจัดการและการควบคุมการเข้าถึงระบบปฏิบัติการ

๘.๑ กำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ขององค์กร

๘.๒ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน และรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ขององค์กรร่วมกัน

๘.๓ ควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๘.๔ ควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๘.๕ ยุติการใช้งานระบบสารสนเทศ กรณีมีการว่างเว้นจากการใช้งานเกินกว่า ๓๐ นาที

๙. การจัดการและการควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ

๙.๑ การจำกัดการเข้าถึงสารสนเทศ

๙.๑.๑ ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบได้ กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน เป็นต้น

๙.๑.๒ ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ โดยใช้ชื่อผู้ใช้งาน และรหัสผ่าน

๙.๑.๓ การแยกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง ได้แก่

๑) การจัดทำบัญชีรายชื่อแยกประเภทโดยแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในองค์กร

๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กรต้องได้รับการแยกออกจากระบบงานอื่น ๆ ขององค์กร

๓) ระบบซึ่งไวต่อการรบกวน ต้องควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

๔) การเข้าถึงระบบสารสนเทศที่มีความสำคัญสูง อนุญาตให้ทำผ่านช่องทางที่กำหนดให้ ตามข้อ ๒ ของแนวปฏิบัตินี้

๙.๑.๔ บันทึกข้อมูลการใช้งานไว้เป็น Log File

๙.๒ การควบคุมอุปกรณ์สื่อสารประเภทพกพา และการปฏิบัติงานจากภายนอกองค์กร

๙.๒.๑ การป้องกันข้อมูลและสารสนเทศที่อยู่ในอุปกรณ์สื่อสารประเภทพกพา ผู้ใช้งานต้องมีวิธีป้องกันข้อมูลและสารสนเทศในอุปกรณ์สื่อสารประเภทพกพาเมื่อปฏิบัติงานนอกสถานที่ ได้แก่

๑) ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

๒) ต้องเข้ารหัสข้อมูลที่สำคัญไว้

๙.๒.๒ การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายขององค์กร ต้องพิสูจน์ตัวตนก่อนเข้าใช้งาน

๑) การแสดงตัวตน ด้วยชื่อผู้ใช้งาน

๒) การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่านแบบ ๒ Factor หรือ One time Password (OTP)

๓) การเข้าสู่ระบบสารสนเทศขององค์กร จะต้องตรวจสอบผู้ใช้งานอีกครั้ง

๔) การเข้าสู่ระบบจากระยะไกลต้องใช้การเข้ารหัสข้อมูล ได้แก่ SSL หรือ VPN และหรือกระบวนการเข้ารหัสวิธีอื่นที่เหมาะสม เพื่อเพิ่มความปลอดภัยของการรับส่งข้อมูล

๙.๒.๓ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่เปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว กำหนดการเชื่อมต่อเข้าสู่ระบบไม่เกิน ๑ ชั่วโมง

๙.๒.๔ การปฏิบัติงานนอกองค์กร ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด

๑๐. การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน

๑๐.๑ องค์กรที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการสำรองข้อมูล ตาม**<u>แนวปฏิบัติการสำรองและกู้คืนข้อมูล</u>**

๑๐.๒ ต้องสำรวจข้อมูล และจัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล

๑๐.๓ ข้อมูลที่มีความสำคัญสูงต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกองค์กร

๑๐.๔ ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

๑๐.๕ ต้องทดสอบข้อมูลที่สำรองอย่างสม่ำเสมอ

๑๐.๖ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๑๐.๗ หากต้องมีการกู้คืนข้อมูลให้ดำเนินการกู้คืนข้อมูลตาม **แนวปฏิบัติการสำรองและกู้คืนข้อมูล**

๑๑. การบริหารจัดการความมั่นคงปลอดภัยเพื่อสร้างความต่อเนื่องขององค์กร

๑๑.๑ ผู้ดูแลระบบต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) ตาม**แนวปฏิบัติการสำรองและกู้คืนข้อมูล**

๑๑.๒ ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ตาม**แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ**

๑๑.๓ ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ ๑ ครั้ง

๑๑.๔ อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

๑๒. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑๒.๑ จัดทำประกาศนโยบาย และแนวปฏิบัติ คู่มือการใช้งานสารสนเทศ พร้อมทั้งเผยแพร่ทางเว็บไซต์

๑๒.๒ ผู้ดูแลระบบต้องจัดให้มีหลักสูตรที่สอดคล้องกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ใช้ซึ่งไม่ได้รับอนุญาต

๑๒.๓ ต้องจัดประชุมหรือสัมมนา เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน

๑๒.๔ ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ใน ลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์

๑๒.๕ ห้ามผู้ใช้งานทำซ้ำ เผยแพร่ ข้อมูลที่เป็นการละเมิดลิขสิทธิ์ หรือซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กร

๑๒.๖ มีนโยบายปกป้องข้อมูลส่วนบุคคลและให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนภารกิจโดยไม่ตรวจดูจดหมายอิเล็กทรอนิกส์ที่รับส่งตามปกติ แต่มีภาระผูกพันตามกฎหมายที่ต้องติดตั้งระบบบันทึกข้อมูลจราจรและการเฝ้าระวังเพื่อคงไว้ซึ่งบริการที่มั่นคงปลอดภัยและมีประสิทธิภาพ สงวนสิทธิ์ในการใช้ระบบเฝ้าระวังเพื่อตรวจเนื้อหาจดหมายอิเล็กทรอนิกส์ที่เป็นภัยต่อระบบคอมพิวเตอร์ และกลั่นกรองหรือระงับการเผยแพร่นั้นโดยอัตโนมัติ ตลอดจนสงวนสิทธิ์การเข้าถึงจดหมายอิเล็กทรอนิกส์ เพื่อสืบสวน สอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้จดหมายอิเล็กทรอนิกส์ใด ๆ หรือการร้องขอจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๒.๗ มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลง และระเบียบข้อบังคับทั้งหมดที่เกี่ยวข้อง

หมวดที่ ๒
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ระดับผู้ใช้งาน

๑. แนวปฏิบัติหน้าที่โดยทั่วไป

๑.๑ เข้าร่วมการฝึกอบรม สัมมนา เกี่ยวกับนโยบายและแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร เพื่อให้เกิดความตระหนักและมีความรู้เท่าทันเหตุการณ์ที่จะทำให้เกิดภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศ โดยต้องผ่านการฝึกอบรม สัมมนา หลักสูตรนโยบายและแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่องค์กรได้จัดขึ้นอย่างน้อย ๑ หลักสูตร

๑.๒ ลงนามรับทราบในข้อนโยบายและแนวทางปฏิบัติในทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่องค์กรประกาศ

๑.๓ ให้ความร่วมมือในการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือข้อกำหนดอื่นใดที่เกี่ยวข้องตามที่องค์กรได้จัดทำขึ้น ตลอดจนให้ข้อเสนอแนะในการปรับปรุงให้มีประสิทธิภาพดีขึ้น

๑.๔ รักษาความลับและความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร จากผู้ไม่ได้รับอนุญาตหรือไม่มีหน้าที่รับผิดชอบโดยตรงตามกฎหมาย ไม่ว่าจะเป็นผู้บังคับบัญชา หรือผู้มีตำแหน่งสูงกว่าก็ตาม รวมถึงหน่วยงานภายนอกหรือบุคคลภายนอกที่ไม่มีส่วนเกี่ยวข้อง โดยอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๕ ดูแลรักษาป้องกันและใช้งานสินทรัพย์ขององค์กรอย่างถูกวิธี ทั้งสินทรัพย์ในครอบครองและสินทรัพย์ส่วนกลางตามมาตรการต่าง ๆ ที่กำหนดไว้ ตามแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒. แนวปฏิบัติการใช้งานเครือข่าย

๒.๑ สิทธิ์การใช้เครือข่าย

๒.๑.๑ สิทธิ์การใช้เครือข่ายเป็นสิทธิ์พิเศษเฉพาะ (Privilege) ที่องค์กรมอบให้บุคคลหรือหน่วยงานที่ได้รับสิทธิ์ไม่สามารถโอนสิทธิ์ให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

๒.๑.๒ ผู้ใช้งานต้องเคารพในสิทธิ์ส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้งานรายอื่น

๒.๑.๓ ผู้ใช้งานต้องใช้ระบบเครือข่ายคอมพิวเตอร์ตามมารยาทและจรรยาบรรณของการใช้เครือข่ายตามที่องค์กรกำหนดและตามวิถีสากล

๒.๒ การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

๒.๒.๑ การใช้ระบบเครือข่ายคอมพิวเตอร์เพื่อกระทำสิ่งที่ผิดกฎหมาย

๒.๒.๒ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

๒.๒.๓ การเข้าถึงข้อมูลของผู้อื่นเพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต

๒.๒.๔ การเผยแพร่ข้อมูลของผู้ใช้งาน หรือขององค์กรโดยไม่ได้รับอนุญาต

๒.๒.๕ การใช้งานที่เป็นสาเหตุให้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหายหรือมีผลต่อประสิทธิภาพการทำงานของระบบ

๒.๒.๖ การพยายามทำลายหรือทำลายระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

๒.๒.๗ การใช้หรือเผยแพร่ซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

๒.๒.๘ การลักลอบดักจับข้อมูลในระบบเครือข่ายคอมพิวเตอร์

๒.๒.๙ การปลอมแปลงเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิดให้แก่ระบบคอมพิวเตอร์และผู้ใช้งานอื่น

๒.๒.๑๐ การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์หรือเครือข่ายอื่น

๒.๒.๑๑ การเผยแพร่ และหรือการเข้าถึงสื่อลามกอนาจาร

๒.๒.๑๒ การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อเปิดให้บริการใด ๆ โดยไม่ได้รับอนุญาต

๒.๒.๑๓ การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจ

๒.๒.๑๔ การนำไอพีแอดเดรสขององค์กรไปจดทะเบียนชื่อโดเมนอื่นนอกเหนือจากชื่อโดเมน oncb.go.th โดยไม่ได้รับอนุญาต

๒.๒.๑๕ การใช้ระบบเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบายและระเบียบขององค์กร

๒.๓ การฝ่าฝืนระเบียบและการพิจารณาโทษ

๒.๓.๑ องค์กรจะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้นจากผู้ใช้งาน และหรือบัญชีผู้ใช้งาน

๒.๓.๒ ผู้ใช้งานที่ฝ่าฝืนระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์จะถูกพิจารณาระงับและหรือยกเลิกบัญชีผู้ใช้

๒.๓.๓ ศูนย์เทคโนโลยีสารสนเทศจะแจ้งหน่วยงานต้นสังกัดเพื่อพิจารณาโทษแก่ผู้ใช้งานที่ฝ่าฝืนระเบียบ

๓. แนวปฏิบัติการเข้าถึงระบบเครือข่ายไร้สาย

๓.๑ ผู้ใช้งานทำการลงทะเบียนรหัสประจำตัวผู้ใช้งานกับผู้ดูแลระบบของศูนย์เทคโนโลยีสารสนเทศ

๓.๒ ผู้ใช้งานยินยอมเปิดเผยข้อมูลส่วนบุคคล เพื่อใช้สำหรับลงทะเบียน

๓.๓ ผู้ใช้งานทำการติดตั้ง Certificate สำหรับการใช้งานบนเครื่องคอมพิวเตอร์พกพา

๓.๔ ผู้ใช้งานไม่เปิดเผยรหัสลับที่เกี่ยวข้องในการใช้งานให้ผู้อื่นรู้

๓.๕ ผู้ใช้งานไม่กระทำการสิ่งใด ๆ อันเป็น การรุกล้ำ อุปกรณ์ คอมพิวเตอร์ หรือข้อมูลทางคอมพิวเตอร์ของผู้อื่น หรือกระทำการที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๓.๖ ผู้ใช้งานต้องใช้งานอย่างระมัดระวังตาม <u>แนวปฏิบัติการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์ (Use of the Internet & Social Network)</u>

๔. แนวปฏิบัติการเข้าถึงระบบปฏิบัติการ

๔.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศ

๔.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงาน หรือด้านเทคนิค

๔.๓ สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น สมาร์การ์ด RFID เครื่องอ่านลายนิ้วมือ เป็นต้น

๕. แนวปฏิบัติการใช้งานบัญชีผู้ใช้บริการ (Account / Username)

๕.๑ ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศขององค์กร การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน

๕.๒ ผู้ใช้งานต้องกรอกแบบฟอร์มการขอสิทธิ์การเข้าใช้งานระบบสารสนเทศ โดยกรอกรายละเอียดคำขอตาม E-Form ในระบบสนับสนุนงานให้บริการสารสนเทศ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดสิทธิ์การใช้งานหรือบัญชีผู้ใช้งาน (Account) ได้แก่ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

๕.๓ การใช้งานรหัสผ่านผู้ใช้งานต้องปฏิบัติดังนี้

๕.๓.๑ รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย

๕.๓.๒ รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก โดยเลือกรหัสผ่านที่ปลอดภัยและเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ (ทุก ๙๐ วัน หรือเมื่อระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน)

๕.๓.๓ ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตนทั้งหมด เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ

๕.๓.๔ ไม่ลักลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้ใช้งานอื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

๕.๓.๕ หากมีการล่วงละเมิดความปลอดภัยในระบบให้รายงานผู้ดูแลระบบทราบในทันที

๖. แนวปฏิบัติการกำหนดรหัสผ่าน (Password) การเปลี่ยนรหัสผ่าน และการใช้งานรหัสผ่าน

๖.๑ การกำหนดรหัสผ่านต้องประกอบไปด้วยอักษร ภาษาอังกฤษตัวพิมพ์เล็ก และพิมพ์ใหญ่อย่างน้อย อย่างละ ๑ ตัวอักษร อักขระพิเศษ เช่น ! # $ % ^ & เป็นต้น อย่างน้อย ๑ ตัวอักษร ตัวเลขอย่างน้อย ๑ ตัว และมีความยาวของรหัสผ่านไม่น้อยกว่า ๘ ตัวอักษร

๖.๒ รหัสผ่านห้ามซ้ำกันจากรหัสผ่านเดิมที่เคยใช้ ๒ รหัสผ่านล่าสุด

๖.๓ ผู้ใช้งานใส่รหัสผ่านผิดเกิน ๕ ครั้ง ระบบจะต้องทำการยึดชื่อผู้ใช้ (Lock Username) ไม่ให้ทำการล็อกอิน (Log in) จนกว่าจะครบ ๑๕ นาที หรือ ติดต่อผู้ดูแลระบบ เพื่อปลดล็อก

