ประกาศองค์การตลาด กระทรวงมหาดไทย
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ขององค์การตลาด ประจำปี ๒๕๖๘

ด้วยองค์การตลาดต้องมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การตลาด กระทรวงมหาดไทย เพื่อให้มีความเหมาะสมและสอดคล้องกับการพัฒนาของเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไปอย่างรวดเร็ว

อาศัยอำนาจตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ องค์การตลาด กระทรวงมหาดไทย จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี ๒๕๖๘ ตามเอกสารแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๔ กุมภาพันธ์ พ.ศ.๒๕๖๘

(นายบูรณิศ ยุกตะนันทน์)
ผู้อำนวยการองค์การตลาด

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
องค์การตลาด กระทรวงมหาดไทย
ประจำปี ๒๕๖๘

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การตลาด กระทรวงมหาดไทย (Information Security Policy)

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบสารสนเทศขององค์การตลาด กระทรวงมหาดไทย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์การและหน่วยงานในสังกัด อีกทั้งเป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ หน่วยงานของรัฐ ต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ องค์การจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบ เทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ขององค์การ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อเผยแพร่ให้พนักงานทุกระดับในองค์การได้รับทราบและพนักงานทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร พนักงาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์การสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๔ กำหนดความรับผิดชอบ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรือ อันตรายใด ๆ แก่องค์การหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๕ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศปีละ ๑ ครั้ง

๑.๖ กำหนดให้ฝ่ายความเสี่ยงดำเนินการในการตรวจสอบและประเมินความเสี่ยง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๗ นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา ๑ ครั้งต่อปี

๒. องค์ประกอบของนโยบาย

คำนิยาม

ส่วนที่ ๑ นโยบายการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(IT asset management)

ส่วนที่ ๒ นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
(Data and Information security)

ส่วนที่ ๓ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access control)

ส่วนที่ ๔ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and environmental security)

ส่วนที่ ๕ นโยบายการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
(Communications security)

ส่วนที่ ๖ นโยบายการรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
(IT operations security)

ส่วนที่ ๗ นโยบายการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ
(System acquisition and development)

ส่วนที่ ๘ นโยบายการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ
(IT incident and problem management)

ส่วนที่ ๙ นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

ส่วนที่ ๑๐ นโยบายการบริหารจัดการผู้ให้บริการภายนอก
(Third party management)

ส่วนที่ ๑๑ นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี
(Malicious Software Prevention)

ส่วนที่ ๑๒ นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต
(Website and Internet Security)

ส่วนที่ ๑๓ นโยบายการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

ส่วนที่ ๑๔ นโยบายการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ(Cryptography)
และการบริหารจัดการกุญแจ (Key management)

ส่วนที่ ๑๕ นโยบายการใช้คลาว์ดภาครัฐ (Cloud First Policy)

ส่วนที่ ๑๖ นโยบายการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security risk Management)

ส่วนที่ ๑๗ นโยบายนโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน
(Role and responsibility)

ส่วนที่ ๑๘ นโยบายนโยบายการปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษ
ของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
(Compliance)

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การ แต่ละส่วนที่กล่าว ข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ(Procedure)ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์การ เพื่อที่จะทำให้องค์การมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน สินทรัพย์ บุคลากร ขององค์การทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบสารสนเทศขององค์การนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบสารสนเทศขององค์การ ซึ่งพนักงานขององค์การและหน่วยงานภายนอกจะต้องปฏิบัติ ตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **องค์การ** หมายถึง องค์การตลาด กระทรวงมหาดไทย
- **ผู้บริหารระดับสูง** หมายถึง ประธานกรรมการจนไปถึงคณะกรรมการ
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์การ
- **ฝ่ายสารสนเทศ** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในองค์การ
- **หัวหน้าฝ่ายสารสนเทศ** หมายถึง ผู้มีอำนาจในด้านสารสนเทศขององค์การ ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งาน ระบบเทคโนโลยีสารสนเทศ
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์การ
- **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์การ โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์การกำหนดไว้ ดังนี้

  ๑. **ผู้บริหาร** หมายถึง ผู้อำนวยการองค์การตลาด รองผู้อำนวยการองค์การตลาดที่ได้รับมอบหมาย และหรือเลขานุการองค์การตลาดที่ได้รับมอบหมาย

  ๒. **ผู้ดูแลระบบ** (System Administrator) หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

  ๓. **พนักงาน** หมายถึง พนักงานขององค์การ
- **สิทธิ์ของผู้ใช้งาน** หมายถึง สิทธิ์ทั่วไป สิทธิพิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบ สารสนเทศของหน่วยงาน
- **หน่วยงานภายนอก** หมายถึง องค์การหรือหน่วยงานภายนอก ที่องค์การตลาดอนุญาตให้มีสิทธิ์ในการเข้าถึง และใช้งานข้อมูลต่าง ๆ ของหน่วยงาน และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
- **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบ ให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่

ประมวลผลข้อมูลโดยอัตโนมัติ

- **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์การได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น
  ๑. **ระบบ LAN และระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อ สื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
  ๒. **ระบบ Internet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของหน่วยงาน ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศ ที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
- **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น
  ๑. **พื้นที่ทำงานทั่วไป (General Working Area)** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  ๒. **พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)**
  ๓. **พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)**
  ๔. **พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)**
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยงาน
- **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP๓ และ IMAP เป็นต้น
- **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงคำสั่งที่กำหนดไว
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการ

เข้าถึง โดยมิชอบเอาไว้ด้วย

- **<u>ความมั่นคงปลอดภัยด้านสารสนเทศ</u>** หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
- **<u>เหตุการณ์ด้านความมั่นคงปลอดภัย</u>** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- **<u>สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด</u>** หมายถึง สถานการณ์ ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์การถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ส่วนที่ ๑
นโยบายการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(IT Asset Management)

๑. วัตถุประสงค์

๑.เพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์การตลาด

๒.เพื่อป้องกันทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กรและกำหนดระดับของการป้องกันด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

๓.เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ พนักงาน หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับองค์การตลาด และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศขององค์การตลาด รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติ

๓.๑ หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร

๑.๑ ควบคุมและกำกับให้มีการเก็บบันทึกทะเบียนทรัพย์สิน โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

๑.๒ กำหนดบุคลากรผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินด้านสารสนเทศอย่างเหมาะสม

๑.๓ กำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสารและมีการประกาศใช้ในองค์กร

๓.๒. การจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน (Inventory of assets)

๓.๒.๑ ทะเบียนทรัพย์สิน (Inventory of assets)

๑.มีบริหารจัดการทรัพย์สิน ต้องจัดทำและเก็บทะเบียนทรัพย์สินซึ่งรวมถึงทรัพย์สินข้อมูล และเอกสาร (Information and Document Asset) ทรัพย์สินซอฟต์แวร์ (Software Asset) ทรัพย์สิน อุปกรณ์ (Hardware Asset) ทรัพย์สินงานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูล เบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อทรัพย์สินอย่างเหมาะสมรวมถึงเป็นการควบคุมและจัดการทรัพย์สินขององค์การตลาด

๒.มีการจัดทำทะเบียนทรัพย์สินสารสนเทศ และกำหนดเข้าของหรือผู้รับผิดชอบทรัพย์สินสารสนเทศ พร้อมทั้งปรับปรุงข้อมูลให้เป็นปัจจุบัน โดยกำหนดให้มีการทบทวนทะเบียนทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลง

๓.การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๔.มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สิน สารสนเทศตามระดับชั้นความลับข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อให้สามารถกำหนดวิธีการในการป้องกันได้อย่างเหมาะสม

๕.จัดให้มีการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามหมวดหมู่ที่กำหนดไว้ ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์ทรัพย์สิน

ด้านสารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศ ส่วนข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัย อย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการ ทำลาย และกำหนดเป็นระเบียบปฏิบัติให้พนักงานต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุม และรักษา ความปลอดภัย

๖.มีการกำหนดขั้นตอนปฏิบัติการจัดชั้นความลับและการจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางหรือหลักเกณฑ์การจัดระดับชั้นความลับข้อมูลสารสนเทศที่องค์การตลาดกำหนด

๗.ประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของทรัพย์สิน เมื่อมีทรัพย์สินใหม่ หรือ ทรัพย์สินที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

๘.ความเป็นเจ้าของทรัพย์สิน (Ownership for Assets) กำหนดบุคคลหรือหน่วยงานผู้รับผิดชอบข้อมูลและทรัพย์สิน ทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์การตลาดอย่างชัดเจน

๓.๒.๒ การอนุญาตให้ใช้ทรัพย์สิน (Acceptable Use for Assets)

๑.การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์มีดังนี้ ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมด ที่องค์การตลาดเป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานขององค์การตลาด การใช้งานระบบและ อุปกรณ์ต่างๆ เพื่อกิจธุระส่วนตัวนั้นอนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของพนักงาน ตลอดจนหน่วยงานภายนอกที่ได้รับการว่าจ้างโดยองค์การตลาดจะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศขององค์การตลาด

๒.ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ขององค์การตลาด อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นทรัพย์สินของตนจัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานขององค์การตลาด การใช้งานระบบและ อุปกรณ์ต่างๆ

๓.พนักงานตลอดจนหน่วยงานภายนอก ที่ได้รับการว่าจ้างโดยองค์การตลาดจะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศขององค์การตลาด ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ขององค์การตลาด อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นทรัพย์สินของตน

๔.เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดขององค์การตลาด ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งาน อุปกรณ์เป็นระยะเวลาหนึ่ง

๕.ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายขององค์การตลาด รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ขององค์การตลาด ก่อนได้รับอนุญาตจากผู้บริหารฝ่ายสารสนเทศหรือผู้อำนวยการองค์การตลาด

๖.เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในองค์การตลาด อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกัน สปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอฯลฯ ทั้งนี้ผู้ใช้งานต้องทำการปกป้อง อุปกรณ์และข้อมูลใน อุปกรณ์ตามคำแนะนำที่ระบุไว้ใน เอกสารขั้นตอนการปฏิบัติงาน เรื่องการใช้ เครื่องคอมพิวเตอร์

ประเภท พกพาในการปฏิบัติงานนอกสถานที่ (Mobile Computing and Communications)

๗.อุปกรณ์คอมพิวเตอร์ขององค์การตลาดต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับ อนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง และผู้ดูแลระบบต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการ ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ขององค์การตลาดอย่างเด็ดขาด

๘.การอนุญาตให้ใช้งานทรัพย์สินด้านซอฟต์แวร์มีดังนี้ ห้ามพนักงานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ขององค์การตลาด ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์การตลาด ทั้งที่ ได้มาจากการพัฒนาขึ้นโดยพนักงานหรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และ อนุมัติ อย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศขององค์การตลาด

๙.ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปขององค์การตลาด มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

๑๐.รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารระดับสูงของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่า ซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานขององค์การตลาดเท่านั้น

๓.๒.๓ การจัดการทรัพย์สิน (Handling of Asset)

๑.ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการ ปกป้อง โดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม

๒.ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้น ไว้โดยไม่อยู่ที่โต๊ะทำงาน ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์เครื่องโทรสาร เครื่องถ่าย เอกสาร ฯลฯ โดยทันที

๓.พนักงานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอกยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

๔.พนักงานต้องไม่พูดคุยหรือใช้งานข้อมูลลับขององค์การตลาดในพื้นที่สาธารณะ เช่น ลิฟท์ ร้านอาหาร ฯลฯ สื่อบันทึกข้อมูลและ อุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น โทรศัพท์มือถือ ,PDA,USB-Drive, CD-Rom เป็นต้น) ที่มีข้อมูลลับขององค์การตลาด บันทึกอยู่ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

๓.๒.๔ การคืนทรัพย์สิน (Return on Assets)

๑.พนักงาน ซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงาน คอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน คอมพิวเตอร์และ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน โดยปฏิบัติตามวิธีปฏิบัติงาน เรื่องการส่งคืนทรัพย์สิน (Return of assets)

๓.๒.๕. การบำรุงรักษาอุปกรณ์ (equipment maintenance)

๑.กำหนดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต หรือ

กำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ ๑ ครั้ง

๒.ปฏิบัติตามคำแนะนำในการบำรุงรักษาอุปกรณ์ตามที่ผู้ผลิตแนะนำ

๓.จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง ตรวจสอบหรือประเมินในภายหลัง

๔.จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๕.ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๖.จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอกที่มาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๒.๖.การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of property)

๑.ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๒.กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออองค์การตลาดกหน่วยงาน

๓.กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๔.เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๕.บันทึกการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้ง บันทึกข้อมูลเพิ่มเติม เมื่อนำอุปกรณ์ส่งคืน

๓.๒.๗.การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of equipment off-premises)

๑.กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่งเกิดอุบัติเหตุกับอุปกรณ์

๒.ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๓.พนักงานมีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเมือนเป็นทรัพย์สินของตนเอง

๓.๒.๘.การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use-of equipment)

๑.ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๒.มีมาตราการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๓.๒.๙.การจัดสื่อที่ใช้บันทึกข้อมูล เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต มีการป้องกันในการนำส่งหรือการขนย้าย หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัยเมื่อหมดความต้องการในการใช้งาน

ส่วนที่ ๒
นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
(Data and Information security)

๑. วัตถุประสงค์

๑. เพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security)

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ พนักงาน หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงาน และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศรับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการ รักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๓.๑.๑ ประเภทข้อมูลขององค์การ แบ่งได้ดังนี้

๑) ข้อมูลสารสนเทศด้านการบริหาร

๒) ข้อมูลนโยบาย

๓) ข้อมูลยุทธศาสตร์

๔) ข้อมูลบุคคล

๕) ข้อมูลงบประมาณบัญชีและการเงิน

๓.๑.๒ ข้อมูลสารสนเทศด้านการให้บริการ

๑) ข้อมูลทะเบียนห้องเช่า

๒) ข้อมูลทะเบียนแผงเช่า

๓) ข้อมูลทะเบียนอาคารเช่า

๓.๒ ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าว เป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสาร ที่สำคัญไว้ดังนี้

๓.๒.๑ การกำหนดชั้นความลับ ตามความสำคัญของข้อมูลในเอกสาร กำหนดไว้ ๓ ระดับ ได้แก่ ลับ ลับมาก ลับที่สุด และมีการกำหนดความรับผิดชอบ ให้แก่ผู้มีอำนาจกำหนดชั้นความลับ เป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสาร และการยกเลิกหรือปรับระดับชั้น ความลับของเอกสารตามความจำเป็น

๓.๒.๒ การควบคุมเอกสาร โดยกำหนดให้มีมาตรการควบคุมต่าง ๆ คือ การจัดทำเอกสาร การสำเนา การส่งและการรับ การเก็บรักษา การทำลาย การปฏิบัติในเวลาฉุกเฉิน เวลาสูญหาย รวมถึงการเปิดเผยข้อมูลในเอกสาร

๓.๓ ระดับชั้นการเข้าถึง

๓.๓.๑ ระดับชั้นสำหรับผู้บริหาร (ผู้อำนวยการ, รองผู้อำนวยการ)

๓.๓.๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป (พนักงานองค์การ)

๓.๓.๓ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย (ผู้ดูแลระบบสารสนเทศและผู้ที่มีสิทธิ์ในการเข้าถึงระบบสารเทศ)

๓.๔ เวลาที่ได้เข้าถึง

๓.๔.๑ การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.)

๓.๔.๒ การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ – ๑๖.๓๐ น.)

