ประกาศองค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ
เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามที่มีประกาศคณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัล เรื่อง นโยบายเทคโนโลยีดิจิทัล องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ ลงวันที่ ๘ กรกฎาคม ๒๕๖๔ เพื่อเป็นแนวทางการบริหารจัดการเทคโนโลยีดิจิทัล นั้น

เพื่อให้เกิดความชัดเจนในการนำไปปฏิบัติตามประกาศดังกล่าว ในการจัดการระบบเทคโนโลยีดิจิทัล และการสื่อสารขององค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้อง และการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัล ในการประชุมครั้งที่ ๑/๒๕๖๘ เมื่อวันที่ ๑๖ มกราคม ๒๕๖๘ มีมติเห็นชอบแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามเอกสารแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๓ เมษายน พ.ศ. ๒๕๖๘

(นายสุวรงค์ วงษ์ศิริ)
รองผู้อำนวยการองค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

NSM
องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ

แนวปฏิบัติ
การรักษาความมั่นคงปลอดภัย สารสนเทศ อพวช.

ฉบับปรับปรุง 2568

INFORMATION SECURITY
National Science Museum Thailand
UPDATE 2025

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(Information Security Policy)

องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (อพวช.)

คำนำ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) ขององค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (อพวช.) หรือต่อไปนี้เรียกว่า “อพวช.” เป็นแนวทางในการจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของ อพวช. ให้เป็นไปอย่างเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัยและสามารถดำเนินงาน ได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารใน ลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่ อพวช.

แนวปฏิบัติฯ ฉบับนี้ ได้กำหนดวัตถุประสงค์ ผู้รับผิดชอบ และแยกออกเป็น 20 ส่วนแนวปฏิบัติไว้อย่างชัดเจน เพื่อให้บุคลากรกองเทคโนโลยีดิจิทัลขององค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ และผู้ที่เกี่ยวข้องใช้เป็นแนวทางในการปฏิบัติงานต่อไป

กองเทคโนโลยีดิจิทัล
สำนักวิศวกรรมและการผลิตสื่อ
องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ

สารบัญ

บทนำ

1. ข้ออ้างอิงตามกฎหมาย

เป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

มาตรา 5 หน่วยงานของรัฐต้องจัดทำแนวปฏิบัติและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

มาตรา 7 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวแนวปฏิบัติและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

อพวช. จึงเห็นสมควรกำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน (Standard) และแนวปฏิบัติ (Guideline) ที่ชัดเจน

2. วัตถุประสงค์

1) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของ อพวช. ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
2) เพื่อให้ อพวช. มีการกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
3) เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับใน อพวช. ได้รับทราบ และเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด
4) เพื่อกำหนดมาตรฐานและแนวทางปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอก ที่ปฏิบัติงานให้กับ อพวช. ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ อพวช. สำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
5) เพื่อเป็นการกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศขององค์กร (CIO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่ อพวช.หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวปฏิบัติและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
6) แนวปฏิบัตินี้ต้องมีการดำเนินการตรวจสอบ ประเมิน และปรับปรุงแนวปฏิบัติและข้อปฏิบัติ ตามระยะเวลา 1 ครั้งต่อปี

3. ขอบเขตของแนวปฏิบัติที่สำคัญ

หน่วยงานของรัฐต้องจัดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

1.2 จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

1.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

4. องค์ประกอบของแนวปฏิบัติ

กำหนดแนวปฏิบัติด้านการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ แยกตามเนื้อหาสาระ เพื่อการจัดองค์ประกอบของแนวปฏิบัติ สามารถแบ่งเนื้อหาสาระได้จำนวน 20 ส่วนองค์ประกอบ อันได้แก่ 1 กลุ่มคำนิยาม และ 19 ส่วนแนวปฏิบัติและ 1 ส่วนตัวชี้วัด ดังนี้คือ

ส่วนที่ 1 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security Policy)

ส่วนที่ 2 แนวปฏิบัติการการควบคุมการเข้า-ออก ห้องควบคุมระบบเครือข่าย (Network System Control Room Policy)

ส่วนที่ 3 แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control Policy)

ส่วนที่ 4 แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

ส่วนที่ 5 แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

ส่วนที่ 6 แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Policy)

ส่วนที่ 7 แนวปฏิบัติการใช้งานอินเตอร์เน็ต (Internet Security Policy)

ส่วนที่ 8 แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

ส่วนที่ 9 แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

ส่วนที่ 10 แนวปฏิบัติป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious Software Protection Policy)

ส่วนที่ 11 แนวปฏิบัติป้องกันระบบเครือข่ายและตรวจจับการบุกรุก (Firewall & IPS Policy)

ส่วนที่ 12 แนวปฏิบัติการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

ส่วนที่ 13 แนวปฏิบัติด้านการปฏิบัติตามข้อบังคับ (Compliance Policy)

คำนิยาม

คำนิยาม ที่ใช้ในแนวปฏิบัตินี้ ประกอบด้วย

- **องค์กร** หมายถึง องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ ซึ่งใช้อักษรย่อ “ อพวช.”
- **หน่วยงานภายในองค์กร** หมายถึง หน่วยงานตั้งแต่ระดับสำนักขององค์กรลงมา ได้แก่
    1) สำนักตรวจสอบภายใน
    2) สำนักผู้อำนวยการ
    3) สำนักวิชาการพิพิธภัณฑ์วิทยาศาสตร์
    4) สำนักวิชาการพิพิธภัณฑ์ธรรมชาติวิทยา
    5) สำนักวิทยาศาสตร์สู่ชุมชน
    6) ศูนย์พัฒนาความตระหนักด้านวิทยาศาสตร์
    7) สำนักบริการผู้เข้าชม
    8) สำนักบริการกลาง
    9) สำนักนโยบายและยุทธศาสตร์
    10) สำนักวิศวกรรมและการผลิตสื่อ
    11) สำนักพัฒนาธุรกิจและเครือข่าย
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารองค์กร
- **เครือข่ายคอมพิวเตอร์ภายในองค์กร** หมายถึง เครือข่ายคอมพิวเตอร์ที่จัดให้บริการขององค์กร เช่น ระบบ WIFI LAN หรือ VPN เป็นต้น
- **เครือข่ายคอมพิวเตอร์ภายนอกองค์กร** หมายถึง เครือข่ายคอมพิวเตอร์อื่นๆ ที่ไม่ใช่เครือข่ายคอมพิวเตอร์ภายในองค์กร
- **กองเทคโนโลยีดิจิทัล** หมายถึง หน่วยงานระดับกองภายใต้สำนักวิศวกรรมและการผลิตสื่อ ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร
- **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดแนวปฏิบัติมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และให้หมายรวมถึง หน้าที่ความรับผิดชอบตาม คำสั่งที่ 58/2563 เรื่อง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศ (Chief Information Officer – CIO)

- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร
- **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ดังนี้
    - ⟹ **ผู้บริหาร** หมายถึง ผู้อำนวยการพิพิธภัณฑ์ รองผู้อำนวยการพิพิธภัณฑ์ ผู้เชี่ยวชาญ ผู้อำนวยการสำนักฯ ผู้อำนวยการกองฯ
    - ⟹ **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้า ที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
    - ⟹ **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานรัฐวิสาหกิจ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการของ อพวช.
- **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอก ที่ อพวช. อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
- **สารสนเทศ** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กร ได้ เช่น ระบบ LAN ระบบ Intranet และระบบ
  Internet เป็นต้น
  - ⇒ **ระบบ LAN และระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
  - ⇒ **ระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
- **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร** (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
  - ⇒ พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  - ⇒ พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
  - ⇒ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)
  - ⇒ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
  - ⇒ พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบหมายอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

- **จดหมายอิเล็กทรอนิกส์** (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP เป็นต้น
- **รหัสผ่าน** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย
- **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
- **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนแนวปฏิบัติด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุมคาม

ส่วนที่ 1
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security Policy)

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและจำเป็นต้องได้รับการป้องกันความปลอดภัย โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ และหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

2. ผู้รับผิดชอบ

หน่วยงานภายในองค์กร

3. แนวปฏิบัติการควบคุมการเข้า-ออก อาคาร สถานที่

3.1 จัดทำเอกสารระบุสิทธิ์ของผู้ใช้ และ “หน่วยงานภายนอก” ในการเข้าถึงสถานที่ โดยแบ่งแยกได้ดังนี้

3.1.1 องค์กรต้องกำหนดสิทธิ์ผู้ใช้ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

3.1.2 รณรงค์หรือออกกฎให้เจ้าหน้าที่องค์กรแขวนบัตรพนักงานเพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน

3.1.3 การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประจำตัวประชาชน ในอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้า-ออก พร้อมกับบัตรผู้ติดต่อ (Visitor)

3.1.4 บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในองค์กร

3.1.5 กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้า-ออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง

3.1.6 บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และ รปภ. ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

3.2 ผู้ใช้จะได้รับสิทธิ์ให้เข้า-ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

3.3 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้ ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต ทั้งนี้ จะต้องแสดงบัตรประจำตัวที่องค์กรออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้า-ออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

4. แนวปฏิบัติการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะซึ่งเสียงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

4.1 การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter)

4.1.1 มีการจัดสภาพแวดล้อมทางกายภาพ ด้านประตูทางเข้าอาคารสำนักงานในลักษณะที่ปลอดภัย เพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในองค์กร

4.1.2 มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง

4.1.3 ผนังล้อมรอบของสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในควรสร้างเป็นผนังทึบ

4.1.4 ประตูหรือทางเข้าออกของห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อคได้ เพื่อป้องกันการบุกรุกทางกายภาพ

4.1.5 บุคลากรที่ปฏิบัติงานภายในศูนย์สารสนเทศ ต้องปิดประตูและหน้าต่างให้ล็อคอยู่เสมอภายหลังเลิกงาน และนอกเวลาราชการ

4.1.6 มีการจัดระบบการรักษาความมั่นคงปลอดภัย โดยมีพนักงานรักษาความปลอดภัย (รปภ.) และควรมีการติดตั้งกล้องวงจรปิดภายในอาคารสำนักงาน เพื่อควบคุมการเข้าถึงของบุคคลภายนอก

4.2 การจัดวางและการป้องกันอุปกรณ์ (Equipment Siting and Protection)

4.2.1 ต้องจัดวางอุปกรณ์ในพื้นที่ที่ปลอดภัยและเหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในหน่วยงานหรือสำนักงานให้น้อยที่สุด

4.2.2 ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสม เพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอก

4.2.3 ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์/ระบบเครื่องคอมพิวเตอร์แม่ข่าย

4.2.4 ดำเนินการตรวจสอบ สอดส่อง ระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์/ระบบเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

4.2.5 มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน หรือไฟฟ้ากระชาก

4.3 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

4.3.1 ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรที่เพียงพอต่อความต้องการใช้งาน เช่น ระบบปรับอากาศและควบคุมความชื้น ระบบไฟฟ้าสำรอง ระบบกล้องวงจรปิด (CCTV) ระบบตรวจจับควันไฟ ระบบควบคุมประตูทางเข้า-ออกพื้นที่ (Access Door Control System) และระบบแจ้งเตือนภัยต่างๆ เป็นต้น และต้องการมีการตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

4.3.2 ต้องมีการใช้ระบบสำรองไฟฟ้าหรือยูพีเอส (UPS) กับระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า และต้องทดสอบระบบ UPS อย่างสม่ำเสมอ โดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

4.4 การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่นๆ

4.4.1 เจ้าหน้าที่ทุกคนต้องปฏิบัติ ในการป้องกันทรัพย์สิน

4.4.2 เจ้าหน้าที่ต้องออกจากระบบทันที เมื่อได้ใช้งานระบบ

4.4.3 ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อค และไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของทรัพย์สินของราชการ

4.4.4 ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่างๆ เช่น เครื่องคอมพิวเตอร์ เครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น โดยไม่ได้รับอนุญาต

4.4.5 นำเอกสารออกจากเครื่องพิมพ์ และเครื่องสำเนาเอกสารทันที ที่พิมพ์เสร็จ

4.5 มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

4.5.1 ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

4.5.2 ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการทำลายหรือจำหน่าย

4.5.3 ต้องทำการฟอร์แมต (Format) ฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์

4.5.4 ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

ส่วนที่ 2

แนวปฏิบัติการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย

(Network System Control Room Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้า-ออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่าย

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล สำนักวิศวกรรมและการผลิตสื่อ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. คำจำกัดความของผู้เกี่ยวข้อง

3.1 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศภายในห้องควบคุมระบบเครือข่าย

3.2 เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์กรที่มีสิทธิ์ในการเข้า-ออกสถานที่ อาคาร ห้อง ตามที่กำหนดในทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่

3.3 ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่างๆ ของห้องควบคุมระบบเครือข่าย

4. บทบาทและความรับผิดชอบ

4.1 ผู้อำนวยการกองเทคโนโลยีดิจิทัล

4.1.1 อนุมัติสิทธิ์เข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

4.1.2 อนุมัติกระบวนการควบคุมการเข้า-ออก ห้องควบคุมระบบเครือข่าย

4.2 ผู้ดูแลระบบ ห้องควบคุมระบบเครือข่าย

4.2.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบเครือข่าย ให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

4.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้า-ออกห้องควบคุมระบบเครือข่าย ต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กรเท่านั้น

5. แนวปฏิบัติการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย

5.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย และเจ้าหน้าที่องค์กร มีแนวทางปฏิบัติ ดังนี้

5.1.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ควรจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

5.1.2 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

5.1.3 สิทธิ์ในการเข้า-ออกห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

5.1.4 เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบเครือข่าย ตามกระบวนการที่ระบุในข้อ 6.4 “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน” (ระบุไว้ในส่วนที่ 3 เรื่อง แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ)

5.1.5 ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกห้องควบคุมระบบเครือข่าย ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่”

5.1.6 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่าย ก็ต้องมีการควบคุมอย่างรัดกุม

5.1.7 การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า-ออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

5.1.8 กรณีผู้ติดต่อจากหน่วยงานภายนอก มีความจำเป็นต้องเข้าห้องควบคุมระบบเครือข่าย เจ้าหน้าที่ผู้ดูแลระบบขององค์กรจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่อง กำกับดูแลตลอดการปฏิบัติงาน

5.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

5.2.1 ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่

5.2.2 ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์การขออนุญาตเข้า-ออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

5.2.3 ผู้ติดต่อจากหน่วยงานภายนอกต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในห้องควบคุมระบบเครือข่ายหรือศูนย์สารสนเทศ

5.2.4 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้า-ออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

5.2.5 ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้า-ออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง

5.2.6 เจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้า-ออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

5.2.7 เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้า-ออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ส่วนที่ 3

แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(Access Control Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย
3) เจ้าหน้าที่ขององค์กร และผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

3. ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

3.1 ประเภทของข้อมูลองค์กร แบ่งได้ดังนี้

3.1.1 ข้อมูลสารสนเทศด้านการบริหาร ได้แก่

- แนวปฏิบัติและแผนงานโครงการ
- ข้อมูลงบประมาณ การเงินและบัญชี
- ข้อมูลบริหารทรัพยากรมนุษย์
- ข้อมูลบริหารงานพัสดุ จัดซื้อ-จัดจ้าง/อาคารสถานที่/ยานพาหนะ
- ข้อมูลงานนิติการ
- ข้อมูลประชาสัมพันธ์และเผยแพร่ข้อมูลข่าวสาร
- ข้อมูลสารบรรณและเลขานุการ
- ข้อมูลเทคโนโลยีสารสนเทศ

3.1.2 ข้อมูลเพื่อการเผยแพร่ความรู้แก่ครู/นักเรียน/บุคคลทั่วไป ได้แก่

- ข้อมูลเกี่ยวกับโรงเรียนกรมสามัญศึกษา
- ข้อมูลเกี่ยวกับ อพวช.