๖.๔ กรณีมีการแจ้งเตือนให้เปลี่ยนรหัสผ่านล่วงหน้าอย่างน้อย ๑ สัปดาห์ ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ทันที

๖.๕ ผู้ใช้งานต้องลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ และไม่เปิดเผยให้ผู้อื่นทราบ

๖.๖ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๗. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๗.๑ แนวทางปฏิบัติการใช้งานทั่วไป

๗.๑.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลที่องค์กรอนุญาตให้ผู้ใช้งานใช้งานเป็นสินทรัพย์ขององค์กร ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลอย่างมีประสิทธิภาพเพื่องานขององค์กร

๗.๑.๒ โปรแกรมที่ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร ต้องเป็นไปตามมาตรฐานที่ศูนย์เทคโนโลยีสารสนเทศกำหนด และไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร ยกเว้นการปรับปรุงเพื่อแก้ไขปัญหาช่องโหว่ของโปรแกรมระบบปฏิบัติการ

๗.๑.๓ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัส ด้วยโปรแกรมป้องกันไวรัสที่ศูนย์เทคโนโลยีสารสนเทศติดตั้งให้ใช้งาน

๗.๑.๔ ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๗.๑.๕ ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร

๗.๑.๖ ไม่ควรจัดเก็บข้อมูลบน Desktop แบบถาวร เพราะจะมีผลทำให้ประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ช้าลง

๗.๑.๗ ผู้ใช้งานมีหน้าที่ตรวจสอบค้นหาพร้อมลบไฟล์ขยะทิ้ง เช่น Temp, Cookie เป็นต้น

๗.๑.๘ ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล ควรปฏิบัติ ดังนี้

๑) ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๒) ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์

๗.๑.๙ ผู้ใช้งานต้องใช้รหัสผู้ใช้งาน และรหัสผ่านของตนเองในการเข้าใช้เครื่องคอมพิวเตอร์ส่วนบุคคลผ่านการควบคุมแบบ Domain ตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนด

๗.๑.๑๐ ผู้ใช้งานควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที เพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๗.๑.๑๑ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานควร Logout ออกจากเครื่องคอมพิวเตอร์ส่วนบุคคล หรือล็อกหน้าจอด้วยโปรแกรม Screen Saver

๗.๒ แนวทางปฏิบัติการนำเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเองหรือของบริษัทเอกชนเชื่อมต่อกับระบบเครือข่ายขององค์กร

๗.๒.๑ ผู้ใช้งานหรือเจ้าของเครื่องคอมพิวเตอร์ส่วนบุคคลต้องได้รับอนุญาตจาก ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เท่านั้น

๗.๒.๒ ผู้ใช้งานหรือเจ้าของเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องแจ้งวัตถุประสงค์การใช้งานและลงทะเบียนเครื่องคอมพิวเตอร์ส่วนบุคคล พร้อมระบุวันเวลาในเริ่มต้นใช้งานและวันเวลาสิ้นสุดการใช้งานกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ หรือผู้ประสานงาน

๘. แนวปฏิบัติการนำอุปกรณ์โมบายส่วนบุคคล (Mobile-BYOD) มาใช้งานและเข้าถึงข้อมูลที่มีชั้นความลับขององค์กร

การใช้ข้อมูลที่มีชั้นความลับ ๓ ระดับ คือ ข้อมูลลับ ข้อมูลลับมาก ข้อมูลลับที่สุด ต้องจัดให้มีการควบคุมดูแล ดังนี้

๘.๑ ผู้ใช้งานต้องไม่ดาวน์โหลดข้อมูลชั้นความลับไปเก็บไว้บนเครื่องตัวเอง

๘.๒ การเข้าใช้งานระบบสารสนเทศต้องมีกระบวนการเข้ารหัสการสื่อสารข้อมูลอย่างเหมาะสม

๘.๓ องค์กรสงวนสิทธิ์ในการควบคุมอุปกรณ์โมบายส่วนบุคคล (Mobile-BYOD) นั้น ๆ ในการติดตั้งโปรแกรมเครื่องมือ ผู้ใช้งานต้องยินยอมส่งมอบตัวเครื่องให้องค์กรยึมเป็นหลักฐานทางกฎหมาย หรือตรวจสอบหาหลักฐาน พร้อมสามารถทำการ Recovery หรือ Remote ลบข้อมูลสำคัญ ได้ตลอดเวลาตามที่ร้องขอจากองค์กร

๘.๔ เมื่อผู้ใช้งานพบว่า อุปกรณ์โมบายส่วนบุคคลนั้นสูญหาย ให้รีบดำเนินการแจ้งศูนย์เทคโนโลยีสารสนเทศโดยเร็ว และให้ Remote ลบล้างข้อมูล หรือค่าพารามิเตอร์ (Parameter)

๙. แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๙.๑ หลีกเลี่ยงเว็บไซต์ที่ให้ข้อมูลละเมิดลิขสิทธิ์

๙.๒ อย่าเปิดไฟล์แนบในอีเมลจากบุคคลหรือบริษัทที่ไม่รู้จัก

๙.๓ อย่าคลิกลิงค์ในอีเมลที่ไม่พึงประสงค์ วางเมาส์ไว้เหนือลิงค์ดูก่อนเสมอ (โดยเฉพาะอย่างยิ่งลิงค์ที่มี URL Shortener) ดูก่อนคลิกลิงค์เชื่อมโยง

๙.๔ หากจำเป็นต้องดาวน์โหลดไฟล์จากอินเทอร์เน็ต อีเมล FTP Site หรือบริการแชร์ไฟล์ต่าง ๆ ให้สแกนไฟล์ก่อนเรียกใช้งาน

๑๐. แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

จดหมายอิเล็กทรอนิกส์ (e-mail) เป็นบริการที่องค์กรจัดให้มีเพิ่มสนับสนุนการบริหารจัดการตามภารกิจขององค์กร ผู้ใช้จดหมายอิเล็กทรอนิกส์ขององค์กรภายใต้ชื่อโดเมน (Domain) ที่จดทะเบียนโดยองค์กร มีหน้าที่พึงปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ โดยไม่ขัดกับนโยบายการใช้คอมพิวเตอร์ขององค์กร

๑๐.๑ ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

๑๐.๑.๑ ผู้ใช้งานมีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ ผู้ใช้งานต้องรักษารหัสผ่านเป็นความลับเฉพาะตัวและไม่อนุญาตให้ผู้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี ผู้ใช้งานเป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์ และการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเอง

๑๐.๑.๒ ผู้ใช้งานพึงทราบว่าไม่มีสิทธิ์ที่จะถามหรือร้องขอให้ผู้ใช้งานเปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

๑๐.๑.๓ ผู้ใช้งานต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

๑๐.๑.๔ การใช้จดหมายอิเล็กทรอนิกส์ ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

๑) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น

๒) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่จดหมายลูกโซ่

๓) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลชั้นความลับขององค์กร

๔) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลการประชุมของที่ประชุมผู้บริหารองค์กรหรือในการประชุมอื่น ๆ โดยที่มิได้มีหน้าที่ หรือมิได้รับมอบหมายจากประธานในที่ประชุม

๕) การปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้น ๆ ส่งมาจากบุคคลอื่น

๖) การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

๗) การปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง เป็นต้น

๘) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล

๙) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่ดูหมิ่น เหยียดหยาม หรือแบ่งแยกทาง ศาสนา เชื้อชาติ หรือเพศ

๑๐) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่มีลักษณะหยาบคาย หรือลามกอนาจาร

๑๑) การส่งจดหมายอิเล็กทรอนิกส์ เพื่อเผยแพร่โปรแกรมหรืองาน หรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองาน ในลักษณะที่ละเมิดลิขสิทธิ์

๑๒) การส่งจดหมายอิเล็กทรอนิกส์ กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

๑๓) การส่งจดหมายอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบให้ระบบจดหมายอิเล็กทรอนิกส์ หรือเครือข่ายลดทอนประสิทธิภาพลง

๑๔) การส่งจดหมายอิเล็กทรอนิกส์ กระจายไวรัส หรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

๑๐.๒ โควต้าบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีจดหมายอิเล็กทรอนิกส์ ของผู้ใช้งานแต่ละรายจะมีโควต้ากำหนดการใช้งานดังนี้

๑๐.๒.๑ ขนาดข้อมูลรวมที่เก็บในเซิร์ฟเวอร์

๑๐.๒.๒ ขนาดของไฟล์แนบต่อการส่งจดหมายอิเล็กทรอนิกส์หนึ่งฉบับ

๑๐.๒.๓ จำนวนบัญชีผู้รับต่อการส่งจดหมายอิเล็กทรอนิกส์หนึ่งฉบับ

๑๐.๒.๔ อัตราส่งจดหมายอิเล็กทรอนิกส์ต่อวันเวลาที่กำหนด

๑๐.๒.๕ จำนวนจดหมายอิเล็กทรอนิกส์ต่อวันเวลาที่กำหนด

๑๐.๒.๖ โควต้าเหล่านี้อาจแตกต่างกันตามประเภทและภารกิจของผู้ใช้งาน การกำหนดโควต้าให้อยู่ในดุลยพินิจของศูนย์เทคโนโลยีสารสนเทศ โดยสามารถเพิ่มหรือลดค่าแต่ละบัญชีจดหมายอิเล็กทรอนิกส์ตามความเหมาะสมเพื่อให้การใช้งาน และการบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ

๑๐.๓ การตรวจระวังระบบ องค์กรมีนโยบายปกป้องข้อมูลส่วนบุคคลและให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนภารกิจขององค์กร โดยไม่ตรวจดูจดหมายอิเล็กทรอนิกส์ที่รับส่งตามปกติ แต่องค์กรมีภาระผูกพันตามกฎหมายที่ต้องติดตั้งระบบบันทึกข้อมูลจราจรทางคอมพิวเตอร์ และการเฝ้าระวังเพื่อคงไว้ซึ่งบริการที่มั่นคงปลอดภัยและมีประสิทธิภาพ องค์กรสงวนสิทธิ์ในการใช้ระบบเฝ้าระวังเพื่อตรวจเนื้อหาจดหมายอิเล็กทรอนิกส์ ที่เป็นภัยต่อระบบคอมพิวเตอร์และกลั่นกรอง หรือระงับการเผยแพร่นั้นโดยอัตโนมัติ ตลอดจนสงวนสิทธิ์ การเข้าถึงจดหมายอิเล็กทรอนิกส์เพื่อสืบสวน สอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้จดหมายอิเล็กทรอนิกส์ใด ๆ หรือการร้องขอจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๐.๔ การระงับบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิ์พิเศษเฉพาะ (Privilege) ที่องค์กรเอื้ออำนวยให้ผู้ใช้งาน ซึ่งผู้ใช้งานไม่สามารถโอนสิทธิ์ให้แก่ผู้อื่นใช้ได้ องค์กรคงไว้ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิ์ให้แก่ผู้ใช้งาน โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหา ความมั่นคงปลอดภัยหรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์ มีแนวปฏิบัติ ดังนี้

๑๐.๔.๑ เมื่อผู้ใช้งานพ้นสภาพการอยู่ในสังกัดขององค์กร ศูนย์เทคโนโลยีสารสนเทศสามารถระงับบัญชีผู้ใช้งาน ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย

๑๐.๔.๒ ผู้ใช้งานสามารถร้องขอการขยายสิทธิ์การใช้บัญชีผู้ใช้งานเพื่อคงสิทธิ์การใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้ เมื่อต้องพ้นสภาพการอยู่ในสังกัดขององค์กร โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัด

พร้อมแนบเหตุผลความจำเป็นส่งถึงศูนย์เทคโนโลยีสารสนเทศ การอนุญาตและระยะเวลาการขยายสิทธิ์ให้เป็นอำนาจของผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ผู้บริหารมอบหมาย

๑๐.๔.๓ บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้งาน สามารถถูกระงับการใช้งาน โดยคำร้องขอจากผู้อำนวยการกอง/สำนัก/กลุ่มขึ้นตรง หากพบว่ามีการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้

๑๐.๔.๔ บัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ของผู้ใช้งาน สามารถถูกระงับการใช้งานโดยทันที โดยหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบให้ประสิทธิภาพระบบเครือข่ายด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้งาน หรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศ มีสิทธิ์ระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

๑๑. แนวปฏิบัติการจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๑๑.๑ ห้ามผู้ใช้งานลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ขององค์กร หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้บริหาร

๑๑.๒ ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๑๑.๓ ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสขององค์กร ก่อนเปิดใช้งานเสมอ

๑๑.๔ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ขององค์กร

๑๒. แนวปฏิบัติการเคลื่อนย้ายและการทำสำเนาสารสนเทศ

๑๒.๑ ห้ามมิให้คัดลอกหรือทำสำเนาเอกสาร ข้อมูลคอมพิวเตอร์ ข้อมูลและสารสนเทศที่มีระดับลับขึ้นไปในระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑๒.๒ ห้ามมิให้ส่งข้อมูลและสารสนเทศของระบบสารสนเทศขององค์กรออกไปนอกเครือข่ายขององค์กร หรือนำสำเนาสารสนเทศระดับลับขึ้นไปในระบบสารสนเทศขององค์กรออกนอกพื้นที่รักษาการณ์โดยไม่ได้รับอนุญาต ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑๒.๓ การทำสำเนาข้อมูลและการส่งข้อมูลของระบบสารสนเทศที่มีระดับลับตามข้อ ๑๒.๑ ขององค์กรออกไปนอกเครือข่ายหรือนอกระบบสารสนเทศขององค์กร ผู้ร้องขอหรือผู้ที่ต้องการใช้สำเนาหรือส่งข้อมูลดังกล่าวเพื่อใช้ในราชการ จะต้องขออนุญาตจากผู้บริหารระดับสูง และให้ผู้ที่ได้รับอนุญาตจากหัวหน้าส่วนราชการในการเข้าถึงเอกสารลับเป็นผู้ทำสำเนาออกจากระบบสารสนเทศขององค์กร โดยส่งสำเนาดังกล่าวให้กับผู้ร้องขอด้วยแผ่น CD/DVD หรือ e-mail ขององค์กรเท่านั้น และห้ามมิให้คัดลอกหรือทำสำเนาส่งต่อให้ผู้ที่มิได้รับอนุญาต

๑๒.๔ การใช้งานการสื่อสารข้อมูลในระบบอีเมลหรือจดหมายอิเล็กทรอนิกส์ ให้ปฏิบัติตาม **<u>แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)</u>**

