



นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย  
ของระบบเทคโนโลยีสารสนเทศ กรมชลประทาน  
(Information Security Policy)

โดย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร  
กรมชลประทาน กระทรวงเกษตรและสหกรณ์  
เมษายน พ.ศ. ๒๕๕๖

# สารบัญ

	หน้า
นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมชลประทาน	๑
องค์ประกอบของนโยบาย	
คำนิยาม	๔
ส่วนที่ ๑ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	๗
ส่วนที่ ๒ นโยบายการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย	๑๒
ส่วนที่ ๓ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ	๑๕
ส่วนที่ ๔ นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ	๒๓
ส่วนที่ ๕ นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย	๒๕
ส่วนที่ ๖ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ	๒๙
ส่วนที่ ๗ นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ	๓๒
ส่วนที่ ๘ นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล	๓๖
ส่วนที่ ๙ นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา	๓๘
ส่วนที่ ๑๐ นโยบายการใช้งานอินเทอร์เน็ต	๔๑
ส่วนที่ ๑๑ นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์	๔๓
ส่วนที่ ๑๒ นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย	๔๕
ส่วนที่ ๑๓ นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี	๔๖
ส่วนที่ ๑๔ นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก	๔๗
ส่วนที่ ๑๕ นโยบายการสำรองและกู้คืนข้อมูล	๔๙
ส่วนที่ ๑๖ นโยบายด้านการปฏิบัติตามข้อบังคับ	๕๒
ส่วนที่ ๑๗ นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	๕๔
ส่วนที่ ๑๘ นโยบายการสร้างตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ	๕๖
ภาคผนวก	
การจัดสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน	๕๘
แนวปฏิบัติเพื่อการบริหารจัดการการเข้าถึงข้อมูล	๖๑

# นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมชลประทาน (Information Security Policy)

## ๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมชลประทาน หรือต่อไปนี้อาจเรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กรและหน่วยงานในสังกัด อีกทั้งเป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาคี พ.ศ. ๒๕๔๙ มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังนี้

- ๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
- ๑.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ รวมทั้งมีการปรับปรุงอย่างต่อเนื่อง
- ๑.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบ และเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- ๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
- ๑.๕ การกำหนดความรับผิดชอบ กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศขององค์กร (CIO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น
- ๑.๖ นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา ๑ ครั้ง ต่อปี

## ๒. องค์ประกอบของนโยบาย

คำนิยาม

- ส่วนที่ ๑ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security Policy)
- ส่วนที่ ๒ นโยบายการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย (Network System Control Room Policy)
- ส่วนที่ ๓ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control Policy)
- ส่วนที่ ๔ นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy)
- ส่วนที่ ๕ นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)
- ส่วนที่ ๖ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
- ส่วนที่ ๗ นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control)
- ส่วนที่ ๘ นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Policy)
- ส่วนที่ ๙ นโยบายการใช้งานเครื่องคอมพิวเตอร์พกพา (Use of Notebook Computer Policy)
- ส่วนที่ ๑๐ นโยบายการใช้งานอินเทอร์เน็ต (Internet Security Policy)
- ส่วนที่ ๑๑ นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Policy)
- ส่วนที่ ๑๒ นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)
- ส่วนที่ ๑๓ นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious Software Protection Policy)
- ส่วนที่ ๑๔ นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก (Firewall & IPS Policy)
- ส่วนที่ ๑๕ นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)
- ส่วนที่ ๑๖ นโยบายด้านการปฏิบัติตามข้อบังคับ (Compliance Policy)
- ส่วนที่ ๑๗ นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ส่วนที่ ๑๘ นโยบายการสร้างตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Policy)

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย

ช่วยลดความเสี่ยงต่อการดำเนินงาน สิ้นทรัพย์ บุคลากรขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

## คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- ❖ **องค์กร** หมายถึง กรมชลประทาน
- ❖ **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- ❖ **ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร
- ❖ **CIO (Chief Information Officer)** หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงขององค์กร (รองอธิบดีฝ่ายบริหาร)
- ❖ **ผู้บริหารสูงสุด** หมายถึง อธิบดีกรมชลประทาน
- ❖ **ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแล การใช้งานระบบเทคโนโลยีสารสนเทศ
- ❖ **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์กร
- ❖ **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- ❖ **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- ❖ **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- ❖ **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ ดังนี้
  - **ผู้บริหาร** หมายถึง อธิบดี รองอธิบดี ผู้เชี่ยวชาญ ผู้ตรวจราชการกรมชลประทาน ผู้อำนวยการสำนัก ผู้อำนวยการกองฯ ศูนย์ และ หัวหน้าหน่วยงานราชการ
  - **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
  - **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กร
- ❖ **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมชลประทานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