- ข้อมูลรายชื่อผู้ประกอบการบริการท่องเที่ยว
- ข้อมูลปริมาณนักท่องเที่ยวต่างประเทศ
- ข้อมูลบุคคลทั่วไปที่เข้าชมพิพิธภัณฑ์วิทยาศาสตร์แยกตามประเภทเด็ก ผู้ใหญ่ นักเรียน เป็นหมู่คณะ

3.1.3 ข้อมูลนวัตกรรม/ผลงานสิ่งประดิษฐ์/วัสดุอุเทศ ได้แก่

- ข้อมูลทะเบียนชิ้นงานนิทรรศการ และวัสดุตัวอย่างตามมาตรฐานสากล
- ข้อมูลการจัดเก็บ บำรุงรักษาชิ้นงานนิทรรศการและวัสดุตัวอย่าง

3.1.4 ข้อมูลการจัดนิทรรศการ/การเผยแพร่ผลงาน

- ข้อมูลการจัดนิทรรศการ
- ข้อมูลสถิติผู้เข้าชมนิทรรศการ
- ข้อมูลการจำหน่ายบัตรเข้าชม
- ข้อมูลการสำรวจ/ศึกษาผู้เข้าชมนิทรรศการเพื่อการประมวลผล
- ข้อมูลการจัดนิทรรศการเสริม
- ข้อมูลสถิติผู้เข้าร่วมกิจกรรมเสริม
- ข้อมูลผู้เข้าร่วมโครงการ

3.1.5 ข้อมูลบริการกิจกรรม/ข้อมูลข่าวสาร/วัสดุอุเทศ

- ข้อมูลผู้ใช้บริการด้านการวิเคราะห์/ที่ปรึกษาแยกตามหัวเรื่อง
- ข้อมูลเกี่ยวกับการวิเคราะห์/ผลการวิเคราะห์
- ข้อมูลข่าวสารด้านวิทยาศาสตร์
- ข้อมูลที่เกี่ยวข้องกับวัสดุตัวอย่างที่เก็บรวบรวมไว้เพื่อจัดพิมพ์ออกเผยแพร่สิ่งตีพิมพ์ในรูปแบบต่างๆ

3.1.6 ข้อมูลส่งเสริม/สนับสนุนการวิจัย

- ข้อมูลโครงการวิจัย
- ข้อมูลติดตามประเมินผลรายงานความก้าวหน้าโครงการวิจัย
- ข้อมูลงานวิจัย
- ข้อมูลผลงานวิจัย
- ข้อมูลผู้ให้การสนับสนุนงานวิจัย/การจัดนิทรรศการ/การจัดกิจกรรมเสริม
- ข้อมูลแหล่งเงินทุนสนับสนุนงานวิจัย
- ข้อมูลสนับสนุนงานวิจัยอื่นๆ

3.1.7 ข้อมูลมาตรฐานพิพิธภัณฑ์ ว & ท
- ข้อมูลเกี่ยวกับวิธีการเก็บรวบรวมตัวอย่างการจัดการและการเก็บรักษาวัสดุตัวอย่างที่ถูกต้องทางอนุกรมวิธาน (Taxonomy) ตามมาตรฐานสากล
- ข้อมูลเกี่ยวกับมาตรฐานในการจัดตั้งพิพิธภัณฑ์วิทยาศาสตร์

3.1.8 ข้อมูลความร่วมมือต่างประเทศ/วิเทศสัมพันธ์
- ข้อมูลกิจกรรมของพิพิธภัณฑ์วิทยาศาสตร์ในต่างประเทศ
- ข้อมูลรายชื่อพิพิธภัณฑ์วิทยาศาสตร์ในต่างประเทศ
- ข้อมูลองค์กร/หน่วยงานต่างประเทศที่ให้การสนับสนุนหรือให้ความร่วมมือในการวิจัย
- ข้อมูลติดต่อประสานงานความร่วมมือกับต่างประเทศ

3.1.9 กลุ่มข้อมูลร่วมทุน/การลงทุน
- ข้อมูลศึกษาความเหมาะสมในการร่วมทุน/ลงทุนในโครงการต่างๆ
- ข้อมูลโครงการที่เข้าร่วมทุน/ลงทุน
- ข้อมูลติดตามประเมินผลโครงการที่เข้าร่วมทุน/ลงทุน
- ข้อมูลแหล่งเงินกู้

3.2 ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี

3.2.1 การกำหนดชั้นความลับ ตามความสำคัญของข้อมูลในเอกสาร กำหนดไว้ 3 ระดับ ได้แก่ ลับ ลับมาก ลับที่สุด และมีการกำหนดความรับผิดชอบ ให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสาร และการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

3.2.2 การควบคุมเอกสาร โดยกำหนดให้มีมาตรการควบคุมต่างๆ คือ การจัดทำทะเบียน การตรวจสอบการจัดทำเอกสาร การสำเนาและการแปล การโอน การส่งและการรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉิน เวลาสูญหาย รวมถึงการเปิดเผยข้อมูลในเอกสาร

3.3 เวลาที่ได้เข้าถึง

3.3.1 การเข้าถึงสารสนเทศในเวลาราชการ (09.00 – 17.00 น.)

3.3.2 การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา 09.00 – 17.00 น.)

3.3.3 การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

3.3.4 การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลาและจำนวนระยะเวลาการเข้าถึง ระยะเวลาการเข้าถึง ได้แก่ 1-3 วัน, 1 สัปดาห์, 1 เดือน, 3 เดือน, ครึ่งปีงบประมาณ, หรือตามเวลาที่ร้องขอ

3.4 ช่องทางการเข้าถึง

3.4.1 ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

3.4.2 เคาน์เตอร์บริการ (เข้าถึงได้ในเวลาราชการ)

3.4.3 โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)

3.4.4 หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)

3.4.5 ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

3.4.6 ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

3.4.7 ระบบอินเตอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

3.4.8 ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

3.4.9 เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนด)

3.4.10 การประชุมทางไกล (เข้าถึงได้ทุกช่วงเวลา)

4. แนวปฏิบัติในการควบคุมการเข้าถึงระบบ

4.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

4.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอทุก 6 เดือนเป็นอย่างน้อย ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

4.3 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

4.4 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลที่สำคัญ

4.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

5. แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

5.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องทำเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

5.2 เจ้าของข้อมูลและเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

5.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

6. แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้

6.1 การลงทะเบียนเจ้าหน้าที่ใหม่ขององค์กร

6.1.1 จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

6.1.2 ผู้ดูแลระบบจะต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิ์จากเจ้าของระบบ สำหรับการใช้งานระบบสารสนเทศและบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิ์จากผู้บริหารอย่างชัดเจน

6.1.3 ผู้ดูแลระบบจะต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

6.1.4 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และมีความสอดคล้องกับแนวปฏิบัติความมั่นคงปลอดภัยขององค์กร

6.1.5 ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

6.1.6 การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องดำเนินการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

6.1.7 การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

1) เจ้าหน้าที่ใหม่ขององค์กรกรอกข้อมูลคำขอใช้บริการลงแบบฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เช่น คำขอใช้อินเตอร์เน็ต ระบบอีเมล์ หรือระบบงานต่างๆ

2) ยื่นคำขอกับผู้อำนวยการกองเทคโนโลยีดิจิทัล หรือเจ้าหน้าที่ที่ได้รับมอบหมาย

6.1.8 การให้สิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

1) ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นต์ของผู้ขอเข้าใช้งานระบบ ลายเซ็นต์ของบุคคลผู้มีสิทธิ์อนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

3) ผู้ดูแลระบบให้สิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม

6.1.9 การแจ้งยกเลิกการใช้งานระบบเทคโนโลยีสารสนเทศ

1) หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการกองเทคโนโลยีดิจิทัลหรือผู้มีอำนาจ

2) ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

6.2 กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

6.3 ผู้ใช้ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

6.4 การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

6.4.1 ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ความรับผิดชอบ

6.4.2 การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

6.4.3 การส่งรหัสผ่านชั่วคราวให้กับผู้ใช้ ควรใช้วิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลที่สามหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

6.4.4 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

6.4.5 การกำหนดชื่อผู้ใช้หรือรหัส ID ต้องเป็นหนึ่งเดียวคือไม่ซ้ำกัน

6.4.6 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

1) ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ

2) ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

4) ควรมีการเปลี่ยนแปลงรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

6.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

6.5.1 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ระยะเวลาในการเข้าถึง ช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
2) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
4) การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น
5) ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
6) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

6.5.2 ผู้ใช้สามารถนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544

6.5.3 เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลอย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

6.6 การบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน

6.6.1 ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

6.6.2 ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ และรหัสผ่านที่กำหนดใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม

6.6.3 ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

6.6.4 ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใดๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

6.6.5 ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใดๆ ทั้งสิ้น เว้นแต่ กรณีผู้ใช้งานที่มีอำนาจอนุมัติใดๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติราชการอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้ว ให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

6.6.6 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

6.6.7 กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน 3 ครั้ง

6.6.8 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

6.6.9 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

6.6.10 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

6.6.11 ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

6.6.12 เมื่อมีปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน

6.6.13 การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และแนบเอกสาร “แนวปฏิบัติสำหรับการบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าโดยเคร่งครัด

6.7 การใช้งานรหัสผ่าน

6.7.1 เก็บรหัสผ่านไว้เป็นความลับ

6.7.2 หลีกเลี่ยงการบันทึกรหัสผ่าน เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่างๆ นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

6.7.3 เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

6.7.4 เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิพิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

6.7.5 กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

6.7.6 ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ

6.7.7 ไม่ควรให้รหัสผ่านของตนให้แก่ผู้อื่นไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

6.7.8 ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว ควรแนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างต้น สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านี้ควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

6.8 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

6.8.1 สิทธิการเข้าถึงข้อมูลของผู้ใช้ควรได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เช่น ทุกๆ 3 เดือน และทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง เป็นต้น

6.8.2 สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่ เมื่อมีการเคลื่อนย้ายบุคลากรภายในองค์กร

6.8.3 การจัดสรรสิทธิ์พิเศษควรได้รรับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อให้มั่นใจได้ว่า ไม่มีการได้สิทธิ์พิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

6.8.4 ความเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิ์พิเศษควรถูกบันทึก เพื่อการทบทวน

6.9 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

6.9.1 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงาน

6.9.2 ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

6.9.3 ผู้ดูแลระบบต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

7. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่าย

7.1 ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้ อย่างเป็นระบบ

7.2 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

7.3 ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

7.4 ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

7.5 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

7.6 ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกองค์กร ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

7.7 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

7.8 การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเตอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

7.9 IP Address ภายในของระบบงานเครือข่ายภายในองค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของกองเทคโนโลยีดิจิทัล ได้โดยง่าย

7.10 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

7.11 การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

7.12 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กองเทคโนโลยีดิจิทัล เท่านั้น

8. แนวปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

8.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

8.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

8.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ Telnet FTP หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

8.4 ควรดำเนินการติดตั้งอัพเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

8.5 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กองเทคโนโลยีดิจิทัลเท่านั้น

9. แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

9.1 ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

9.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

9.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

10. แนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากเครือข่ายภายนอกองค์กร

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

10.1 การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกล จึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

10.2 วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติตามแบบฟอร์มของกองเทคโนโลยีดิจิทัลก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

10.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

10.4 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

11. แนวปฏิบัติการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ไม่ว่าจะเป็นการเข้าสู่ระบบสารสนเทศทางอินเตอร์เน็ตหรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กรอย่างน้อย 1 วิธี สำหรับในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

11.1 การแสดงตัวตน (Identification) คือ ขั้นตอนป้อนชื่อผู้ใช้ (Username)

11.2 การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนป้อนรหัสผ่าน (Password)

ส่วนที่ 4

แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศขององค์กร โดยมีการกำหนดแนวปฏิบัติและแนวปฏิบัติควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่างๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

3.1 การใช้งานบริการเครือข่าย

3.1.1 องค์กรไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่ายขององค์กร เช่น การประกาศแจ้งความการซื้อ หรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

3.1.2 ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์กรไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

3.1.3 ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาตการบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่า เป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

3.1.4 องค์กรให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

3.1.5 บัญชีผู้ใช้งาน (UserAccount) ที่องค์กรให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่า ผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3.1.6 กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

3.1.7 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

3.1.8 ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างปฏิบัติงาน

3.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

3.2.1 ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

3.2.2 ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคลโดยการใช้รหัสผ่าน (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

3.2.3 จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานอย่างน้อย 1 วิธี

3.2.4 ต้องมีการตรวจสอบผู้ใช้งาน เมื่อมีการเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต

3.3 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์กร มีแนวทางปฏิบัติดังนี้

3.3.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องกำหนดสิทธิบุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

3.3.2 สิทธิในการเข้า-ออกห้องต่างๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย เป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

3.3.3 ต้องจัดทำระบบเก็บบันทึกการเข้า-ออก ตามกระบวนการที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

3.3.4 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

3.3.5 การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

3.4 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

3.4.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

3.4.2 ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออก ตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

3.4.3 เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

3.5 การระบุอุปกรณ์บนเครือข่าย

3.5.1 ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ตั้ง

3.5.2 กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

3.5.3 อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

3.5.4 ผู้ขอใช้บริการต้องทำหนังสือเป็นลายลักษณ์อักษรถึงกองเทคโนโลยีดิจิทัล เรื่อง “การขอเชื่อมต่อเครือข่าย” และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

3.6 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

3.6.1 ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

3.6.2 บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องควบคุมระบบเครือข่าย ระบบคอมพิวเตอร์ จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้อง และได้รับการอนุมัติจากหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

3.6.3 บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์ เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

3.6.4 ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

3.7 การแบ่งแยกเครือข่าย

3.7.1 องค์กรแบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

3.7.2 องค์กรจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

3.7.3 องค์กรติดตั้ง Firewall เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี

3.8 การควบคุมการเชื่อมต่อทางเครือข่าย

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

3.8.1 มีการตรวจสอบการเชื่อมต่อเครือข่าย

3.8.2 จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

3.8.3 ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

3.8.4 มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

3.8.5 ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

3.9 การควบคุมการจัดเส้นทางบนเครือข่าย

ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

3.9.1 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

3.9.2 กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

3.9.3 กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ส่วนที่ 5

แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติการจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

3.1 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนการปฏิบัติ สำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

3.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเตอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

3.3 ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่า 10 นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ login เข้าระบบสารสนเทศอีกครั้ง