๑๓. แนวปฏิบัติการทำลายสื่อบันทึกข้อมูล หรือการทำลายไฟล์ข้อมูลที่มีระดับลับขึ้นไป

๑๓.๑ เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูล

๑๓.๒ กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้

(หรือใช้มาตรฐาน DoD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา)

ประเภทสื่อ	วิธีการทำลาย และนำกลับมาใช้ใหม่	วิธีทำลาย	ระยะเวลาทำลาย
กระดาษ		หั่นย่อยด้วยเครื่องทำลายเอกสาร	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
Flash Drive	Format	- ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
CD/DVD Rom	Format	ใช้การหั่น ตัด เผา ให้สิ้นสภาพการใช้งาน	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
Hard Disk	Format	- ทำลายข้อมูลบน Hard Drive ตามมาตรฐาน DoD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
ม้วนเทป บันทึกข้อมูล	Format	ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลาย	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด

๑๔. แนวปฏิบัติการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์ (Use of the Internet & Social Network)

๑๔.๑ การใช้งานอินเทอร์เน็ต มีดังนี้

๑๔.๑.๑ ผู้ใช้งานยื่นคำขอใช้เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

๑๔.๑.๒ ผู้ใช้งานต้องได้รับการอนุญาตจากผู้บังคับบัญชา และต้องลงทะเบียนกับผู้ดูแลระบบแล้วเท่านั้น ผู้ใช้งานต้องใช้รหัสผู้ใช้งาน และรหัสผ่านของตนเอง ตามที่กำหนดโดยศูนย์เทคโนโลยีสารสนเทศเท่านั้น ในการ Log on เพื่อเข้าถึงอินเทอร์เน็ตโดยต้องมีการทบทวนสิทธิ์การเข้าถึงอินเทอร์เน็ตอย่างสม่ำเสมอ

๑๔.๑.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

๑๔.๑.๔ ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

๑๔.๑.๕ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ลามก อนาจาร เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๑๔.๑.๖ ผู้ใช้งานต้องไม่เผยแพร่ หรือจัดเก็บข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่มีลักษณะลามก อนาจาร หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๑๔.๑.๗ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๑๔.๑.๘ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๑๔.๑.๙ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๔.๑.๑๐ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๔.๑.๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากเจ้าของผลิตภัณฑ์หรือผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๑๔.๑.๑๒ การใช้งานเว็บบอร์ด (Web Board) ขององค์กร ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร

๑๔.๑.๑๓ ผู้ใช้งานต้องไม่เสนอความคิดเห็นด้วยการใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

๑๔.๑.๑๔ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๔.๒ การใช้งานเครือข่ายสังคมออนไลน์ มีดังนี้

๑๔.๒.๑ ผู้ใช้งานสามารถใช้งานเครือข่ายสังคมออนไลน์ที่ได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อใช้ประโยชน์ในการปฏิบัติงานราชการ

๑๔.๒.๒ ผู้ใช้งานไม่สามารถติดตั้งโปรแกรมหรืออุปกรณ์ใช้งานเครือข่ายสังคมออนไลน์ใด ๆ ในระบบเครือข่ายขององค์กร ยกเว้น โปรแกรมประเภทเครือข่ายสังคมออนไลน์ที่ได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อใช้ประโยชน์ในการปฏิบัติงานราชการ

๑๔.๒.๓ ผู้ใช้งานที่มีความต้องการหรือมีความจำเป็นที่ต้องการใช้โปรแกรมหรือเว็บไซต์เครือข่ายสังคมออนไลน์เพื่อปฏิบัติงานราชการ ต้องขออนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

หมวดที่ ๓
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ระดับผู้ดูแลระบบ

๑. แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๑.๑ กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่องต่อไปนี้

๑.๑.๑ จัดทำแบบฟอร์มลงทะเบียนผู้ใช้งานระบบสารสนเทศเพื่อตรวจสอบสิทธิ์ และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๑.๑.๒ ต้องจัดทำเอกสารแสดงถึงสิทธิ์ และความรับผิดชอบของผู้ใช้งานซึ่งต้องมีการลงนามรับทราบ

๑.๑.๓ ต้องบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๑.๑.๔ กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

๑) ต้องเป็นผู้ใช้งาน หรือผู้ใช้งานภายนอกที่มีบัญชีรายชื่อที่ออกโดยศูนย์เทคโนโลยีสารสนเทศ และ/หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้สินทรัพย์ขององค์กร และยังไม่สิ้นสุดสถานภาพ

๒) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าของข้อมูล และได้รับมอบหมายจากผู้บังคับบัญชาหรือผู้บริหาร

๓) ได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๑.๕ กำหนดหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

๑) การตัดออกจากทะเบียน การโยกย้ายหน่วยงาน การระงับการปฏิบัติงาน หรือเมื่อสิ้นสุดสถานภาพการเป็นผู้ใช้งาน

๒) การใช้งานที่ขัดต่อข้อกำหนดการใช้งานเครือข่าย

๑.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (Privileges Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ์เพื่อให้สามารถเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๑.๒.๑ ต้องมอบหมายหรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งานที่เหมาะสมต่อสถานภาพหรือหน้าที่ความรับผิดชอบ

๑.๒.๒ ต้องกำหนดระดับสิทธิ์ในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

๑.๒.๓ ต้องมอบหมายสิทธิ์สอดคล้องกับ **<u>แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ</u>**

๑.๒.๔ ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๑.๓ การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเปลี่ยนแปลงสถานภาพ

๑.๔ ต้องกำหนดหลักสูตร และฝึกอบรมเกี่ยวกับการสร้างความรู้ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ และความตระหนักเรื่องความมั่นคงปลอดภัย และกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒. แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย

๒.๑ ผู้ดูแลระบบ ต้องออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยประกอบด้วย โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

๒.๒ การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกพื้นที่ขององค์กร ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตให้ผู้ใช้งานสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศขององค์กร ได้แก่

๒.๒.๑ การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

๒.๒.๒ การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password) แบบ ๒ Factor หรือ One time Password (OTP)

๒.๒.๓ การเข้าสู่ระบบสารสนเทศขององค์กร จะต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

๒.๒.๔ การเข้าสู่ระบบจากระยะไกล ต้องมีการใช้การเข้ารหัสข้อมูล ได้แก่ SSL VPN เพื่อเพิ่มความปลอดภัยของระบบสารสนเทศ

๒.๓ การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายขององค์กร และเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

๒.๔ ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย ผู้ดูแลระบบต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติ ด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกัน ระหว่างองค์กรกับหน่วยงานภายนอก

๒.๕ การควบคุมผู้ใช้งานในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ได้แก่

๒.๕.๑ ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย

๒.๕.๒ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย

๒.๕.๓ ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

๒.๕.๔ ต้องจัดลำดับความสำคัญของช่องบริการเครือข่าย (Quality of Service : QOS) สำหรับเครื่องคอมพิวเตอร์ให้เหมาะสม ตามข้อตกลงการให้บริการด้านเทคโนโลยีสารสนเทศ (Service Level Agreement : SLA และ Operational Level Agreement : OLA)

๒.๖ การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ (Switch) เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๒.๗ ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

๒.๘ ผู้ดูแลระบบจะต้องทำการป้องกันพอร์ต ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ได้แก่

๒.๘.๑ ต้องตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ

๒.๘.๒ ต้องควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) ของระบบเครือข่าย

๒.๘.๓ การขอใช้งานพอร์ตดังกล่าวต้องได้รับอนุญาตจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผ่านช่องทางที่ศูนย์เทคโนโลยีสารสนเทศจัดเตรียมไว้ให้

๒.๘.๔ ต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้อง หรือตู้ RACK ที่มีการควบคุมการเข้าถึง และเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจ เพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต

๒.๙ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓.๑ ต้องลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๒ กำหนดจำนวนอุปกรณ์ที่สามารถใช้งานพร้อมกันได้ไม่เกิน ๓ อุปกรณ์ หรือตามความเหมาะสม สำหรับผู้ใช้งานแต่ละคน

๓.๓ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตี (Hacker) สามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๓.๔ เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๓.๕ เปลี่ยนค่าชื่อบัญชีรายชื่อผู้ใช้งานและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อผู้ใช้งานและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๓.๖ ต้องกำหนดค่าใช้ WPA (Wi-Fi Protected Access) หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณเพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๓.๗ เลือกใช้วิธีการควบคุม MAC Address ชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้งานและรหัสผ่านตามที่กำหนดไว้เท่านั้น หรือเลือกใช้วิธีการ และ/หรือเทคโนโลยีอื่นที่เหมาะสมให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๓.๘ ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๓.๙ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย เมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบโดยทันที

๓.๑๐ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบค้นหาเครือข่ายไร้สายแปลกปลอม (Rogue Access Point) ภายในขอบเขตพื้นที่บริการขององค์กร พร้อมส่งสัญญาณรบกวนและลดทอนคลื่นสัญญาณ เพื่อป้องกันการบุกรุกโจมตี หรือดักจับข้อมูลจากผู้ไม่ประสงค์ดี ยกเว้น WiFi ที่เป็นการให้บริการจากโครงสร้างพื้นฐานของภาครัฐ หรือผู้ให้บริการจากสัมปทานของภาครัฐ และหรือ WiFi ที่ขออนุญาตเปิดให้บริการภายในขอบเขตพื้นที่ขององค์กรอย่างถูกต้อง

๓.๑๑ ต้องทำการปิดกั้นการสื่อสาร หรือช่องสื่อสาร หรือการสื่อสารข้อมูลเฉพาะผู้ใช้งาน หรืออุปกรณ์ต้นเหตุ หรือทั้งหมดทันที โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบก่อนล่วงหน้า เมื่อตรวจพบว่ามีการใช้งานผิดจากวัตถุประสงค์ตามที่แจ้งไว้ หรือมีพฤติการณ์ หรือมีเหตุการณ์ ที่มีความเสี่ยงต่อความปลอดภัยระบบสารสนเทศขององค์กร หรือมีเหตุต้องสงสัยว่ามีการกระทำความผิดตามกฎหมายที่เกี่ยวข้อง แล้วรายงานผู้บังคับบัญชาตามลำดับชั้นให้ทราบต่อไป การดำเนินการปิดกั้นนี้ให้ดำเนินการจนกว่าจะมีการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรอีกครั้งหนึ่ง

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๑ กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับระบบที่มีความสำคัญสูงหรือมีความเสี่ยงสูง การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวสำหรับระบบสารสนเทศ ดังนี้

๔.๑.๑ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๔.๑.๒ จำกัดเข้าถึงระบบปฏิบัติการเฉพาะระบบอินทราเน็ต

๔.๒ การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบสารสนเทศ ได้แก่

๔.๒.๑ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อผู้ใช้งาน (Username) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๔.๒.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันเกิดจากการใช้ชื่อผู้ใช้งาน เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๓ การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ได้แก่

๔.๓.๑ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๔.๓.๒ กำหนดให้ผู้ใช้งานต้องลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองไว้เป็นความลับและไม่เปิดเผยให้ผู้อื่นทราบ

๔.๓.๓ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

๔.๓.๔ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๔.๓.๕ กำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๔.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิ์พิเศษที่ได้รับ

๔.๓.๗ กำหนดให้มีการแจ้งเตือนให้เปลี่ยนรหัสผ่านล่วงหน้าอย่างน้อย ๑ สัปดาห์

๔.๔ กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย ผู้ดูแลระบบต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการปฏิเสธการใช้งาน หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง เป็นต้น

๔.๕ การพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์

๔.๖ การตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์เมื่อเครื่องคอมพิวเตอร์ นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

๔.๗ การควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมอรรถประโยชน์สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๔.๗.๑ จำกัดการใช้งานโปรแกรมอรรถประโยชน์ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

๔.๗.๒ ให้แยกโปรแกรมอรรถประโยชน์ออกจากโปรแกรมระบบงาน

๔.๗.๓ โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๔.๘ การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง ผู้บริหารต้องจัดให้ติดตั้งระบบเตือนภัยให้กับผู้ใช้งานที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

๔.๙ การใช้งานระบบเทคโนโลยีสารสนเทศต้องกำหนดให้ตัด และหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานเกิน ๓๐ นาที

๔.๑๐ องค์กรจะ "ไม่" จำกัดระยะวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) เพื่อประโยชน์สูงสุดในการใช้งานให้เป็นไปตามภารกิจที่องค์กรกำหนด แต่จะมีมาตรการเฝ้าระวังการใช้งานที่ผิดปกติ เช่น กรณีการใช้งานนอกเวลาราชการผู้ดูแลระบบจะทำการบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File และตรวจสอบความผิดปกติในการใช้งานนอกเวลาราชการ ผู้ใช้งานจะต้อง login ผ่านระบบ Active Directory ขององค์กรทุกครั้ง พร้อมกับการยืนยันตัวตนผ่าน Two Factors Authentication

๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๕.๑ การจัดสรรไอพีแอดเดรส (IP Address)

๕.๑.๑ ไอพีแอดเดรส รุ่น ๔ (IPV๔) ๒๐๒.๕๘.๑๒๖.๐/๒๔ รวมถึง ไอพีแอดเดรส รุ่น ๖ (IPV๖) ที่จัดหาใช้งานต่อไป ของระบบเครือข่ายคอมพิวเตอร์ เป็นสินทรัพย์ขององค์กร โดยองค์กรมอบอำนาจให้ศูนย์เทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการ

๕.๑.๒ สำหรับเครือข่ายภายในองค์กร มอบอำนาจให้ศูนย์เทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการ โดยใช้ไอพีแอดเดรส รุ่น ๔ (IPV๔) ช่วง Private Network ตามความเหมะสม รวมถึงไอพีแอดเดรส รุ่น ๖ (IPV๖) ที่จัดหาใช้งานต่อไป

๕.๑.๓ ให้ศูนย์เทคโนโลยีสารสนเทศทำหน้าที่จัดสรรไอพีแอดเดรสให้กับหน่วยงานตามที่ร้องขอเพื่อให้ใช้งานได้อย่างเพียงพอและมีประสิทธิภาพ โดยศูนย์เทคโนโลยีสารสนเทศสามารถปรับเปลี่ยนไอพีแอดเดรสที่ได้จัดสรรให้กับกอง/สำนัก/กลุ่มขึ้นตรง จากหมายเลขเดิมเป็นหมายเลขใหม่ได้ตามหลักวิชาการ เพื่อให้สามารถบริหารและจัดการได้อย่างมีประสิทธิภาพ