๓.๔.๓ การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

๓.๕ ช่องทางการเข้าถึง

๓.๕.๑ ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

๓.๕.๒ โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)

๓.๕.๓ หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)

๓.๕.๔ ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

๓.๕.๕ ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

๓.๕.๖ ระบบอินเตอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

๓.๕.๗ เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา)

๓.๕.๘ การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และ ในช่วงเวลาพิเศษเป็นรายครั้ง)

๓.๖ ข้อกำหนดการใช้งานตามภารกิจ

๓.๖.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ

๓.๖.๒ มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๓.๗ แนวปฏิบัติในการควบคุมการเข้าถึงระบบ

๑ สถานที่ตั้งของระบบสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๒ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลได้

๓ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓.๘ แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

๑ เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยง ในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำ ในการใช้งานตามภารกิจเท่านั้น

๒ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการ ใช้งานระบบสารสนเทศ

๓.๙ แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้

๑ การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒ การลงทะเบียนผู้ใช้งานใหม่ขององค์การ

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ โดยต้องระบุข้อมูลพื้นฐานเป็นอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่ง ฝ่าย

๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานว่าไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๕) ผู้ดูแลระบบต้องกาหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ โดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตาแหน่งงาน

๖) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทาการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ โดยไม่ได้รับอนุญาต

๓ กำหนดสิทธิ์การใช้ระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิ์ เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบ จากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๔ การบริหารจัดการสิทธิ์ของผู้ใช้งาน

๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การโดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๒ ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสม สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ

๓ ผู้ดูแลระบบต้องมอบหมายสิทธิ์ ให้มีความสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

๔ ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๕ ผู้ใช้บริการต้องรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ และต้องปฏิบัติตามอย่างเคร่งครัด

๖ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๑ ผู้ดูแลระบบต้องกำหนดการตั้งเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๒ ผู้ดูแลระบบต้องส่งมอบรหัสผ่านให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๓ ผู้ดูแลระบบต้องให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคน

๔ ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น

๕ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง และกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๖ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนาม เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

๖ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๖.๑ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการ เข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ระยะเวลาในการเข้าถึง ช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้น ความลับ ดังต่อไปนี้

๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ดังกล่าว

๔) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจ ซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๖.๒ เจ้าของข้อมูล จะต้องมีการตรวจทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลอย่างน้อย ปีละ ๔ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๖.๓ การเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ มีแนวปฏิบัติ ดังนี้

๑ ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน

๒ กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล

๓ การจัดเก็บ username และ password ของระบบสารสนเทศลงในฐานข้อมูลใดๆ จะต้องทำการเข้ารหัสด้วย MD5 ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

๔ ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล https สาหรับระบบสารสนเทศแบบ web application เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราว์เซอร์และเว็บเซิร์ฟเวอร์

๕ กำหนดช่องทางการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสมกับองค์การ สำหรับช่องทาง ดังต่อไปนี้

๑) ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต

๒) เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย

๓) สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (จากตัวเครื่องคอมพิวเตอร์)

๖.๔ กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัสข้อมูล ดังนี้

๑ วิธีการป้องกันกุญแจที่ใช้สาหรับการเข้ารหัสข้อมูล

๒ วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย

๓ บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจ การสร้างกุญแจ ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่จัดการกรณีกุญแจเกิดการสูญหาย

๖.๕ ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับ หรือวิธีการรักษาความลับของข้อมูล ดังนี้

๑ ต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

๒ ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการกำหนดรหัสผ่านสำหรับไฟล์ที่มีการใช้งาน

๖.๖ ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายขององค์การ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

๖.๗ ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

๑ ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

๒ ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

๖.๘ การบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน

๑ ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

๒ ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ และรการหัสผ่านที่กำหนดใหม่ ต้องไม่ซ้ำกับ รหัสผ่านเดิม

๓ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านที่ได้รับ โดยทันที

๔ ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบสารสนเทศ

๕ ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่ กรณีผู้ใช้งานทีมอำนาจอนุมัติใด ๆ ในระบบสารสนเทศไม่สามารถปฏิบัติหน้าที่อันจะเป็นเหตุให้ระบบสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้ง ผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ์ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้วให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

๖ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๗ ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕”

๘ ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

๙ ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

๑๐ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

๑๑ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

๑๒ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๑๓ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคล

อื่น

๑๔ ในกรณีที่ไม่ใช้ระบบสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

๑๕ เมื่อมีปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งาน หรือรหัสผ่าน

๑๖ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยโดยใส่ซองปิดผนึก และประทับตรา“ลับ” และส่งไปยังผู้ใช้งาน และแนบเอกสาร “แนวปฏิบัติสำหรับการ บริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน”รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบ ดังกล่าวโดยเคร่งครัด

๖.๙ การใช้งานรหัสผ่าน

๑ เก็บรหัสผ่านไว้เป็นความลับ

๒ หลีกเลี่ยงการบันทึกรหัสผ่าน (เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพกต่าง ๆ) นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับ การอนุมัติแล้ว

๓ เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

๔ กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวเพียงพอ

๑) ง่ายสำหรับจดจำ

๒) ไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่ายหรือสามารถหาได้จากข้อมูลเกี่ยวกับตน เช่น ชื่อ หมายเลขโทรศัพท์และวันเกิด เป็นต้น

๓) ไม่สร้างจุดอ่อนโดยการใช้คำที่อยู่ในพจนานุกรม

๔) ไม่มีคำซ้ำหรือตัวอักษรซ้ำไม่ควรเป็นตัวเลขทั้งหมด หรือไม่เป็นตัวอักษรทั้งหมด

๕ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ไดสิทธิ์พิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

๖ กำหนดใหเปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

๗ ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ

๘ ไม่ใช้รหัสผ่านรวมกับผู้อื่น

๙ ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

๑๐ ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว แนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างตน สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

๖.๑๐ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

๑ ผู้ดูแลระบบดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน ๑ ครั้ง / ปี เป็นอย่างน้อย

๒ ผู้ดูแลระบบทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ในระดับผู้ดูแลระบบด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๓ ผู้ดูแลระบบทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ ที่มีนัยสำคัญ

๔ ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูงเพื่อใช้ในการทบทวนในภายหลัง

๖.๑๑ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๑ ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงาน

๒ ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๓ ผู้ดูแลระบบต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๔ ผู้ใช้งานต้องกำหนดให้มีการตั้งล๊อกหน้าจอเครื่องคอมพิวเตอร์หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน ๒๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๓.๑๐ แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่าย

๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒ ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๓ ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่าย ไปยังเครืองแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

๔ ระบบเครือข่ายทั้งหมดขององค์การทีมีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์การ ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

๕ IP address ภายในของระบบงานเครือข่ายภายในขององค์การ จำเป็นต้องมีการป้องกันมิให้ หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของฝ่ายสารสนเทศได้โดยง่าย

๖ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบัน อยู่เสมอ

๗ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๘ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายสารสนเทศเท่านั้น

๓.๑๑ แนวปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๑ ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้ งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องกำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ Telnet Ftp หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๔ ควรดำเนินการติดตั้งอัพเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๕ ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความ

ปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สารสนเทศ เท่านั้น

๓.๑๒ แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

๑ ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๓ เดือน

๒ ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๓.๑๓. แนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์สารสนเทศ

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์การ เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์การ ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์การ การควบคุมบุคคลที่เข้าสู่ระบบขององค์การจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษา ความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติ จากหัวหน้าฝ่ายสารสนเทศ และหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดทั้งที่เป็นลายลักษณ์อักษรและไม่เป็นลายลักษณ์อักษรก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้อง ปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๓ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับองค์การอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็น ทางการ

๔ ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๓.๑๔ แนวปฏิบัติการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบไม่ว่าจะเป็นการเข้าสู่ระบบสารสนเทศทางอินเตอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์การ อย่างน้อย ๑ วิธีสำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

๑. การแสดงตัวตน (Identification) คือ ขั้นตอนป้อนชื่อผู้ใช้ (Username)

๒. การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนป้อนรหัสผ่าน (Password)

๓.๑๕ แนวปฏิบัติการควบคุมการเข้าถึงข้อมูล

๑. เจ้าของข้อมูล ต้องกำหนดสิทธิตามระดับชั้นของผู้ใช้งานข้อมูลในการเข้าถึงข้อมูล

๒. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าของข้อมูลที่รับผิดชอบข้อมูลก่อนเข้าถึงข้อมูล

๓.๑๖ แนวปฏิบัติการควบคุมการเข้าถึงอุปกรณ์ในการประมวลผลข้อมูล

๑. เจ้าของอุปกรณ์ต้องกำหนดผู้ใช้งานในการเข้าถึงอุปกรณ์ในการประมวลผลข้อมูล

๒. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าของอุปกรณ์ในการเข้าถึงอุปกรณ์ในการประมวลผลข้อมูล

๓.๑๗ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล กำหนดบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน (Password) วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงการใช้งานสารสนเทศใน แต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบเทคโนโลยีสารสนเทศ รวมถึงวิธีการ ทำลายข้อมูลในแต่ละประเภทชั้นความลับ

๒ เจ้าของข้อมูล (Information Owner) ต้องทบทวนความเหมาะสมของของสิทธิ์ในการเข้าถึงการใช้งานระบบสารสนเทศของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง

๓ การรับส่งข้อมูลสำคัญผ่านเครือข่ายอินเตอร์เน็ต (Internet) ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลได้แก่ SSL, VPN หรือ XML Encryption

๓.๑๘ การแลกเปลี่ยนสารสนเทศ

๑ ต้องกำหนดให้มีนโยบายและขั้นตอนปฏิบัติงานสำหรับการแลกเปลี่ยนสารสนเทศระหว่าง หน่วยงานภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก รวมทั้งควบคุมการแลกเปลี่ยนข้อมูล สารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

๒ การแลกเปลี่ยนสารสนเทศผ่านช่องทางการสื่อสารทุกชนิดระหว่างองค์การตลาด กับหน่วยงาน ภายนอก ต้องได้รับการอนุมัติจากผู้อำนวยการองค์การตลาด

๓ ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

๔ ข้อตกลงการแลกเปลี่ยนสารสนเทศต้องดำเนินการจัดทำอย่างเป็นลายลักษณ์อักษร

๕ การแลกเปลี่ยนสารสนเทศระหว่าง องค์การตลาดกับหน่วยงานภายนอกต้องดำเนินการการแลกเปลี่ยนสารสนเทศด้วยวิธีการที่มีความมั่นคงปลอดภัยและสอดคล้องกับการจัดระดับชั้นสารสนเทศ

๖ ผู้ดูแลระบบต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online Transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูลหรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

๗) ผู้ดูแลระบบต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) EDI หรือ Instant Messaging)

๓.๑๙ การควบคุมการโอนย้ายข้อมูล (Data Migration)

๑ การโอนย้ายข้อมูล (data migration) ต้องกำหนดขั้นตอนการปฏิบัติอย่างชัดเจนด้วยวิธีการที่มีความมั่นคงปลอดภัย ทั้งนี้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงมีความครบถ้วนถูกต้อง และพร้อมใช้งานอยู่เสมอ

๓.๒๐ การทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable media) ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์การตลาด ที่ประกาศใช้ในปัจจุบัน

ส่วนที่ ๓
นโยบายการควบคุมการเข้าถึง
(Access control)

๑. วัตถุประสงค์

๑. เพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการควบคุมการ เข้าถึงและการใช้งานสารสนเทศ

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ พนักงาน หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงาน และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศรับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๓. เพื่อให้มีการตรวจสอบและติดตามการพิสูจน์ตัวบุคคลที่เข้าถึงและใช้งานสารสนเทศของ องค์การตลาดได้อย่างถูกต้อง

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ บทบาทและความรับผิดชอบ

๑ หัวหน้าฝ่ายสารสนเทศ และหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดที่เป็นลายลักษณ์อักษร

๒ อนุมัติสิทธิ์เข้า-ออกพื้นที่ใช้งานระบบสารสนเทศ

๓ อนุมัติกระบวนการควบคุมการเข้า-ออก ห้องควบคุมระบบเครือข่าย

๔ ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย และหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดที่เป็นลายลักษณ์อักษร

๓.๒ นโยบายควบคุมการเข้าถึง (Access Control Policy)

๑.มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้เข้าได้ เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (Access Control) โดยมีการพิจารณาอนุมัติตามสายบังคับบัญชา

๒.ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวน สิทธิ์การ เข้าถึงอย่างน้อยปีละ ๑ ครั้ง (Review of User Access Rights Procedure) ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน

๓.ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้ ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การตลาด และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๔.ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ การเข้าถึงข้อมูล และระบบสารสนเทศขององค์การตลาดจะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดย

ผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น ๆ เท่านั้น

๕.ความปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึงการให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูลและการกู้ข้อมูลที่เสียหายกลับคืนมา

๓.๒ การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network Control and Network Services)

๓.๒.๑ การใช้บริการเครือข่าย

๑.ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

๒.ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคง ปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ อาทิ ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย อาทิ Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP) จำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ-ส่งไฟล์ขนาดใหญ่ ฟังเพลง ออนไลน์ ดูทีวีออนไลน์ หรือ เล่นเกมส์ออนไลน์ ในช่วงเวลาทำการ ยกเว้นกรณีที่ได้รับอนุญาต

๓.ผู้ใช้งานจะต้องสามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔.ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดต้องได้รับการตั้งค่าให้มีความปลอดภัยและการมีการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย

๕.ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรมและได้รับการติดตั้งโดยผู้ที่มีความชำนาญที่ผ่านการพิจารณาอนุมัติแล้ว

๖.อุปกรณ์เครือข่าย อาทิ Router, Firewall, Switch, Wireless Access Point ต้องได้รับการตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้น ๆ หรือตามคำแนะนำขององค์การตลาด ด้านความมั่นคงปลอดภัยต่าง ๆ อาทิ SANS Institute หรือ NSA

๗.อุปกรณ์เครือข่ายที่สำคัญ เช่น Router, Core Switch ต้องมีอุปกรณ์สำรองไฟฟ้า (UPS) เสมอ การเปลี่ยนแปลงระบบเครือข่ายหรืออุปกรณ์เครือข่ายต้องได้รับการควบคุมโดยปฏิบัติตามเอกสาร

๘.วิธีการปฏิบัติงานเรื่องการจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management)

๙.ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)

๑๐.ข้อตกลงการให้บริการเครือข่ายต้องระบุถึงรายละเอียด และข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยระดับการให้บริการ และการบริหารจัดการบริการเครือข่ายทั้งหมดหากบริการเครือข่ายนั้น

๑๑.หากได้รับการดำเนินการโดยหน่วยงานภายนอก ต้องมีการระบุถึงสิทธิในการติดตามตรวจสอบ และตรวจประเมินการทำงานของหน่วยงานภายนอกด้วย

๑๒. ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่า อยู่นอกเหนือ ความรับผิดชอบขององค์การ

๑๓.องค์การไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อ หรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๑๔.ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่นการใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียวองค์การไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๑๕.ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๑๖.องค์การให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

๑๗.บัญชีผู้ใช้งาน (User Account) ที่องค์การให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ทีเกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๑๘.กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑๙.ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓.๒.๒ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์การมีแนวทางปฏิบัติดังนี้

๑ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

๒ ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกห้องควบคุมระบบเครือข่ายขององค์การตามกระบวนการที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

๓ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องมีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบ

เครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

๔ การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

๓.๒.๓ ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้

๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุ ไว้ในเอกสาร“แบบฟอร์มการเข้า-ออกพื้นที”

๒ เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

๓.๒.๔. การระบุอุปกรณ์บนเครือข่าย

๑. ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๒. กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

๓ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๓.๒.๕ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๑ ผู้ดูแลระบบต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อ ระบบเครือข่าย