3.4 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

3.4.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

3.4.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่มีการป้องกันในการส่งรหัสผ่าน

3.4.3 กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

3.4.4 กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

3.4.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

3.4.6 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

3.5 เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ องค์กรได้กำหนดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่องค์กรพัฒนาในรูปแบบของ Web Base Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายใน ซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายดังกล่าว

3.6 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ดังต่อไปนี้

3.6.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

3.6.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

3.6.3 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.6.4 การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

3.6.5 กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

3.6.6 กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

4. แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

4.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

4.2 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศเมื่อไม่มีการใช้งานเกิน 30 นาที ต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่

5. แนวปฏิบัติงานจากภายนอกสำนักงาน (Teleworking and Work at Home)

5.1 ต้องมีการกำหนดมาตรการและการเตรียมการต่างๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

5.2 ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

5.3 ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกล โดยผู้ไม่ประสงค์เพื่อเข้าสู่ระบบงานขององค์กร

5.4 ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว

5.5 ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน

5.6 ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟล์วอลล์ตามที่องค์กรต้องการ

5.7 ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

5.8 องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่างๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

5.9 องค์กรกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

ส่วนที่ 6
แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ในองค์กร
(Use of Personal Computer Policy)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ใช้งาน

3. แนวปฏิบัติทั่วไป

3.1 เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

3.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

3.3 ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร

3.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ของกองเทคโนโลยีดิจิทัลเท่านั้น

3.5 การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของกองเทคโนโลยีดิจิทัลเท่านั้น

3.6 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

3.7 ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาเครื่องคอมพิวเตอร์ โดยควรปฏิบัติดังนี้

3.7.1 ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

3.7.2 ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

4. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

4.2 ผู้ใช้ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4.3 ในระหว่างการพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver เมื่อไม่มีการใช้งาน โดยตั้งเวลาอย่างน้อย 10 นาที

4.4 มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

4.5 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

4.6 ซอฟต์แวร์ที่ใช้งานภายในองค์กรจะต้องมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

4.7 ซอฟต์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

4.8 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นขององค์กร เพื่อประโยชน์ทางการค้า

4.9 ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม

5. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้ปฏิบัติตามแนวทางการใช้รหัสผ่านตาม ข้อ 6.7 “การใช้งานรหัสผ่าน” (ระบุไว้ในส่วนที่ 3 เรื่อง แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ)

6. แนวปฏิบัติการป้องกันจากโปรแกรมประยุกต์ชุดคำสั่งไม่พึงประสงค์ (Malware)

6.1 เครื่องคอมพิวเตอร์ จะต้องมีการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

6.2 ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Flash Drive และ External Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.3 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

6.4 เครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กรที่ผู้ใช้ครอบครองอยู่ จะต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่องค์กรได้จัดซื้อลิขสิทธิ์ไว้เท่านั้น และผู้ใช้มีหน้าที่ในการตรวจสอบการ Update ไฟล์ป้องกันไวรัส และ Scan ไวรัส อย่างสม่ำเสมอ

7. แนวปฏิบัติการสำรองข้อมูล

7.1 ผู้ใช้ควรสำรองข้อมูลที่มีความสำคัญจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น Flash Drive CD/DVD External Hard Disk เป็นต้น

7.2 ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.3 ผู้ใช้ไม่ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

ส่วนที่ 7
แนวปฏิบัติการใช้งานอินเตอร์เน็ต
(Internet Usage Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย
3) ผู้ใช้งาน

3. แนวปฏิบัติในการใช้งานอินเตอร์เน็ต

3.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy Firewall IPS/IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น หรือผ่านช่องทางที่องค์กรไม่ได้จัดสรรไว้ให้ เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลจำเป็นและทำการขออนุญาตจากกองเทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษรแล้ว

3.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์ติดตั้งอยู่

3.3 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

3.4 ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

3.5 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

3.6 ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

3.7 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือ ภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

3.8 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

3.9 ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

3.10 ผู้ใช้ต้องตระหนักถึงความเสี่ยงในความปลอดภัยจากการใช้งานโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ต

3.11 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ส่วนที่ 8
แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
(E-mail Policy)

1. วัตถุประสงค์

กำหนดมาตรการ การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย
3) ผู้ใช้งาน

3. แนวปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

3.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การย้ายหน่วยงานที่สังกัด เป็นต้น

3.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

3.3 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

3.4 การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามข้อ 6.7 “การใช้งานรหัสผ่าน” (ระบุไว้ในส่วนที่ 3 เรื่อง แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ)

3.5 ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ Logout ออกจากหน้าจอ ตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

3.6 ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

3.7 ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3 เดือน

3.8 ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กร หรือละเมิดสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

3.9 ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่าน รับ-ส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

3.10 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

3.11 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

3.12 ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

3.13 ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ที่ไม่รู้จัก

3.14 ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร

3.15 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

3.16 ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

3.17 ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ในระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ 9

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

3.1 ผู้ใช้งานจะต้องมีบัญชีผู้ใช้งานระบบเครือข่ายขององค์กร จึงจะสามารถใช้งานระบบเครือข่ายไร้สายนี้ได้ โดยผู้ใช้จะต้องทำการลงทะเบียนกับผู้ดูแลระบบเครือข่ายขององค์กร และได้รับอนุญาตจากผู้อำนวยการสำนักที่ผู้ใช้งานสังกัดและผู้อำนวยการกองเทคโนโลยีดิจิทัลอย่างเป็นลายลักษณ์อักษร

3.2 ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ-ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

3.3 ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

3.4 ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

3.5 ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

3.6 ผู้ดูแลระบบต้องกำหนดค่าใช้ WEB หรือ WPA หรือ WPA2 ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

3.7 ผู้ดูแลระบบใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้ รหัสผ่าน ตามที่กำหนดไว้เท่านั้น ให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

3.8 ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

3.9 ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

3.10 ในการใช้งานเครือข่ายไร้สายต้องปฏิบัติตามแนวปฏิบัติความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด ทางองค์กรสงวนสิทธิ์ในการยกเลิกสิทธิ์ในการเข้าใช้เครือข่ายไร้สายโดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

ส่วนที่ 10
แนวปฏิบัติป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี
(Virus and Malicious Software Protection Policy)

1. วัตถุประสงค์

เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย
3) ผู้ใช้งาน

3. แนวปฏิบัติในการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

3.1 ก่อนนำซอฟต์แวร์จากภายนอกมาใช้งานภายในองค์กร ผู้ใช้งานต้องทำการตรวจสอบซอฟต์แวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้นๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

3.2 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์

3.3 ผู้ดูแลระบบต้องกำหนดให้โปรแกรมค้นหาไวรัสทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะที่มีการใช้ระบบด้วย นอกจากนี้ ผู้ดูแลระบบต้องมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ

3.4 ผู้ดูแลระบบต้องทำการตรวจทานระบบข้อมูล เพื่อตรวจหาไวรัสและซอฟต์แวร์อันตรายอยู่เป็นประจำ

3.5 ผู้ใช้งานต้องตรวจหาไวรัสของไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตก่อนนำไปใช้งาน

3.6 ห้ามมิให้เจ้าหน้าที่ดำเนินการใดๆ ที่เกี่ยวกับการพัฒนาไวรัสหรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

3.7 ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกองค์กรมาใช้ ผู้ใช้งานสื่อข้อมูลนั้นต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

ส่วนที่ 11

แนวปฏิบัติป้องกันระบบเครือข่ายและตรวจจับการบุกรุก (Firewall & IPS Policy)

1. วัตถุประสงค์

เพื่อควบคุมการใช้งานเครือข่าย และกรองแพ็กเก็ต (Packet) ที่ผ่านเข้ามาในเครือข่ายองค์กร

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติในการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

3.1 อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งาน บริการเครือข่ายอื่นๆ ที่เหลือ ปิดให้หมด

3.2 ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือข่าย ด้วยโปรแกรประเภท Network Scanning Tools เช่น Nmap เป็นต้น

3.3 ปิดบริการ ซอฟต์แวร์ที่ไม่จำเป็นบนไฟล์วอลล์

3.4 จำกัดบริการเครือข่ายที่ทำงานบนไฟล์วอลล์ให้มีน้อยที่สุด โดยให้แยกบริการอื่นๆ เหล่านั้นไปทำงานบนเครื่องอื่น

3.5 จำกัดชื่อบัญชีผู้ใช้บนเครื่องไฟล์วอลล์ให้มีน้อยที่สุด และไม่รันไฟล์วอลล์โดยใช้ชื่อบัญชีผู้ใช้ที่เป็น Root หรือ Administrator

3.6 เปลี่ยนรหัสผ่านสำหรับ Root หรือ Administrator ที่ผู้ขายกำหนดมาให้ ให้เป็นรหัสอื่นที่ยากต่อการเดา

3.7 ควรใช้ไฟล์วอลล์หลายชนิดรวมกัน เช่น ไฟล์วอลล์แบบกรองแพ็กเก็ต ไฟล์วอลล์แบบพร็อกซี่ เพื่อเป็นการเสริมความมั่นคงปลอดภัยในแง่มุมที่ต่างกัน

3.8 ควรใช้ระบบอื่นทำงานร่วมกับไฟล์วอลล์ ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟล์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) โปรแกรมกรองอีเมล์และกรองเว็บ (Anti Spam) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยให้สูงขึ้น

3.9 กำหนดกฎในไฟล์วอลล์ให้กรองแพ็กเก็ตที่ไม่ประสงค์ดีตามรายการช่องโหว่ ที่แพร่ระบาดอยู่ในปัจจุบันเสมอ

3.10 ป้องกันการเข้าถึงทางกายภาพต่อไฟล์วอลล์ให้มีความแข็งแกร่ง เช่น จัดทำเป็นห้องที่มีการควบคุมการเข้า-ออกอย่างเข้มงวด

3.11 หมั่นตรวจสอบกฎของไฟล์วอลล์ เพื่อกำจัดกฎที่ไม่มีความจำเป็นทิ้งไป เพื่อเพิ่มประสิทธิภาพของการประมวลผลกฎที่กำหนดไว้ของไฟล์วอลล์

3.12 เมื่อเพิ่มกฎข้อใหม่เข้าไปในไฟล์วอลล์ ตรวจสอบว่ากฎที่ใส่เข้าไปนั้นไม่ขัดแย้งกับกฎที่มีอยู่แล้วเดิม รวมทั้งทดสอบด้วยว่าไฟล์วอลล์สามารถป้องกันได้จริงตามกฎข้อใหม่นั้น

3.13 ตรวจสอบว่ากฎที่กำหนดไว้บนไฟล์วอลล์ ไม่มีข้อใดขัดแย้งกับแนวปฏิบัติความมั่นคงปลอดภัยขององค์กรอย่างน้อยควรทำปีละครั้ง

3.14 ไม่อนุญาตให้เข้าถึงไฟล์วอลล์จากทางไกล โดยโปรแกรมประเภท Telnet หรือแม้แต่ SSH โดยการเข้าถึงให้ทำได้จากตัวเครื่องไฟล์วอลล์โดยตรง

3.15 สร้างความแข็งแกร่งให้กับระบบปฏิบัติการของไฟล์วอลล์ โดยการ Update Patch อยู่เสมอ

3.16 ตรวจสอบและติดตั้งโปรแกรมอุดช่องโหว่สำหรับระบบปฏิบัติการของไฟล์วอลล์อย่างสม่ำเสมอ

3.17 ก่อนการอัพเกรดหรือแก้ไขช่องโหว่ของไฟล์วอลล์ ให้ทำสำรองข้อมูลแบบ Full Backup ของเครื่องไฟล์วอลล์นั้นเก็บไว้ก่อน หากมีปัญหาจะได้นำกลับมาติดตั้งและใช้งานได้อย่างรวดเร็ว

3.18 ใช้ไฟล์วอลล์ร่วมกันเราท์เตอร์ (Router) เพื่อป้องกันปัญหา DoS (Denial of Service) และปัญหาการเจาะระบบเข้าสู่ไฟล์วอลล์ได้โดยตรง

3.19 ใช้ไฟล์วอลล์เพื่อกั้นเครือข่ายภายใน ในกรณีที่มีความจำเป็น เช่น เครือข่ายส่วนนั้นอนุญาตให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นในการเข้าถึง

3.20 บันทึกข้อมูล Log ของการเข้าถึงไฟล์วอลล์เก็บไว้ รวมทั้ง หากไฟล์วอลล์มีขีดความสามารถในการแจ้งเตือน ให้เปิดใช้ขีดความสามารถนี้ด้วย

3.21 หากหน่วยงานอื่นต้องการนำระบบขึ้น จะต้องแจ้งกองเทคโนโลยีดิจิทัล ให้ดำเนินการเป็นกรณีไป

ส่วนที่ 12
แนวปฏิบัติการสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

1. วัตถุประสงค์

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติในการคัดเลือกการสำรองข้อมูล

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

3.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

3.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูลดังนี้

3.2.1 กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

3.2.2 กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น สำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

3.2.3 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

3.2.4 ตรวจสอบข้อมูลทั้งหมดของระบบว่า มีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น

3.2.5 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

3.2.6 ควรจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

3.3 ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูลนอกสถานที่

3.4 ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่า ยังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

3.5 จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหาย จากข้อมูลที่ได้สำรองเก็บไว้ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

4. แนวปฏิบัติในการสำรองและกู้คืนข้อมูล

เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ฮาร์ดดิสก์เสียหาย ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูบโดยผู้ใช้งานเอง โดยมีมาตรการ ดังนี้

4.1 การสำรองข้อมูล

4.1.1 ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเอง ตามความเหมาะสมของแต่ละระบบ ไม่ต่ำกว่า 1 ครั้งต่อเดือน

4.1.2 ผู้ดูแลระบบต้องตั้งค่าสำรองข้อมูลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server)

4.1.3 ผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละหนึ่งครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ให้ทดสอบบนระบบทดสอบ

4.1.4 ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร และเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย

4.2 การกู้คืนข้อมูล

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

4.2.1 ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย

4.2.2 ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

ส่วนที่ 13
แนวปฏิบัติด้านการปฏิบัติตามข้อบังคับ
(Compliance Policy)

1. วัตถุประสงค์

การปฏิบัติตามข้อบังคับด้านกฎหมายเพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมายที่เกี่ยวข้องกับการดำเนินงานขององค์กร การที่องค์กรทราบถึงข้อกำหนดต่างๆ ที่เกี่ยวข้องจะสามารถทำให้องค์กรมีความตระหนักถึงความเสี่ยงที่เกิดขึ้น รวมทั้งวางมาตรการควบคุมที่เหมาะสมได้ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการละเมิดดังกล่าว

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) กองกฎหมาย
3) สำนักผู้อำนวยการ
4) ผู้ดูแลระบบที่ได้รับมอบหมาย
5) เจ้าหน้าที่ที่ได้รับมอบหมาย
6) ผู้ใช้งาน

3. แนวปฏิบัติในการปฏิบัติตามข้อบังคับ

3.1 การปฏิบัติตามข้อบังคับด้านกฎหมาย

บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานคอมพิวเตอร์จะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานคอมพิวเตอร์กระทำผิดตามกฎหมายดังกล่าว องค์กรถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล

3.2 การปกป้องข้อมูลส่วนบุคคล

3.2.1 ข้อมูลรายละเอียดที่เกี่ยวกับการดำเนินงานขององค์กร ถือว่าเป็นข้อมูลที่มีความสำคัญ เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บริหารเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวได้