๕.๒ การจัดการชื่อโดเมน

๕.๒.๑ องค์กรได้ขึ้นทะเบียนชื่อโดเมนอินเทอร์เน็ต (Internet) ขององค์กรภายใต้ชื่อ “oncb.go.th” โดยศูนย์เทคโนโลยีสารสนเทศรับภาระชำระค่าธรรมเนียม การขึ้นทะเบียนและค่าบำรุงรักษาชื่อโดเมน

๕.๒.๒ ให้ศูนย์เทคโนโลยีสารสนเทศทำหน้าที่ให้บริการจดทะเบียนชื่อโดเมนประจำองค์กรภายใต้ชื่อโดเมนขององค์กร “oncb.go.th” และ สำหรับระบบอินทราเน็ต (Intranet) พร้อมชื่อเครื่องภายใต้ชื่อโดเมน “oncbnet.go.th”

๕.๒.๓ องค์กรมีสิทธิ์ในการใช้ชื่อโดเมน oncb.go.th โดยยื่นเรื่องขออนุมัติต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ คำขออนุมัติจะต้องลงนามรับรองโดยผู้อำนวยการกอง/สำนัก/กลุ่มขึ้นตรง

๕.๒.๔ โครงการพิเศษหรือโครงการใด ๆ ที่ได้รับอนุมัติจากองค์กร สามารถขอจดชื่อโดเมนประจำโครงการได้ โดยหากเป็นโครงการระดับหน่วยงานให้จดทะเบียนภายใต้ชื่อโดเมนย่อยประจำกอง/สำนัก/กลุ่มขึ้นตรงนั้น หรือในกรณีที่เป็นโครงการระดับองค์กรจะสามารถยื่นขอจดชื่อโดเมนภายใต้ชื่อโดเมนขององค์กรได้

๕.๒.๕ การใช้ไอพีแอดเดรสขององค์กรเพื่อจดทะเบียนชื่อโดเมนนอกสารบบชื่อโดเมนขององค์กรโดยมิได้รับอนุญาตเป็นสิ่งต้องห้าม ยกเว้นกรณีมีเหตุผลความจำเป็นอย่างยิ่ง ทั้งนี้ ให้ผู้อำนวยการกอง/สำนัก/กลุ่มขึ้นตรง ดำเนินการยื่นคำร้องต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ โดยชี้แจงเหตุผลและความจำเป็นที่ต้องขอจดทะเบียนชื่อโดเมนนอกสารบบ การอนุมัติจดทะเบียนให้อยู่ในดุลยพินิจของผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๖. แนวปฏิบัติการควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

๖.๑ ผู้ดูแลระบบต้องกำหนดการตั้งชื่อ (Computer Name) เครื่องคอมพิวเตอร์ส่วนบุคคลและการเชื่อมต่อเข้ากับระบบควบคุม Domain กำหนด IP Address ค่าพารามิเตอร์ (Parameter) ต่าง ๆ และการเชื่อมต่อเข้ากับระบบเครือข่ายภายในองค์กร ดังนี้

๖.๑.๑ การตั้งชื่อเครื่องต้องประกอบด้วย ชื่อย่อ กอง/สำนัก/กลุ่มขึ้นตรง เป็น อักษรภาษาอังกฤษ ตามด้วยเครื่องหมาย “-” หมายเลขไอพีแอดเดรสประจำเครือข่าย ตามด้วยเครื่องหมาย “-” และตามด้วย สามดิจิตสุดท้ายของหมายเลขไอพีแอดเดรส

๖.๑.๒ การใช้หมายเลขไอพีแอดเดรส รุ่น๔ (IPV๔) แบบ Private Network

รายการ	ช่วงของ IP Address
สงวนไว้สำหรับ ศูนย์เทคโนโลยีสารสนเทศ	๑๙๒.๑๖๘.X.๑-๕๐
เครื่องคอมพิวเตอร์ลูกข่าย (PC)	๑๙๒.๑๖๘.X.๕๑-๑๕๐
เครื่องคอมพิวเตอร์ลูกข่าย (Notebook)	๑๙๒.๑๖๘.X.๑๕๑-๒๐๐
เครื่องพิมพ์คอมพิวเตอร์และอุปกรณ์อื่น ๆ	๑๙๒.๑๖๘.X.๒๐๑-๒๓๐
เครื่องคอมพิวเตอร์ สำหรับผู้มาติดต่อ/ประสานงาน	๑๙๒.๑๖๘.X.๒๓๑-๒๕๔

๖.๒ ผู้ดูแลระบบต้องลงโปรแกรมค้นหาทำลายไวรัสที่มีความน่าเชื่อถือในเครื่องคอมพิวเตอร์ส่วนบุคคล

๖.๓ ผู้ดูแลระบบต้องจัดให้มีระบบการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control : NAC) สำหรับควบคุมเครื่องที่นำมาเชื่อมต่อกับระบบเครือข่ายขององค์กร

๖.๔ ผู้ดูแลระบบ หรือผู้ประสานงานจะทำการยกเลิกการเชื่อมต่อทันที โดยไม่แจ้งให้ผู้ใช้งานทราบก่อนล่วงหน้า เมื่อตรวจพบว่าผู้ใช้งานใช้งานผิดจากวัตถุประสงค์ตามที่แจ้งไว้ หรือมีพฤติการณ์เสี่ยงต่อความปลอดภัยระบบสารสนเทศขององค์กร

๗. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต และรวมความถึงการกำหนดหน้าที่ของผู้ใช้งาน การเข้าถึงเครือข่าย การใช้งานระบบสารสนเทศ การเฝ้าดูการใช้งานระบบสารสนเทศ และอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศขององค์กร

ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

๗.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- สิทธิ์อ่านอย่างเดียว
- สิทธิ์การเพิ่มข้อมูล
- สิทธิ์การแก้ไขข้อมูล
- สิทธิ์การลบข้อมูล
- สิทธิ์การอนุมัติ/อนุญาต
- ไม่มีสิทธิ์

๗.๒ กำหนดการระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตาม **แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)** ที่ได้กำหนดไว้

๗.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตผ่าน E-Form ในระบบสนับสนุนงานให้บริการสารสนเทศ และได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย

๗.๔ การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการ และกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๗.๔.๑ จัดแบ่งประเภทข้อมูลออกเป็น

๑) ข้อมูลทั่วไปที่เปิดเผยได้

๒) ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ์ ได้แก่

๒.๑) ข้อมูลสารสนเทศด้านการบริหาร

๒.๒) ข้อมูลสารสนเทศตามพันธกิจ

๗.๔.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ

๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

๒) ข้อมูลที่มีระดับความสำคัญมาก

๓) ข้อมูลที่มีระดับความสำคัญปานกลาง

๔) ข้อมูลที่มีระดับความสำคัญน้อย

หากข้อมูลที่นอกเหนือจากที่กำหนด การจัดระดับความสำคัญของข้อมูลให้พิจารณาในระดับฐานข้อมูล ซึ่งประกอบไปด้วย ด้านป้องกันยาเสพติด ด้านปราบปรามยาเสพติด ด้านบำบัดรักษายาเสพติด และด้านบริหารจัดการ ด้วยการประเมินมูลค่าความเสียหายต่อองค์กร หากข้อมูลมีปัญหา ไม่สมบูรณ์ แนวปฏิบัติในการพิจารณาจัดลำดับความสำคัญของข้อมูล มีดังนี้

ระดับความสำคัญของข้อมูล	การประเมินมูลค่าความเสียหายหากข้อมูลมีปัญหาหรือไม่สมบูรณ์
ความสำคัญมากที่สุด	มีผลกระทบรุนแรงต่อการดำรงอยู่ของหน่วยงาน หรือปิดหน่วยงาน
ความสำคัญมาก	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
ความสำคัญปานกลาง	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
ความสำคัญน้อย	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ

๗.๔.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๗.๔.๔ จัดแบ่งระดับชั้นการเข้าถึง ดังนี้

๑) เข้าถึงได้ทุกกลุ่มผู้ใช้งาน ได้แก่ ข้อมูลทั่วไปที่เปิดเผยได้

๒) เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ์ ได้แก่ ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ์ข้อมูลลับ

๓) เข้าถึงได้เฉพาะผู้มีสิทธิ์ในการบริหารจัดการระบบสารสนเทศ ได้แก่ ข้อมูลระบบ

๗.๔.๕ กำหนดช่องทางในการเข้าถึงข้อมูล

๑) ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายภายในได้ตลอด ๒๔ ชั่วโมง

๒) ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายอินเทอร์เน็ตที่อยู่ภายนอกผ่านระบบ VPN ได้ตลอด ๒๔ ชั่วโมง

๗.๔.๖ กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล

๑) ระบบงานบริการสำหรับผู้ใช้งานทั่วไปเข้าถึงได้ตลอดเวลา

๒) ระบบงานภายในสำหรับผู้ใช้งานสามารถเข้าถึงระบบตามช่วงเวลา ดังนี้

๒.๑) เวลาราชการ (เวลา ๘.๓๐-๑๖.๓๐ น.)

๒.๒) นอกเวลาราชการ (นอกช่วงเวลา ๘.๓๐-๑๖.๓๐ น.)

๒.๓) ช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

๒.๔) ช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุช่วงเวลา ระยะเวลาการเข้าถึง

๒.๕) เข้าถึงได้ตลอดเวลา

๒.๖) เข้าถึงได้ตามข้อตกลงการให้บริการด้านเทคโนโลยีสารสนเทศ (Service Level Agreement : SLA และ Operational Level Agreement : OLA)

๗.๕ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็นสองส่วน คือ

๗.๕.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ

๗.๕.๒ มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๗.๖ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๗.๗ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

๗.๘ การใช้บริการจากผู้ใช้งานภายนอก บางครั้งผู้ใช้งานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของผู้ใช้งานภายนอกเพื่อความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร โดยแนวปฏิบัตินี้ต้องตรวจสอบและประเมินตามระยะเวลา ๑ ครั้งต่อปี

๗.๘.๑ จัดทำเอกสารแบบฟอร์มสำหรับผู้ใช้งานภายนอก ต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

๑) เหตุผลในการขอใช้งาน

๒) ระยะเวลาในการใช้งาน

๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๔) การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๗.๘.๒ กำหนดให้ผู้ใช้งานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงานต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบสารสนเทศ

๗.๘.๓ กำหนดให้ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

๗.๘.๔ เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๗.๘.๕ องค์กรมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้บริการ เพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

๗.๘.๖ ในการจ้างเหมาพัฒนา บำรุงรักษาระบบ ผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ใช้งานภายนอก ได้แก่

๑) ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิ์ในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๒) ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศ ได้แก่ การกำหนดชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

๓) ต้องบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File

๔) ในระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

๘. แนวปฏิบัติการควบคุมการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์ (Use of the Internet & Social Network)

๘.๑ การใช้งานอินเทอร์เน็ต

๘.๑.๑ ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS/IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem เป็นต้น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรแล้ว

๘.๑.๒ ผู้ดูแลระบบต้องจัดให้มีการแสดงตัวตน (Identification) และพิสูจน์ยืนยันตัวตน (Authentication) ก่อนที่ผู้ใช้งานเข้าถึงเครือข่ายอินเทอร์เน็ตทุกครั้ง เพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบในการกระทำของผู้ใช้งานเอง ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๘.๒ การปิดกั้นการเข้าถึงอินเทอร์เน็ต หรือเว็บไซต์ที่ไม่พึงประสงค์

๘.๒.๑ ผู้ดูแลระบบจะปิดกั้นการเข้าถึงเว็บไซต์ ตามประกาศหรือการแจ้งให้ปิดกั้นอันเนื่องมาจากขัดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จากหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงยุติธรรม เป็นต้น และตามที่ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศพิจารณาแล้วเห็นว่า เป็นเว็บไซต์ที่ไม่พึงประสงค์และเป็นอันตรายต่อระบบสารสนเทศขององค์กร เช่น การแพร่ระบาดไวรัสคอมพิวเตอร์จากเว็บไซต์นั้น ๆ เว็บไซต์ปลอมดักจับข้อมูล เว็บไซต์ที่ไม่ก่อให้เกิดผลประโยชน์ต่อการปฏิบัติงานราชการ เป็นต้น โดยศูนย์เทคโนโลยีสารสนเทศจะต้องประกาศให้ทราบเป็นครั้ง ๆ ไป

๘.๒.๒ ผู้ดูแลระบบจะต้องปิดกั้นการเข้าถึงอินเทอร์เน็ตชั่วคราว สำหรับเครื่องคอมพิวเตอร์หรือผู้ใช้งานที่มีพฤติการณ์เสี่ยงต่อการรักษาความปลอดภัยสารสนเทศและส่งผลทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้ เช่น เครื่องคอมพิวเตอร์ส่วนบุคคลติดไวรัสแล้วมีพฤติการณ์ส่งข้อมูลภายในเครื่องออกสู่อินเทอร์เน็ต การ Download ไฟล์ข้อมูลที่มีไวรัสคอมพิวเตอร์แฝงมาด้วย การรับส่งไฟล์ข้อมูล (Up Load-Download) ขนาดใหญ่มาก ๆ แล้วทำให้ระบบเครือข่ายภายในองค์กรติดขัด ผู้ใช้งานลักลอบใช้รหัสประจำตัวของผู้อื่น หรือการปลอมแปลงตัวตนในระบบเครือข่ายคอมพิวเตอร์เสมือนดูเสมือนเข้าใช้งานโดยผู้ใช้งานคนอื่นโดยมิชอบ เป็นต้น จนกว่าจะสามารถพิสูจน์ได้ว่ามีความปลอดภัย ไม่ส่งผลเสียต่อระบบสารเทศและการสื่อสารขององค์กร หรือจนกว่าจะปฏิบัติตามนโยบายนี้ได้อย่างถูกต้อง จึงยกเลิกได้

๘.๒.๓ ผู้ดูแลระบบเครือข่ายขององค์กร จะต้องจัดลำดับความสำคัญของการเปิดขนาดช่องบริการเครือข่ายส่วนเชื่อมต่ออินเทอร์เน็ต (Quality of Service : QOS) สำหรับเครื่องคอมพิวเตอร์ให้เหมาะสมดังนี้

๑) ช่องบริการที่ก่อให้เกิดผลประโยชน์ต่อการปฏิบัติงานราชการ ให้ความสำคัญมากเป็นอันดับหนึ่ง