๒ ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างน้อยสัปดาห์ละครั้ง

๓ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องควบคุมระบบเครือข่าย/ ระบบคอมพิวเตอร์ จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า-ออกพื้นที่ ” ให้ถูกต้อง

๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบและหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดเป็นลายลักษณ์อักษรเท่านั้น

๓.๒.๖ การแบ่งแยกเครือข่าย

๑ องค์การแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๒ องค์การจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

๓ องค์การติดตั้ง Firewall เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี

๓.๒.๗ การการควบคุมการเชื่อมต่อทางเครือข่าย

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๑ มีการตรวจสอบการเชื่อมต่อเครือข่าย

๒ จำกัดสิทธิ์ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๓ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๓.๒.๘ การควบคุมการจัดเส้นทางบนเครือข่าย

ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๑ ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address)

๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓ กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทาง ที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่าย

๓.๓ การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

๑.การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration) การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียน ผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์ การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์การตลาด เป็นต้น โดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (Access Control) และวิธีปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศ โดยผู้ใช้งานต้องได้รับการทบทวนและพิจารณาอนุมัติตามขั้นตอนขององค์การตลาดอย่างเคร่งครัด

๒.ผู้ใช้งานมีสิทธิ์การเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบในส่วนงานนั้น ๆ โดยการเข้าถึงข้อมูลจะต้องได้รับการอนุมัติจากผู้บริหารสายงาน และ ฝ่ายบุคคลเป็นผู้แจ้งดำเนินการกำหนดสิทธิ์การเข้าถึงข้อมูลในกรณีพนักงานเข้างานใหม่ ย้ายสายงาน หรือ พ้นสถาพการเป็นพนักงาน กรณีเป็นการขอสิทธิ์ เข้าถึงข้อมูลข้ามสายงาน จะต้องได้รับการอนุมัติจากผู้บริหารของหน่วยงานเจ้าของข้อมูลเพิ่มเติม

๓.๔ การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

๑.ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ทบทวนสิทธิ์โดยหัวหน้างาน หรือ ผู้บริหารสายงาน

๓.๕ การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights)

๑.สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๓.๖ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibility)

๑.การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

•พนักงานต้องเก็บรักษา Username และ Password ต้องเป็นความลับห้ามเปิดเผยให้บุคคลอื่นทราบ

•พนักงานต้องหลีกเลี่ยงการเก็บบันทึกข้อมูลการตรวจสอบความลับ เว้นแต่สามารถเก็บไว้อย่างปลอดภัย

•เมื่อพนักงานได้รับข้อมูล Password ซึ่งเป็นข้อมูล Default ควรมีการแก้ไขทันที

เมื่อเข้าใช้งานระบบครั้งแรก

๓.๗ การควบคุมการเข้าถึงระบบ (Application and information access control)

๓.๗.๑. การจำกัดการเข้าถึงสารสนเทศ (Information Access control)

๑.ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๒.บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๓.บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ขององค์การตลาดอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์การตลาด

สำหรับผู้ดูแลระบบ

๔.ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์การควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติ สำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๕.ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินทราเน็ต (Intranet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์ อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๖.ผู้ดูแลระบบ (System Administrator) ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ(Limitation of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งาน ไม่มีการใช้งานระบบสารสนเทศ เกินกว่า ๑๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Login
เข้าระบบสารสนเทศอีกครั้ง

๗. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน ของบุคลากรดังต่อไปนี้

๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มี การป้องกันในการส่งรหัสผ่าน (Password)

๓ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้อง ได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้ งานและระงับการใช้

งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมี การกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัส ผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๘. เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ องค์การได้กำหนดช่องทางการเข้าถึงระบบสารสนเทศที่สำคัญที่องค์การพัฒนาในรูปแบบของ Web base Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายใน ซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยง เครือข่ายดังกล่าว

๙.ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้น ความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการ เข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการ เข้าถึงผ่านระบบงาน

๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรอง และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๑ ต้องกำหนดให้ระบบสารสนเทศหรือแอพพลิเคชั่น มีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุ และพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ ทุก ๆ ๑ ชั่วโมง

๒ ต้องมีการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น

แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน

๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์การ ได้แก่ ระบบ GFMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงาน ด้านการงบประมาณการบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ซึ่งดูแล รับผิดชอบโดยกรมบัญชีกลางจะได้รับการแยกออกจากระบบงานอื่น ๆ ขององค์การ

๒ ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

๓ ระบบซึ่งไวต่อการรบกวน มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกสำนักงานที่เกี่ยวของกับระบบดังกล่าว

แนวปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑ ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาต ให้เริ่มปฏิบัติงานจากระยะไกล

๒ ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์การ ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงาน จากระยะไกล

๓ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกล โดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์การ

๔ ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์การในสถานที่ดังกล่าว

๕ ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์การ

๖ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศขององค์การจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์การต้องการ

๗ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๘ องค์การไม่อนุญาตให้ ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบสารสนเทศ ขององค์การจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยองค์การ

๙ องค์การต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงาน และบริการต่าง ๆ ขององค์การที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๐ องค์การต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๓.๗.๒.ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure) กำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย กำหนดให้ระบบปฏิเสธการให้บริการหากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน ๕ ครั้ง

๓.๗.๓. ระบบบริหารจัดการรหัสผ่าน (Password Management System)

๑.กำหนดให้ระบบตรวจสอบคุณภาพของรหัสผ่านและ มีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านทุก ๙๐ วัน

๒.มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๓.๗.๔.การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

๑.การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบต้องมีการขออนุมัติจากหัวหน้าสายงาน และ ต้องได้รับการตรวจสอบจากฝ่ายเทคโนโลยีสารสนเทศ

ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

๒.ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

๓.จัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น

๔. จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๕. การใช้งานโปรแกรมอรรถประโยชน์ จะต้องได้รับอนุญาตให้ใช้งานตามสิทธิ์ในการใช้งานกำหนดไว้แล้วโดยจะได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๖. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๗. มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๘. กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๙. ผู้ใช้งานต้องใช้งานโปรแกรมอรรถประโยชน์ที่องค์การมีลิขสิทธิ์ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานโปรแกรมอรรถประโยชน์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๓.๗.๕.การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)

๑.ผู้พัฒนาระบบสารสนเทศควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง หรือให้บริการ โดยไม่เก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย และไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

๓.๗.๖.แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ต้องกำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิด ความผิดพลาดผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้น จากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๔ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชี ผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็น

ทางด้านธุรกิจหรือด้านเทคนิค

๓.๗.๘.แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

๑ ต้องกำหนดการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๒๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๐ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๒ ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๓ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๓.๘ การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

เครื่องคอมพิวเตอร์ส่วนบุคคล

๑ เครื่องคอมพิวเตอร์ที่องค์การตลาด จัดหาให้ถือเป็นสินทรัพย์ขององค์การตลาด ผู้ใช้งานควรใช้งานอย่างเหมาะสมกับการทำงานเพื่อตอบสนองต่อภารกิจขององค์การตลาด อย่างมีประสิทธิ์ภาพ

๒ซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์ขององค์การตลาด ต้องมีลิขสิทธิ์อย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกซอฟต์แวร์ต่างๆ รวมทั้งการนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย และไม่อนุญาตให้ผู้ใช้งานติดตั้งเปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์ในเครื่องคอมพิวเตอร์ขององค์การตลาด

๓ ผู้ใช้งานต้องตรวจสอบไวรัสจากซอฟต์แวร์ป้องกันไวรัสที่เชื่อถือได้ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ

๔ ผู้ใช้งานต้องรับผิดชอบในการป้องกันการสูญหาย และความสูญหายของคอมพิวเตอร์และอุปกรณ์ที่องค์การตลาดจัดหาให้

๕ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงหรือแก้ไขส่วนประกอบย่อย (sub component) ที่ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์ขององค์การตลาด รวมถึงแบตเตอรี่ของเครื่องคอมพิวเตอร์แบบพกพา

๖ เครื่องคอมพิวเตอร์ที่องค์การอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์การ ดังนั้น ผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์การ

๗ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์การ ต้องเป็นโปรแกรมที่องค์การได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๘ ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์การ

๙ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ขององค์การเท่านั้น

๑๐ การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของฝ่ายสารสนเทศเท่านั้น

๑๑ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกัน ไวรัส

๑๒ ไม่เก็บข้อมูลสำคัญขององค์การไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๑๓ ไม่สร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ

องค์การ

๑๔ ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยปฏิบัติดังต่อนี้

๑ ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๒ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

๑ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD External Hard Disk เป็นต้น

๒ ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๓ ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับ การทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์การ

๔ แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสม

๕ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๓.๙ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

สำหรับผู้ดูแลระบบ

๑ กำหนดสิทธิ์ตามความเหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบของผู้ใช้งาน

๒ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๕ ครั้ง

๓ ทบทวนสิทธิ์การเข้าใช้งานและปรับปรุงบัญชีรายชื่อผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือในทันทีเมื่อมีการเปลี่ยนแปลง ได้แก่ ลาออกเปลี่ยนตำแหน่งโอนย้ายหรือสิ้นสุดการจ้าง

๔ ควบคุมการเข้าถึงตามแนวทางการบริหารจัดการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้อย่างเคร่งครัด

สำหรับผู้ใช้งาน

๕ ลงทะเบียนขอใช้งาน โดยกรอกคำขอเข้าใช้งาน แล้วยื่นกับพนักงานเพื่อ ดำเนินการกำหนดสิทธิ์ในบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Password)

๖ เมื่อได้รับรายชื่อผู้ใช้งานและรหัสผ่าน (Password) แล้ว การเข้าสู่ระบบในครั้ง แรกนั้นต้องเปลี่ยนรหัสผ่านโดยทันที

๗ ต้องไม่บันทึกหรือจัดเก็บรหัสผ่านในเครื่องคอมพิวเตอร์ส่วนบุคคลในรูปแบบที่ ไม่ได้รับการป้องกันหรือการเข้ารหัสข้อมูล

๘ ต้องเปลี่ยนรหัสผ่าน (Password) ตามช่วงระยะเวลาที่กำหนด ทุก ๓ เดือน

๙ ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่น เพื่ออ่านหรือ รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ต้องเป็นผู้รับผิดชอบต่อการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของตน

๑๐ หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ของตัวเอง

๑๑ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับต้องระบุความสำคัญลงในหัวข้อจดหมายอิเล็กทรอนิกส์ พร้อมกับทำการเข้ารหัส (Encryption)

๑๒ ต้องเก็บรักษาบัญชีรายชื่อผู้ใช้ (User account) และรหัสผ่าน (Password) ของตนเองให้เป็นความลับ

๑๓ ปฏิบัติตามวิธีการใช้งานรหัสผ่าน (Password use) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๔ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๕ ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

๑๖ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์การหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ ผ่านระบบเครือข่ายขององค์การ

๑๗ ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน รับ-ส่ง ความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมาย อิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑๘ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์การ เพื่อการทำงานขององค์การเท่านั้น

๑๙ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒๐ ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

๒๑ ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒๒ ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพ หรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์การ ทำให้เกิดความแตกแยกระหว่างองค์การผ่านทางจดหมายอิเล็กทรอนิกส์

๒๓ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒๔ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒๕ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๒๖ ข้อควรระวัง ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๓.๑๐ การควบคุมการใช้งานระบบอินเทอร์เน็ต (Internet)

๑ ผู้ใช้งานต้องเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้นและห้ามผู้ใช้งานทำการเชื่อมต่อเครื่องคอมพิวเตอร์ ผ่านช่องทางอื่นยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้บริหารฝ่ายสารสนเทศเป็นลายลักษณ์อักษร ก่อนการดำเนินการ

๒ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่และความรับผิดชอบเพื่อประสิทธิ์ ภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลขององค์การตลาด และต้องไม่ใช้ระบบอินเทอร์เน็ตขององค์การตลาด เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับองค์การตลาด

๓ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์การตลาด ที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดซอฟแวร์จากระบบอินเตอร์เน็ตรวมถึงการดาวน์โหลด การอัพเดท (Update) ซอฟแวร์ต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือสินทรัพย์ทางปัญญา

๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Web board) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์การตลาด

๖ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Web board) ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กรการทำลายความสัมพันธ์กับบุคคลากรของหน่วยงาน

๗ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้วให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๓.๑๑ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social network)

๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่องค์การตลาดได้กำหนดไว้เท่านั้น

๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใดๆที่มีผลกระทบกับองค์กรจากการใช้งานเครือข่ายสังคมออนไลน์

๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับ องค์การตลาด ผู้ใช้งานต้องแจ้งต่อฝ่ายเทคโนโลยีสารสนเทศโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

๓.๑๒ การควบคุมการเข้าใช้งานระบบจากภายนอก

๑ การเข้าสู่ระบบจากระยะไกล (remote access) สู่ระบบสารสนเทศและเครือข่ายต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๒ การเข้าสู่ระบบจากระยะไกล (remote access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนเองของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๓ วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากหัวหน้าฝ่ายสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

๔ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุมัติจากหัวหน้าฝ่ายสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมายเป็นลายลักษณ์อักษร

๕ มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการ

โทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๖ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด port และ modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๗ ระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติดังนี้

๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศ

๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

๓.๑๓ มีการควบคุมการใช้สื่อบันทึกข้อมูลแบบพกพา (Removable media) ตามชั้นความลับของข้อมูล ดังนี้

๑.ให้มีการเข้ารหัส (Encryption) ข้อมูลบนสื่อบันทึกข้อมูลแบบพกพาตามระดับชั้นความลับ

๒.ตรวจสอบสื่อบันทึกข้อมูลแบบพกพา ไม่มีโปรแกรมไม่พึงประสงค์ (Malware) ก่อนที่จะเชื่อมต่อกับระบบคอมพิวเตอร์

ส่วนที่ ๔
นโยบายการรักษาความความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and environmental security)

๑. วัตถุประสงค์

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้ง และพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็น ทรัพย์สินขององค์การตลาด และเพื่อป้องกันการสูญหาย ความเสียหาย การขโมย หรือภาวะเป็นอันตรายต่อทรัพย์สินสารสนเทศและ ป้องกันการหยุดชะงักต่อการดำเนินงานขององค์การตลาด

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑.การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

๑.จำแนก และกำหนดพื้นที่ในการใช้งานระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับ อนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ เมื่อมีการกำหนดพื้นที่แล้วให้มีการควบคุม การเข้าออก

๒.จำแนก กำหนด และแบ่งบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspaces)” รวมทั้งจัดทำแผนผังแสดงตำแหน่ง และชนิดของพื้นที่ใช้งาน ระบบเทคโนโลยีสารสนเทศ และ ประกาศให้ทราบทั่วกัน (หน่วยงานควรระบุให้ชัดเจนว่ามีพื้นที่ใช้งาน ระบบเทคโนโลยีสารสนเทศประเภทใดบ้าง และมีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศใดที่อาจจำแนก ได้มากกว่า ๑ ประเภท)

๓.การติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศใน “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” จะต้อง สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ ฝ่ายสารสนเทศ/ผู้ดูแลระบบต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน

๓.๒.การควบคุมการเข้าออก (Physical Entry Controls)

๑.การควบคุมการเข้าออกใน บริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะ “พนักงานที่มี สิทธิ์เท่านั้น และมีแนวทางปฏิบัติ ดังนี้

๑) ต้องกำหนดพนักงาน ที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน

๒) พนักงาน จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๓) หากมีบุคคลอื่นใดที่ไม่ใช่พนักงานที่ได้รับอนุญาต ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็น การล่วงหน้าหน่วยงานต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่ เป็นการชั่วคราว ต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Data Center) ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย ๑ ปี

๔) บุคคลภายนอกต้องทำการสแกนใบหน้าของตนก่อนได้รับอนุญาตให้เข้าถึงพื้นที่สำนักงาน

๕) พนักงานองค์การตลาด ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายใน พื้นที่ สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับ

อนุญาต

๖) ผู้ใช้งานต้องแจ้งพนักงานรักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าเข้ามาติดต่อในพื้นที่สานักงาน

๗) พนักงานองค์การตลาดควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สำนักงาน

๓.๓.การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

๑.เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ห้ามตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออกของบุคคลเป็นจำนวนมาก ไม่มีป้าย หรือ สัญลักษณ์ ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตู หน้าต่างของสำนักงาน หรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่ ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

๒.พนักงานควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓.ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงานในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๔.ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลาย อย่างเหมาะสม วิธีการทำลายข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์เหล่านี้โดยปฏิบัติตามเอกสารวิธีปฏิบัติงาน เรื่องการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล (Disposal of Media Procedure)

๕.พนักงานต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นพนักงานที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๓.๔.การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (Protecting against External and Environmental Threats) เพื่อประโยชน์ในการรักษาความปลอดภัยสถานที่ติดตั้งและเก็บรักษาทรัพย์สินด้านสารสนเทศต้องจัดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ พร้อมทั้งให้ทดสอบระบบรักษาความปลอดภัยภายในอย่างน้องปีละ ๑ ครั้ง

๓.๕.การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

๑.หัวหน้าของแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ” และ “ห้ามสูบ บุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

๓.๖.การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับส่งสิ่งของ (Delivery and Loading Areas)

๑.หน่วยงานต้องมีการจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ หากเป็นไปได้ ควรแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทำงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น บริเวณเก็บและ จัดส่งสินค้าจะต้องไม่อยู่ในพื้นที่ที่บุคคลภายนอกเข้าถึงได้

๒.พนักงานและพนักงานของหน่วยงานภายนอก (Third Party) ต้องติดบัตรประจำตัวตลอดเวลาขณะปฏิบัติหน้าที่ในบริเวณสำนักงาน และหากผู้ใดพบเห็นผู้ที่ไม่ติดบัตรประจำตัวถือเป็นหน้าที่ที่จะต้องแจ้งพนักงานรักษาความปลอดภัยโดยทันที

๓.๗. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment) เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์ คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

๓.๗.๑.การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Seting and Protection)

๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อให้เกิดความเป็นระเบียบเรียบร้อย และไม่เกิดความเสี่ยงจากความร้อน แสงแดด ฝุ่นละออกและความชื้น

๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย

๓) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ ตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติ

๔) ไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานขององค์การตลาดโดยมิได้รับอนุญาต

๓.๗.๒ การดูแลอุปกรณ์ต่าง ๆ (Supporting Utilities)

๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบ ดังต่อไปนี้

๑. ระบบสำรองกระแสไฟฟ้า (UPS)

๒. ระบบระบายอากาศ

๓. ระบบปรับอากาศ และควบคุมความชื้น

๔. ระบบดังเพลิง

๕. ระบบกล้องวงจรปิด

๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านี้อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๓.๗.๓ การเดินสายไฟและสายเคเบิล (Cabling Security)

๑) สายเคเบิ้ลที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อ สายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณและป้องกันสัตว์ต่าง ๆ กัดแทะสาย

๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน

๓) ทำป้ายชื่อสำหรับสายสัญญาณ

๔) จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๓.๗.๔ การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

๑) ให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนดและต้องปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๒) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจในภายหลัง

๓) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๔) ควบคุมและสอดส่องดูแลการปฏิบัติงานขององค์การตลาดผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในองค์การตลาด

๕) ควบคุมการส่งอุปกรณ์ที่นำออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือ

การเข้าถึง ข้อมูลโดยไม่ได้รับอนุญาต หรือส่งอุปกรณ์ดังกล่าวไปซ่อมบำรุง ทั้งนี้เพื่อเป็นการป้องกันการรั่วไหลของข้อมูล

๓.๗.๕ การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of Asset)

๑) ห้ามนำทรัพย์สินด้านสารสนเทศขององค์การตลาดออนอกองค์กร โดยไม่ได้รับอนุญาต

๒) ให้มีบันทึกการนำทรัพย์สินด้านสารสนเทศก่อนนำออกจากองค์กรและบันทึกการส่งคืนเพื่อเก็บเป็นหลักฐานป้องกันการสูญหาย

๓.๗.๖ การป้องกันอุปกรณ์และสินทรัพย์ด้านสารสนเทศที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment and asset Off-Premises)

๑) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินด้านสารสนเทศขององค์การตลาดไว้นอกพื้นที่องค์กรโดยไม่มีผู้ดูแล

๒) ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินขององค์การตลาดเสมือนเป็นทรัพย์สินของตนเอง

๓.๗.๗ การจัดการอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

๑) ผู้ดูแลระบบฯ หรือผู้ใช้งานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ ทั้งนี้เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลดังกล่าว

๓.๗.๘ การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)

๑) ผู้ใช้งานต้องออกจากระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการปฏิบัติงาน และปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการปฏิบัติงานประจำวัน หรือเมื่อไม่มีการใช้งานเกิน ๑ ชั่วโมง

๒) ผู้ใช้งานต้องล๊อคอุปกรณ์เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๓) ผู้ใช้งานต้องปิด ล็อกพื้นที่เพื่อจัดเก็บอุปกรณ์ในสถานที่ปลอดภัยเมื่อไม่มีการใช้งาน

๔) กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอเมื่อไม่มีผู้ใช้งานนานเกินกว่า ๑๕ นาที และมีการใส่รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๓.๗.๙ การควบคุมการไม่ทิ้งทรัพย์สินด้านสารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)

๑) ข้อมูลความลับหรือข้อมูลที่มีความสำคัญที่บันทึกอยู่ในเอกสารในรูปแบบกระดาษหรือที่จัดเก็บใน สื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์ ต้องมีการจัดเก็บอย่างปลอดภัยเมื่อไม่มีความจำเป็นต้องใช้งาน

๒) ต้องล็อกหน้าจอเครื่องคอมพิวเตอร์ด้วยรหัสผ่าน หรือระบบการยืนยันตัวตนอื่นเมื่อไม่ได้ใช้งาน

๓) ไม่วางเอกสารที่มีชั้นความลับหรือเอกสารสำคัญ ซึ่งสั่งพิมพ์ผ่านเครื่องพิมพ์ทิ้งไว้

ส่วนที่ ๕
นโยบายการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
(Communications security)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึงล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหาย ต่อข้อมูลและระบบสารสนเทศขององค์การ โดยมีการกำหนดนโยบายและแนวปฏิบัติควบคุมการเข้าใช้งาน เครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ การใช้งานบริการเครือข่าย

๓.๑.๑ ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่า อยู่นอกเหนือความรับผิดชอบขององค์การ

๓.๑.๒ องค์การไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อ หรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่นคือผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่นการใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์การไม่มีส่วนร่วมรับผิดชอบ ความเสียหายดังกล่าว

๓.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๓.๑.๕ องค์การให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

๓.๑.๖ บัญชีผู้ใช้งาน (User Account) ที่องค์การให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ทีเกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๑.๗ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๑.๘ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓.๒ ต้องมีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่นอกองค์การ ก่อนที่จะอนุญาตให้เข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์การได้

๓.๓ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์การมีแนวทางปฏิบัติดังนี้

๓.๓.๑ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

๓.๓.๒ ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกห้องควบคุมระบบเครือข่ายขององค์การตามกระบวนการที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

๓.๓.๓ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องมีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

๓.๓.๔ การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

๓.๔ ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้

๓.๔.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุ ไว้ในเอกสาร“แบบฟอร์มการเข้า-ออกพื้นที”

๓.๔.๒ เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

๓.๕ การระบุอุปกรณ์บนเครือข่าย

๓.๕.๑ ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๓.๕.๒ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

๓.๕.๓ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๓.๖ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๓.๖.๑ ผู้ดูแลระบบต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อ ระบบเครือข่าย

๓.๖.๒ ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างน้อยสัปดาห์ละครั้ง

๓.๖.๓ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องควบคุมระบบเครือข่าย/ ระบบคอมพิวเตอร์ จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า-ออกพื้นที่ ” ให้ถูกต้อง

๓.๖.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบและหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดเป็นลายลักษณ์อักษรเท่านั้น

๓.๗ การแบ่งแยกเครือข่าย

๓.๗.๑ องค์การแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๓.๗.๒ องค์การจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งาน ระบบสารสนเทศ

๓.๗.๓ องค์การติดตั้ง Firewall เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี

๓.๘ การการควบคุมการเชื่อมต่อทางเครือข่ายต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๓.๘.๑ มีการตรวจสอบการเชื่อมต่อเครือข่าย

๓.๘.๒ จำกัดสิทธิ์ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๓.๘.๓ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๓.๘.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๓.๘.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๓.๙ การควบคุมการจัดเส้นทางบนเครือข่าย ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๓.๙.๑ ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address)

๓.๙.๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓.๙.๓ กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่าย

๓.๓ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN access control)

ผู้ดูแลระบบ (System Administrator)

๑) ต้องทำการลงทะเบียนกำหนดสิทธิ์การเข้าถึงระบบเครือข่ายไร้สายของผู้ใช้งาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ดูแลระบบอนุญาตให้ผู้ใช้งานตามความจำเป็นในการใช้งานเท่านั้น

๒) ต้องทำการลงทะเบียนอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย (Wireless LAN client) ทุกตัว

๓ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์กระจายสัญญาณรั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๔ ต้องเปลี่ยนค่า SSID (Service set identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้นที่มาจาก ผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๕ ต้องกำหนดค่าใช้ WPA๒ (Wi-Fi protected access) ในการเข้ารหัสข้อมูล ระหว่างอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย (Wireless LAN client) และอุปกรณ์กระจายสัญญาณ (Access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๖) ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับระบบเครือข่ายภายในขององค์การตลาด

๗) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานตามสายบังคับบัญชาทราบโดยทันที

ส่วนที่ ๖
นโยบายการรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
(IT operations security)

๑. วัตถุประสงค์

เพื่อเพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

๓.๑.๑ ขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

<u>สำหรับผู้ดูแลระบบ</u>

๑) ต้องจัดทำเอกสารวิธีปฏิบัติที่เหมาะสมสำหรับแต่ละระบบสารสนเทศที่อยู่ในความรับผิดชอบของตนและประกาศให้ผู้ปฏิบัติงานทราบ

๒) ต้องปรับปรุงเอกสารวิธีปฏิบัติตามความเหมาะสมต่อสภาวะแวดล้อมการปฏิบัติงาน

๓) มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศถูกเข้าถึงโดยมิได้รับอนุญาต

๓.๑.๒ การจัดการการเปลี่ยนแปลง (Change Management)

๑) ก่อนทำการเปลี่ยนแปลงกับระบบสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือ ฐานข้อมูล โดยผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้องดำเนินการขออนุมัติการดำเนินการเปลี่ยนแปลงจากผู้อำนวยการองค์การตลาดอย่างเป็นลายลักษณ์อักษร

๒) การเปลี่ยนแปลงกับระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือฐานข้อมูลโดยผู้ใช้บริการภายนอกต้องได้รับการควบคุมดูแลจากผู้ดูแลระบบฯ

๓) ผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้องมีการประเมินผลกระทบการเปลี่ยนแปลงระบบ ก่อนที่จะทำการเปลี่ยนแปลงนั้น เพื่อป้องกันกระทบกับการทำงานของระบบที่ใช้ดำเนินงานอยู่ในปัจจุบัน

๔) ผู้ดูแลระบบฯ ต้องบันทึกรายละเอียดการเปลี่ยนแปลงระบบสารสนเทศ

๕) ผู้ดูแลระบบฯ หรือผู้ใช้บริการภายนอกต้องมีการทดสอบการเปลี่ยนแปลงนั้นก่อนเสมอ

๖) ผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้องกำหนดแผนย้อนคืน (Fallback Plan) เพื่อรองรับหากการเปลี่ยนแปลงไม่เป็นไปตามที่คาดคิด

๗) ผู้ดูแลระบบฯ หรือผู้ให้บริการจากภายนอกต้องกำหนดระยะเวลาในการติดตามการเปลี่ยนแปลงนั้น เพื่อตรวจสอบผลกระทบที่อาจเกิดขึ้นกับระบบหลังจากการเปลี่ยนแปลง

๓.๑.๓ การจัดการขีดความสามารถ (Capacity Management) ผู้ดูแลระบบฯ ต้องเฝ้าติดตามสังเกตการใช้งานทรัพยากรสารสนเทศ และมีการติดตามประเมินผลอย่างสม่ำเสมอ เพื่อวางแผนบริหาร

ทรัพยากรสารสนเทศให้รองรับการ ปฏิบัติงานในอนาคตอย่างเหมาะสม อย่างน้องปีละ ๑ ครั้ง

๓.๑.๔ การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบและสภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment) กำหนดให้มีการแยกระบบสารสนเทศสำหรับการทดสอบ และใช้งานจริง ออกจากกันเพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต

๓.๒ การสำรองข้อมูล (Backup) เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัย ธรรมชาติ ระบบเสียหาย ฯลฯ

๓.๒.๑ การสำรองข้อมูล (Information Backup)

๑) ผู้ดูแลระบบฯ และเจ้าของข้อมูลทำบัญชีรายชื่อข้อมูลที่มีความสำคัญและปรับปรุงบัญชี รายชื่อให้มีความทันสมัยอยู่เสมอ

๒) ผู้ดูแลระบบฯ กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลไว้อย่างน้อยต้อง ประกอบด้วยข้อมูลในฐานข้อมูลของระบบสารสนเทศหรือไฟล์ข้อมูลที่เกี่ยวข้อง

๓) ผู้ดูแลระบบฯ กำหนดความถี่ในการสำรอบข้อมูล

๓.๒.๒ แนวปฏิบัติการสำรองข้อมูล

๑) ผู้ดูแลระบบฯ ต้องจัดให้มีการสำรองและทดสอบการกู้คนข้อมูลอย่างน้องปีละ ๑ ครั้ง

๒) ผู้ดูแลระบบฯ ต้องจัดทำบันทึกการสำรองข้อมูล (Operation Logs)

๓) ผู้ดูแลระบบฯ ต้องจัดทำรายงานข้อผิดพลาด (Fault Logging) ที่เกิดจากการสำรองข้อมูล รวมทั้งวิธีการแก้ไข

๔) กำหนดชนิดและช่วงเวลาของการสำรองข้อมูล พร้อมทั้งสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรอง ข้อมูลมี ๒ ชนิด คือ การสำรองข้อมูลแบบเต็ม และ การสำรองข้อมูลแบบเพิ่มส่วนต่าง

๕) ในกรณีพบปัญหาทำให้ไม่สามารสำรองข้อมูลได้อย่างครบถ้วนสมบูรณ์ให้ผู้ดูแลจัดการระบบงาน ดำเนินการแก้ไขปัญหา และ สรุปผลให้ผู้บังคับบัญชาทราบ

๖) ผู้ดูแลระบบฯ ต้องสำรองข้อมูลตามความถี่ที่ผู้วิเคราะห์ระบบแนะนำ หรือดังนี้เป็นอย่างน้อย

รายการ	**ข้อมูลที่ต้องสำรอง**	**ความถี่ในการสำรองข้อมูลแบบเต็ม**
ระบบ Web Server	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ข้อมูลบนเว็บที่เผยแพร่	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
ระบบ Database server	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ฐานข้อมูลที่มีความสำคัญ	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
อุปกรณ์ Firewall	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
อุปกรณ์ Server อื่น ๆ	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ฐานข้อมูลที่มีความสำคัญต่อระบบ	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า