3.2.2 ข้อมูลส่วนตัวของเจ้าหน้าที่ถือว่าเป็นข้อมูลลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ เช่น เจ้าหน้าที่เอง หรือผู้ทำงานที่มีความเกี่ยวข้องเท่านั้น อย่างไรก็ดี องค์กรสงวนสิทธิ์ในการเข้าถึงข้อมูลทั้งหมดที่สร้างและเก็บอยู่ในระบบสารสนเทศขององค์กร

3.3 ลิขสิทธิ์ซอฟต์แวร์

3.3.1 ห้ามมิให้เจ้าหน้าที่นำซอฟต์แวร์ภายนอกมาใช้ในระบบประมวลผลขององค์กร โดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในหน่วยงาน โดยผู้บังคับบัญชาฯ ต้องสอบทานกับศูนย์สารสนเทศ ในเรื่องลิขสิทธิ์ขององค์กรและความเสี่ยงด้านความปลอดภัยสารสนเทศในการนำซอฟต์แวร์ดังกล่าวมาใช้ตามลำดับ

3.3.2 เจ้าหน้าที่ต้องไม่ทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

3.3.3 ซอฟต์แวร์ที่พัฒนาภายในองค์กร ทั้งโดยบุคคลอื่นหรือเจ้าหน้าที่ขององค์กรถือว่าเป็นทรัพย์สินขององค์กร องค์กรไม่อนุญาตให้เจ้าหน้าที่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินขององค์กรโดยไม่ได้รับการอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร

3.3.4 ผู้ที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรทั้งหมด ต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์ และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

3.3.5 ซอฟต์แวร์ที่ได้จัดซื้อจากภายนอกอาจมีเงื่อนไขในเรื่องลิขสิทธิ์ด้านการใช้งานที่แตกต่างกัน หน่วยงานที่รับผิดชอบด้านการจัดซื้อต้องรับผิดชอบในการศึกษาถึงเงื่อนไขดังกล่าวจากศูนย์สารสนเทศ ต้องสร้างความตระหนักถึงผู้ใช้งานซอฟต์แวร์ดังกล่าว ให้ทราบถึงเงื่อนไขต่างๆ และข้อห้ามที่เกี่ยวข้อง

3.3.6 การจัดซื้อหรือใช้ซอฟต์แวร์ของบุคคลอื่น ต้องปฏิบัติให้สอดคล้องกับข้อตกลงด้านลิขสิทธิ์ ห้ามนำซอฟต์แวร์ที่ซื้อไปติดตั้งที่คอมพิวเตอร์เครื่องอื่นนอกเหนือจากเครื่องที่ได้มีการติดตั้งแล้วตามข้อตกลงเรื่องลิขสิทธิ์ซอฟต์แวร์

3.3.7 ทำการตรวจสอบการใช้งานคอมพิวเตอร์ขององค์กรอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์คอมพิวเตอร์ทุกชนิดเป็นไปตามข้อตกลงด้านลิขสิทธิ์ซอฟต์แวร์

3.3.8 เจ้าหน้าที่ที่ฝ่าฝืน ละเมิดข้อตกลงด้านลิขสิทธิ์ของเจ้าของซอฟต์แวร์ ถือว่าเป็นการละเมิดแนวปฏิบัติความปลอดภัยสารสนเทศขององค์กร ถึงแม้การละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานขององค์กรก็ตาม เจ้าหน้าที่ต้องรับผิดชอบผลเสียหายทั้งหมด

ส่วนที่ 14
แนวปฏิบัติการสอบทานตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. วัตถุประสงค์

การสอบทานการปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มั่นใจว่าแนวปฏิบัติและมาตรฐานต่างๆ ด้านความปลอดภัยสารสนเทศมีการปฏิบัติตามอย่างมีประสิทธิผล ในทางปฏิบัติองค์กรจำเป็นต้องมีการตรวจสอบอย่างสม่ำเสมอ ทั้งทางด้านกระบวนการทำงานรวมถึงด้านเทคนิค ทั้งนี้ การตรวจสอบมิได้จำกัดเฉพาะหน่วยงานตรวจสอบหรือคณะทำงานสอบทาน แต่ยังรวมถึงการตรวจสอบภายในโดยหน่วยงานของตนเอง

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ตรวจสอบภายใน (Internal Audit) หรือคณะทำงาน
3) ผู้ตรวจสอบจากภายนอก (External Auditor)
4) หัวหน้าหน่วยงานในองค์กร
5) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
6) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติในการสอบทาน

3.1 การปฏิบัติตามแนวปฏิบัติและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1.1 ควรกำหนดให้มีคณะทำงานเฉพาะกิจที่ทำหน้าที่สอบทานระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

3.1.2 กองเทคโนโลยีดิจิทัลดำเนินการสอบทานระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติตาม ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศว่าสอดคล้องกับแนวปฏิบัติหรือไม่ โดยรายงานสรุปผลเป็นรายไตรมาสหรืออย่างน้อยทุก 6 เดือน ให้ CIO ผู้ตรวจสอบภายใน หรือ คณะทำงาน ทราบพร้อมเสนอแนะแนวทางปรับปรุงแก้ไข ในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง

3.1.3 หัวหน้างานในแต่ละหน่วยงานในองค์กรต้องรับผิดชอบในการสอบทานอย่างสม่ำเสมอถึงการปฏิบัติงานว่าสอดคล้องกับแนวปฏิบัติและกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ โดยกองเทคโนโลยีดิจิทัลรับผิดชอบในการสนับสนุนด้านการให้คำแนะนำในการปฏิบัติตามข้อกำหนดด้านความปลอดภัยสารสนเทศที่เกี่ยวข้องกับการปฏิบัติงานดังกล่าว

3.1.4 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายในหน่วยงานภาครัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง

3.1.5 รายการที่สอบทาน

3.1.5.1 การป้องกันการบุกรุกระบบ

3.1.5.2 การสำรองข้อมูล

3.1.5.3 การควบคุมการเข้าห้องควบคุมระบบเครือข่าย

3.1.5.4 การควบคุมผู้เข้า-ออกอาคาร

3.1.5.5 การซ้อมรับสถานการณ์ฉุกเฉิน

3.2 การกำกับดูแลการปฏิบัติตามด้านเทคนิค

3.2.1 CIO ต้องกำกับดูแล เพื่อให้มั่นใจว่าเจ้าหน้าที่ทราบถึงความรับผิดขอบด้านการรักษาความปลอดภัยสารสนเทศและได้มีการปฏิบัติในทางที่เหมาะสม ซึ่งอาจรวมถึงการจัดให้มีมาตรการในการวัดผลการปฏิบัติงานของเจ้าหน้าที่จากการปฏิบัติตามมาตรฐานความปลอดภัยของสารสนเทศ

3.2.2 ผู้ตรวจสอบภายในหรือคณะทำงานสอบทาน ต้องตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่ รวมทั้งการปฏิบัติตามการควบคุมเหล่านั้น

3.2.3 ในระบบสารสนเทศ โดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความปลอดภัย

3.2.4 เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ระบบงานและเอกสาร ที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

ส่วนที่ 15

แนวปฏิบัติการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Cryptographic Control)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางในการ จัดทำการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และป้องกันความลับ การปลอมแปลง เพื่อให้ได้มาซึ่งความ น่าเชื่อถือถูกต้องและความสมบูรณ์ของสารสนเทศ

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Cryptographic Controls)

3.1 มาตรการการเข้ารหัสข้อมูล (policy on the Use of Cryptographic Controls)

3.1.1 เจ้าของข้อมูลต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานสากล เช่น อัลกอริทึม RSA, DES, 3DES เป็นต้น และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศเพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

3.1.2 อัลกอริทึมที่เรียกใช้ต้องรองรับซอฟต์แวร์ประยุกต์ที่นำไปใช้งานได้เช่น PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Transport Layer Security) เป็นต้น

3.1.3 ความยาวของคีย์ในการเข้ารหัสต้องไม่น้อยกว่า 256 บิตสำหรับการเข้ารหัสแบบสมมาตร (Symmetric) และแบบไม่สมมาตร (Asymmetric) ต้องมีความยาวไม่น้อยกว่าตามที่ตกลงกันไว้

3.1.4 เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานของคีย์ที่เข้ารหัสในทุก ๆ ปีเพื่อให้สอดคล้องกับความปลอดภัยและประสิทธิภาพของเครื่องที่ดำเนินงาน

3.1.5 กรณีที่ไม่ทราบหรือต้องการข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติมให้ติดต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและแนวปฏิบัติฯ

3.2 การบริหารจัดการกุญแจ (Key Management)

3.2.1 ข้อมูลที่มีการเข้ารหัสต้องจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพโดยการดำเนินการเกี่ยวกับกุญแจทุกประเภท เช่น การสร้าง การจัดเก็บ การจัดส่ง และการเปลี่ยนควรกระทำอย่างปลอดภัยและมีการควบคุมที่เหมาะสม

3.2.2 กุญแจส่วนตัวที่ใช้ในการเข้ารหัสข้อมูลต้องถูกจัดเก็บให้เป็นความลับและจัดเก็บอย่างมั่นคงปลอดภัยเสมอ

3.2.3 การส่งกุญแจถึงผู้รับกุญแจต้องส่งผ่านในช่องทางที่มีความมั่นคงปลอดภัยเสมอ

3.2.4 กุญแจต้องได้รับการเพิกถอนทันทีเมื่อทราบว่ากุญแจมีความเสี่ยงที่จะก่อให้เกิดการล่วงละเมิดทางด้านความมั่นคงปลอดภัย เช่น เมื่อกุญแจส่วนตัว (private key) รั่วไหลไปยังบุคคลอื่น เป็นต้น

3.2.5 การเพิกถอนการใช้งานกุญแจต้องมีการแจ้งให้ผู้เกี่ยวข้องกับกุญแจหรือผู้ที่ใช้งานกุญแจทราบ โดยต้องรวมถึงรหัสกุญแจเหตุผลของการเพิกถอนวันที่และเวลาที่กุญแจถูกเพิกถอน

3.2.6 การทำ Archive กุญแจเมื่อไม่มีการใช้งานกุญแจเป็นระยะเวลานาน ต้องใช้วิธีการ Archive ที่มีความมั่นคงปลอดภัยโดยต้องมีการเข้ารหัสกุญแจที่ถูก Archive ด้วยเสมอ

3.2.7 การทำลายกุญแจต้องทำด้วยความระมัดระวังเป็นพิเศษโดยต้องทำลายด้วยวิธีการทำลายกุญแจแบบมั่นคงปลอดภัย (Secure Deletion) และต้องแน่ใจว่ากุญแจนั้นจะไม่มีความต้องการในการใช้งานถอดรหัสข้อมูลอีกในอนาคต

3.2.8 การกระทำใด ๆ ที่เกี่ยวข้องกับกุญแจต้องได้รับการจัดเก็บบันทึกอย่างมั่นคงปลอดภัยเสมอเพื่อให้สามารถตรวจสอบได้ในภายหลัง

ส่วนที่ 16

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับข้อมูล การกำหนดกระบวนการกำกับดูแลข้อมูลส่วนบุคคลสำหรับระบบสารสนเทศ (Personal Data Privacy)

1 วัตถุประสงค์

เพื่อกำหนดแนวทางในการ กำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำหรับระบบสารสนเทศและเว็บไซต์ อพวช.

2 ผู้รับผิดชอบ

1) อพวช.
2) คณะทำงานกำกับดูแลการดำเนินการตามพระราชบัญญัติข้อมูลส่วนบุคคล

3. คำจำกัดความของผู้ที่เกี่ยวข้อง

“ผู้ใช้บริการ” หมายความว่า ผู้ที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์กับ อพวช. ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject) เช่น บุคลากร ลูกจ้าง ผู้รับบริการ และผู้เข้าร่วมการวิจัย

“ผู้ดูแลระบบ” หมายความว่า ผู้ทำหน้าที่บริหารและจัดการระบบคอมพิวเตอร์ในส่วนงาน โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้งและการปรับปรุงซอฟต์แวร์ สร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้

“เจ้าหน้าที่” หมายความว่า พนักงาน และลูกจ้างของ อพวช.

“ระบบสารสนเทศ” หมายความว่า ระบบงานหรือโปรแกรมประยุกต์ที่ประกอบด้วย ฮาร์ดแวร์หรือตัวอุปกรณ์และซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่พัฒนาบนระบบเว็บแอปพลิเคชัน (Web Application) ที่ผู้ใช้งานเปิดใช้งานด้วยโปรแกรมเบราว์เซอร์ (Web Browser) หรือโมบาย (Mobile Application) ที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายข้อมูล เพื่อสนับสนุนการปฏิบัติงานของส่วนงานต่างๆ ของ อพวช. ตามวัตถุประสงค์ ภารกิจ และอำนาจหน้าที่ตามกฎหมายของ อพวช.

“เว็บไซต์”หมายความว่า แหล่งที่เก็บรวบรวมข้อมูลเอกสารและสื่อประสมที่เข้าถึงได้ผ่านอินเทอร์เน็ต เพื่อนำเสนอข้อมูลส่วนงานของ อพวช.

4. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับข้อมูลการกำหนดกระบวนการกำกับดูแลข้อมูลส่วนบุคคลสำหรับระบบสารสนเทศ (Personal Data Privacy)

4.1 ข้อมูลเบื้องต้น

4.1.1 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับข้อมูลการกำหนดกระบวนการกำกับดูแลข้อมูลส่วนบุคคลสำหรับระบบสารสนเทศ (Personal Data Privacy) จัดทำขึ้นเพื่อใช้บังคับตามประกาศ อพวช. เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล ขององค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ อพวช.

4.1.2 กำหนดขอบเขตให้การคุ้มครองข้อมูลส่วนบุคคลนี้ใช้กับการดำเนินการใดๆ ของ อพวช. ต่อข้อมูลส่วนบุคคลที่ อพวช. รวบรวม จัดเก็บ หรือตามวัตถุประสงค์เท่านั้น

4.2 การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

4.2.1 การเก็บรวบรวมข้อมูลส่วนบุคคลของ อพวช.

1) การบริการทางระบบสารสนเทศ ในแนวปฏิบัติตามประกาศนี้ จะหมายถึง ระบบสารสนเทศสำหรับผู้ใช้ที่เป็นบทบาท (User Role) ผู้ใช้บริการเท่านั้น จะไม่รวมถึง ผู้ใช้ที่เป็นบทบาทเจ้าหน้าที่หรือผู้ดูแลระบบโดยระบบสารสนเทศจะเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น ทั้งข้อมูลของผู้ใช้บริการ และของผู้ซึ่งได้รับมอบหมายหรือรับมอบอำนาจที่ถูกต้องตามกฎหมาย ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้ดำเนินการตามประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ อพวช. ซึ่ง อพวช. จะนำข้อมูลดังกล่าวไปดำเนินการตามขั้นตอนต่อไป

2) การเก็บรวบรวมข้อมูลส่วนบุคคลโดยการกรอกข้อมูลทางกระดาษ แล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์ โดย อพวช. จะเก็บข้อมูลเท่าที่จำเป็น โดยมีวิธีการดังนี้ อพวช. จะให้เจ้าหน้าที่ที่เกี่ยวข้องเป็นผู้แปลงข้อมูลส่วนบุคคลของผู้ใช้บริการที่ได้กรอกลงในระบบสารสนเทศของ อพวช. ทั้งนี้ อพวช. จะรักษาข้อมูลของการให้บริการดังกล่าวข้างต้นไว้เป็นความลับเว้นแต่กรณีอื่นๆ ตามที่กำหนดไว้ในประกาศ อพวช. เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล ขององค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (อพวช.)