๒) ช่องบริการที่ไม่ใช่เพื่องานราชการ เช่น การ Download ไฟล์เพลง ภาพยนตร์ เกมออนไลน์ เพื่อความบันเทิง เป็นต้น ให้ความสำคัญน้อยสุด โดยจัดให้เข้าถึงบริการดังกล่าวได้ในเวลานอกเวลาทำการเท่านั้น ยกเว้นเครื่องคอมพิวเตอร์ที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเห็นควรอนุญาตให้เข้าถึงในเวลาทำการได้

๘.๒.๔ องค์กรสงวนสิทธิ์ในการบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ (Computer Traffic Log) อันแสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา และชนิดการบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ในการใช้งานระบบอินเทอร์เน็ตนั้น เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๘.๒.๕ ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีระบบบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ พร้อมดำเนินการจัดเก็บบันทึกข้อมูลดังกล่าว โดยต้องสามารถเรียกดูข้อมูลย้อนหลังได้ไม่น้อยกว่า ๙๐ วัน และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ต้องอนุญาตให้กับเจ้าหน้าที่ผู้ดูแลระบบสามารถมีสิทธิ์ในการ เข้าถึงข้อมูล เพื่อรองรับการประสานงานจากเจ้าพนักงาน เมื่อมีการร้องขอตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๘.๒.๖ ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีเจ้าหน้าที่สำหรับประสานงานและคอยดูแลควบคุม ข้อมูลจราจรทางคอมพิวเตอร์ พร้อมสามารถส่งมอบให้กับเจ้าพนักงาน เมื่อร้องขอตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๙. แนวปฏิบัติการนำอุปกรณ์โมบายส่วนบุคคล (Mobile-BYOD) มาใช้งานและเข้าถึงข้อมูลที่มีชั้นความลับขององค์กร

๙.๑ ศูนย์เทคโนโลยีสารสนเทศประเมินและจัดแบ่งลำดับชั้นความลับของข้อมูล ระบบสารสนเทศที่มีแผนงานจะให้บริการผ่านอุปกรณ์โมบายส่วนบุคคล (Mobile-BYOD) ตาม**แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ** และนำเสนอคณะกรรมการกำหนดนโยบายและแผนพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการป้องกันและแก้ไขปัญหายาเสพติด (Steering Committee) พิจารณา

๙.๒ ชั้นความลับของข้อมูล เป็น ข้อมูลลับ ข้อมูลลับมาก ข้อมูลลับที่สุด ต้องจัดให้มีการควบคุมดูแล ดังนี้

๙.๒.๑ ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีระบบบริหารจัดการอุปกรณ์โมบายส่วนบุคคลและลงทะเบียนอุปกรณ์สำหรับควบคุมดูแล โดยจัดให้อยู่ในความดูแลของกลุ่มงานระบบปฏิบัติการช่วยเหลือ (Help Desk) และจัดให้มีข้อตกลงการให้บริการด้านเทคโนโลยีสารสนเทศ (Service Level Agreement : SLA และ Operational Level Agreement : OLA)

๙.๒.๒ อุปกรณ์โมบายส่วนบุคคลต้องใช้ภาษาไทย และหรือภาษาอังกฤษ เป็นหลัก

๙.๒.๓ โปรแกรมใด ๆ รวมถึง Plugins ที่ติดตั้งบนตัวอุปกรณ์โมบายส่วนบุคคล ต้องมีความน่าเชื่อถือ และหรือมีลิขสิทธิ์ถูกต้อง พิสูจน์ได้

๙.๒.๔ ต้องติดตั้งโปรแกรมประเภททำลายไวรัส และหรือประเภท Anti-malware

๑๐. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ หรือห้องปฏิบัติการเครื่องคอมพิวเตอร์ (Data Centre : DC)

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญอันหนึ่งของระบบรักษาความปลอดภัย ความมั่นคงทางกายภาพรวมถึงการป้องกันสถานที่และอุปกรณ์ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม เป็นต้น การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิ หรือความชื้น ในห้องควบคุมที่สูงเกินขีดจำกัด หรือการกระทำโดยประมาท เช่น การทำน้ำกรดโดนเครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ ดังนั้น จึงมีความจำเป็นในการป้องกันอาคารและอุปกรณ์ โดยกำหนดแนวปฏิบัติในเรื่องการสร้างห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย รวมถึงมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๑๐.๑ จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษา ความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ โดยจัดแบ่งพื้นที่ ดังนี้

๑๐.๑.๑ ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

๑๐.๑.๒ พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีเซิร์ฟเวอร์ ระบบเครือข่ายคอมพิวเตอร์ติดตั้งอยู่

๑๐.๒ การเข้าไปในพื้นที่ควบคุม

๑๐.๒.๑ ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงาน หรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม

๑๐.๒.๒ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๑๐.๒.๓ ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่ควบคุม เว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐.๒.๔ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อสินทรัพย์ขององค์กร จะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐.๒.๕ บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงาน หรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายและต้องอยู่ด้วยตลอดเวลา

๑๐.๓ การเข้าไปในพื้นที่จำกัดการเข้าถึง

๑๐.๓.๑ ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ หรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย และต้องมีผู้ดูแลระบบที่ได้รับมอบหมายอย่างน้อย ๑ คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๑๐.๓.๒ ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า ๑๕ ปี เข้าไปในพื้นที่จำกัดการเข้าถึง

๑๐.๓.๓ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

๑๐.๓.๔ ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่จำกัดการเข้าถึง เว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐.๓.๕ ไม่อนุญาตให้เข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

๑๐.๓.๖ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อสินทรัพย์จะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐.๔ ด้านกายภาพของห้องควบคุมระบบ

๑๐.๔.๑ แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น Router, Switch, Server, UPS เป็นต้น

๑๐.๔.๒ มี Rack ในการจัดเก็บอุปกรณ์ต่าง ๆ ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

๑๐.๔.๓ ตำแหน่งของการวางอุปกรณ์ต่าง ๆ ไม่ควรวางใกล้ประตู หน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรง เพื่อหลีกเลี่ยงความชื้น

๑๐.๔.๔ การจัดวางสาย Cable Network สายไฟฟ้า ต้องติดป้ายชื่อสายต้นทาง ปลายทาง และเก็บสายให้เรียบร้อย เพื่อป้องการการเดินสะดุด

๑๐.๔.๕ ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแล ระบบที่รับผิดชอบอุปกรณ์แต่ละชนิด

๑๐.๔.๖ มีระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV ระบบการเข้าออกห้อง โดยระบบ Fingerprint Scan หรือ RFID เป็นต้น

๑๐.๔.๗ มีระบบสังเกตการณ์อุณหภูมิภายใน Rack ระบบแจ้งเตือนและป้องกันอัคคีภัย

๑๐.๔.๘ มีระบบสำรองไฟฟ้าเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติ และระบบสำรองไฟฟ้าอัตโนมัติ เป็นต้น

๑๐.๔.๙ มีระบบป้องกันกระแสไฟฟ้าจากฟ้าผ่า

๑๐.๔.๑๐ มีระบบปรับอากาศแบบควบคุมอุณหภูมิ (๕๐-๘๐°F) และความชื้น (๒๐-๘๐%)

๑๐.๔.๑๑ ติดตั้งฉนวนกันไฟไหม้ที่ฝ้าเพดานและกำแพง

๑๐.๕ การบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

๑๐.๕.๑ กรณีติดตั้งเซิร์ฟเวอร์หรืออุปกรณ์ต่าง ๆ ให้แกะหีบห่อและประกอบให้แล้วเสร็จจากภายนอกพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงก่อนนำไปติดตั้ง เว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐.๕.๒ กรณีที่จำเป็นต้องทำงานก่อสร้าง แก้ไข และติดตั้ง ในพื้นที่ควบคุมและพื้นที่จำกัด การเข้าถึงต้องมีอุปกรณ์ควบคุม ฝุ่น ความร้อน เพื่อป้องกันความเสียหาย โดยผ่านความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนการปฏิบัติงาน

๑๐.๕.๓ ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยอย่างน้อยปีละ ๑ ครั้ง

๑๐.๕.๔ จัดทำแผนบริหารความเสี่ยงเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟฟ้าลัดวงจร ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือมีผู้บุกรุก เป็นต้น

๑๐.๕.๕ ซ้อมการปฏิบัติงานตามแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๑๐.๕.๖ มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

๑๑. แนวทางปฏิบัติการควบคุม เข้า-ออก ศูนย์คอมพิวเตอร์สำรอง

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญของศูนย์คอมพิวเตอร์สำรอง ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลที่มีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์สำรอง

๑๑.๑ บทบาทหน้าที่และความรับผิดชอบ

๑๑.๑.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑) อนุมัติสิทธิ์การเข้า-ออกพื้นที่ศูนย์คอมพิวเตอร์สำรอง

๒) อนุมัติกระบวนการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์สำรอง

๑๑.๑.๒ ผู้ควบคุมและผู้ประสานงาน และหรือผู้ที่ได้รับมอบหมาย

๑) ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในพื้นที่ให้ปฏิบัติตามข้อกำหนดของศูนย์เทคโนโลยีสารสนเทศ และสำนักงานป้องกันและปราบปรามยาเสพติด ภาค ๓ อย่างเคร่งครัด

๒) ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้า-ออกศูนย์คอมพิวเตอร์สำรอง ต้องได้รับอนุญาตเท่านั้น

๑๑.๒ กระบวนการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์สำรอง

ผู้ดูแลระบบและผู้ประสานงาน และ/หรือผู้ที่ถูกมอบหมายมีแนวทางปฏิบัติ ดังนี้

๑) จัดระเบียบระบบเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมถึงอุปกรณ์ส่วนประกอบต่าง ๆ ให้เป็นสัดส่วนชัดเจนตามความสำคัญ เพื่อสะดวกในกาปฏิบัติงานและควบคุมการเข้าถึง

๒) ทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้อง และมีการบันทึกการเข้า-ออกพื้นที่

๓) สิทธิ์ในการเข้า-ออกห้องต่าง ๆ ของแต่ละบุคคลต้องได้รับการอนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร หรืออนุมัติผ่าน E-Form และสิทธิ์ของแต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงาน

๔) บุคคลที่เกี่ยวข้องต้องทำบันทึกประวัติ หรือรหัสประจำตัว หรือบัตรผ่าน หรือบันทึกลายนิ้วมือ สำหรับใช้ในการเข้า-ออก

๕) จัดทำบันทึกการเข้า-ออกเป็นเอกสารแบบฟอร์ม หรือไฟล์ดิจิตอล สามารถตรวจสอบข้อมูลย้อนหลังได้

๖) บุคคลใดที่ไม่มีหน้าที่เกี่ยวข้อง แต่อาจมีความจำเป็นต้องเข้า-ออก ต้องทำบันทึกประวัติและต้องควบคุมอย่างรัดกุม

๗) การเข้าถึงพื้นที่ศูนย์คอมพิวเตอร์สำรอง ต้องมีการลงบันทึกการผ่านเข้า-ออกทุกครั้ง

๘) ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์ม กับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

๙) ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๑๒. แนวปฏิบัติการนำระบบงานไปติดตั้งบนคลาวด์ (Cloud Computing)

๑๒.๑ การวางแผนการนำระบบงานไปติดตั้งบนคลาวด์

๑๒.๑.๑ คัดเลือกผู้ให้บริการคลาวด์ที่มีความน่าเชื่อถือในการให้บริการด้านความมั่นคงปลอดภัย

๑๒.๑.๒ การจัดการส่วนที่เกี่ยวข้องกับเขตอำนาจรัฐ รัฐบาลประเทศไทย และกฎหมายระหว่างประเทศ (ที่เกี่ยวข้อง)

๑๒.๑.๓ ระบุระบบงานและข้อมูลของระบบงานที่จะนำขึ้นคลาวด์

๑๒.๑.๔ ระบุชั้นความลับและเจ้าของข้อมูลว่าสอดคล้องกับนโยบายการนำระบบงานและข้อมูลไปติดตั้งบนคลาวด์ที่องค์กรกำหนดไว้หรือไม่

๑๒.๑.๕ ดำเนินการจัดการกับข้อมูลตามชั้นความลับของข้อมูล

๑๒.๑.๖ จัดทำบัญชีทรัพย์สินขององค์ประกอบของระบบที่จะนำขึ้นคลาวด์

๑๒.๑.๗ ประเมินความเสี่ยงกับระบบและจัดทำแผนการลดความเสี่ยง

๑๒.๑.๘ กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงาน

๑๒.๑.๙ กำหนดข้อตกลงการควบคุมการเชื่อมต่อระบบ (The Agreed and Finalized Interface Control Document : ICD)

๑๒.๒ การวิเคราะห์และออกแบบความมั่นคงปลอดภัยทางเครือข่าย

๑๒.๒.๑ ออกแบบและจัดทำผังเครือข่ายของระบบ

๑๒.๒.๒ แบ่งแยกเครือข่ายตามผังเครือข่ายที่กำหนด

๑๒.๒.๓ แยกเครื่องคอมพิวเตอร์แม่ข่ายเสมือนสำหรับการทดสอบไว้ในเครือข่ายที่แยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่ายเสมือนสำหรับการให้บริการจริง

๑๒.๒.๔ ศึกษาการจราจร (Traffic) ที่เข้าออกเครือข่ายทั้งหมด เพื่อกำหนดเป็น Traffic ที่อนุญาตและไม่อนุญาต ซึ่งเป็นการกำหนดการไหลของข้อมูลในเครือข่าย

๑๒.๒.๕ กำหนดนโยบาย (Policy) ไฟร์วอลล์ (Firewall) เพื่อจำกัด Traffic ที่เข้า-ออกเครือข่าย

๑๒.๒.๖ ติดตั้งไฟร์วอลล์และกำหนด Rule บนไฟร์วอลล์ตามนโยบายไฟร์วอลล์ที่กำหนดไว้

๑๒.๒.๗ ติดตั้งระบบป้องกันการบุกรุก

๑๒.๒.๘ ติดตั้งระบบป้องกันไวรัส

๑๒.๒.๙ ติดตั้งระบบ VPN สำหรับผู้ดูแลระบบใช้งาน

๑๒.๒.๑๐ ติดตั้งระบบตั้งสัญญาณนาฬิกาให้ตรง

๑๒.๓ การวิเคราะห์และออกแบบระบบงานด้านความมั่นคงปลอดภัย

๑๒.๓.๑ กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานอย่างน้อย ดังต่อไปนี้

๑) ด้านการตรวจสอบข้อมูลนำเข้าและออกจากระบบงาน

๒) ด้านการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่สำคัญและอาจจำเป็นต้องตรวจสอบในภายหลัง