๗) ผู้ใช้งานต้องสำรองข้อมูลตามความจำเป็นและเหมาะสมไว้บนสื่อบันทึกอื่น ๆ เป็นประจำทุกเดือน

๘) ผู้ใช้งานต้องรักษาสื่อบันทึกข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของ ข้อมูล และ ห้ามนำข้อมูลไปเปิดเผยต่อบุคคลภายนอกองค์การตลาดฯ โดยตั้งใจ หรือไม่ตั้งใจ

๓.๓ การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring) เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

๓.๓.๑ การบันทึกข้อมูลเหตุการณ์ (Event logging)

๑) ระบบคอมพิวเตอร์หรือระบบเครือข่ายต้องมีการเก็บบันทึกข้อมูลล็อก ต้องบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการ สืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง รวมทั้งให้มีการวิเคราะห์ข้อมูลล็อก ดังกล่าวอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดอย่างเหมาะสม

๒) มีการติดตามสังเกต และประเมินผลการติดตามดังกล่าวอย่างสม่ำเสมอ

๓) ต้องจัดเก็บข้อมูลล็อกทางคอมพิวเตอร์เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน

๓.๓.๒ การป้องกันข้อมูลล็อก (Protection of Log Information) ระบบสารสนเทศที่จัดเก็บข้อมูลล็อก ต้องได้รับการปกป้องเพื่อป้องกันการเข้าถึงหรือแก้ไข เปลี่ยนแปลงโดยมิได้รับอนุญาต

๓.๓.๓ ข้อมูลล็อกของผู้ดูแลระบบและพนักงานปฏิบัติการ (Administrator and Operator Logs) กำหนดให้มีการเก็บข้อมูลล็อกที่เกี่ยวข้องกับการดูแลระบบโดยผู้ดูแลระบบฯ

๓.๓.๔ การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และระบบเครือข่ายให้มีเวลาตรงกันทั้งหมดโดยให้อ้างอิงเวลา สากล (Stratum ๐) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๓.๔ การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software) เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

๓.๔.๑ การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems) ผู้ดูแลระบบฯ ต้องควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี ซอฟต์แวร์อุดช่องโหว่า ลงใน เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการอยู่ โดยต้องมีการทดสอบซอฟต์แวร์เหล่านั้นก่อน เพื่อให้มั่นใจ ว่าจะไม่ ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

๓.๕ การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management) เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ระบบสารสนเทศ รวมทั้ง สารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจาการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือ ตีพิมพ์ในสถานที่ต่าง ๆ

๓.๕.๑ การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

๑) ผู้ดูแลระบบฯ ต้องปรับปรุงระบบซอฟต์แวร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ อย่าสม่ำเสมอ

๒) ผู้ดูแลระบบฯ ต้องประเมินความเสี่ยงของช่องโหว่ทางเทคนิค และกำหนดมาตรการเพื่อลดความ เสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๓) ผู้ดูแลระบบคอมพิวเตอร์ต้องกำหนดและจำกัดรายการของซอฟต์แวร์ที่ติดตั้งบนเครื่อง คอมพิวเตอร์ลูกข่าย

๓.๖ การพิจารณาการตรวจสอบระบบสารสนเทศ(Information System Audit Considerations) เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

๓.๖.๑ การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)ผู้ตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องตรวจสอบและประเมินความเสี่ยง ด้านสารสนเทศตามแนวทาง ดังนี้

๑) ให้มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศโดยเจ้าของระบบสารสนเทศ

๒) ให้มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๓) ให้มีการตรงจสอบและประเมินความเสี่ยงของระบบสารสนเทศที่ให้บริการ

๔) ให้มีการตรวจสอบและประเมนความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๕) ภายหลังการตรวจสอบให้รายงานผลการตรวจสอบ และประเมินความเสี่ยงของระบบสารสนเทศต่อ เจ้าของระบบสารสนเทศทราบต่อไป

๖) เจ้าของระบบสารสนเทศที่ได้รับการตรวจสอบและประเมินความเสี่ยงต้องจัดทำแผนดำเนินการเพื่อบริหารจัดการความเสี่ยงที่ตรวจพบเหล่านั้น

๗) รายการที่ต้องมีการตรวจประเมินอย่างน้อยดังนี้

- การป้องกันการบุกรุกระบบสารสนเทศ
- การสำรองข้อมูล
- การควบคุมการเข้าถึงพื้นที่ Data Center
- การควบคุมการเข้า-ออกอาคาร
- การเตรียมความพร้องรับสถานการณ์ฉุกเฉิน
- การเข้าถึงระบบสารสนเทศ
- การกำหนดใช้งานตามภารกิจ

ส่วนที่ ๗
นโยบายการจัดหา การพัฒนาและดูแลระบบเทคโนโลยีสารสนเทศ
(System acquisition development and Maintenance)

๑. วัตถุประสงค์

เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการ พัฒนา ระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

๓.๑.๑ การกำหนดความต้องการด้านความมั่นคงปลอดภัย (Information Security Requirements analysis and Specification)

๑) กำหนดให้มีเกณฑ์การตรวจรับ ระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชันใหม่ หรือควรมีการ ทดสอบ ระบบสารสนเทศก่อนการตรวจรับ

๒) กำหนดให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศในการ จัดทำข้อกำหนดขั้นต่อของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม

๓) ข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้ รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

๔) กำหนดให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง Authenticity และความถูกต้อง ครบถ้วน Integrity ของข้อมูลใน แอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสมต้องมีการดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์

๓.๑.๒ ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks) สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการ ป้องกัน และการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

๓.๑.๓ การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูล ที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดย ไม่ได้รับ อนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

๓.๑.๔ ความมั่นคงปลอดภัยสาหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัยครอบคลุมทั้งวงจรการพัฒนา ระบบสารสนเทศ (development lifecycle)

๓.๒ ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

๓.๒.๑ นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย(Secure development policy) มีการแยกระบบสารสนเทศสำหรับการพัฒนาและใช้งานจริงออกจากกันเพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต

๓.๒.๒ กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

๑) ผู้ดูแลระบบต้องแจ้งให้ผู้ที่เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงหรือเปลี่ยนแปลงระบบเพื่อให้บุคคล เหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการปรับปรุงหรือเปลี่ยนแปลง ระบบ

๒) ผู้ดูแลระบบ ต้องวางแผนดำเนินการปรับปรุงหรือเปลี่ยนแปลงระบบ ก่อนเปลี่ยนไปใช้ระบบใหม่ ผู้ดูแลระบบ ต้องทดสอบโปรแกรมระบบ (System Software) ที่มีความสำคัญ และประสิทธิภายการใช้งานโดยทั่วไป หลังจากการแก้ไข หรือบำรุงรักษาระบบ

๓.๒.๓ การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes) เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบ ซอฟต์แวร์ต่างๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

๓.๒.๔ การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages) เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการ เปลี่ยนแปลง ทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุง ซอฟต์แวร์ใน อนาคต

๓.๒.๕ หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ

๓.๒.๖ สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment) ต้องมีการจัดทำหรือป้องกันสภาพแวดล้อมในการทำงานต่างๆ ให้มีความเหมาะสมและปลอดภัยทั้ง การพัฒนา และปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

๓.๒.๗ การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Out sourced Development) ในการทำสัญญาว่าจ้างการพัฒนาระบบขององค์การตลาด ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึง การรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

๓.๒.๘ การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing) โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมี การทดสอบอยู่ในช่วงระหว่างการพัฒนา

๓.๒.๙ การทดสอบเพื่อรับรองระบบ (System acceptance testing) มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับ ระบบใหม่ และระบบที่ปรับปรุงและต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ระบบที่จัดซื้อเข้ามาใช้งานหรือทรัพยากรสารสนเทศอื่นๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มี การเซ็นชื่อพนักงานทำการทดสอบและลายเซ็นผู้ส่งมอบ

๓.๓ ข้อมูลสำหรับการทดสอบ (Test data) เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

๓.๓.๑ การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data) ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูล นั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็น หลักฐานว่าได้นำข้อมูล

จริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยัง ผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

ส่วนที่ ๘
นโยบายการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ
(IT incident and problem management)

๑. วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสา นักงาน ได้รับการดาเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

๓.๑.๑ หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

๑) ผู้ใช้งานระบบสารสนเทศขององค์การตลาดมีหน้าที่ในการรายงานเหตุละเมิดหรือจุดอ่อนด้านความมั่นคงใดๆ ที่พบเห็น หรือที่ต้องสงสัยต่อผู้บังคับบัญชาและ/ หรือผู้ดูแลระบบ โดยทันที เพื่อให้สามารถแก้ไขปัญหาได้ อย่างรวดเร็ว ตัวอย่างของเหตุละเมิดความมั่นคงที่ต้องรายงานตรวจพบไวรัส หรือโปรแกรมไม่ประสงค์ดีต่าง ๆ ตรวจพบความพยายามเจาะระบบ หรือเครื่องมือเจาะระบบ การใช้งานข้อมูลหรือระบบสารสนเทศอย่างไม่เหมาะสม การเข้าถึงข้อมูลหรือระบบสารสนเทศโดยไม่ได้รับอนุญาต ช่องโหว่หรือจุดอ่อนของซอฟต์แวร์ การละเมิดนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย การกระทำที่ผิดกฎหมาย หรือข้อบังคับขององค์การตลาด

๒) ผู้ใช้งานระบบสารสนเทศขององค์การตลาดซึ่งพบเห็นเหตุละเมิด หรือจุดอ่อนด้านความมั่นคงต้องไม่บอกเล่า ถึงเหตุที่ตนพบเห็นนั้นกับบุคคลอื่นใด ยกเว้นผู้บังคับบัญชาและผู้ดูแลระบบฯ ทั้งนี้ ผู้ใช้งานต้องหลีกเลี่ยงการ พิสูจน์จุดอ่อนด้านความมั่นคงที่ต้องสงสัยด้วยตนเอง

๓) ผู้ดูแลระบบฯ มีหน้าที่ต้องรับผิดชอบต่อการรับมือเหตุละเมิดความมั่นคงปลอดภัยต้องดำเนินการ ตอบสอนต่อเหตุด้วยความรวดเร็ว มีสติรอบคอบ และต้องติดต่อประสานงานกับหน่วยงานต่าง ๆ ที่เกี่ยวข้องอย่างเหมาะสม รวมถึง บันทึกข้อมูล และจัดทำเอกสารเกี่ยวกับเหตุละเมิดความมั่นคงปลอดภัยโดยละเอียด

๔) ข้อมูลและหลักฐานที่เกี่ยวข้องกบเหตุละเมิดความมั่นคงที่เกิดขึ้นทั้งหมด ต้องได้รับการบันทึกและ จัดเก็บอย่างปลอดภัยโดยผู้ดูและระบบฯ เพื่อนำมาศึกษาและป้องกันไม่ให้เกิดเหตุซ้ำในอนาคต

๕) จัดฝึกอบรมในห้วข้อที่เกี่ยวข้องกับการตอบสนอง รับมือต่อเหตุละเมิดความมั่นคงโดยผู้เชี่ยวชาญ จากหน่วยงานภายนอกให้แก่ผู้ดูแลระบบฯ ที่มีหน้าที่รับผิดชอบในการรับมือเหตุละเมิดความมั่นคง

๖) เครื่องคอมพิวเตอร์ของผู้ใช้งานที่ถูกปลอดออก โอนย้าย และลดตำแหน่งจากการกระทำผิดที่ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ต้องถูกแยกออกจากเครือข่ายทั้งภายในและภายนอกโดยทันที และก่อนที่จะนำกลับมาใช้ใหม่ ต้องมีการสำรองข้อมูลจากฮาร์ดไดรฟ์เสียก่อน แล้วจึงทำการฟอร์แมตเครื่อง คอมพิวเตอร์นั้น เพื่อป้องกันการแพร่กระจายของซอฟต์แวร์มุ่งร้าย หรือเพื่อกำจัดซอฟต์แวร์ที่ไม่ได้รับ อนุญาตซึ่งอาจถูกติดตั้งไว้ในระบบเครือข่าย

๗) กระบวนการที่ใช้คอมพิวเตอร์ในการประมวลผลข้อมูลสำคัญต้องได้รับการควบคุมด้วยมาตรการ ต่าง ๆ ได้แก่ การตรวจสอบภูมิหลังของผู้ใช้งานการแบ่งแยกอำนานหน้าที่ของผู้ใช้งาน การบังคับให้ผู้ใช้งานหยุดพักร้อนหรือหมุนเวียนตำแหน่งงานเพื่อทำการตรวจสอบ หรือมาตรการอื่น ๆ เพื่อให้แน่นใจว่าไม่มีผู้ใดมีสิทธิขาดในการควบคุมข้อมูลสำคัญเพียงลำพัง ทั้งนี้เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล

๓.๒ การรับมือเหตุการณ์ผิดปกติทางไซเบอร์

๑) ต้องมีมาตรการในการเตรียมความพร้อมสำหรับเหตุการณ์ด้านความปลอดภัยไซเบอร์ (Preparing for a Cyber security Incident)

๒) ต้องมีมาตรการในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (responding to cyber security incident)

๓) ต้องมีการติดตามสถานการณ์ด้านความปลอดภัยทางไซเบอร์ (Following up the cyber security incident)

ส่วนที่ ๙
นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

๑. วัตถุประสงค์

เพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์การตลาดฯ ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑. การพิจารณาระบบเทคโนโลยีสารสนเทศที่สำคัญ

๑) จัดทำบัญชีระบบเทคโนโลยีสารสนเทศและกำหนดลำดับความสำคัญ

๒) กำหนดวิธีการและความถี่ของการสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้ตามที่

๓.๒ ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

๓.๒.๑ การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

๓.๒.๑ การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน

๓.๒.๒ ผู้ดูแลระบบฯ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Contingency Plan) เพื่อรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นได้ทั้งวิธีการทางอิเล็กทรอนิกส์และทางกายภาย โดยแผนเตรียมความพร้อมกรณีฉุกเฉินต้องมีรายละเอียดอย่างน้อย ดังนี้

๑) การกำหนดหน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้อง

๒) การกำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบสารสนเทศ

๓) การกำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้

๔) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก

๕) ให้ปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๖) ให้ทำการทดสอบแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง หากมีปัญหาเกิดขึ้นในระหว่าการกู้คืนให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหาเหล่านั้น พร้อมทั้งวิธีการแก้ไขอย่างเป็น ลายลักษณ์อักษร

๓.๓ การจัดทำแผนความต่อเนื่องของธุรกิจ หรือ Business Continuity Plan (BCP)

๑) ประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่มีความสำคัญและกำหนดมาตรการเพื่อลดความเสี่ยง ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง การปิดล้อมพื้นที่จนทำให้ไม่สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศได้

๒) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล การกู้คืนระบบ และการทดสอบการกู้คืน

ระบบ เทคโนโลยีสารสนเทศ

๓) กำหนดช่องทางการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการระบบสำรองข้อมูล ผู้ให้บริการเครือข่าย หรือ ผู้ให้บริการคลาวด์

๓.๔ การเตรียมอุปกรณ์ประมวลผลสำรอง(Redundancies)เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

๓.๔.๑ สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนทศ (Availability of information processing facilities)

๑) ระบบปฏิบัติงานสำรอง

๑.๑ กำหนดให้ผู้ดูแลระบบฯ ประเมินและกำหนดระบบสารสนเทศสำหรับระบบสำคัญรวมไปถึง จัดเตรียมอุปกรณ์ที่สามารถทำงานทดแทนได้อย่างเหมาะสม

๑.๒ กำหนดให้ผู้ดูแลระบบฯ กำหนดสถานที่และตรียมพื้นที่ให้อยู่ในสภาพพร้อมใช้งานสำหรับระบบทำงานทดแทน