3) กำหนดให้ทำการวิเคราะห์เขตข้อมูล (Field) ของข้อมูลส่วนบุคคลที่จะจัดเก็บด้วยเหตุผลของฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) หรือฐานความยินยอม (Consent Basis) และมีข้อความเตือนในครั้งแรกของการเข้าใช้ระบบสารสนเทศและเว็บไซต์ พร้อมระบุเขตข้อมูลของข้อมูลส่วนบุคคลที่จะจัดเก็บ และวัตถุประสงค์การนำไปใช้ ให้ผู้ใช้บริการทราบ โดยกรณีที่เป็นการจัดเก็บด้วยเหตุผลของฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) ให้แสดงการรับทราบ ด้วยคำว่า รับทราบ Accept และกรณีที่เป็นการจัดเก็บด้วยเหตุผลของฐานความยินยอม (Consent Basis) ให้แสดงความยินยอม ด้วยคำว่า ยินยอม / Agree

4) ควรจัดให้มีหน้าจอแสดงชื่อเขตข้อมูล (Field) ที่ชัดเจน เพื่อบ่งชี้ถึงข้อมูลส่วนบุคคลที่จะเก็บรวบรวม โดยมีเครื่องหมายระบุเขตข้อมูลให้ชัดเจนสำหรับเขตข้อมูลที่จำเป็นต้องกรอก (Required Field) และเขตข้อมูลที่ไม่จำเป็นต้องกรอก (Optional Field) โดยหากผู้ใช้บริการไม่กรอกข้อมูลที่จำเป็นต้องกรอกระบบจะไม่จัดเก็บข้อมูลของผู้ใช้บริการ และไม่สามารถดำเนินการต่อไปได้

5) จัดให้ระบบมีระยะเวลาสำหรับผู้ใช้บริการตรวจสอบข้อมูลส่วนบุคคลก่อนที่จะทำการยืนยันเพื่อให้ระบบบันทึกข้อมูลได้ถูกต้อง

4.2.2 การพัฒนาเว็บไซต์

1) ผู้ดูแลเว็บไซต์ต้องแจ้งวัตถุประสงค์ของการใช้ข้อมูลที่ได้รับมาบนหน้าแนวปฏิบัติความเป็นส่วนตัวให้ชัดเจน

2) ต้องจัดให้มีช่องทางสื่อสารแบบมั่นคงปลอดภัยกับข้อมูลส่วนบุคคล โดยการเข้ารหัสลับข้อมูลเมื่อส่งผ่านข้อมูลบนระบบเครือข่ายสื่อสาร อาทิ การใช้ SSL อนึ่ง ในกรณีที่หน่วยงานยังไม่สามารถดำเนินการเรื่อง SSL ได้ ขอให้มีแผนการดำเนินงานที่ชัดเจนและเร่งรัดกำกับติดตามได้

3) ต้องตรวจสอบเว็บไซต์กรณีส่วนงานมีการดำเนินการในประเด็น ดังต่อไปนี้

- การเก็บข้อมูลผู้ใช้บริการ
- มีระบบสมัครสมาชิก
- การรับข่าวสาร (Subscribe) การสมัครรับข้อมูลข่าวสาร (ต้องมีช่องทางให้สามารถ Unsubscribe ได้)
- การติดตั้งระบบวิเคราะห์อื่นๆบนเว็บไซต์ เช่น Google Analytics หรือ Facebook Pixels หรือ Power BI ถ้าจะใช้ต้องแจ้งและให้ผู้ใช้บริการอนุญาตทุกครั้งเมื่อมีการเปิดใช้งาน
- การใช้งานเกี่ยวกับการบอกตำแหน่ง Web Beacons หรือ GPS ถ้าจะใช้ต้องแจ้งและให้ผู้ใช้บริการอนุญาตทุกครั้งเมื่อมีการเปิดใช้งานถ้ามีการดำเนินการดังกล่าว ต้องเขียนระบุแจ้งเตือนให้ผู้ใช้บริการรับทราบด้วยว่า ข้อมูลเก็บอะไรบ้าง ถ้าไม่ได้เก็บข้อมูลที่ระบุถึงตัวตนได้สามารถเขียนแจ้งรวมกับการใช้งานคุกกี้

4) กรณีการนำเสนอหน้าเว็บของการประชาสัมพันธ์ ซึ่งมีรูปภาพที่ถ่ายติดใบหน้า ให้มีการแจ้งผู้ที่ถูกถ่ายรูปไว้ก่อน เช่น แจ้งในงาน หรือแจ้งตอนลงทะเบียน

4.2.3 การใช้งานคุกกี้ (Cookies)

1) กรณีส่วนงานมีการใช้งาน “คุกกี้” (Cookies) เพื่อช่วยอำนวยความสะดวกให้แก่ผู้ใช้บริการในการเข้าถึงเว็บไซต์และบริการธุรกรรมทางอิเล็กทรอนิกส์ของ อพวช. โดย “คุกกี้” เป็นไฟล์ข้อมูลขนาดเล็กซึ่งจะถูกส่งไปยังโปรแกรมเบราว์เซอร์ (Web Browser) ของผู้ใช้บริการและอาจมีการบันทึกลงในเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ผู้ใช้บริการใช้เข้าถึงเว็บไซต์และ

บริการธุรกรรมทางอิเล็กทรอนิกส์ของ อพวช. โดยคุกกี้มีประโยชน์สำคัญในการทำให้เว็บไซต์สามารถจดจำการตั้งค่าต่างๆ บนอุปกรณ์ของผู้ใช้บริการได้ ทำให้การเข้าใช้บริการมีความสะดวกและเป็นไปอย่างปกติทั้งนี้ ส่วนงานจะต้องมีลิงก์เกี่ยวกับการใช้งานคุกกี้ (Cookies) เพื่อให้ผู้ใช้บริการเข้าไปกดอ่านได้ซึ่งผู้ใช้บริการสามารถเลือกปฏิเสธและปิดการใช้งานคุกกี้บนโปรแกรมเบราว์เซอร์ (Web Browser) หรืออุปกรณ์ของผู้ใช้บริการได้ โดยผู้ใช้บริการยังคงสามารถเข้าเยี่ยมชมเว็บไซต์และบริการธุรกรรมทางอิเล็กทรอนิกส์ของ อพวช.ได้ แต่อาจพบบางส่วนของเว็บไซต์ไม่สามารถทำงานหรือให้บริการธุรกรรมทางอิเล็กทรอนิกส์ได้อย่างปกติ

2) กรณีผู้ดูแลระบบพัฒนาโปรแกรม“คุกกี้” ควรเก็บข้อมูลส่วนบุคคลที่จำเป็นต้องใช้เท่านั้น และไม่ควรเก็บรหัสผ่านและข้อมูลเลข CVV บัตรเครดิตไว้ในคุกกี้โดยผู้ดูแลระบบต้องมีระบบการป้องกันความมั่นคงปลอดภัยของการเก็บข้อมูลส่วนบุคคลดังกล่าว ทั้งนี้คณะทำงานอาจทำการ Audit ระบบพัฒนาโปรแกรม“คุกกี้”เป็นครั้งคราว หรือขอให้ส่วนงานส่งข้อมูลเพิ่มเติมในบางเงื่อนไข รวมถึงขอให้ปรับแก้ไขได้กรณีตรวจพบว่ามีความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลหรือความมั่นคงปลอดภัยของการเก็บข้อมูลส่วนบุคคล

4.2.3 การเก็บข้อมูลสถิติเกี่ยวกับผู้ใช้บริการ (User Information) อพวช. มีระบบสารสนเทศในการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยข้อมูลสามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ หากเป็นกรณีสถิติของรายบุคคล เพื่อประโยชน์ตามวัตถุประสงค์ ภารกิจ และอำนาจหน้าที่ตามกฎหมายของ อพวช.

4.2.4 สิทธิในการให้ข้อมูลของผู้ใช้บริการ อพวช. มีการระบุข้อมูลที่มีการจัดเก็บข้อมูลผ่านทางระบบสารสนเทศของ อพวช. โดยมีข้อมูลบางประเภทที่ผู้ใช้บริการมีสิทธิเลือกที่จะ “ให้” หรือ “ไม่ให้” ก็ได้ โดยข้อมูลที่จำเป็นต่อ การประมวลผลและการดำเนินการของการใช้ระบบสารสนเทศของ อพวช. จะมีการทำสัญลักษณ์ไว้ เช่น ระบุด้วยตัวอักษรสีแดง หรือจะมีเครื่องหมาย (*) เช่น ชื่อ-นามสกุล หมายเลขโทรศัพท์ เป็นต้น ทั้งนี้ ผู้ใช้บริการสามารถเลือกที่จะให้หรือไม่ให้ข้อมูลอื่นที่ไม่มีการทำสัญลักษณ์ดังกล่าว เช่น ชื่อกลาง เป็นต้น

4.3 การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น อพวช.อาจมีระบบสารสนเทศที่มีการเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ของผู้ใช้บริการ โดยที่ข้อมูลส่วนบุคคลของผู้ใช้บริการจะได้รับการเก็บรักษาเป็นความลับทั้งในรูปเอกสารและข้อมูลอิเล็กทรอนิกส์ รวมทั้งในระหว่างการส่งผ่านข้อมูลทุกขั้นตอน ทั้งนี้ จะอนุญาตให้เฉพาะเจ้าหน้าที่ของหน่วยงานหรือองค์กรที่เกี่ยวข้องหรือผู้มีสิทธิ ซึ่งได้ทำข้อตกลงหรือสัญญาที่เกี่ยวข้องข้างต้นในรูปแบบที่เหมาะสมกับ อพวช. เช่น สัญญาว่าจะไม่เปิดเผยข้อมูลส่วนบุคคล (Nondisclosure Agreement : NDA) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA) ข้อตกลงเปิดเผยข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) จึงจะสามารถเข้าถึงข้อมูลของ

ผู้ใช้บริการได้ ทั้งนี้ อพวช.กำหนดให้เจ้าหน้าที่ดังกล่าวต้องปฏิบัติตามแนวปฏิบัติและนโยบายการคุ้มครองข้อมูลส่วนบุคคลขององค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (อพวช.) ตามที่ประกาศไว้

4.4 การรวมข้อมูลจากที่มาหลายแห่ง อพวช. อาจนำข้อมูลส่วนบุคคลที่ผู้ใช้บริการให้ข้อมูลดังกล่าวผ่านทางระบบสารสนเทศหรือบริการธุรกรรมทางอิเล็กทรอนิกส์ของ อพวช. รวมเข้ากับข้อมูลที่ได้มาจากแห่งอื่นเพื่อทำให้ข้อมูลของ อพวช.มีความครบถ้วนและถูกต้องเป็นปัจจุบัน และเพื่อประโยชน์ตามอำนาจและภารกิจของ อพวช.

4.5 การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล อพวช.จะไม่ให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บ รวบรวมไว้ เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นกรณีที่เป็นการเปิดเผยข้อมูลตามที่กฎหมายกำหนดให้กระทำได้ หรือตามคำสั่งศาล หรือเจ้าหน้าที่ของรัฐที่มีอำนาจตามกฎหมาย ในกรณีที่มีการจ้างหน่วยงานอื่น (Outsource) ที่ดำเนินการเกี่ยวกับข้อมูลของผู้ใช้บริการ อพวช.จะกำหนดให้ผู้รับจ้างเก็บรักษาความลับและความปลอดภัยของข้อมูล โดยห้ามผู้รับจ้างนำข้อมูลดังกล่าวไปใช้นอกเหนือจากภารกิจ หรือกิจกรรมที่มอบหมายให้ดำเนินการกรณีที่ อพวช.มีความจำเป็นต้องดำเนินการส่ง หรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เว้นแต่จะได้รับความยินยอมจากผู้ใช้บริการ หรือมีกฎหมาย กำหนดให้กระทำการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

4.6 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ อพวช.จะไม่นำข้อมูลส่วนบุคคลที่เก็บรวบรวม จัดเก็บ ใช้ และเปิดเผยไปดำเนินการอื่นนอกเหนือไปจากวัตถุประสงค์ที่ได้ระบุไว้ ตามภารกิจและหน้าที่ตามกฎหมายของ อพวช.

4.7 บันทึกผู้เข้าชมเว็บ (Log Files) ระบบสารสนเทศของ อพวช.จัดให้มีการจัดเก็บข้อมูลบันทึกกิจกรรมการใช้งาน หรือการเก็บบันทึกการเข้าออกและระหว่างการเข้าใช้บริการระบบสารสนเทศของผู้ใช้บริการโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคล เช่น หมายเลขไอพี (IP Address) ประเภทของเว็บเบราว์เซอร์(Web Browser) ที่เข้าใช้งานระบบสารสนเทศ (Browser Type) ซึ่งเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ที่กำหนดให้เก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบสารสนเทศ

4.8 การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบันในกระบวนการการให้บริการระบบสารสนเทศที่ผู้ใช้บริการให้ข้อมูลส่วนบุคคล อพวช.อนุญาตให้ผู้ใช้บริการสามารถแก้ไขข้อมูลให้ถูกต้องและปรับปรุงให้เป็นปัจจุบันได้ ภายในกระบวนการที่กำหนดอาทิ หากการขอรับบริการดังกล่าว ยังไม่ได้รับการพิจารณาหรือการอนุมัติได้ ณ ที่ทำการของหน่วยงานภายใน อพวช. หรือผู้ประมวลผลข้อมูลส่วน

บุคคลที่ให้บริการในกิจการหรือกิจกรรมในระบบสารสนเทศ ทั้งนี้ หากเป็นกรณีที่คำขอรับบริการได้รับการพิจารณาหรือการอนุมัติแล้ว ผู้ใช้บริการไม่สามารถแก้ไข ปรับปรุงข้อมูลส่วนบุคคลได้

4.9 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม และป้องกันการเปลี่ยนแปลงข้อมูลดังกล่าวโดยมิชอบ อพวช.มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้บริการอย่างเหมาะสม โดยสอดคล้องตามแนวปฏิบัติและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ อพวช. นอกจากนี้ อพวช. ควรมีระบบตรวจจับและป้องกันการโจมตีของเว็บแอปพลิเคชัน (Web Application Firewall) รวมถึงการออกแบบและพัฒนาระบบความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้สามารถป้องกันการโจมตีจากผู้ไม่ประสงค์ดี ตามรายการช่องโหว่ 10 อันดับสำหรับระบบสารสนเทศบนเว็บที่เรียกว่า OWASP (Open Web Application Security Project) Top 10 Vulnerabilities เป็นอย่างน้อย และกรณีที่ส่วนงานมีระบบสารสนเทศเกี่ยวกับบริการการชำระเงินผ่านบัตรเครดิต ควรอ้างอิงมาตรฐาน Payment Card Industry Data Security Standard (PCI DSS) ซึ่งเป็นมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีการจัดการเกี่ยวกับข้อมูลบัตรเครดิต ในการเก็บรักษา ประมวลผล และรับส่งข้อมูลบัตรได้อย่างมั่นคงปลอดภัย ให้สามารถป้องกันการฉ้อโกงซึ่งเกิดจากการทำธุรกรรมผ่านบัตรชำระเงิน