๓) ด้านกลุ่มผู้ใช้งาน บทบาท และสิทธิ์การเข้าถึงระบบงาน

๔) ด้านการลงทะเบียนและถอดถอนการเข้าถึงระบบงาน

๕) ด้านการตัดหรือหมดเวลาใช้งาน

๖) ด้านการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย

๗) ด้านหน้าจอการล็อคอิน (Login) ที่มีความมั่นคงปลอดภัย

๘) ด้านการติดตามปริมาณการใช้ระบบและขีดความสามารถ หรือประสิทธิภาพของระบบ

๙) ด้านการป้องกันข้อมูลรหัสผ่าน (Password) ของผู้ใช้งาน

๑๐) ด้านการป้องกันข้อมูลสำคัญที่จัดเก็บไว้ในระบบงาน

๑๑) ด้านการป้องกันข้อมูลสำคัญที่มีการส่งผ่านเครือข่าย

๑๒) ด้านการเข้ารหัสข้อมูลและการลงลายมือชื่อดิจิตอล

๑๓) ด้านการวิเคราะห์จุดอ่อนของซอร์สโค้ด (Source Code)

๑๔) ด้านการกู้คืนระบบงาน

๑๒.๓.๒ ดำเนินการวิเคราะห์และออกแบบระบบด้านความมั่นคงปลอดภัย

๑๒.๔ การทดสอบระบบ

๑๒.๔.๑ ทดสอบระบบให้ครอบคลุมตามความต้องการด้านความมั่นคงปลอดภัยของระบบงานที่กำหนดไว้ (Security Test)

๑๒.๔.๒ กำหนดให้มีการป้องกันข้อมูลสำคัญ (Data Masking Technique)

๑) กำหนดให้เจ้าของข้อมูลลบข้อมูลส่วนที่สามารถบ่งชี้ตัวบุคคลทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบ

๒) กำหนดให้เจ้าของข้อมูลลบข้อมูลส่วนที่เป็นความลับทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบ

๑๒.๔.๓ ทดสอบโดยการป้อนอินพุท (Input) ที่จะทำให้ระบบทำงานผิดพลาด ไม่ถูกต้อง ทำให้ระบบล่ม หรือถึงขั้นระบบถูกบุกรุกได้ (Fuzzing Technique)

๑๒.๔.๔ ทดสอบและรับรองระบบ (User Acceptance Test)

๑๒.๕ การติดตั้งระบบ

๑๒.๕.๑ จัดทำแผนการติดตั้งระบบงาน

๑๒.๕.๒ ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ ที่เกี่ยวข้องกับระบบงานให้แล้วเสร็จ ก่อนที่จะติดตั้งระบบงาน

๑๒.๕.๓ ปิดบริการ (Service) ที่ไม่มีความจำเป็นต้องใช้งานในระบบงาน

๑๒.๕.๔ จัดทำ Security Baseline ของระบบที่จะทำการติดตั้ง

๑๒.๕.๕ ปรับแต่งค่าพารามิเตอร์ต่าง ๆ ที่มีผลต่อความมั่นคงปลอดภัยของระบบงานตาม Security Baseline ของระบบที่ได้กำหนดไว้

๑๒.๕.๖ จำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของระบบงาน หลีกเลี่ยงการติดตั้งซอร์สโค้ดของระบบงานบนเครื่องให้บริการ (ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้โดยตรงในขณะที่ทำงาน)

๑๒.๕.๗ ตรวจสอบและปิดช่องโหว่ในระบบที่ทำการติดตั้ง

๑๒.๕.๘ ติดตั้งโปรแกรมเพื่อติดตามและตรวจสอบการเปลี่ยนแปลงแก้ไขไฟล์ต่าง ๆ ของระบบโดยไม่ได้รับอนุญาต

๑๒.๕.๙ จัดทำแผนการตรวจสอบและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log) บนเครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการระบบงานที่ทำการติดตั้ง

๑๒.๕.๑๐ จัดทำแผนการสำรองข้อมูลของระบบงานและดำเนินการตามแผนฯ ทดสอบการกู้ข้อมูลเป็นครั้งคราว

๑๒.๕.๑๑ จัดทำแผนการตรวจสอบและติดตามสภาพความพร้อมใช้ของระบบงานและดำเนินการตามแผนฯ

๑๒.๕.๑๒ จัดทำแผนการตรวจสอบและติดตามทรัพยากรของระบบงานและดำเนินการตามแผนฯ

๑๒.๕.๑๓ จัดทำแผนการกู้คืนระบบงานและดำเนินการทดสอบปีละครั้ง

๑๓. แนวปฏิบัติการติดตั้งระบบสารสนเทศ

๑๓.๑ การวางแผนในการติดตั้ง

๑๓.๑.๑ ระบุระบบงานและข้อมูลของระบบงานที่จะติดตั้ง

๑๓.๑.๒ ระบุชั้นความลับและเจ้าของข้อมูลว่าสอดคล้องกับนโยบายการนำระบบงานและข้อมูลไปติดตั้งให้บริการตามรูปแบบ หรือมีข้อตกลงใด ๆ หรือไม่

๑๓.๑.๓ ดำเนินการจัดการกับข้อมูลตามชั้นความลับของข้อมูล

๑๓.๑.๔ จัดทำบัญชีสินทรัพย์ขององค์ประกอบของระบบ

๑๓.๑.๕ ประเมินความเสี่ยงกับระบบและจัดทำแผนการลดความเสี่ยง

๑๓.๑.๖ กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงาน

๑๓.๑.๗ กำหนดข้อตกลงการควบคุมการเชื่อมต่อระบบ (The Agreed and Finalized Interface Control Document : ICD)

๑๓.๒ การวิเคราะห์และออกแบบความมั่นคงปลอดภัยทางเครือข่าย

๑๓.๒.๑ ออกแบบและจัดทำผังเครือข่ายของระบบ

๑๓.๒.๒ แบ่งแยกเครือข่ายตามผังเครือข่ายที่กำหนด

๑๓.๒.๓ แยกเครื่องคอมพิวเตอร์แม่ข่ายสำหรับการทดสอบไว้ในเครือข่ายที่แยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่ายสำหรับการให้บริการจริง

๑๓.๒.๔ ศึกษาการจราจร (Traffic) ที่เข้า-ออกเครือข่ายทั้งหมด เพื่อกำหนดเป็น Traffic ที่อนุญาตและไม่อนุญาต ซึ่งเป็นการกำหนดการไหลของข้อมูลในเครือข่าย

๑๓.๒.๕ กำหนดนโยบาย (Policy) บนอุปกรณ์ไฟร์วอลล์ (Firewall) เพื่อจำกัด Traffic ที่เข้าออกเครือข่าย

๑๓.๒.๖ เปิดใช้ระบบป้องกันการบุกรุก

๑๓.๒.๗ ติดตั้งระบบป้องกันไวรัส

๑๓.๒.๘ ติดตั้งระบบ Remote Control สำหรับผู้ดูแลระบบใช้งาน

๑๓.๒.๙ ติดตั้งระบบตั้งสัญญาณนาฬิกาให้ตรง

๑๓.๓ การวิเคราะห์และออกแบบระบบงานด้านความมั่นคงปลอดภัย

๑๓.๓.๑ กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานอย่างน้อย ดังต่อไปนี้

๑) ด้านการตรวจสอบข้อมูลนำเข้าและออกจากระบบงาน

๒) ด้านการบันทึกจราจรทางคอมพิวเตอร์ (Log) ที่สำคัญและอาจจำเป็นต้องตรวจสอบในภายหลัง

๓) ด้านกลุ่มผู้ใช้งาน บทบาท และสิทธิ์การเข้าถึงระบบงาน

๔) ด้านการลงทะเบียนและถอดถอนการเข้าถึงระบบงาน

๕) ด้านการตัดหรือหมดเวลาใช้งาน

๖) ด้านการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย

๗) ด้านหน้าจอการล็อคอิน (Login) ที่มีความมั่นคงปลอดภัย

๘) ด้านการติดตามปริมาณการใช้ระบบและขีดความสามารถ หรือประสิทธิภาพของระบบ

๙) ด้านการป้องกันข้อมูลรหัสผ่าน (Password) ของผู้ใช้งาน

๑๐) ด้านการป้องกันข้อมูลสำคัญที่จัดเก็บไว้ในระบบงาน

๑๑) ด้านการป้องกันข้อมูลสำคัญที่มีการส่งผ่านเครือข่าย

๑๒) ด้านการเข้ารหัสข้อมูลและการลงลายมือชื่อดิจิตอล

๑๓) ด้านการวิเคราะห์จุดอ่อนของซอร์สโค้ด (Source Code)

๑๔) ด้านการกู้คืนระบบงาน

๑๓.๓.๒ ดำเนินการวิเคราะห์และออกแบบระบบด้านความมั่นคงปลอดภัย

๑๓.๔ การทดสอบระบบ

๑๓.๔.๑ ทดสอบระบบให้ครอบคลุมตามความต้องการด้านความมั่นคงปลอดภัยของระบบงานที่กำหนดไว้ (Security Test)

๑๓.๔.๒ กำหนดให้มีการป้องกันข้อมูลสำคัญ (Data Masking Technique)

๑) กำหนดให้เจ้าของข้อมูลลบข้อมูลส่วนที่สามารถบ่งชี้ตัวบุคคลทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบ

๒) กำหนดให้เจ้าของข้อมูลลบข้อมูลส่วนที่เป็นความลับทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบ

๑๓.๔.๓ ทดสอบโดยการป้อนอินพุท (Input) ที่จะทำให้ระบบทำงานผิดพลาด ไม่ถูกต้อง ทำให้ระบบล่ม หรือถึงขั้นระบบถูกบุกรุกได้ (Fuzzing Technique)

๑๓.๔.๔ ทดสอบและรับรองระบบ (User Acceptance Test)

๑๓.๕ การติดตั้งระบบ

๑๓.๕.๑ จัดทำแผนการติดตั้งระบบ

๑๓.๕.๒ ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ ที่เกี่ยวข้องกับระบบงานให้แล้วเสร็จ ก่อนที่จะติดตั้งตัวระบบงาน

๑๓.๕.๓ ปิดบริการ (Service) ที่ไม่มีความจำเป็นต้องใช้งานโดยตัวระบบงาน

๑๓.๕.๔ จัดทำ Security Baseline ของระบบที่จะทำการติดตั้ง

๑๓.๕.๕ ปรับแต่งค่าพารามิเตอร์ต่าง ๆ ที่มีผลต่อความมั่นคงปลอดภัยของระบบงานตาม Security Baseline ของระบบที่ได้กำหนดไว้

๑๓.๕.๖ จำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของระบบงาน หลีกเลี่ยงการติดตั้งซอร์สโค้ดของระบบงานบนเครื่องให้บริการ (ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้โดยตรงในขณะที่ทำงาน)

๑๓.๕.๗ ตรวจสอบและปิดช่องโหว่ในระบบที่ทำการติดตั้ง

๑๓.๕.๘ ติดตั้งโปรแกรมเพื่อติดตามและตรวจสอบการเปลี่ยนแปลงแก้ไขไฟล์ต่าง ๆ ของระบบโดยไม่ได้รับอนุญาต

๑๓.๕.๙ จัดทำแผนการตรวจสอบและวิเคราะห์จราจรทางคอมพิวเตอร์ (Log) บนเครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการระบบงานที่ทำการติดตั้ง

๑๓.๕.๑๐ จัดทำแผนการสำรองข้อมูลของระบบงานและดำเนินการตามแผนฯ ทดสอบการกู้ข้อมูลเป็นครั้งคราว

๑๓.๕.๑๑ จัดทำแผนการตรวจสอบและติดตามสภาพความพร้อมใช้ของระบบงานและดำเนินการตามแผนฯ

๑๓.๕.๑๒ จัดทำแผนการตรวจสอบและติดตามทรัพยากรของระบบงานและดำเนินการตามแผนฯ

๑๓.๕.๑๓ จัดทำแผนการกู้คืนระบบงานและดำเนินการทดสอบปีละครั้ง

๑๔. แนวปฏิบัติการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๑๔.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๑๔.๒ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่เก็บรักษาไว้

๑๔.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๔.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๕. แนวปฏิบัติการพัฒนาระบบสารสนเทศและความต้องการด้านความมั่นคงปลอดภัย

๑๕.๑ การตรวจสอบข้อมูลนำเข้าและออกจากระบบงาน

๑๕.๑.๑ การตรวจสอบข้อมูลนำเข้า (Input) และผลผลิต (Output) ของระบบงาน

ระบบต้องสามารถตรวจสอบข้อมูลนำเข้า และผลผลิตของระบบว่าสามารถบันทึกข้อมูลเข้าไปได้อย่างถูกต้องหรือไม่ รวมทั้งสามารถออกผลผลิตต่าง ๆ ได้อย่างถูกต้องหรือไม่ ตลอดจนมีการประมวลผลข้อมูลนำเข้า และผลผลิตที่ออกมาได้อย่างถูกต้องหรือไม่

๑๕.๑.๒ การตรวจสอบข้อมูลนำเข้าระบบงาน และความสามารถป้องกันปัญหาที่เกี่ยวข้องกับการบุกรุกต่าง ๆ อย่างน้อย ดังต่อไปนี้

๑) SQL Injection

๒) Cross-site Scripting

๓) การรับไฟล์ประเภทที่ไม่ประสงค์ดีเข้ามาในระบบงาน เช่น ไฟล์ที่เป็นไวรัส หรือไฟล์โปรแกรมที่แอบทำงานอย่างอื่นแอบแฝง เป็นต้น

๔) Insecure Direct Object Reference การรับข้อมูลนำเข้าระบบที่เป็น Object ดังนี้ File, Directory, Database Record, URL, Form Parameter ซึ่งสามารถอ้างอิงไปยังข้อมูลในระบบตามที่ต้องการ อาทิ อ้างอิงไปยังไฟล์ที่ผู้บุกรุก (Hacker) ต้องการเข้าถึง สามารถใส่ค่าที่เป็น Object ใด ๆ ก็ตามที่ต้องการทดลองดูว่าสามารถเข้าถึงได้หรือไม่ ถ้าได้ก็แสดงว่าสามารถเข้าถึงข้อมูลนั้นโดยไม่ได้รับอนุญาต ดังนั้น ระบบงานต้องทำการตรวจสอบก่อนว่าผู้ใช้งานนั้นมีสิทธิ์ในการเข้าถึง Object หนึ่งในระบบงานหรือไม่