๑.๓ กำหนดให้ผู้ดูแลระบบฯ ทดสอบระบบปฏิบัติงานสำรองอย่างสม่ำเสมอเพื่อมั่นใจได้ว่าจะสามารถทำงานทดแทนระบบหลักได้ เมื่อมีความจำเป็นต้องใช้งาน

ส่วนที่ ๑๐
นโยบายการบริหารจัดการผู้ให้บริการภายนอก
(Third party management)

๑. วัตถุประสงค์

เพื่อให้มีการป้องกันทรัพย์สินขององค์การตลาดที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

๒. ผู้รับผิดชอบ

๑. ผู้ให้บริการภายนอก

๒. บุคคลภายนอกที่ปฏิบัติงานให้กับ องค์การตลาด

๓. บุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ องค์การตลาด

๓.แนวปฏิบัติการ

๓.๑ การบริหารจัดการข้อตกลงการให้บริการ (Service Level Agreement - SLA) และข้อตกลง ด้านการรักษาความลับของข้อมูล (Non-Disclosure Agreement - NDA)

๑) การจัดจ้างผู้ให้บริการภายนอกเพื่อเข้ามาดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดและข้อตกลงการให้บริการ (SLA) และข้อตกลงด้านการรักษาความลับของข้อมูล (NDA) ไว้ในเอกสารจัดจ้างหรือสัญญา

๒) กำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกให้สอดคล้องข้อกำหนดการจ้าง (SLA) กับระยะเวลาในการจ้างผู้ให้บริการภายนอกรายนั้นๆ ซึ่งการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอกเพื่อทำให้มั่นใจว่าผู้ให้บริการภายนอกยังคงปฏิบัติตามข้อตกลงการให้บริการ (SLA) และเงื่อนไขที่ได้ระบุไว้ในข้อตกลง

๓) การจัดจ้างผู้ให้บริการภายนอกเพื่อเข้ามาดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดและตกลงเกี่ยวกับความต้องการด้านความมั่นคงปลอดภัย สารสนเทศกับผู้ให้บริการภายนอกไว้ในเอกสารจัดจ้างหรือสัญญา เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการ เข้าถึงทรัพย์สินของบริษัทฯโดยผู้ให้บริการภายนอก

๔). มีการระบุความเสี่ยงอันเกิดจากการจ้างช่วงและการสื่อสารโดยผู้ให้บริการภายนอก เช่น การจ้าง ช่วงต้องมีการแจ้งให้บริษัทฯ ได้รับทราบหากผู้รับจ้างมีการดำเนินการในลักษณะดังกล่าวอย่างเป็นลาย ลักษณ์อักษรและระบุในสัญญาเกี่ยวกับความรับผิดชอบต่อความเสี่ยงที่เกิดขึ้นจากการจ้างช่วง

๕) กำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกให้ สอดคล้องกับระยะเวลาในการจ้างผู้ให้บริการภายนอกรายนั้นๆ ซึ่งการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอกเพื่อท ำให้มั่นใจว่าผู้ให้บริการภายนอกยังคงปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศและเงื่อนไขที่ได้ระบุไว้ในข้อตกลง

๖) การเปลี่ยนแปลงที่เกี่ยวข้องกับบริการที่ได้รับจากผู้ให้บริการภายนอกทั้งในส่วนที่ร้องขอการ เปลี่ยนแปลงโดยบริษัทฯ เองและส่วนที่ร้องขอการเปลี่ยนแปลงโดยผู้ให้บริการภายนอก

๓.๒ ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

๓.๒.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

๑) กำหนดให้มีพนักงานผู้ควบคุมงานเพื่อคอยกำกับดูแลการดำเนินงานต่าง ๆ ของผู้ให้บริการ ภายนอกซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

๒) กำหนดให้ผู้ให้บริการภายนอกต้องรับทราบและปฏิบัติตามระเบียบ นโยบาย แนวปฏิบัติขั้นตอน การปฏิบัติงานและวิธีการปฏิบัติงานต่าง ๆ ขององค์การตลาดอย่างเคร่งครัด

๓.๒.๒ การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก(Assessing security within supplier agreements)

๑) ผู้ให้บริการภายนอกต้องติดบัตรผู้มาติดต่อตลอดเวลาที่ปฏิบัติงานในพื้นที่

๒) ผู้ให้บริการภายนอกทุกคน ต้องรักษาข้อมูลต่าง ๆ ที่ได้รับทราบระหว่างการปฏิบัติงานให้แก่ องค์การตลาดไว้เป็นความลับ และอนุญาตให้ใช้ข้อมูลเพื่อการปฏิบัติงานให้กับทางองค์การตลาดเท่านั้น ห้ามมิให้ทำการ เปิดเผยต่อบุคคลอื่นก่อนได้รับอนุญาตจากทางองค์การตลาดอย่างเป็นลายลักษณ์อักษร

๓) กรณีที่ผู้ให้บริการภายนอกมีความจำเป็นต้องขอใช้งานข้อมูลสำคัญขององค์การตลาดให้ทำการแจ้งต่อ พนักงานที่เป็นผู้ติดต่อประสานงานเพื่อขออนุญาติให้งานข้อมูลจาก เจ้าของข้อมูลหรือผู้มีอำนาจโดยผู้ ให้บริการภายนอกได้รับอนุญาติให้ใช้งานข้อมูลเท่าที่จำเป็นต้องรับรู้หรือใช้เพื่อการปฏิบัติงานเท่านั้น

๔) ผู้ให้บริการภายนอกต้องแจ้งรายชื่อของพนักงานที่จะเข้าปฏิบัติงานต่อองค์การตลาดก่อนเริ่มการปฏิบัติงาน และหากมีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน หรือมีการเปลี่ยนแปลงตำแหน่งหน้าที่ที่อาจ ส่งผลกระทบต่อองค์การตลาดต้องแจ้งให้ทางองค์การตลาดทราบล่วงหน้าทุกครั้ง

๕) ผู้ใช้บริการภายนอกสามารถนำอุปกรณ์สารสนเทศส่วนบุคคล เช่น คอมพิวเตอร์พกพาเข้าใช้งาน ในพื้นที่สำนักงานขององค์การตลาดได้โดยห้ามเชื่อต่อกับระบบเครือข่ายหรือระบบคอมพิวเตอร์ภายในขององค์การตลาด กรณีที่มีความจำเป็นต้องเชื่อมต่อต้องแจ้งความจำนงต่อพนักงานที่เป็นผู้ติดต่อประสานงาน เพื่อดำเนินการ ขออนุมัติตามขั้นตอนขององค์การตลาด

๖) ห้ามผู้ใช้บริการภายนอกนำสื่อบันทึกข้อมูลใด ๆ มาเชื่อต่อกับอุปกรณ์สารสนเทศภายในพื้นที่ของ องค์การตลาดฯ หากมีความจำเป็นต้องถ่ายโอนข้อมูลให้ดำเนินการโดยพนักงานที่เป็นผู้ติดต่อประสานงานเท่านั้น

๗) หากผู้ให้บริการภายอกมีความจำเป็น ต้อง เข้าใช้งานระบบสารสนเทศขององค์การตลาดเข้าปฏิบัติงานใน พื้นที่ควบคุมเฉพาะ ต้องแจ้งความจำนงต่อพนักงานที่เป็นผู้ติดต่อประสานงานเพื่อดำเนินการขออนุมัติตาม ความเหมาะสม โดยองค์การตลาดจะอนุญาตให้สามารถเข้าใช้งานได้ตามความจำเป็นเท่านั้น ทั้งนี้ พนักงานจากผู้ ให้บริการภายนอกต้องให้ความร่วมมือกับองค์การตลาดในการตรวจสอบอุปกรณ์ที่นำเข้ามาใช้งานอย่างเหมาะสม

๘) ผู้ให้บริการภายนอกต้องไม่นำเอกสารหรือซอฟต์แวร์ที่มีลิขสิทธิ์ขององค์การตลาดไปใช้งานส่วนตัวหรือใช้ งานในทางที่ผิด และห้ามมิให้นำเอกสารหรือซอฟต์แวร์ที่ไม่มีสิขสิทธิ์มาใช้งานในองค์การตลาด

๙) ในการปฏิบัติงาน หากผู้ใช้บริการภายนอกต้องการติดตั้งโปรแกรมปรับแต่งระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย หรือกระทำการใด ๆ ที่ก่อให้เกิดความเปลี่ยนแปลงต่อระบบ สารสนเทศขององค์การตลาด ต้องแจ้งต่อพนักงานผู้ติดต่อประสานงานเพื่อดำเนินการขออนุมัติ ผู้ดูแลระบบฯ ก่อนดำเนินการทุกครั้ง

๑๐) ห้ามผู้ใช้บริการภายนอกทำการสแกนระบบเครือข่ายดักฟังข้อมูลบนระบบเครือข่ายหรือ พยายามเข้าถึงระบบสารสนเทศขององค์การตลาดโดยไม่ได้รับอนุญาต

๑๒) ผู้ให้บริการภายนอกต้องไม่นำบุคคลอื่นที่ไม่เกี่ยวข้อง เข้ามาในพื้นที่องค์การตลาดโดยไม่ได้รับอนุญาต

๑๓) ห้ามผู้ให้บริการภายนอกทำการถ่ายรูป หรือ บันทึกเสียง ภายในพื้นที่องค์การตลาดก่อนได้รับอนุญาต

๑๔) ขณะปฏิบัติงานหากพบว่ามีสิ่งผิดปกติใด ๆ เกิดขึ้น ผู้ให้บริการภายนอกต้องรายงานให้ พนักงานที่เป็นผู้ติดต่อประสานงานทราบทันที

๑๕) องค์การตลาดสงวนสิทธิ์ในการตรวจสอบการทำงานของผู้ให้บริการภายนอก รวมถึง การเพิกถอนสิทธิ ต่าง ๆ ในการเข้าใช้ข้อมูลและระบบสารสนเทศ เมื่อพบสิ่งผิดปกติหรือมีเหตุการะทบด้านความมั่นคง โดยไม่ ต้องแจ้งให้ทราบล่วงหน้า

๑๖) ผู้ให้บริการภายนอกต้องปฏิบัติงานตามขอบเขตและหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย หรือที่ระบุไว้ในสัญญาเท่านั้น

๑๗) ผู้ให้บริการภายนอกต้องปฏิบัติงานด้วยความระมัดระวัง เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ต่อองค์การตลาด

๑๘) การกระทำใด ๆ ของผู้ให้บริการภายนอกที่ก่อให้เกิดความเสียหายหรือละเมิดข้อตกลงหรือ สัญญาต่าง ๆ ที่ได้ทำไว้กับองค์การตลาด ผู้ให้บริการภายนอกต้องรับผิดชอบต่อความเสียหายทั้งหมด

๑๙) ในวันสุดท้ายของการปฏิบัติงานตามข้อตกลงหรือสัญญาผู้ให้บริการภายนอกต้องทำการ ส่งคืนทรัพย์สินต่าง ๆ เช่น กุญแจ อุปกรณ์ต่าง ๆ และรหัสเข้าระบบ ให้แก่พนักงาน ผู้ติดต่อประสานงาน อย่างครบถ้วน

๒๐) กรณีที่ผู้ให้บริการภายนอกมีการดำเนินการเปลี่ยนแปลงใด ๆ ที่อาจะส่งผลกระทบต่อการ ให้บริการตามข้อตกลงหรือสัญญา ผู้ให้บริการภายนอก ต้องแจ้งต่อทางองค์การตลาดอย่างเป็นลายลักษณ์อักษร ล่วงหน้าอย่างน้อง ๓๐ วัน เพื่อให้องค์การตลาดทำการพิจารณา วิเคราะห์ผลกระทบและหาวิธีในการแก้ไขควบคุม ความเสี่ยงได้อย่างเหมาะสม

๓.๓ การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management) เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ใน ข้อตกลงการให้บริการ ของผู้ให้บริการภายนอก

๓.๓.๑ การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services) ผู้ดูแลผู้ให้บริการภายนอกจะต้องตรวจสอบสภาพแวดล้อมการ ทำงาน รวมทั้งการตรวจสอบการ ทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของ หน่วยงานภายนอกต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๓.๓.๒ การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

๑) การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้าน สารสนเทศ จะต้องแจ้งก่อนการเปลี่ยนแปลงล่วงหน้าอย่างน้อย ๓๐ วันทำการ

๒) การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการ ปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของ สารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมิน ความเสี่ยงใหม่

๓.๔ การควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายนอก หรือ Outsource

๓.๔.๑ หน่วยงานภายนอกจะต้องแจ้งรายชื่อผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศล่วงหน้าก่อนการดำเนินงาน ในกรณีที่มีการเปลี่ยนแปลงรายชื่อ

หน่วยงานภายนอกจะต้องแจ้งล่วงหน้าก่อนทุกครั้ง

๓.๔.๒ ในการเข้าไปปฏิบัติงานภายในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ขององค์การ หน่วยงานภายนอกจะต้องบันทึกรายละเอียดตามเอกสารที่ทางองค์การจัดไว้ให้

๓.๔.๓ ทุกครั้งที่จะทำการแก้ไขค่า Configuration ของอุปกรณ์ทุกชนิดภายในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ขององค์การ หน่วยงานภายนอกจะต้องทำการสำรองค่า Configuration เดิมไว้ก่อน รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้น ไม่สามารถใช้งานได้ตามต้องการ จะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมา ให้สามารถใช้งานได้ตามสภาพเดิม

๓.๔.๔ ในกรณีที่หน่วยงานภายนอกจะเข้ามาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ขององค์การ ในวันหยุดหรือนอกเวลาราชการ จะต้องขอความเห็นชอบจากผู้รับผิดชอบหรือผู้ดูแลระบบขององค์การ และหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดทั้งที่เป็นลายลักษณ์อักษรและไม่เป็นลายลักษณ์อักษรล่วงหน้าก่อนทุกครั้ง และการดำเนินงานทุกครั้งจะต้องอยู่ในความดูแลของผู้รับผิดชอบหรือผู้ดูแลระบบขององค์การและหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดทั้งที่เป็นลายลักษณ์อักษรและไม่เป็นลายลักษณ์อักษร

๓.๔.๕ หากหน่วยงานภายนอกจะทำการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ขององค์การ จะต้องแจ้งให้ผู้รับผิดชอบหรือผู้ดูแลระบบขององค์การและหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดทั้งที่เป็นลายลักษณ์อักษรและไม่เป็นลายลักษณ์อักษร ทราบล่วงหน้าก่อนทุกครั้ง ซึ่งจะต้องระบุวัน เวลา ระยะเวลาในการทำงานให้ชัดเจน

๓.๔.๖ ในกรณีที่เจ้าหน้าที่ของหน่วยงานภายนอกประมาท ทำให้อุปกรณ์ และระบบสารสนเทศขององค์การ ได้รับความเสียหายหรือสูญหาย หน่วยงานภายนอกนั้น จะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม

๓.๔.๗ หน่วยงานภายนอกจะต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การ ที่กำหนดไว้ไม่มีข้อยกเว้น หากมีการฝ่าฝืน ทางองค์การจะทำหนังสือแจ้งไปยังหน่วยงานภายนอกนั้นและจะไม่อนุญาตให้เจ้าหน้าที่ของหน่วยงานภายนอกนั้น เข้ามาดำเนินการใดๆ ภายในองค์การ

ส่วนที่ ๑๑
นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี
(Malicious Software Prevention)

๑. วัตถุประสงค์

เพื่อให้ระบบสารสนเทศมีความปลอดภัยสารสนเทศและป้องกันโปรแกรมไม่ประสงค์ดี

๒. ผู้รับผิดชอบ

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware) เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