ส่วนที่ 17

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยในการติดต่อสื่อสารและเครือข่ายขององค์กร (Communications and Network Security Management)

1. วัตถุประสงค์

เพื่อกำหนดเป็นแนวทางในการ ป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายขององค์กร

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของ อพวช. ในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศบนระบบเครือข่ายให้มีความมั่นคงปลอดภัย

3.1 การป้องกันการใช้งานเครือข่าย (Network Controls) ผู้ดูแลระบบต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

3.1.1 ระบบเครือข่ายภายใน อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่ายเพื่อการทำงานภายใน อพวช. ประกอบด้วย Router, Switch และ HUB มีข้อปฏิบัติดังนี้

1) อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่ายต้องปิด Service Port ที่ไม่จำเป็น และในการส่ง ข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password
2) การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะสามารถกระทำได้ก็ต่อเมื่อได้รับ อนุญาต
3) ผู้ดูแลระบบต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ
4) ผู้ดูแลระบบต้องติดตั้งอุปกรณ์ซอฟต์แวร์ระบบ การเข้ารหัสข้อมูลอัตโนมัติหรือ ระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ
5) ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลลับหรือส่งผ่าน เครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

3.1.2 ระบบ Remote Access อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้ งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS), Remote VPN, Remote Router มีข้อปฏิบัติดังนี้

1) อุปกรณ์ RAS จะต้องทำ Harden และบันทึกการทำ Configuration Set up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
2) เมื่อเสร็จสิ้นการทดสอบการใช้งานอุปกรณ์ RAS แล้วให้ลบ User/Password ที่ใช้ในงานทดสอบทันที
3) อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้จะต้องไม่มีค่า Default Community, Default Username และ Default Password

3.1.3 อุปกรณ์ Server ที่ติดตั้งเพื่อการทำงานภายใน อพวช. มีข้อปฏิบัติดังนี้

1) ผู้ดูแลระบบต้องไม่ใช้ Default Username/Default Password
2) ต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ Server และจัดทำเป็นเอกสารทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
3) ให้เปิด Service Port ที่จำเป็นเท่านั้นส่วน Port ที่ไม่ใช้งานให้ปิดทั้งหมด และต้องมีการบันทึกการติดตั้ง Service Patch ทุกครั้ง
4) ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ
5) เมื่อจบการใช้งานที่ Console ต้อง Log - off User นั้นโดยทันที
6) ผู้ดูแลระบบต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ 2 ครั้งโดยสอดคล้องกับความสำคัญของระบบ

3.1.4 อุปกรณ์ PC Terminal มีข้อปฏิบัติดังนี้

1) ให้เปิด Service Port ที่จำเป็นเท่านั้นส่วน port ที่ไม่ใช้งานให้ทำการปิดให้หมดและต้องมีการบันทึกการติดตั้ง Service Patch ทุกครั้ง
2) ต้องติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น
3) การ Remote Terminal Console เมื่อไม่ใช้งานแล้วจะต้อง Log off ทุกครั้ง

3.1.5 การป้องกันการใช้งานเครือข่าย

1) ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของ อพวช. โดยไม่ได้รับอนุญาต
2) ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย เช่น การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของ อพวช. เอง

3.1.6 ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย (Security of Network Services) ต้องจัดทำข้อกำหนดหรือข้อตกลงของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกัน ซึ่งมีแนวทางปฏิบัติดังนี้

1) ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิของผู้ใช้งาน เพื่อควบคุมให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
2) ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน
3) ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย
4) ระบบเครือข่ายทั้งหมดของ อพวช. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก อพวช. ต้องมีการใช้อุปกรณ์หรือซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย
5) ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง อพวช. และต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เท่านั้น หากเป็นไปได้ควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของ อพวช. ทั้งทาง Physical และ Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย อพวช. ได้โดยอิสระ
6) การแบ่งแยกเครือข่าย (Segregation in Networks) ผู้ดูแลระบบต้องจัดแบ่งระหว่างเครือข่ายภายในและเครือข่ายภายนอก (Segregation in Networks) โดยพิจารณาจากบริการเครือข่ายของกลุ่มผู้ใช้งานทั้งสองฝ่าย

ส่วนที่ 18

แนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ

(IT Asset, Data and Information Security Management)

1. วัตถุประสงค์

เพื่อกำหนดเป็นแนวทางในการป้องกันความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ ทั้งภายในและภายนอกองค์กร

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล
2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติด้านการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer) ในการรักษาไว้ซึ่งความมั่นคงปลอดภัยในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งภายในองค์กร และกับหน่วยงานภายนอก

3.1 ขั้นตอนปฏิบัติสำหรับการแลกข้อมูลเปลี่ยนสารสนเทศ (Information Transfer Policies and Procedures) ขั้นตอนปฏิบัติและมาตรการสำหรับการถ่ายโอนข้อมูลสารสนเทศ เพื่อป้องกันปัญหาของการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กร โดยผ่านทางช่องทางการสื่อสารทุกชนิด ควรพิจารณาดังต่อไปนี้

1) การป้องกันจากการถูกดักจับคัดลอกแก้ไขส่งผิดเส้นทางและการทำลายข้อมูล
2) การตรวจจับและป้องกัน Source Code ที่ไม่พึงประสงค์ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์
3) การป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร (Attachment File)
4) แนวทางปฏิบัติต้องสอดคล้องกับแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)
5) การสื่อสารไร้สายต้องคำนึงถึงความเสี่ยงจะที่เกิดขึ้นด้วย
6) ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ ไม่ฝ่าฝืนแนวปฏิบัติหรือกฎระเบียบของ อพวช. เช่น การหมิ่นประมาท การข่มขู่หรือ ก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ เป็นต้น
7) เทคนิคการเข้ารหัสเพื่อปกป้องความลับความสมบูรณ์และความถูกต้องของสารสนเทศ
8) แนวทางในการเก็บรักษาและทำลายจดหมายธุรกิจต้องเป็นไปตามที่กฎหมายกำหนด
9) ไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

10) ควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่น การส่งต่ออีเมลอัตโนมัติไปนอก อพวช.
11) เตือนผู้ใช้งานให้มีความระมัดระวัง เช่น ข้อมูลสำคัญต้องไม่รั่วไหลโดยการดักฟังหรือได้ยินแบบไม่ตั้งใจในขณะใช้โทรศัพท์
12) เตือนผู้ใช้งานเกี่ยวกับปัญหาในการใช้เครื่องโทรสาร เช่น การเข้าถึงของผู้ที่ไม่ได้รับอนุญาตเพื่อดึงข้อมูลภายในเครื่องที่จัดเก็บไว้ การตั้งโปรแกรมในการส่งไปยังเลขหมายปลายทางโดยตั้งใจและไม่ตั้งใจการส่งเอกสารหรือข้อความผิดเลขหมายโดยการโทรที่ผิดพลาดหรือบันทึกเลขหมายผิด เครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่จะมีหน่วยความจำในการเก็บเอกสารบางหน้าหรือการส่งที่ ผิดพลาดซึ่งจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

3.2 ข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศ (Agreements on Information Transfer) ในการแลกเปลี่ยนข้อมูลสารสนเทศ ควรคำนึงถึงความปลอดภัยในการแลกเปลี่ยน ดังต่อไปนี้

1) การบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสารการส่งและการรับ
2) การแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสารการส่งและการรับ
3) กระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้
4) มาตรฐานทางเทคนิคขั้นต่ำในการบรรจุและส่งออก
5) สัญญาข้อตกลง
6) มาตรฐานในการระบุตัวผู้ส่งเอกสาร
7) ใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญเพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและเป็นการปกป้องสารสนเทศอย่างเหมาะสม
8) ความเป็นเจ้าของและความรับผิดชอบสำหรับการปกป้องข้อมูลลิขสิทธิ์การปฏิบัติตาม
9) ใบอนุญาตการใช้งานซอฟต์แวร์และค่าตอบแทนต่าง ๆ
10) การควบคุมพิเศษที่จำเป็นในการปกป้องข้อมูลสำคัญ เช่น กุญแจรหัส

3.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) การป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์ควรพิจารณา ดังต่อไปนี้

1) ปกป้องข้อความจากผู้ที่ไม่ได้รับอนุญาตไม่ให้มีการแก้ไขข้อความหรือปฏิเสธบริการ (Denial of Service)
2) ต้องมั่นใจว่าที่อยู่ปลายทางและการส่งข้อความถูกต้อง
3) มีความน่าเชื่อถือและสามารถใช้บริการได้
4) ข้อกำหนดทางกฎหมาย เช่น การใช้ลายมืออิเล็กทรอนิกส์
5) การใช้บริการแบบสาธารณะ ต้องระวังในการรับ - ส่งข้อมูลที่เป็นความลับของ อพวช. เช่น การ Chat การแชร์ไฟล์เป็นต้น
6) การระบุตัวตนในการควบคุมการเข้าถึงจากระบบเครือข่ายสาธารณะจะต้องเข้มงวด

3.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-disclosure Agreements)

ต้องจัดให้มีการลงนามในสัญญาระหว่างผู้ใช้งานและ อพวช. ว่าจะไม่เปิดเผยความลับของ อพวช. ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 3 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว พนักงาน ลูกจ้าง และบุคลากรจากหน่วยงานภายนอก รวมถึงนักศึกษาฝึกงานทุกคน จะต้องลงนามในสัญญารักษาความลับ (หรือสัญญาไม่เปิดเผยข้อมูล) ซึ่งเป็นส่วนหนึ่งของเงื่อนไขและข้อกำหนดในการจ้างหรือการฝึกงาน โดยให้จัดเก็บหลักฐานการลงนาม เพื่อพร้อมรับการตรวจสอบ

ส่วนที่ 19

แนวปฏิบัติในการจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

1. วัตถุประสงค์

เพื่อให้เป็นความมั่นคงปลอดภัยด้านสารสนเทศเป็นข้อกำหนดสำคัญในการจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ และเพื่อให้มีการทดสอบระบบสารสนเทศตามข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศ

2. ผู้รับผิดชอบ

1) เจ้าของระบบสารสนเทศ
2) ผู้ดูแลระบบคอมพิวเตอร์
3) ผู้พัฒนาระบบสารสนเทศ

3. อ้างอิงมาตรฐาน

1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
2. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

4. แนวปฏิบัติ

4.1 แนวปฏิบัติด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Requirements of Information Systems) เพื่อเป็นส่วนประกอบสำคัญในการบริหารจัดการระบบสารสนเทศตลอดวงจรของชีวิตของการพัฒนาระบบ ทั้งนี้ รวมถึงระบบสารสนเทศที่ให้บริการบนเครือข่ายสาธารณะด้วย

4.1.1 การจัดทำข้อกำหนดด้านความมั่นคงปลอดภัย (Information Security Requirements Analysis and Specification)

1) ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศจะต้องถูกระบุไว้ในข้อกำหนดในการพัฒนาระบบใหม่หรือการปรับปรุงระบบที่มีอยู่เดิม โดยข้อกำหนดควรครอบคลุมหัวข้อต่อไปนี้

(1.1) การพิสูจน์ตัวตนและการกำหนดสิทธิของผู้ใช้งานระบบ

(1.2) บทบาทหน้าที่ของผู้ใช้งานระบบและเจ้าหน้าที่ดูแลระบบ

(1.3) แนวทางในการป้องกันสินทรัพย์ที่เกี่ยวข้อง โดยเฉพาะในด้านการรักษา ความลับ การรักษาความสมบูรณ์และความพร้อมใช้

2) ข้อกำหนดด้านความมั่นคงปลอดภัยจะต้องถูกระบุไว้ในเอกสารข้อกำหนด (Terms of Reference (TOR)) และ/หรือในขั้นตอนการเก็บข้อมูลความต้องการของผู้ใช้ในระหว่างการพัฒนาหรือการ ปรับปรุงระบบ

3) ในการจัดทำข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการจัดซื้อจัดจ้างทรัพยากรสารสนเทศนั้น ควรครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้

(3.1) มีระบบในการการระบุและพิสูจน์ตัวตน (User Identification and authentication)

(3.2) มีระบบควบคุมและตรวจสอบสิทธในการเข้าถึง (Access control and authorization)

(3.3) มีกระบวนการหรือการป้องกันข้อมูลให้มีความครบถ้วนสมบูรณ์ (Integrity Protection)

(3.4) สามารถรองรับการตั้งค่าเพื่อใช้ในการตรวจสอบระบบ (Audit Requirements)

(3.5) สามารถกำหนดค่าต่างๆ ในระบบให้สอดคล้องกับข้อกำหนดในแนวปฏิบัติของศูนย์ปฏิบัติการ soc (System Configuration)

(3.6) สามารถรองรับการปฏิบัติตามข้อกำหนดเชิงกฎหมาย และระเบียบปฏิบัติ อื่นๆ ที่เกี่ยวข้อง

(3.7) สามารถรองรับหรือสนับสนุนการกู้คืนระบบในกรณีเกิดเหตุการณ์ภัยพิบัติ (Disaster Recovery)

(3.8) การรักษาความลับในการพัฒนาระบบสารสนเทศ เพื่อไม่ให้บุคคลภายนอก ทราบ (Need for development confidentiality) เป็นต้น

4) กำหนดให้มีการตรวจสอบความถูกต้องในการติดตั้งระบบ และความถูกต้องในการทำงานของฟังก์ชั่นต่างๆ ในแต่ละขั้นตอนของการพัฒนาระบบ (The development lifecycle) โดยจากทีมพัฒนา ระบบและ/หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย (Security Specialist) เพื่อให้แน่ใจว่ามาตรการด้าน ความมั่นคงปลอดภัยที่ได้กำหนดขึ้นมานั้นได้ถูกนำไปออกแบบ พัฒนา และทดสอบ ตามที่กำหนดไว้

5) ข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ข้างต้น จะต้องถูกนำมาใช้ในการประเมินก่อนการจัดซื้อซอฟต์แวร์สำเร็จรูปมาใช้ในการให้บริการของฝ่าย อพวช. ด้วยเช่นกัน

6) การจัดซื้อจัดจ้างภายในขอบเขตการดำเนินงานของเอกสารแนวปฏิบัติฉบับนี้ให้มีการดำเนินงานตามกระบวนการจัดซื้อ จัดจ้างของ อพวช.