๕) การรับค่า URL เข้ามาในระบบงานที่นอกเหนือจากที่ระบบงานต้องการหรือคาดหมาย ผู้บุกรุกสามารถเข้าถึงข้อมูลในระบบงานโดยไม่ได้รับอนุญาต โดยการทดลองเปลี่ยนค่า URL เป็นค่าต่าง ๆ เพื่อดูว่าสามารถเข้าถึงข้อมูลตาม URL ที่ทดลองเหล่านั้นได้หรือไม่

๑๕.๒ การบันทึกข้อมูลล็อคที่สำคัญและจำเป็นต้องตรวจสอบในภายหลัง

๑๕.๒.๑ การใช้งานระบบของผู้ใช้งาน เพื่อการป้องกันการปฏิเสธ

ระบบต้องสามารถบันทึกกิจกรรมการใช้ระบบของผู้ใช้งานได้

๑๕.๒.๒ การบริหารจัดการระบบของผู้ดูแลระบบ เพื่อป้องกันการปฏิเสธ

ระบบต้องสามารถบันทึกกิจกรรมการบริหารจัดการระบบของผู้ดูแลระบบได้

๑๕.๒.๓ การเข้าถึงระบบ

ระบบต้องสามารถบันทึกข้อมูลการ Login เข้าใช้งานระบบของผู้ใช้งานไม่ว่าจะสำเร็จหรือไม่ก็ตาม โดยอย่างน้อยต้องบันทึก ชื่อผู้ใช้งาน วันเวลา ที่ Login เข้าใช้งาน หมายเลข IP Address

๑๕.๓ กลุ่มผู้ใช้งาน บทบาทหน้าที่ และสิทธิ์การเข้าถึงระบบงาน

การกำหนดกลุ่มผู้ใช้งานต่าง ๆ บทบาทหน้าที่และสิทธิ์เข้าถึงระบบต้องสามารถกำหนดกลุ่มผู้ใช้งานต่าง ๆ บทบาทหน้าที่ และสิทธิ์การเข้าถึงที่เหมาะสม โดยสอดคล้องกับนโยบายควบคุมการเข้าถึงระบบงานที่กำหนดได้

๑๕.๔ การลงทะเบียน ถอดถอน และทบทวนสิทธิ์การเข้าถึงระบบงาน

การลงทะเบียนและถอดถอนผู้ใช้งานของระบบ

๑) ระบบต้องสามารถสร้างบัญชีผู้ใช้งานระบบฯ แยกออกจากกัน เช่น บัญชีผู้ดูแลระบบ บัญชีผู้ตรวจสอบ บัญชีผู้ใช้งาน เป็นต้น กล่าวคือต้องไม่อนุญาตให้สร้างบัญชีผู้ใช้งานซ้ำซ้อนกัน

๒) ระบบต้องมีหน้าจอสำหรับผู้ดูแลระบบ เพื่อทำการลงทะเบียน ถอดถอน และทบทวนสิทธิ์ของผู้ใช้งาน

๑๕.๕ การระบุและพิสูจน์ตัวตนสำหรับการเข้าใช้ระบบงาน

๑๕.๕.๑ การป้องกันข้อมูล Login เพื่อเข้าใช้งานระบบ

ระบบต้องใช้การเข้ารหัสข้อมูล เพื่อป้องกันข้อมูลการ Login เช่น ชื่อบัญชีผู้ใช้งาน และรหัสลับ เป็นต้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

๑๕.๕.๒ การกำหนดรหัสผ่านที่มีความปลอดภัย

ระบบต้องกำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่นดังนี้

๑) กำหนดให้ตั้งรหัสผ่าน ตาม**<u>แนวปฏิบัติการกำหนดรหัสผ่าน (Password) การเปลี่ยนรหัสผ่าน และการใช้งานรหัสผ่านของผู้ใช้งาน</u>**

๒) กำหนดให้ตั้งรหัสผ่านที่เป็นคำที่ผสมกันระหว่างตัวอักษร ตัวเลข และอักขระพิเศษ

๓) ไม่อนุญาตให้ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๔) ไม่อนุญาตให้ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓ abc เป็นต้น หรือเป็นกลุ่มของอักขระที่เหมือนกัน เช่น ๑๑๑๑, aaaa, bbbb เป็นต้น

๑๕.๕.๓ การบริหารจัดการรหัสผ่านที่มีความมั่นคงปลอดภัย

๑) ระบบต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตัวเอง และต้องมีขั้นตอนปฏิบัติเพื่อยืนยันรหัสผ่านใหม่ที่ตั้งอีกครั้ง

๒) ระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้โดยผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๓) ระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่โดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการ Login เข้าใช้งานระบบงานเป็นครั้งแรก

๔) ระบบต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูล Login เช่น ให้แสดงเป็นเครื่องหมายจุด หรือดอกจันทร์ บนหน้าจอ เป็นต้น

๕) ระบบต้องจัดเก็บรหัสผ่านเดิมของผู้ใช้งานไว้เป็นจำนวน ๒ ครั้ง เพื่อป้องกันการกลับไปใช้รหัสผ่าน ๒ ครั้ง ล่าสุดที่ได้เคยตั้งไว้

๑๕.๖ หน้าจอการ Login ที่มีความมั่นคงปลอดภัย

๑๕.๖.๑ การแสดงรายละเอียดและข้อมูลที่เกี่ยวกับการ Login

๑) ระบบต้องแสดงรายละเอียดของระบบงาน ภายหลังจากที่ Login สำเร็จแล้วเท่านั้น

๒) ระบบต้องแสดงข้อความเตือน หรือห้ามผู้ไม่มีสิทธิ์ หรือไม่ได้รับอนุญาตเข้าถึงระบบโดยเด็ดขาด

๓) ระบบต้องไม่มี หรือแสดงระบบให้ความช่วยเหลือใด ๆ ในระหว่างที่ทำการ Login เข้าใช้งาน เพื่อไม่ให้ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากข้อมูลดังกล่าวได้

๔) ระบบต้องสามารถแสดงวันเวลาที่ Login เข้าใช้งานครั้งที่แล้ว ทั้งที่สำเร็จและไม่สำเร็จ เพื่อให้ผู้ใช้งานได้รับทราบอย่างน้อยเป็นจำนวน ๕ ครั้ง

๕) ระบบต้องไม่มีกลไกในการจดจำรหัสผ่านเพื่อให้ผู้ใช้งานสามารถเข้าใช้ระบบได้โดยอัตโนมัติในครั้งถัดไปโดยไม่ต้องใส่รหัสผ่านได้

๑๕.๖.๒ การตัดการใช้งานกรณี Login ไม่สำเร็จ

ระบบต้องสามารถตัดการ Login ของผู้ใช้งานที่ Login ไม่สำเร็จเกินกว่า ๓ ครั้ง

๑๕.๗ การตัดหรือหมดเวลาการใช้งาน (Session time-out)

การตัดหรือหมดเวลาใช้งานระบบต้องสามารถตัดหรือหมดเวลาใช้งานหลังจากที่เข้าระบบงานมาแล้ว และไม่ได้ใช้งานหรือมีกิจกรรมกับระบบเกินกว่าช่วงระยะเวลาหนึ่งที่ได้กำหนดไว้ เช่น ๕ นาที หากไม่มีการใช้งานระบบจะตัดการใช้งาน เป็นต้น

๑๕.๘ การติดตามปริมาณการใช้ระบบและขีดความสามารถ หรือประสิทธิภาพของระบบ

การติดตามปริมาณการใช้ระบบและขีดความสามารถของระบบต้องสามารถตรวจสอบและติดตามปริมาณการใช้ทรัพยากรของระบบ เช่น การใช้หน่วยประมวลผลกลาง (Central Processing Unit : CPU) หน่วยความจำ (Memory) หน่วยบันทึกข้อมูล (Hard Disk) ของระบบ จำนวนผู้ใช้ระบบงาน ณ ที่เวลาหนึ่ง จำนวนธุรกรรมที่เกิดขึ้นต่อหน่วยของเวลา จำนวน Concurrent Session ที่อนุญาตให้ผู้ใช้งานเปิดใช้งานได้ เป็นต้น

๑๕.๙ การป้องกันข้อมูลรหัสผ่านของผู้ใช้งาน

๑) ระบบต้องทำการแปลงรหัสผ่านของผู้ใช้งานก่อนที่จะจัดเก็บไว้ในระบบ เพื่อป้องกันระบบถูกเจาะและสามารถเข้าถึงข้อมูลรหัสผ่านเหล่านั้นได้โดยง่าย โดยที่เทคนิคการแปลงรหัสผ่าน เพื่อนำไปจัดเก็บต้องยากแก่การเดาโดยผู้ไม่ประสงค์ดี

๒) ระบบต้องไม่มีการจัดเก็บข้อมูลรหัสผ่านใด ๆ ไว้ในซอร์สโค้ดของระบบงาน

๓) ระบบต้องไม่มีการส่งข้อมูลรหัสผ่านไปในเครือข่ายโดยที่ไม่มีการเข้ารหัสข้อมูลเพื่อป้องกันข้อมูลรหัสผ่านนั้น

๑๕.๑๐ การป้องกันข้อมูลที่จัดเก็บไว้ในระบบงาน

๑๕.๑๐.๑ การป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลที่เกี่ยวข้องกับการบริหารจัดการระบบโดยผู้ดูแลระบบ

ระบบต้องสามารถกำหนดสิทธิ์ผู้ที่สามารถเข้าถึงและทำการเปลี่ยนแปลงหรือแก้ไขข้อมูลที่เกี่ยวข้องกับการบริหารจัดการระบบดังนี้

๑) ข้อมูลจราจรคอมพิวเตอร์ซึ่งบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกิดขึ้น

๒) ข้อมูลทะเบียนผู้ใช้งาน

๑๕.๑๐.๒ การป้องกันข้อมูลสำคัญที่จัดเก็บไว้ในระบบ

ระบบต้องสามารถใช้การเข้ารหัสข้อมูล หรือวิธีอื่นที่เหมาะสม เพื่อป้องกันข้อมูลสำคัญที่จัดเก็บไว้ในระบบ เช่น ข้อมูลลับ ข้อมูลเงินเดือน เป็นต้น

๑๕.๑๑ การป้องกันข้อมูลสำคัญที่มีการส่งไปในเครือข่าย

ระบบต้องสามารถใช้การเข้ารหัสข้อมูล เพื่อป้องกันข้อมูลสำคัญที่มีการส่งไปในเครือข่าย และป้องกันการดักแอบดูข้อมูลนั้นในระหว่างที่มีการส่ง

๑๕.๑๒ การเข้ารหัสข้อมูลและการลงลายมือชื่อดิจิตอล

๑๕.๑๒.๑ การเข้าและถอดรหัสข้อมูลสำคัญ

ระบบต้องสามารถใช้งานกุญแจสำหรับการเข้าและถอดรหัสข้อมูลสำคัญได้

๑๕.๑๒.๒ การลงลายมือชื่อดิจิตอล

๑) ระบบต้องสามารถลงลายมือชื่อดิจิตอลกับข้อมูลที่ต้องการได้ รวมทั้งสามารถตรวจสอบได้ว่าใครเป็นผู้ลงลายมือชื่อดิจิตอล

๒) ในกรณีที่ข้อมูลที่มีการลงลายมือชื่อดิจิตอลมาถูกเปลี่ยนแปลงแก้ไขในระหว่างที่ส่งมา ระบบต้องสามารถแจ้งให้ผู้รับข้อมูลทราบว่าข้อมูลเกิดการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๑๕.๑๓ การกู้คืนระบบ

การออกแบบระบบสำหรับการกู้คืนระบบ ระบบต้องได้รับการออกแบบด้านเทคโนโลยีให้สามารถกู้คืนได้ภายในระยะเวลาที่เหมาะสม

๑๖. แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องตอบสนองต่อเหตุการณ์อย่างทันท่วงที ดังนั้น จึงต้องมีแนวปฏิบัติเมื่อเกิดเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๑๖.๑ ระบบป้องกันการบุกรุกเครือข่าย (Fire wall)

๑๖.๑.๑ ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุกอย่างน้อยเดือนละครั้ง

๑๖.๑.๒ ดำเนินการตรวจสอบบันทึกของเหตุการณ์ (Log File) และรายงานของระบบป้องกันการบุกรุกเครือข่ายสิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๑) กลุ่มข้อมูล (Packet) ที่ระบบป้องกันการบุกรุกเครือข่ายได้ปิดกั้น

๒) ลักษณะของกลุ่มข้อมูลที่ถูกปิดกั้น

๓) หมายเลขไอพีแอดเดรสของเครือข่ายใดที่ถูกปิดกั้นเป็นจำนวนมาก

๑๖.๑.๓ หากตรวจสอบพบการโจมตี หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศให้แจ้งผู้บังคับบัญชาเพื่อตัดสินใจดำเนินการแก้ไขปัญหา หากไม่สามารถแก้ไขปัญหาได้ให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑๖.๑.๔ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๑๖.๒ เครื่องคอมพิวเตอร์แม่ข่าย

๑๖.๒.๑ ต้องตรวจสอบความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายก่อนเปิดให้บริการ โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

๑) ปิด Service ที่ไม่ได้ใช้งาน

๒) ติดตั้ง NTP เพื่อเทียบเวลาให้ถูกต้อง

๓) จำกัดการเข้าถึงจาก Root หรือ Administrator โดยตรง

๑๖.๒.๒ หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และกำหนดผู้ดูแลรับผิดชอบหลัก และผู้รับผิดชอบสำรอง

๑๖.๒.๓ หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบความมั่นคงปลอดภัย ต้องจดบันทึก ตรวจสอบแก้ไข และรายงาน เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยต่อผู้บังคับบัญชา

๑๖.๒.๔ ต้องตรวจสอบ แก้ไข และรายงานช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายต่อผู้บังคับบัญชา

๑๖.๒.๕ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ต้องดำเนินการแจ้งไปยังผู้รับผิดชอบขององค์กร หรือผู้มีอำนาจที่ได้รับมอบหมาย ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๑๖.๓ ภัยคุกคามทางอินเทอร์เน็ต ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

๑๖.๓.๑ องค์กรต้องดำเนินการจัดหาซอฟต์แวร์เพื่อป้องกัน

๑๖.๓.๒ หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต ต้องดำเนินการติดตั้งโปรแกรมป้องกันภัยคุกคามทางอินเทอร์เน็ต และต้องตั้งให้ Update อย่างน้อยสัปดาห์ละครั้ง

๑๖.๓.๓ ดำเนินการตรวจสอบบันทึกของไฟล์เหตุการณ์ (Log File) และรายงานของอุปกรณ์สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๑) การคุกคามทางอินเทอร์เน็ตใดที่มีเป็นจำนวนมาก