๓.๑.๑ มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

๑) เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่ได้รับการอัพเดทข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส และต้องเปิดใช้งานตลอดเวลาที่ใช้เครื่อง

๒) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริหารป้องกันไวรัส ต้องมีการอัพเดทข้อมูลล่าสุดอยู่เสมอ

๓) ผู้ใช้งานต้องตรวจสอบไฟล์แนบที่มากับจดหมายอิเล็กทรอนิกส์ (e-mail) หรือไฟล์ที่ได้รับมา จากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๔) ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมไม่ประสงค์ดีเข้าสู่ระบบคอมพิวเตอร์ ขององค์การตลาด

๕) ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๖) เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

๗) ผู้ใช้ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๘) ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk Thumb Drive และ Data อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๙) ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๑๐) ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ ๑๒
นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต
(Website and Internet Security)

๑. วัตถุประสงค์

เพื่อปกป้องข้อมูลของผู้ใช้งานจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิในการเข้าถึงข้อมูล

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ Website Security Policy

๓.๑.๑ ผู้ดูแลระบบควรติดตั้งระบบ Firewall ซึ่งเป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิอนุมัติเท่านั้นจึงจะผ่าน Fire Wall เพื่อเข้าถึงข้อมูลได้

๓.๑.๒ ผู้ใช้งานควรมีการติดตั้ง Software ป้องกัน Virus ที่มี ประสิทธิภาพสูง และ Update อย่างสม่ำเสมอ

๓.๑.๓ ผู้ใช้งานควรมีการติดตั้งโปรแกรมประเภท Personal Fire wall เพื่อป้องกันเครื่องคอมพิวเตอร์จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker

๓.๑.๔ ผู้ใช้งานควรระมัดระวังในการ Download Program จาก Internet มาใช้งาน และควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login เข้าใช้บริการ เพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์

๓.๒ การใช้งานระบบอินเทอร์เน็ต (Internet)

๓.๒.๑ ผู้ใช้งานต้องเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้นและห้ามผู้ใช้งานทำการเชื่อมต่อเครื่องคอมพิวเตอร์ ผ่านช่องทางอื่นยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้บริหารฝ่ายสารสนเทศเป็นลายลักษณ์อักษร ก่อนการดำเนินการ

๓.๒.๒ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่และความรับผิดชอบเพื่อประสิทธิ์ ภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลขององค์การตลาด และต้องไม่ใช้ระบบอินเทอร์เน็ตขององค์การตลาด เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับองค์การตลาด

๓.๒.๓ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์การตลาดที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๓.๒.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดซอฟแวร์จากระบบอินเตอร์เน็ตรวมถึงการดาวน์โหลดการอัพเดท (Update) ซอฟแวร์ต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือสินทรัพย์ทางปัญญา

๓.๒.๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Web board) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์การตลาด

๓.๒.๖ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Web board) ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงานการทำลาย

ความสัมพันธ์กับบุคคลากรของหน่วยงานอื่นๆ

๓.๒.๗ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้วให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๓.๓ การใช้งานเครือข่ายสังคมออนไลน์ (Social network)

๓.๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่องค์การตลาดได้กำหนดไว้เท่านั้น

๓.๓.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใดๆที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๓.๓.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับองค์การตลาด ผู้ใช้งานต้องแจ้งต่อฝ่ายเทคโนโลยีสารสนเทศโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

ส่วนที่ ๑๓
นโยบายการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน
(Endpoint Security)

๑. วัตถุประสงค์

เพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยสารสนเทศ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint)

๓.๑.๑ กำหนดกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน เพื่อให้ผู้ใช้งานปฏิบัติตามโดยกำหนดรายการ Software Baseline ที่อนุญาตให้ติดตั้งและซอฟต์แวร์ที่ห้ามติดตั้ง

๓.๑.๒ ต้องกำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ

๓.๑.๓ มีมาตรการในการตรวจหา ป้องกันและกู้คืนจากโปรแกรมไม่ประสงค์ดี ด้วยการติดตั้ง ซอฟต์แวร์ Anti Virus และ Update ให้ทันสมัยอย่างสม่ำเสมอ

๓.๑.๔ จำกัดสิทธิ์การเข้าถึงเครื่องแม่ข่ายเพื่อควบคุมให้ผู้ใช้งานสามารถใช้งานเฉพาะระบบที่ได้รับอนุญาตเท่านั้น

๓.๑.๕ ระบบเครือข่ายทั้งหมดขององค์การตลาด ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (IPS/IDS)

๓.๑.๖ ติดตั้งระบบตรวจจับการบุกรุกเพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์การตลาดในลักษณะที่ผิดปกติ

๓.๑.๗ หมายเลข IP Address ภายในของระบบเครือข่ายภายในของ องค์การตลาด จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายขององค์การตลาดสามารถมองเห็นได้

๓.๑.๘ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของ ระบบเครือข่ายภายในและระบบเครือข่ายภายนอกที่สามารถระบุบนระบบเครือข่ายและต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันพร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๑.๙ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้ งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

ส่วนที่ ๑๔
นโยบายการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ (Cryptography) และการบริหารจัดการกุญแจ (Key management)

๑. วัตถุประสงค์

เพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยสารสนเทศ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑.การกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

๑.นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls) การควบคุมการเข้ารหัสข้อมูลตามข้อตกลง โดยอยู่ภายใต้กฎหมาย และระเบียบที่ เกี่ยวข้อง

๓.๒.การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

๑.นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอด วงจรชีวิตของกุญแจ โดยกำหนดให้มีการเปลี่ยนทุกครั้งที่มีการร้องขอ

๓.๓.การเก็บข้อมูลหรือไฟล์อิเล็กทรอนิกส์บนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์มีระดับชั้นความลับ ได้แก่ ลับ ที่สุด ลับมาก และ ลับ ให้ใช้มาตรฐานในการเข้ารหัสข้อมูล อิเล็กทรอนิกส์

ส่วนที่ ๑๕

นโยบายการใช้คลาว์ดภาครัฐ

๑. วัตถุประสงค์

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับสารสนเทศ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

ส่วนของผู้ดูแลระบบ

๑. ฝ่ายสารสนเทศจะต้องจัดทำแบบคำร้องขอตามที่ผู้ให้บริการกำหนดให้ครบถ้วนสมบูรณ์ หากมีความต้องการในการปรับปรุงแก้ไข ฝ่ายสารสนเทศต้องแจ้งผู้ให้บริการทราบผ่านแบบคำร้องขอทุกครั้ง

๒. ฝ่ายสารสนเทศ มีหน้าที่ จัดเตรียมเครือข่ายคอมพิวเตอร์ ไม่ว่าจะเป็น Dial Up, ADSL Leased Line หรืออื่นๆ เพื่อเชื่อมต่อมายังผู้ให้บริการ โดยผู้ใช้บริการจะต้องแจ้งชุด IP Address ของเครือข่ายที่ใช้งานแก่ผู้ให้บริการ เพื่อควบคุมการใช้งานรวมถึงลดการโจมตีจากผู้ที่ไม่ประสงค์ดี หากในกรณีที่ไม่มีการแจ้งชุด IP Address เพื่อควบคุม ผู้ให้บริการจะไม่รับผิดชอบต่อความเสียหายอันเกิดขึ้นจากผู้ไม่ประสงค์ดี

๓. ผู้ใช้บริการจะต้องไม่ทำการเปลี่ยน Configuration เครือข่ายคอมพิวเตอร์นอกเหนือจากที่ผู้ให้บริการกำหนด

๔. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงขององค์การตลาด ต้องอ่าน ทำความเข้าใจข้อกำหนดและเงื่อนไขการให้บริการนี้เป็นอย่างดี จึงลงนามในแบบคำขอใช้บริการ

๕. ในกรณีสิ้นสุดการใช้บริการ ผู้ใช้บริการจะต้องเป็นผู้จัดหาอุปกรณ์บันทึกข้อมูลเพื่อจัดเก็บข้อมูลจากบริการคลาวด์ภาครัฐและเป็นผู้รับผิดชอบในการถ่ายโอนข้อมูลลงในอุปกรณ์ที่จัดหา

ส่วนของผู้ใช้งาน

๑. ผู้ใช้งานจะต้องเข้าสู่ระบบจากชื่อบัญชีที่ผู้ให้บริการ (GDCC) ออกให้ เพื่อใช้งานเครื่องคอมพิวเตอร์แม่ข่ายเสมือนและทำการติดตั้งโปรแกรมอื่นๆ ที่ต้องการใช้งาน พร้อมกำหนดชื่อบัญชีอื่นๆ ที่ต้องการด้วยตนเอง และทำการถ่ายโอนข้อมูลที่ต้องการใช้บริการมายังเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่ให้บริการ

๒. ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แกไขเพิ่มเติม รวมถึงกฎหมายอื่นๆ ที่เกี่ยวข้องกับการใช้บริการอย่างเคร่งครัด และต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ (GDCC) และนโยบายคุ้มครองความเป็นส่วนตัว (Privacy Policy) ของผู้ให้บริการ (GDCC) และไม่กระทำการใดๆ ที่ก่อให้เกิดความเสียหายแก่ผู้ให้บริการ (GDCC)

๓. หากพบความผิดปกติใดๆ เกิดขึ้นกับเครื่องที่ใช้บริการ จะต้องแจ้งให้ผู้ให้บริการทราบในทันที เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นแก่ทรัพย์สินขององค์การตลาดหรือผู้ให้บริการ(GDCC)

๔. ข้อมูลหรือแฟ้มข้อมูลที่เก็บไว้ในหน่วยความจำของเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่องค์การตลาดมาฝากไว้กับผู้ให้บริการ (GDCC) จะต้องไม่มีลักษณะต้องห้ามหรือขัดต่อกฎหมายหรือศีลธรรมอันดีของประชาชน

ส่วนที่ ๑๖
การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security risk Management)

๑. วัตถุประสงค์

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับสารสนเทศ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑. การประเมินความเสี่ยง (Risk Assessment)

๓.๑.๑ ให้มีการระบุความเสี่ยง (risk identification) เพื่อระบุความเสี่ยงที่อาจส่งผลกระทบต่อองค์กร

๓.๑.๒ ให้มีการวิเคราะห์ความเสี่ยง (risk analysis) เพื่อวิเคราะห์ผลกระทบ (Impact) และโอกาสเกิด (Likelihood) ของเหตุการณ์ความเสี่ยงที่เกิดขึ้นต่อองค์กร

๓.๑.๓ ให้มีการประเมินค่าความเสี่ยง (risk evaluation) หลังจากพิจารณาโอกาสเกิดเหตุการณ์ (Likelihood) และผลกระทบ (Impact) ของแต่ละปัจจัยเสี่ยงแล้ว โดยนำผลที่ได้มาพิจารณาความสัมพันธ์ ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยง ว่าก่อให้เกิดระดับของความเสี่ยงในระดับใด

๓.๑.๔ ให้มีการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรม การควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม

๓.๑.๕ ให้มีการติดตามและทบทวนความเสี่ยง (risk monitoring and review) โดยการกำหนด ผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามตัวชี้วัดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ตามที่กำหนดและทบทวนความเสี่ยงด้านความ

๓.๑.๖ ให้มีการรายงานความเสี่ยง (Risk reporting) โดยการนำเสนอผลการบริหารแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศพร้อมกับการรายงานผลการประเมินและการบริหารจัดการความ เสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร

๓.๑.๗ ให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓.๑.๘ กำหนดให้ผู้ตรวจสอบภายในด้านระบบเทคโนโลยีสารสนเทศ (Internal IT Auditor) ของ องค์การตลาดเป็นผู้ตรวจสอบและประเมินความเสี่ยง

๓.๒. การจัดการความเสี่ยง (Risk Treatment)

๓.๒.๑ ให้มีการกำหนดมาตรการ หรือแผนงาน เพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายของผลกระทบที่อาจเกิดขึ้นจากความเสี่ยง

๓.๒.๒ ให้มีการกำหนดแนวทางการจัดการความเสี่ยง โดยสามารถปรับเปลี่ยนให้เหมาะสมกับ สถานการณ์ เช่น การยอมรับความเสี่ยง (Take), การควบคุมความเสี่ยง (Treat), การถ่ายโอนความเสี่ยง (Transfer), การหลีกเลี่ยงความเสี่ยง (Terminate) เป็นต้น

๓.๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง โดยมีวิธีการปฏิบัติ ดังนี้

๓.๓.๑ มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

๓.๓.๒ มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๓.๓.๓ มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

๓.๓.๔ มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) อย่างน้อย ๑ ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

๓.๔ การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศขององค์การเพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศขององค์การ โดยมีวิธีการปฏิบัติ ดังนี้

๓.๔.๑ กำหนดให้ฝ่ายตรวจสอบภายในขององค์การเป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศขององค์การ และให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อย ๑ ครั้งต่อปี

๓.๔.๒ มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบ ระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

๓.๔.๓ มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ ในลักษณะที่อ่านได้เพียงอย่างเดียว

๓.๔.๔ มีวิธีการที่ปลอดภัยสาหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูล ชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

๓.๔.๕ มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

๓.๔.๖ มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

๓.๔.๗ มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

๓.๔.๘ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสาหรับการตรวจสอบ

๓.๔.๙ มีการกำหนดพนักงานที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศ จากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแลหรือรับผิดชอบ

ส่วนที่ ๑๗
นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน
(Role and responsibility)

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่และแนวทางปฏิบัติสำหรับผู้ปฏิบัติงานในการบริหารจัดการ การพัฒนา ปรับปรุง บำรุงรักษา ตรวจสอบและติดตามระบบเทคโนโลยีสารสนเทศ และเพื่อให้สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิ์ภาพ รวมทั้งกำกับผู้ใช้งานให้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๑.๑ ผู้ปฏิบัติงานระดับนโยบาย

ผู้รับผิดชอบ

๑) คณะกรรมการองค์การตลาด

๒) คณะอนุกรรมการด้านเทคโนโลยีสารสนเทศ

๓) ผู้บริหารระดับสูงสุด (ผู้อำนวยการ)

หน้าที่/ความรับผิดชอบ คือ

๑) กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา บริหารจัดการด้านเทคโนโลยีสารสนเทศ

๒) กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานในระดับบริหาร

๓) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใดๆ ที่จากระบบเทคโนโลยีสารสนเทศเกิดขึ้นกับองค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากละเลย การละเมิดหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ระดับบริหาร

ผู้รับผิดชอบ

๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

หน้าที่/ความรับผิดชอบ คือ

๑) กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานในระดับปฏิบัติ

๒) กำกับดูแลการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๓) ทบทวนแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP-IT)

๔) บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๕) รายงานการละเมิดหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ ระดับปฏิบัติ

ผู้รับผิดชอบ

๑) ผู้ดูแลระบบที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ (ตำแหน่ง นักคอมพิวเตอร์๗-๕)

หน้าที่/ความรับผิดชอบ

๑) กำหนดบัญชีรายชื่อ (User account) และรหัสผ่าน (Password) ของสำหรับผู้ดูแลระบบและผู้ใช้งาน

๒) ดูแลรักษาระบบเทคโนโลยีสารสนเทศ

๓) ติดตั้งเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบการเข้ารหัสสารสนเทศ ระบบ ป้องกันและตรวจจับการบุกรุก ระบบป้องกันและกำจัดซอฟแวร์ประสงค์ร้าย รวมทั้งอุปกรณ์และระบบอื่นใดที่ จำเป็นเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างมั่นคง

๔) ตรวจสอบและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิ์ภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไขในทันทีเพื่อป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้น ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจาการละเมิดหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และพิจารณาระงับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศในทันที

๕) ติดตั้งและปรับปรุงการแก้ไขข้อบกพร่อง (Patch) ของระบบเทคโนโลยีสารสนเทศ ให้มีความมั่นคงและทันสมัยอยู่เสมอ

๖) ตรวจสอบความมั่นคงของระบบเทคโนโลยีสารสนเทศทุก ๖ เดือน

๗) เปลี่ยนรหัสผ่านสำหรับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศทุก ๖ เดือน หรือเมื่อมีความจำเป็น

๘) สำรองข้อมูลที่มีความสำคัญแบบสมบูรณ์ (Full back-up) อย่างน้อยเดือนละ ๑ ครั้ง

๙) ลบหรือทำลายสารสนเทศหรือซอฟแวร์คอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานอย่างถาวร เมื่อไม่มีความจำเป็นหรือเมื่อหมดสัญญาเช่า

๑๐) บันทึกการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ (Log File) ย้อนหลัง อย่างน้อย ๙๐ วัน โดยจัดเก็บไว้ในหน่วยความจำของเครื่องคอมพิวเตอร์อย่างน้อย ๑ เครื่อง ซึ่งแยกต่างหาก จากเครื่องคอมพิวเตอร์แม่ข่ายของระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย

๑๑) ดูแลรักษาและตรวจสอบช่องทางการสื่อสาร (Communication port) ของระบบเทคโนโลยีสารสนเทศทุก ๖ เดือน และปิดช่องทางการสื่อสาร (Communication port) ที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑๒) ดูแลรักษาและปรับปรุงบัญชีรายชื่อผู้ใช้งานให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์ของผู้ใช้งานทันทีที่พ้นสภาพจากการเป็นผู้ใช้งาน

๑๓) กำหนดหลักสูตรและจัดฝึกอบรมเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่งน้อยปีละ ๑ ครั้ง

๑๔) จัดทำรายงานการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ และนำเสนอต่อผู้บังคับบัญชาเพื่อทราบหรือเพื่อพิจารณาสั่งการเกี่ยวกับการแก้ไข การปรับปรุง ประสิทธิ์ภาพและการให้บริการต่อไป

๑๕) ตั้งสัญญาณนาฬิกาของเครื่องคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศให้ตรงกับ เวลามาตรฐานสากลจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเทียบเวลาตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดไว้

๑๖) ซักซ้อมแผนสร้างความต่อเนื่องทางธุรกิจ (BCP-IT) อย่างน้อยปีละ ๑ ครั้ง เพื่อเตรียมพร้อมในกรณีเกิดเหตุฉุกเฉิน

๑๗) การดำเนินการสำหรับระบบเครือข่ายแบบไร้สาย (wireless LAN)

๑๗.๑ กำหนดให้มีการเข้ารหัสสารสนเทศระหว่างเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการรับและส่งสัญญาณ ตามมาตรฐานของเทคโนโลยีไม่ต่ำกว่า WPA (Wi-Fi Protected Access)

๑๗.๒ กำหนดให้มีกลไกการตรวจสอบพิสูจน์ตัวตนของผู้ใช้งาน(User Authentication) ที่มีความมั่นคง เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงและเข้าใช้งานได้ และสนับสนุนการรับ-ส่งสารสนเทศด้วยโปรโตคอล IEEE๘๐๒.๑x ไปยัง RADIUS Server (Remote Authentication Dial-In User Service Server) ที่ติดตั้งไว้เพื่อทำหน้าที่ตรวจสอบพิสูจน์ตัวตนของผู้ใช้งานจากฐานข้อมูลผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

๑๗.๓ ติดตั้งระบบจัดเก็บบันทึกเข้าถึงและการใช้งานระบบเครือข่ายแบบไร้ สายและตรวจสอบและรายงานผลอย่างน้อยเดือยละ ๑ ครั้ง เพื่อให้ผู้บังคับบัญชารับทราบ ในกรณีที่ตรวจสอบพบการใช้ที่ผิดปกติให้ผู้บังคับบัญชาต่อผู้บังคับบัญชาทราบในทันที

๑๗.๔ กำหนดให้ผู้ใช้งานต้องไม่ใช้งานช่องรับและส่งสัญญาณทางอินฟราเรดหรือ Bluetooth ในขณะที่กำลังใช้งานระบบเครือข่ายแบบไร้สายเพื่อป้องกันการรั่วไหลของสารสนเทศ

๑๗.๕ ติดตั้งระบบตรวจจับผู้บุกรุกหรือไฟร์วอลล์ (Firewall)

๑๗.๖ ติดตั้งและใช้งานซอฟแวร์คอมพิวเตอร์สำหรับป้องกันและกำจัด ซอฟแวร์ประสงค์ร้าย รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๑๗.๗ กำกับดูแลไม่ให้ผู้ใช้งานใช้งานระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบเทคโนโลยีสารสนเทศด้านบัญชี การเงิน งบประมาณ การบริหารงานพัสดุ การบริหารงานบุคคล (ระบบ ERP) ระบบอินทราเน็ต (Intranet) ระบบสารบรรณอิเล็กทรอนิกส์ และฐานข้อมูลต่างๆ ผ่านระบบเครือข่าย แบบไร้สาย

๑๘) ปฏิบัติหน้าที่อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

๑.๔ ควบคุมให้มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่างๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

๑.๕ ควบคุมให้มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่างๆ ไว้อย่างชัดเจน

๑.๖ ควบคุมให้มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่างๆ ไว้อย่างชัดเจน

๑.๗ กำหนดให้มีการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างผู้ให้บริการภายนอกเป็นผู้ดำเนินการ

๒. การกำหนดบทบาทด้านทรัพยากรบุคคล

๒.๑ ให้มีการกำหนดลักษณะงาน (Job Description) ซึ่งต้องระบุถึงหน้าที่และความรับผิดชอบ ของแต่ละตำแหน่งงาน และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของบุคลากร หรือ หน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๒ มีกระบวนการคัดเลือกบุคลากรอย่างเหมาะสม เช่น การตรวจสอบภูมิหลังของผู้สมัครงาน ต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับตำแหน่งหน้าที่

๒.๓ มีการทำข้อตกลงการปฏิบัติงานตามที่ องค์การตลาด กำหนดไว้ตามสัญญาการจ้างงาน

๒.๔ ให้มีการฝึกอบรม ให้ความรู้ และสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

๒.๕ ให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบาย หรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในองค์กร

๒.๖ ให้มีกระบวนการในกรณียุติการว่าจ้างหรือเปลี่ยนแปลงหน้าที่งาน รวมทั้งการยกเลิกสิทธิ การเข้าถึงระบบเทคโนโลยีสารสนเทศ และระบบเครือข่ายของ องค์การตลาด และการส่งคืนทรัพย์สินเมื่อหมด ภาระหน้าที่

๓. การประเมินผลการปฏิบัติตามนโยบาย หลักเกณฑ์ หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ คณะทำงาน ต้องควบคุม กำกับ ติดตามให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่

๓.๒ ผู้ใช้งาน ต้องดำเนินงานด้วยความระมัดระวังและป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่ เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดการให้บริการ

๓.๓ คณะกรรมการ คณะอนุกรรมการ และคณะทำงาน ต้องควบคุมให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๓.๔ ผู้ดูแลระบบต้องใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๓.๕ บุคลากร ต้องดำเนินงานอยู่ในขอบเขตความรับผิดชอบตามนโยบายความมั่นคงปลอดภัย สารสนเทศขององค์กร รวมถึงปฏิบัติตามข้อกำหนดสัญญา กฎหมาย พระราชบัญญัติ กฎระเบียบ และข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๓.๖ องค์กรต้องจัดให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑๘
นโยบายการปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษ ของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

๑. วัตถุประสงค์

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ

๒. ขอบเขต

ทุกหน่วยงาน

๓.แนวปฏิบัติการ

๓.๑ การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

๓.๑.๑ การระบุข้อกำหนด และความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

๑) ผู้ใช้งานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด โดยมีรายการ ดังต่อไปนี้เป็นอย่างน้อย

- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
- พระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒
- พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ (ฉบับที่๒) พ.ศ. ๒๕๖๐
- พระราชบัญญัติคุ้มครองข้อมูลสิทธิส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๐
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พระราชบัญญัติการบริหารงานและการใช้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
- พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ ๕) พ.ศ. ๒๕๖๕
- พระราชบัญญัติเผยแพร่ข้อมูลข่าวสาร พ.ศ.๒๕๔๐
- พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์. พ.ศ. ๒๕๖๓
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓
- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ.๒๕๕๐
- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานพนักงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.

๒๕๕๐

• ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

• นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การตลาด

๒) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศขององค์การตลาดฯ ถือเป็น ทรัพย์สินของ องค์การตลาด (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้ องค์การตลาดฯ สามารถเปิดเผยหรือใช้งานข้อมูล เหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้ง ให้ผู้ใช้งานทราบล่วงหน้า เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศ ขององค์การตลาดฯ และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบ คอมพิวเตอร์ และระบบ เครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของ องค์การตลาดฯ กำหนดไว้

๓) องค์การตลาด ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้อง แจ้ง ให้ทราบล่วงหน้า อย่างไรก็ตามองค์การตลาดฯ จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความ จำเป็นเท่านั้น

๔) ห้ามพนักงานองค์การตลาดฯ ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศขององค์การตลาดฯ กระทำการใด ๆ ที่ ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

๕) การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออองค์การตลาดกประเทศ ไม่ขัดต่อข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ ผู้ใช้งานต้อง ปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

๓.๑.๒ สินทรัพย์ทางปัญญา (Intellectual Property Rights)

๑) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่ องค์การตลาดจัดหามาใช้ใช้งาน

๒) ผู้ดูแลระบบฯ ต้องมีการบริหารจัดการและควบคุมดูแลการใช้งานซอฟต์แวร์ให้เป็นไปตามลิขสิทธิ์ที่ได้รับ ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดสิทธิ์บนเครื่องคอมพิวเตอร์แท็บเล็ต หรือสมาร์โฟนขององค์การตลาดโดยเด็ดขาด

๓.๑.๓ การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records) ผู้ดูแลระบบฯ ต้องป้องกันมิให้ข้อมูลที่สำคัญเกิดความเสียหายสูญหายหรือถูกปลอมแปลงโดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ขององค์การตลาดและข้อกำหนดการให้บริการ

๓.๑.๔ ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information) ต้องกำหนดให้มีการคุ้มครอบข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ขององค์การตลาด

๓.๑.๕ การควบคุมการเข้ารหัส (Regulation of cryptographic controls) องค์การตลาดฯ ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

๓.๒ การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews) เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

๓.๒.๑ การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security) ต้องกำหนดให้มีการทบทวนวัตถุประสงค์ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงของสภาวะแวดล้อมขององค์การตลาด

๓.๒.๒ การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards) ต้องกำหนดให้มีการทบทวนขั้นตอนการปฏิบัติงานโดยเทียบกับนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศขององค์การตลาด

๓.๒.๓ การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review) ต้องกำหนดให้มีการทบทวนความสอดคล้องของระบบสารสนเทศเทียบกับนโยบายและแนวปฏิบัติในการ รักษาความมั่นคงปลอดภัยด้านสารสนเทศ และดำเนินการแก้ไขความไม่สอดคล้องที่ตรวจสอบขององค์การตลาด

๑) ให้ผู้บังคับชาเป็นผู้กำกับดูแล ให้ผู้ใต้บังคับบัญชาปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศขององค์การตลาดอย่างเคร่งครัด

๒) ในกรณีที่มีการฝ่าฝืนหรือละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศขององค์การตลาด ให้ผู้บังคับบัญชาชาดำเนินการเพื่อยับยั้งเหตุการณ์ฝ่าฝืนหรือละเลยการ ปฏิบัติดังกล่าวตามสมควร และรายงานตามสายบังคับบัญชาไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อพิจารณาดำเนินการต่อไป

๓) หากบุคคลใดจงใจฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศขององค์การตลาด จะถือว่าเป็นความผิดทางวินัยและให้ดำเนินการตามข้อบังคับเกี่ยวกับพนักงาน ทั้งนี้ หากการกระทำนั้นเป็นเหตุให้องค์การตลาดได้รับความเสียหายองค์การตลาดจะพิจารณาดำเนินคดีตามกฎหมายอีกทางหนึ่งด้วย

๓.๓ การปฏิบัติตามข้อบังคับด้านกฎหมาย บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานคอมพิวเตอร์ จะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานคอมพิวเตอร์ กระทำผิดตามกฎหมายดังกล่าว องค์การถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล

๓.๔ การปกป้องข้อมูลส่วนบุคคล

๓.๔.๑ ข้อมูลรายละเอียดที่เกี่ยวกับการดำเนินงานขององค์การ ถือว่าเป็นข้อมูลที่มีความสำคัญ เฉพาะพนักงานที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บริหารเท่านั้น ที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวได้

๓.๔.๒ ข้อมูลส่วนตัวของพนักงานถือว่าเป็นข้อมูลลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ เช่น พนักงานเอง หรือผู้ทำงานที่มีความเกี่ยวข้องเท่านั้น อย่างไรก็ดีองค์การสงวนสิทธิ์ ในการเข้าถึงข้อมูลทั้งหมดที่สร้างและเก็บอยู่ในระบบสารสนเทศขององค์การ

๓.๕ ลิขสิทธิ์ซอฟต์แวร์

๓.๕.๑ พนักงานต้องไม่ทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่องค์การได้จัดซื้อลิขสิทธิ์เพื่อการใช้งานยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

๓.๕.๒ ซอฟต์แวร์ที่พัฒนาภายในองค์การ ทั้งโดยบุคคลอื่นหรือพนักงานขององค์การถือ

ว่าเป็นทรัพย์สินขององค์การไม่อนุญาตให้พนักงานทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินขององค์การโดยไม่ได้รับการอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร

๓.๕.๓ ผู้ที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์การทั้งหมด ต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

๓.๕.๔ ซอฟต์แวร์ที่ได้จัดซื้อจากภายนอกอาจมีเงื่อนไขในเรื่องลิขสิทธิ์ด้านการใช้งานที่แตกต่างกันหน่วยงานที่รับผิดชอบด้านการจัดซื้อต้องรับผิดชอบในการศึกษาถึงเงื่อนไข ดังกล่าวจากฝ่ายสารสนเทศต้องสร้างความตระหนักถึงผู้ใช้งานซอฟต์แวร์ดังกล่าวได้ทราบถึง เงื่อนไขต่าง ๆ และข้อห้ามที่เกี่ยวข้อง

๓.๕.๕ การจัดซื้อหรือใช้ซอฟต์แวร์ของบุคคลอื่นต้องปฏิบัติให้สอดคล้องกับข้อตกลงด้านลิขสิทธิ์ ห้ามนำซอฟต์แวร์ที่ซื้อไปติดตั้งที่คอมพิวเตอร์เครื่องอื่นนอกเหนือจากเครื่องที่ได้มีการ ติดตั้งแล้วตามข้อตกลงเรื่องลิขสิทธิ์ซอฟต์แวร์

๓.๕.๖ ทำการตรวจสอบการใช้งานคอมพิวเตอร์ขององค์การอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์คอมพิวเตอร์ทุกชนิดเป็นไปตามข้อตกลงด้านลิขสิทธิ์ซอฟต์แวร์

๓.๕.๗ พนักงานที่ฝ่าฝืนละเมิดข้อตกลงด้านลิขสิทธิ์ของเจ้าของซอฟต์แวร์ถือว่าเป็นการละเมิดนโยบายความปลอดภัยสารสนเทศขององค์การ ถึงแม้การละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานขององค์การก็ตามพนักงานต้องรับผิดชอบผลเสียหายทั้งหมด