4.1.2 การป้องกันบริการแอปพลิเคชันบนเครือข่ายสาธารณะ (Securing Application Services on Public Networks) สารสนเทศของบริการแอปพลิเคชันต่าง ๆ ที่มี การส่ง ผ่านทาง เครือข่ายสาธารณะต้อง มีการป้องกันจากการฉ้อโกง การปฏิเสธ การเปิดเผยและการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต โดยต้องมี การพิจารณาส่วนต่อไปนี้

1) สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly Available Information) การป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะครอบคลุมถึงซอฟต์แวร์ ข้อมูล และสารสนเทศอื่น ๆ ที่ต้องการความถูกต้องในระดับสูงที่จะถูกเผยแพร่ออกสู่สาธารณะ จะต้องมีการ ป้องกันที่ดีเช่น ลายมือชื่ออิเล็กทรอนิกส์ การเข้าถึงจากเครือข่ายสาธารณะควรจะตรวจสอบความผิดพลาดต่าง ๆ และได้รับการอนุมัติก่อนควรมีการควบคุม ดังต่อไปนี้
2) สารสนเทศนั้นต้องเป็นไปตามกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูล
3) สารสนเทศที่นำเข้าและประมวลผลโดยระบบจะต้องสมบูรณ์และถูกต้อง ตามสภาวะกาล
4) สารสนเทศสำคัญจะต้องถูกปกป้องในระหว่างที่มีการรวบรวมประมวลผล และจัดเก็บ การป้องกันการโจมตีจากหน้าเว็บไซต์เพื่อไม่ให้มีการเข้าถึงเครือข่ายของ อพวช.

4.1.3 การป้องกันธุรกรรมของบริการแอปพลิเคชัน (Protecting Application Services Transactions)

1) เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ - ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายการเปลี่ยนแปลงสารสนเทศการเปิดเผยสารสนเทศหรือการสำเนาสารสนเทศโดยไม่ได้รับอนุญาตเส้นทางการสื่อสารระหว่างคู่ค้ามีการเข้ารหัส
2) ข้อตกลงที่ใช้ในการสื่อสารระหว่างคู่ค้ามีความมั่นคงปลอดภัยต้องมั่นใจว่าข้อมูลที่เกี่ยวกับรายละเอียดในการทำธุรกรรมไม่สามารถเข้าถึงได้จาก เครือข่ายสาธารณะ เช่น เก็บไว้ใน Intranet และไม่สามารถเข้าถึงโดยผ่าน Internet ได้
3) เมื่อมีการใช้อำนาจที่เชื่อถือได้ เช่น ลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรองอิเล็กทรอนิกส์จะถือได้ว่ากระบวนการจัดการนั้นมีความมั่นคงปลอดภัย

4.2 แนวปฏิบัติด้านความมั่นคงปลอดภัยในการพัฒนาระบบและกระบวนการสนับสนุน (Security in Development and Support Processes) เป็นองค์ประกอบสำคัญในการออกแบบและพัฒนาระบบสารสนเทศ

4.2.1 แนวปฏิบัติการพัฒนาระบบอย่างปลอดภัย (Secure Development)

1) ระบบสารสนเทศต้องได้รับการพัฒนาในสภาพแวดล้อมที่มีความมั่นคงปลอดภัยทั้งทางกายภาพ (Physical) และทางตรรกะ (Logical) เช่น สถานที่ที่ใช้ในการพัฒนาระบบต้องไม่สามารถเข้าถึงโดยผู้ไม่เกี่ยวข้องได้โดยง่าย เป็นต้น
2) การพัฒนาระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของการ

พัฒนาซอฟต์แวร์ (Software Development Lifecycle) โดยครอบคลุมตั้งแต่ขั้นตอนการรวบรวมความ ต้องการ การออกแบบ การพัฒนา การทดสอบ การใช้งานตลอดไปจนถึงการยกเลิกการใช้งานระบบ

3) ขั้นตอนการพัฒนาระบบสารสนเทศต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ โดยคำนึงถึงความต้องการในด้านต่าง ๆ ดังต่อไปนี้
   (1) การป้องกันข้อมูลจากการถูกเปิดเผยโดยไม่ได้รับอนุญาต (Protection from disclosure)
   (2) การป้องกันข้อมูลจากการถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต (Protection from alteration)
   (3) ความต้องการด้านความพร้อมใช้งาน (Availability) ของข้อมูลและระบบ สารสนเทศ
   (4) การพิสูจน์ตัวตนของผู้ใช้งานและผู้ดูแลระบบ (Authentication)
   (5) การจัดการสิทธิในการใช้งานระบบ (Authorization)
   (6) ความต้องการในการตรวจสอบ และจัดเก็บประวิ'ติการใช้งาน (Auditing/Logging)
   (7) การป้องกันการปฏิเสธการทำรายการ (Non-repudiation)
   (8) การบริหารจัดการค่าการปรับแต่ง (Configuration), เซสชั่น (Session) และการจัดการกับข้อผิดพลาดที่เกิดขึ้น (Exceptions handling)
   (9) ความต้องการด้านสมรรถนะ (Capacity) ของระบบสารสนเทศ
   (10) ความต้องการด้านความมั่นคงปลอดภัยอื่น ๆ ที่สอดคล้องกับข้อกำหนด กฎหมาย หรือกฎระเบียบที่องค์กรต้องปฏิบัติตาม
4) ต้องกำหนดจุดทบทวนด้านความมั่นคงปลอดภัย (Security Checkpoint) ในแต่ละระยะ (Phrase) การดำเนินงานของโครงการ เช่น มีการกำหนด ให้มีการสอบทานด้านความมั่นคงปลอดภัยในขึ้นตอน การออกแบบ การพัฒนา การทดสอบ และก่อนการใช้งานจริง เป็นต้น
5) ต้องรักษาความปลอดภัยของพื้นที่ที่ใช้ในการจัดเก็บข้อมูล (Repositories) อย่าง เหมาะสม เช่น มีการกำหนดและจำกัดสิทธิในการเข้าถึงฐานข้อมูล เป็นต้น
6) ผู้พัฒนาระบบสารสนเทศต้องได้รับการอบรมความรู้ด้านการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย เช่น Secure Coding เป็นต้นรวมถึงความรู้เกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัย สารสนเทศเป็นประจำทุกปี

4.2.2 ขั้นตอนการปฏิบัติงานในการควบคุมการเปลี่ยนแปลง (System Change Control Procedures) การเปลี่ยนแปลงระบบงานใด ๆ จะต้องมีการควบคุมเพื่อไม่ให้มีผลกระทบต่อซอฟต์แวร์ ประยุกต์ (Application Software) ซอฟต์แวร์ระบบ (System Software) ระบบเครือข่าย (Network System) หรือการเปลี่ยนแปลงอื่นๆ ที่เกิดจากการเปลี่ยนแปลงระบบงาน เช่น การพัฒนา

ระบบการทดสอบระบบจะต้องอยู่ภายใต้การควบคุมที่เหมาะสมและเพียงพอ โดยวิธีการดังกล่าวจะช่วยให้ระบบสารสนเทศนั้นๆ สามารถทำงาน เข้ากัน ได้ทั้ง ด้านฮาร์ดแวร์และซอฟต์แวร์ การเปลี่ยนแปลงแก้ไขควรมีคำขอการ เปลี่ยนแปลงอย่างเป็นทางการซึ่งมีการอนุมัติในส่วนที่มีอำนาจอนุมัติการเปลี่ยนแปลงระบบงานนั้น ๆ

1) ความต้องการในการขอให้มีการเปลี่ยนแปลง

(11) ผู้ร้องขอ ต้องดำเนินการตามกระบวนการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริงหรือใช้งานอยู่แล้ว โดยทำหนังสือ แจ้ง ไป ยัง หน่วยงานเจ้าของข้อมูลหน่วยงานเจ้าของระบบงานและหรือหน่วยงานที่เกี่ยวข้องทุกส่วนให้รับทราบก่อนทำการแก้ไขซอฟต์แวร์นั้น และต้องมี การอนุมัติ โดยผู้เป็นเจ้าของซอฟต์แวร์ดังกล่าว และปฏิบัติตามระเบียบการปฏิบัติงาน เรื่อง การจัดการกับการแก้ไขเปลี่ยนแปลง

(12) ทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน จะต้องมีการจัดเตรียมและปรับปรุงคู่มือในการใช้งานระบบงานและคู่มือในการอบรมให้กับผู้ใช้งานต้องมีการจัดทำและปรับปรุงให้สอดคล้องกับการ เปลี่ยนแปลงระบบงานอยู่เสมอ

2) การกำหนดบทบาทและหน้าที่การเปลี่ยนแปลง

(1.1) ต้องมีการกำหนดบทบาทและความรับผิดชอบของแต่ละบุคคลที่เกี่ยวข้องกับกระบวนการควบคุมการเปลี่ยนแปลงอย่างชัดเจน เพื่อการควบคุมที่ดีไม่ควรจะทำโดยบุคคลเดียวกัน

(1.2) ซอฟต์แวร์ที่ใช้งานจริงสำหรับระบบงานนั้น ๆ ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการโอนย้ายซอฟต์แวร์ที่พร้อมใช้งานไปยังส่วนที่ใช้งานจริง

(1.3) ควรแบ่งแยกส่วนที่ใช้สำหรับงานต่อไปนี้ออกจากกัน เช่น ส่วนการพัฒนาระบบงานส่วนที่ใช้สำหรับโอนย้ายซอฟต์แวร์ก่อนการย้ายเข้าส่วนที่ใช้งานจริงส่วนที่ใช้ทดสอบระบบสำหรับ ผู้ใช้งานและส่วนที่ใช้งานจริงในแต่ละส่วนต้องมีการควบคุมการเข้าใช้งานที่ดี หมายเหตุ ถ้าไม่สามารถแบ่งแยกส่วนที่ใช้สำหรับทดสอบระบบงานให้แยกส่วนที่ใช้สำหรับการทดสอบระบบโดยผู้ใช้งานออกจากส่วนที่ใช้พัฒนาระบบงาน

3) การเปลี่ยนแปลงระบบคอมพิวเตอร์ฮาร์ดแวร์ อุปกรณ์และสื่อที่ใช้ในการจัดเก็บข้อมูล

(1.1) การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์อุปกรณ์และสื่อที่ใช้ในการจัดเก็บข้อมูลจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรเพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และการ แก้ไขโดยไม่ได้ตั้งใจ

(1.2) การเปลี่ยนแปลงระบบงานใด ๆ ต้องไม่รบกวนหรือขัดขวางการปฏิบัติงานของ

ระบบงานปัจจุบันและการเปลี่ยนแปลงดังกล่าวนั้นจะต้องสามารถใช้งานร่วมกับข้อมูลและระบบงานที่มีการใช้ อยู่ในปัจจุบันได้ด้วย

(1.3) การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลที่ไม่ใช้งานแล้วทั้งหมดของ อพวช.อย่างถาวรออกจากอุปกรณ์หรือสื่อที่ใช้สำหรับเก็บข้อมูลที่มีการเปลี่ยนแปลง

4) การเปลี่ยนแปลงระบบเครือข่าย เช่น Network, Firewalls และ Router เป็นต้น

(1.1) ผู้ร้องขอต้องปฏิบัติตามระเบียบการปฏิบัติงาน เรื่องการจัดการกับการแก้ไขเปลี่ยนแปลง เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ

(1.2) การเปลี่ยนแปลงใดๆ ของระบบเครือข่ายของอพวช. ต้องปฏิบัติตามคู่มือที่ กำหนดไว้ เช่น การเปลี่ยนแปลงระบบเครือข่าย รวมถึงการเพิ่มซอฟต์แวร์ของระบบเครือข่ายการ เปลี่ยนแปลงหมายเลขของเครือข่ายการกำหนดค่าของ Routers ใหม่การเพิ่มเติมคู่สายเพื่อใช้ในการเชื่อมต่อ ระบบ เป็นต้น

(1.3) ผู้ดูแลระบบจะต้องทำการบันทึกข้อมูลของระบบเก่าเก็บไว้ เพื่อใช้แก้ปัญหาในการนำระบบเก่ามาใช้ในกรณีที่ระบบใหม่เกิดปัญหา โดยพิจารณา ว่าข้อมูลใดมีความสำคัญต่อระบบ เช่น บัญชี ผู้ใช้งานและรหัสผ่านค่า Configuration ของระบบ เป็นต้น

(1.4) ผู้ดูแลระบบจะต้องเก็บข้อมูลต่าง ๆ รวมทั้งคู่มือที่มาพร้อมกับระบบใหม่ไว้อย่างดีเพื่อใช้ในการแก้ปัญหาในครั้งต่อไป

(1.5) ผู้ดูแลระบบจะต้องบันทึกข้อมูลที่มีการเปลี่ยนแปลงต่าง ๆ ไว้ในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form)

5) การเปลี่ยนแปลง Source Code

(1.1) สำหรับ Source Code ที่ใช้งานจริงต้องมั่นใจว่า Source Code ทั้งหมดมีการจัดเก็บไว้ที่เดียวกันซึ่งการเปลี่ยนแปลงจะต้องได้รับอนุมัติให้ทำการแก้ไขแล้วเท่านั้น เมื่อมีการแก้ไข ซอฟต์แวร์จะมีการนำเอา Source Code จากที่ จัดเก็บไปทำการแก้ไขการเปลี่ยนแปลงแก้ไข Source Code ที่ใช้งานจริงต้องมีการควบคุม Version ของ Source Code อย่างเคร่งครัด

(1.2) ผู้ทำหน้าที่ในการเปลี่ยนแปลงแก้ไขต้องถูกจำกัดสิทธิในการเข้าถึงส่วนระบบงานที่ใช้จริงผู้ทำการแก้ไขจะได้รับอนุญาตให้ทำการคัดสำเนา Source Code เพื่อใช้ในการแก้ไขพัฒนา ซอฟต์แวร์ในส่วนที่ใช้สำหรับการพัฒนาระบบงานและทำการย้ายซอฟต์แวร์ที่แก้ไขเสร็จเข้าสู่ส่วนที่ใช้สำหรับโอนย้ายซอฟต์แวร์

ก่อนการย้ายเข้าส่วนที่ใช้งานจริงเท่านั้น

6) แนวทางปฏิบัติของการเปลี่ยนแปลง/แก้ไขระบบ (โดยผู้ดูแลระบบและผู้ใช้งาน) ให้ปฏิบัติตามระเบียบการปฏิบัติงาน เรื่องการจัดการกับการแก้ไขเปลี่ยนแปลง

4.2.3 การตรวจสอบระบบสารสนเทศทั้งหมดที่เกี่ยวข้อง (Technical Review of Applications after Operating Platform Changes)

1) การจ้างพัฒนาระบบต้องตรวจสอบระบบสารสนเทศที่เกี่ยวข้อง ภายหลังที่ได้ติดตั้งระบบใหม่เพื่อให้ทราบถึงผลกระทบจากการพัฒนาระบบและเป็นไปตามเงื่อนไขในการว่าจ้าง พร้อมทั้งมีการตรวจสอบจากหน่วยงานที่เกี่ยวข้องหลังจากการติดตั้งระบบใหม่หรือการปรับปรุง

2) ทำการสอบทานและทดสอบการปฏิบัติงานของระบบปฏิบัติการทางธุรกิจที่เกี่ยวข้อง โดยเฉพาะระบบที่มีความสำคัญทุกครั้งที่มีการเปลี่ยนแปลงของแพลตฟอร์มการควบคุมการทำงานของ คอมพิวเตอร์ (Operating Platform) เพื่อให้มั่นใจว่าระบบยังปฏิบัติงานได้ตรงตามวัตถุประสงค์ เช่น การ เข้าถึงระบบ และความสมบูรณ์ถูกต้องในการปฏิบัติงานของระบบ โดยมีข้อควรปฏิบัติทุกครั้งที่จะเกิดการ เปลี่ยนแปลง ดังนี้