๒) ถูกส่งมาจากที่ใด และถูกส่งไปยังที่ใด

๑๖.๓.๔ ต้องศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่มีภัยคุกคามทางอินเทอร์เน็ต โดยเฉพาะที่ตรวจพบว่ามีการกระจายภายในเครือข่ายขององค์กร

๑๖.๓.๕ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

ระดับความรุนแรงของเหตุการณ์

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	หยุดให้บริการ	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

๑๗. แนวปฏิบัติเมื่อเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย (กรณีการเข้าถึงระบบโดยไม่ได้รับอนุญาต)

๑๗.๑ เมื่อผู้ดูแลระบบได้รับแจ้งเหตุให้วิเคราะห์ว่าเป็นเหตุละเมิดประเภทใด เกิดผลกระทบอย่างไร มีวิธีรับมืออย่างไรบ้าง

๑๗.๒ ผู้ดูแลระบบรายงานให้บุคคลและหน่วยงานที่เกี่ยวข้องทราบทันที

๑๗.๓ ผู้ดูแลระบบปฏิบัติการตามวิธีรับมือเหตุละเมิดตามความเหมาะสม ในกรณีนี้อาจได้แก่ การเปลี่ยนแปลงรหัสผ่าน การแยกระบบที่มีปัญหาออก การปิดบริการที่สงสัย การปิดเส้นทางการเข้าสู่ระบบสารสนเทศ การยกเลิกบัญชีผู้ใช้งานที่ถูกใช้ในการเข้าถึงระบบโดยมิได้รับอนุญาต ในบางกรณีเจ้าหน้าที่ที่เกี่ยวข้องจะต้องค้นหาและจับกุมผู้ก่อเหตุละเมิด

๑๗.๔ ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้องรวบรวมข้อมูลและหลักฐานของเหตุการณ์

๑๗.๕ ผู้ดูแลระบบตรวจสอบว่าวิธีการรับมือที่ใช้ได้ผลหรือมีประสิทธิภาพหรือไม่ แล้วเพิ่มเติมมาตรการเพื่อลดช่องโหว่ หรือถอดแยกส่วนของระบบสารสนเทศที่มีปัญหาออก

๑๗.๖ ผู้ดูแลระบบกู้คืนระบบสารสนเทศสู่สภาพเดิม และทำรายงานแจ้งผู้ที่เกี่ยวข้อง

๑๘. แนวปฏิบัติภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย

หลังจากเกิดเหตุละเมิดความมั่นคงปลอดภัย กลุ่มงานรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ต้องสำรวจความเสียหายที่เกิดจากเหตุละเมิดการรักษาความมั่นคงปลอดภัย ตรวจสอบสาเหตุและจุดอ่อนหรือข้อบกพร่องที่ก่อให้เกิดการละเมิด ทำรายงานและทบทวนมาตราการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง เสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เพื่อพิจารณา

๑๙. แนวปฏิบัติการสำรองและกู้คืนข้อมูล

๑๙.๑ การสำรองข้อมูลในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ให้ผู้ดูแลระบบดำเนินการคัดเลือกและจัดทำระบบสำรองข้อมูล ดังนี้

๑๙.๑.๑ สำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และจัดระดับความสำคัญของข้อมูล

๑๙.๑.๒ สำรวจข้อมูล และจัดระดับความสำคัญในการสำรองข้อมูล ดังนี้

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	หยุดให้บริการ	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

๑๙.๑.๓ ต้องจัดให้มีความถี่ในการสำรองให้พอเพียง ในระบบที่มีความสำคัญสูง เครื่องที่มีความสำคัญสูงควรเพิ่มความถี่การสำรองให้มากขึ้น ดังนี้

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Web Servers Application Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่ (ธนาคารแห่งประเทศไทย) และสำรองข้อมูลที่ศูนย์คอมพิวเตอร์สำรอง
๒	Database Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	Full ๒ ครั้งต่อสัปดาห์ และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่ (ธนาคารแห่งประเทศไทย) และสำรองข้อมูลที่ศูนย์คอมพิวเตอร์สำรอง

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๓	Mail Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ็อกซ์	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่ (ธนาคารแห่งประเทศไทย) และสำรองข้อมูลที่ศูนย์คอมพิวเตอร์สำรอง
๔	Domain Control Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลงข้อมูล
		ฐานข้อมูล	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่ (ธนาคารแห่งประเทศไทย) และสำรองข้อมูลที่ศูนย์คอมพิวเตอร์สำรอง
๕	Server อื่น ๆ	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่ (ธนาคารแห่งประเทศไทย) และสำรองข้อมูลที่ศูนย์คอมพิวเตอร์สำรอง

๑๙.๑.๔ ต้องจัดทำผังหรือขั้นตอนการสำรองข้อมูล

๑๙.๑.๕ ต้องทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๙.๑.๖ ต้องจัดทำบันทึกการสำรองข้อมูล และตรวจสอบว่าการสำรองข้อมูลสำเร็จหรือไม่ แก้ไข และรายงานต่อผู้บังคับบัญชา

๑๙.๑.๗ ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงาน ในระบบที่มีความสำคัญระดับสูง โดยนำไปจัดเก็บไว้ในห้องความมั่นคงสูง ธนาคารแห่งประเทศไทย พร้อมสำรองข้อมูล ส่งไปจัดเก็บที่ศูนย์คอมพิวเตอร์สำรอง จังหวัดนครราชสีมา

๑๙.๑.๘ ต้องจัดให้มีการเข้ารหัสข้อมูลที่มีระดับความสำคัญสูง (Encrypted backup) โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๑๙.๑.๙ ต้องดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา หรือในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้

๑๙.๑.๑๐ กำหนดชนิด เช่น Full หรือ Incremental เป็นต้น และช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

๑๙.๑.๑๑ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองอย่างน้อยปีละ ๑ ครั้ง

๑๙.๒ การกู้คืนข้อมูล ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ผู้ดูแลระบบมีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงานต่อผู้บังคับบัญชา ดังนี้

๑๙.๒.๑ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้ หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๑๙.๒.๒ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้งาน ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๑๙.๒.๓ สาเหตุและวิธีการกู้คืน

สาเหตุ	วิธีการ
กรณีที่ ๑ เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source Code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด
กรณีที่ ๒ เกิดความเสียหายขึ้นกับฐานข้อมูล (Database)	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด
กรณีที่ ๓ เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ฮาร์ดแวร์ยังคงทำงานปกติ	ดำเนินการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจากโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด
กรณีที่ ๔ เกิดความเสียหายขึ้นกับฮาร์ดแวร์	ให้บริษัทผู้ดูแลแก้ไขเบื้องต้นให้ฮาร์ดแวร์สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับระบบปฏิบัติการและระบบงาน ให้บริษัทหรือผู้ได้รับมอบหมายดำเนินการติดตั้งระบบปฏิบัติการและระบบงานนั้นใหม่ โดยใช้โปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

๑๙.๓ การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) หน่วยงานที่รับผิดชอบระบบสารสนเทศ มีหน้าที่

๑๙.๓.๑ ต้องจัดทำแผนความพร้อมกรณีฉุกเฉิน โดยแผนความพร้อมกรณีฉุกเฉินต้องได้รับการเห็นชอบจากผู้บริหารประกอบด้วย

๑) การกำหนดชนิดของภัยพิบัติ

๒) ประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีระดับความสำคัญสูงติดขัดหรือไม่สามารถใช้งานได้

๓) กำหนดขั้นตอนรับมือภัยพิบัติ

๑๙.๓.๒ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๑๙.๓.๓ ทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ ๑ ครั้ง

๒๐. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒๐.๑ การตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบระบบสารสนเทศ (Internal IT Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีวิธีการปฏิบัติ ดังนี้

๒๐.๑.๑ กำหนดให้กลุ่มตรวจสอบภายในเป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศและให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อย ๑ ครั้งต่อปี

๒๐.๑.๒ มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบ ระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

๒๐.๑.๓ มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว

๒๐.๑.๔ มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

๒๐.๑.๕ มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

๒๐.๑.๖ มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

๒๐.๑.๗ มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

๒๐.๑.๘ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ

๒๐.๑.๙ มีการกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแลหรือรับผิดชอบ)

๒๐.๒ การตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ (External IT Security Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีวิธีการปฏิบัติ ดังนี้

๒๐.๒.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงขององค์กร เพื่อการตรวจสอบและประเมินความเสี่ยง ดังนี้

๑) ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๒) ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๓) ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๔) ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๒๐.๒.๒ การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๒๐.๒.๓ ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศปีละ ๑ ครั้ง

๒๐.๒.๔ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยง

๒๐.๒.๕ มาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้

๑) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น สำหรับให้ผู้ตรวจสอบใช้งาน และควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้แหล่งจัดเก็บข้อมูลอื่นที่มีข้อกำหนดการเข้าถึงข้อมูล

๓) กำหนดให้ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๔) กำหนดให้เฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลเหตุการณ์ (Event Log) แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาตโดยมีการป้องกันเป็นอย่างดี

๒๐.๓ ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ “ผู้บริหารระดับสูงสุด” เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นโดยตรง รวมถึงในกรณีที่มีการร้องเรียน และฟ้องร้องภายใต้กฎหมาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒๐.๔ รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศปีละ ๑ ครั้ง เสนอต่อคณะกรรมการบริหารเทคโนโลยีสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

๒๑. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒๑.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรม ใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมขององค์กร

๒๑.๒ จัดสัมมนาหรือประชุม เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยมีแผนการการจัดสัมมนาอย่างน้อยปีละ ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๒๑.๓ จัดทำสื่อสร้างการรับรู้ infographic ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ ประชาสัมพันธ์ผ่านช่องทาง intranet กลุ่ม LINE ต่าง ๆ และ G-Chat

๒๑.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

๒๑.๕ สร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้ผู้ใช้งานมีความรู้ ความเข้าใจ และสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๒๑.๖ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยขององค์กร

๒๑.๗ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบขององค์กร และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้ หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๔
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ระดับผู้ใช้งานภายนอกและหน่วยงานภายนอก

๑. แนวปฏิบัติหน้าที่โดยทั่วไป

๑.๑ ผู้ใช้งานภายนอก หรือผู้มาติดต่อจากหน่วยงานภายนอก ที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในองค์กร จะต้องขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์

๑.๒ ผู้ใช้งานภายนอก หรือผู้มาติดต่อจากหน่วยงานภายนอก กรณีจะขอใช้งานเครือข่ายไร้สาย ต้องทำการลงทะเบียนรหัสประจำตัวผู้ใช้งานกับส่วนยุทธศาสตร์และอำนวยการของกอง/สำนัก/กลุ่มขึ้นตรง

๑.๓ ผู้มาติดต่อจากหน่วยงานภายนอกสามารถเข้า-ออกศูนย์เทคโนโลยีสารสนเทศได้ด้วยบัตรผู้ติดต่อ

๑.๔ ผู้มาติดต่อจากหน่วยงานภายนอกที่มาติดต่อศูนย์เทคโนโลยีสารสนเทศ ต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

๒. แนวปฏิบัติการเข้าถึงระบบสารสนเทศ

การจ้างหน่วยงานภายนอกพัฒนาหรือบำรุงรักษาระบบสารสนเทศ (Outsourced Development and Maintenance) ต้องดำเนินการ ดังต่อไปนี้

๒.๑ การทำงานให้กับองค์กร จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบสารสนเทศ

๒.๒ ต้องยินยอมให้องค์กรตรวจสอบตามสัญญาการใช้บริการ เพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

๒.๓ เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๒.๔ ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

๒.๕ กรณีที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศและการสื่อสารขององค์กร ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรตามแบบฟอร์มสำหรับผู้ใช้งานภายนอก เพื่อขออนุมัติจากผู้บริหารขององค์กร

๒.๕ การเข้าถึงระบบสารสนเทศ ต้องดำเนินการ ดังต่อไปนี้

(๑) ตามสิทธิ์ในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ และระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งานเท่านั้น

(๒) ต้องพิสูจน์ตัวตนก่อนที่เข้ามาใช้งานระบบสารสนเทศ ได้แก่ ชื่อผู้ใช้งาน และรหัสผ่านสำหรับเข้าใช้งานระบบสารสนเทศ

(๓) ในระบบที่มีความสำคัญสูงต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

๓. แนวทางปฏิบัติการควบคุม เข้า-ออก ศูนย์คอมพิวเตอร์สำรอง

ผู้ใช้งานภายนอก มีแนวทางปฏิบัติดังนี้

๓.๑ ผู้ใช้งานภายนอก ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูล

๓.๒ อุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่นำเข้ามาใช้ในการปฏิบัติงาน จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์ม หรือหนังสือการขออนุญาตเข้า-ออกให้ถูกต้องชัดเจน

๓.๓ ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในบริเวณสำนักงาน ปปส. ภาค ๓ และพื้นที่ศูนย์คอมพิวเตอร์สำรอง

๓.๔ สามารถเข้า-ออกสำนักงาน ปปส. ภาค ๓ ด้วยบัตรผู้ติดต่อ “Visitor” และพื้นที่ศูนย์คอมพิวเตอร์สำรองด้วยกุญแจ หรือบัตรอื่นใด โดยสิทธิ์จะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงาน

๓.๕ พื้นที่ที่สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์ม หรือหนังสือการขออนุญาตเข้า-ออกนั้นต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

๓.๖ สามารถนำผู้ติดตามเข้ามาช่วยงานได้ แต่ทุกคนจะต้องถูกบันทึกการเข้า-ออกทุกครั้ง

๓.๗ ต้องคืนบัตรผู้ติดต่อ “Visitor” กับเจ้าหน้าที่รักษาความปลอดภัย และต้องได้รับการตรวจสอบการคืนบัตร และตรวจสอบแบบฟอร์ม หรือหนังสือการขออนุญาตเข้า-ออกว่ามีผู้ลงนามอนุญาตแล้วทุกครั้ง

๓.๘ ต้องได้รับการตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์ม หรือหนังสือการขออนุญาตเข้า-ออกและตรวจสอบอุปกรณ์ที่นำออก

๓.๙ การเข้าปฏิบัติงานภายในพื้นที่ศูนย์คอมพิวเตอร์สำรองห้ามไม่ให้นำน้ำดื่ม หรือเครื่องดื่ม และอาหาร หรือของขบเคี่ยวเข้าไปรับประทานหรือดื่ม

๓.๑๐ พื้นที่ศูนย์คอมพิวเตอร์สำรองเป็นเขตปลอดอาวุธทุกชนิดห้ามนำเข้า-ออก