(1.1) จัดทำแผนในการขอเปลี่ยนแปลงและประกาศให้ผู้ที่มีส่วนเกี่ยวข้องได้ทราบ ล่วงหน้า

(1.2) ทำการปรับปรุงแผนความต่อเนื่องทางธุรกิจที่เกี่ยวข้องอย่างเหมาะสม เพื่อให้เกิดความสอดคล้องกับการเปลี่ยนแปลงที่เกิดขึ้น

4.2.4 การควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ (Restrictions on Changes to Software Packages) ผู้ดูแลระบบหรือหน่วยงานที่ดูแลระบบต้องจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจที่จัดซื้อ โดยมีแนวทางปฏิบัติดังนี้

1) หลีกเลี่ยงการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ

2) ในกรณีที่หลีกเลี่ยงไม่ได้ในการเปลี่ยนแปลงแก้ไขให้ขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลงแก้ไขหรือมอบให้ผู้ขายดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจให้

3) ในการเปลี่ยนแปลงซอฟต์แวร์แพ็กเกจ ให้ผู้ที่รับผิดชอบเก็บตัวซอฟต์แวร์ต้นฉบับไว้อีกชุดหนึ่ง

4) ตัวซอฟต์แวร์แพ็กเกจที่แก้ไขจะต้องได้รับการตรวจสอบเป็นอย่างดีว่าจะไม่มีผลกระทบต่อระบบ

4.2.5 ทฤษฎีด้านความปลอดภัยวิศวกรรมระบบ (Secure System Engineering Principles) หลักการวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure System Engineering Principles) กำหนดขึ้นเพื่อให้ระบบสารสนเทศมีระดับของการรักษาความมั่นคงปลอดภัยที่

4.2.6 เหมาะสม และสามารถตอบสนองต่อความต้องการขององค์กรได้โดยหลักการดังกล่าวต้องได้รับการนำไปใช้งานร่วมกับวงจรการพัฒนาระบบสารสนเทศขององค์กรและประกอบด้วย

ประเด็นพื้นฐานที่ต้องได้รับการพิจารณาในระหว่างการออกแบบสร้าง หรือพัฒนาระบบสารสนเทศ ดังต่อไปนี้

1) มาตรการรักษาความมั่นคงปลอดภัยของระบบต้องได้รับการออกแบบให้สอดคล้องกับข้อกำหนดของแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศตลอดจนขั้นตอนปฏิบัติงานมาตรฐาน หรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องขององค์กร
2) พิจารณาและกำหนดมาตรการด้านความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการระบุความต้องการในการพัฒนาระบบสารสนเทศ (Requirements Development Phase) และถือเป็นส่วนหนึ่งของ การออกแบบระบบในภาพรวม
3) ในกรณีที่มีการปรับเปลี่ยนความต้องการของระบบต้องมีการพิจารณาปรับเปลี่ยนหรือเพิ่มเติมมาตรการด้านความมั่นคงปลอดภัยให้มีความสอดคล้องกับความต้องการที่เปลี่ยนแปลงไปเสมอ
4) มาตรการด้านความมั่นคงปลอดภัยที่เลือกใช้ ต้องมีระดับความเข้มงวดที่เหมาะสมกับความเสี่ยงค่าใช้จ่ายวัตถุประสงค์ทางธุรกิจและประสิทธิผลของการใช้งานระบบสารสนเทศโดยมาตรการที่ใช้ ต้องสามารถลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้
5) ระบบต้องได้รับการออกแบบให้มีความซับซ้อนน้อยที่สุด เพื่อลดองค์ประกอบที่ไม่จำเป็นข้อผิดพลาดที่อาจเกิดขึ้น และโอกาสในการถูกโจมตีโดยผู้ไม่ประสงค์ดี
6) มีการวางมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้หลายชั้น (Layered Security) โดยครอบคลุมทั้งทาง Physical และ Logical ทั้งระดับระบบปฏิบัติการฐานข้อมูล แอพลิเคชันและระบบเครือข่าย
7) ระบบต้องได้รับการออกแบบให้มีความสามารถในการต้านทานภัยคุกคาม (เช่น เมื่อมาตรการรักษาความมั่นคงปลอดภัยทำงานผิดพลาดหรือถูกข้ามผ่านระบบต้องจำกัดหรือปฏิเสธการเข้าใช้งาน ไม่ยอมให้เข้าใช้งานได้) และมีความสามารถในการพ้นสภาพ (Recoverability) (โดยอัตโนมัติหรือโดยการสร้าง กระบวนการกู้คืน) ภายในระยะเวลาที่เหมาะสมกับความต้องการของ อพวช.
8) มีการสร้างมาตรการด้านความมั่นคงปลอดภัยเพื่อปกป้องในส่วนของการรักษาความลับของข้อมูล การรักษาความถูกต้อง ครบถ้วนของข้อมูล และความพร้อมใช้ของข้อมูลทั้งในระหว่างการ ประมวลผลการแลกเปลี่ยน และการจัดเก็บ
9) กำหนดให้ผู้ใช้งานมีบัญชีผู้ใช้งานไม่ซ้ำกัน (Unique Identification)
10) ต้องมีการออกแบบมาตรการรักษาความมั่นคงปลอดภัยเชิงป้องกันการโจมตีต่าง ๆ (Attack) โดยพิจารณาในมุมมองของผู้ไม่ประสงค์ดีที่ไม่ได้อยู่ภายใต้กรอบของแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรหรือพยายามข้ามผ่านมาตรการรักษา

ความมั่นคงปลอดภัยที่มีอยู่และต้องสร้าง มาตรการรักษาความมั่นคงปลอดภัยในกรณีที่จำเป็นต้องใช้งานระบบในสภาพแวดล้อมที่ไม่พึงประสงค์ เช่น การใช้งานระบบในระหว่างเกิดเหตุฉุกเฉินหรือภัยพิบัติ

11) ออกแบบสิทธิในการใช้ระบบโดยอาศัยหลักการสิทธิที่น้อยที่สุด (Least Privilege) ตามหน้าที่การทำงานและ/หรือความจำเป็นในการใช้งาน

12) ออกแบบระบบให้มีกลไกในการตรวจสอบการใช้งาน (Audit Mechanism) สำหรับฟังก์ชันการทำงานที่สำคัญเพื่อตรวจจับการใช้งานระบบโดยไม่ได้รับอนุญาตและเพื่อใช้สนับสนุนการตรวจสอบ เหตุการณ์ผิดปกติต่าง ๆ

4.2.7 สภาพแวดล้อมสำหรับการพัฒนาระบบ (Secure Development Environment) มีการจัดเตรียมและปกป้องสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย โดย ครอบคลุมถึงประเด็นต่าง ๆ ดังต่อไปนี้

1) แบ่งแยกสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศออกจากระบบสารสนเทศที่ใช้งานจริง

2) ควบคุมให้มีเฉพาะผู้ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศขององค์กร

3) จัดให้มีการปกป้องข้อมูลที่จัดเก็บและประมวลผลในสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศและข้อมูลที่ส่งผ่านระหว่างสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศและระบบ สารสนเทศที่ใช้งานจริง

4) ทำการตรวจสอบและควบคุมการเคลื่อนย้ายข้อมูลเข้าและออกจากสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศอย่างเข้มงวด เช่น การจ้างพัฒนาระบบโดยหน่วยงานภายนอก (Outsourced Development)

5) ข้อกำหนดสำหรับ Secure Coding จะต้องถูกระบุไว้ในขอบเขตงาน (TOR)

6) เมื่อมีการจ้างพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอกจะต้องกำหนดมาตรการป้องกันให้ครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้

(1.1) จัดทำข้อกำหนดเกี่ยวกับการอนุญาตให้ใช้สิทธิ์ (Licensing arrangements) รูปแบบความเป็นเจ้าของโค้ด (code ownership) และสิทธิ์ในทรัพย์สินทางปัญญา

(1.2) จะต้องมีการรับรองคุณภาพและความถูกต้องผลงาน

(1.3) ผู้ว่าจ้างจะต้องได้รับสิทธในการเป็นเจ้าของ source code และเอกสารอื่นๆ ที่เกี่ยวข้องกับระบบที่ว่าจ้างให้พัฒนา

(1.4) ผู้ว่าจ้างจะต้องสามารถตรวจสอบคุณภาพและความถูกต้องของงานที่จะส่ง มอบได้

(1.5) จัดทำกระบวนการในการตรวจสอบคุณภาพและความถูกต้องในการทำงานของฟังชัน

ขั้นต่าง ๆ ที่ถูกพัฒนาขึ้นว่ามีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้

(1.6) จะต้องมีการทดสอบหา Trojan ที่อาจแฝงอยู่ใน code ที่ถูกเขียนขึ้นก่อนที่จะนำมาติดตั้งเพื่อใช้งานจริง

(1.7) จัดทำข้อกำหนดในสัญญาบำรุงรักษาซอฟต์แวร์ให้มีการแก้ไข หากพบปัญหาที่เกิดจากการใช้งานในภายหลัง

4.2.8 การทดสอบด้านความมั่นคงปลอดภัยระบบ (System Security Testing)

1) ระบบสารสนเทศที่ได้รับการพัฒนาขึ้นหรือได้รับการปรับปรุงแก้ไข ต้องได้รับการทดสอบก่อนนำไปใช้งานจริง โดยผู้ใช้งานต้องร่วมทดสอบการทำงานของระบบด้วย

2) ต้องมีการทดสอบการทำงานทางด้านความมั่นคงปลอดภัยของระบบ (Security Functionality) ในขั้นตอนการพัฒนาระบบงาน

3) ข้อมูลที่ใช้ในการทดสอบระบบสารสนเทศ ควรเป็นข้อมูลที่จัดเตรียมไว้เพื่อการทดสอบโดยเฉพาะ หากจำเป็นต้องใช้ข้อมูลที่มีความสำคัญสูงในการทดสอบต้องได้รับอนุญาตจากเจ้าของข้อมูล และ ทำการปิดบังเปลี่ยนแปลงหรือลบข้อมูลสำคัญออกตาม ความเหมาะสม

4.2.9 เกณฑ์ในการตรวจรับระบบสารสนเทศ (System Acceptance Testing) อพวช.ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ (System acceptance) รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน เช่น การตรวจรับระบบตามขอบเขตงาน (TOR) ที่ได้กำหนดไว้

4.3 แนวปฏิบัติด้านข้อมูลในการทดสอบระบบ (Test Data) เพื่อใช้ในการป้องกันข้อมูลที่ใช้ระหว่างการทดสอบระบบ

4.3.1 หลักการป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ (Protection of Test Data) ข้อมูลจริงที่จะนำใช้ทดสอบระบบต้องได้รับอนุญาตจากหน่วยงานที่รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องลบข้อมูลจริงออกจากระบบทดสอบทันทีและบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ทดสอบอะไรบ้างรวมถึงวันเวลาและหน่วยงานที่ทดสอบแจ้งไปยังหน่วยงานที่รับผิดชอบในการรักษาข้อมูลนั้น อีกครั้ง

ส่วนที่ 20

การกำหนดการวัดติดตามและประเมินผล

1. **วัตถุประสงค์**
   1. เพื่อวัดระดับความรับรู้ของบุคลากรเกี่ยวกับแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
   2. เพื่อสร้างความเข้าใจและความตระหนักรู้ในเรื่องความมั่นคงปลอดภัยของสารสนเทศในองค์กร
   3. เพื่อประเมินผลของกิจกรรมและมาตรการที่ใช้ในการส่งเสริมความมั่นคงปลอดภัยของสารสนเทศ

2. **ผู้รับผิดชอบ**
   กองเทคโนโลยีดิจิทัล

3. **ตัวชี้วัด** : บุคลากร อพวช. รับรู้แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไม่ต่ำกว่าร้อยละ 50 ของ จำนวนบุคลากร อพวช. ทั้งหมด

4. **วิธีการวัดผล**
   4.1 การอบรมและทดสอบความเข้าใจ
      1) จัดอบรมให้กับบุคลากรในหัวข้อเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ
      2) ทำแบบทดสอบความรู้หลังการอบรม โดยบุคลากรที่ได้คะแนนไม่น้อยกว่าร้อยละ 50 ถือว่าผ่านเกณฑ์

   4.2 แบบสำรวจความเข้าใจ
      1) จัดทำแบบสำรวจเกี่ยวกับแนวปฏิบัติด้านความมั่นคงปลอดภัย
      2) หากบุคลากรตอบคำถามได้ถูกต้องมากกว่าร้อยละ 50 ถือว่ามีความรับรู้แนวปฏิบัติ

   4.3 การเข้าร่วมกิจกรรมด้านความมั่นคงปลอดภัย
      1) นับจำนวนบุคลากรที่เข้าร่วมกิจกรรม เช่น e-Learning, Workshop, การทดสอบ Phishing
      2) หากบุคลากรเข้าร่วมกิจกรรมไม่น้อยกว่าร้อยละ 50 ของจำนวนบุคลากรทั้งหมด ถือว่าผ่านตัวชี้วัด

5. **การประเมินผลการวัด ติดตาม**

หมวดหมู่	**จำนวนบุคลากรที่เข้าร่วม**	**ร้อยละของบุคลากรทั้งหมดที่ผ่านการอบรม**
อบรมและผ่านการทดสอบแบบประเมิน	[จำนวนบุคลากร อพ. ทั้งหมดที่ลงทะเบียนเข้าอบรม]	[ร้อยละ 50]
ทำแบบทดสอบความรู้หลังผ่านการอบรมและติดตาม เพื่อวัดระดับความรู้หลังผ่านการอบรม	[บุคลากร อพ. ที่ผ่านการอบรม]	[ร้อยละ 50]
สรุปรวม	[จำนวนบุคลากรทั้งหมดที่เข้าร่วมทั้ง 2 กิจกรรม]	[ร้อยละ 50]

6. **แผนการวิเคราะห์ผลและข้อเสนอแนะ**

6.1 [วิเคราะห์ผลการวัด: เช่น หากบุคลากรผ่านตัวชี้วัดน้อยกว่าร้อยละ 50 ควรมีมาตรการเพิ่มเติม]

6.2 [ข้อเสนอแนะเพื่อปรับปรุง เช่น การเพิ่มกิจกรรมอบรม การใช้มาตรการจูงใจ]

7. **แผนการสรุปผลและแนวทางปรับปรุงในอนาคต**

จากผลการวัดพบว่า [สรุปผลการวัด] ซึ่ง [ผ่าน/ไม่ผ่าน] ตามเกณฑ์ที่กำหนด เพื่อให้บรรลุเป้าหมายในอนาคต อพวช. ควรดำเนินการดังนี้:

7.1 ปรับปรุงเนื้อหาและรูปแบบการอบรมให้เข้าใจง่ายและน่าสนใจ

1) เพิ่มกิจกรรมที่ส่งเสริมให้บุคลากรเข้าร่วมมากขึ้น

2) ใช้เทคโนโลยี เช่น e-Learning หรือแคมเปญสร้างความตระหนักรู้

Information Security

National Science Museum Thailand

องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ
กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
39 หมู่ 9 ต.คลองห้า อ.คลองหลวง จ.ปทุมธานี
www.nsm.or.th