- ❖ **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
- ❖ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- ❖ **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- ❖ **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- ❖ **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบ LAN ระบบ Intranet และระบบ Internet เป็นต้น
  - **ระบบ LAN และ ระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
  - **ระบบ Internet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- ❖ **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
- ❖ **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น
  - พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  - พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
  - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)
  - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
  - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)
- ❖ **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

- ❖ **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- ❖ **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น
- ❖ **รหัสผ่าน (Password)** หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- ❖ **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- ❖ **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมีขอบเอาไว้ด้วย
- ❖ **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ(Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
- ❖ **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- ❖ **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม



**ส่วนที่ ๑**  
**นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม**  
**(Physical and Environment Security Policy)**

**๑. วัตถุประสงค์**

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

**๒. ผู้รับผิดชอบ**

๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ สำนักงานเลขานุการกรม

๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

**๓. แนวปฏิบัติการกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย**

๓.๑ ภายในองค์กรมีการจำแนก และกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๓.๒ จัดให้มีเวรยาม รักษาอาคาร และห้องควบคุมระบบเครือข่าย และอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายในเพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูล และระบบเครือข่าย

๓.๓ ผู้บริหาร ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

๓.๔ ผู้บริหาร ต้องกำหนดสิทธิให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

๓.๔.๑ จัดทำ “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๔.๒ ทำการบันทึกการเข้า-ออกพื้นที่ใช้งาน และกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้า-ออกพื้นที่”

- ๓.๔.๓ จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

#### ๔. แนวปฏิบัติการควบคุมการเข้า-ออก อาคาร สถานที่

- ๔.๑ จัดทำเอกสารระบุสิทธิของ ผู้ใช้งาน และ “หน่วยงานภายนอก” ในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
- ๔.๑.๑ องค์กรต้องกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่สิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน
- ๔.๑.๒ รักรงค์หรือออกกฎให้เจ้าหน้าที่องค์กรแขวนบัตรพนักงานเพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน
- ๔.๑.๓ การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึก และรับแบบฟอร์มการเข้า-ออกพร้อมกับบัตรผู้ติดต่อ (Visitor)
- ๔.๑.๔ บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในองค์กร
- ๔.๑.๕ กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้า-ออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง
- ๔.๑.๖ กรณีที่บุคคลภายนอกเข้ามาติดต่อ เจ้าหน้าที่จะต้องลงชื่ออนุญาตการเข้า-ออกในแบบฟอร์มการเข้า-ออกให้ถูกต้อง
- ๔.๑.๗ บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และ รมภ.ต้องตรวจสอบผู้ติดต่อ อุปกรณ์พร้อมเวลาออกที่สมุดบันทึกให้ถูกต้อง
- ๔.๒ ผู้ใช้งานจะได้รับสิทธิให้เข้า-ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนด เพื่อใช้ในการทำงานเท่านั้น
- ๔.๓ หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่องค์กรออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้า-ออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

#### ๕. แนวปฏิบัติการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน

## ๕.๑. การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter)

- ๕.๑.๑. มีการจัดสภาพแวดล้อมทางกายภาพ เพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในองค์กร
  - ๕.๑.๒. มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง
  - ๕.๑.๓. ผนังล้อมรอบของสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในให้สร้างเป็นผนังทึบ
  - ๕.๑.๔. ประตู หรือทางเข้าสำนักงาน หรืออาคารออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ
  - ๕.๑.๕. ประตูหรือทางเข้าของห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อกได้ เพื่อป้องกันการบุกรุกทางกายภาพ
  - ๕.๑.๖. บุคลากรที่ปฏิบัติงานภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องปิดประตูและหน้าต่างให้ล็อกอยู่เสมอ ภายหลังจากเลิกงาน และนอกเวลาราชการ
  - ๕.๑.๗. มีการจัดระบบการรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัย (รปภ.) และมีการติดตั้งกล้องวงจรปิดภายในลิฟท์ เพื่อควบคุมการเข้าถึงของบุคคลภายนอก
  - ๕.๑.๘. ประตูหนีไฟและผนังในบริเวณข้างเคียงต้องมีการก่อสร้างให้มีความทนทานต่อความร้อนอย่างเพียงพอ
  - ๕.๑.๙. ต้องแยกพื้นที่สำหรับระบบเทคโนโลยีสารสนเทศขององค์กรออกจากพื้นที่ที่มีการดูแล หรือบริหารจัดการโดยผู้ให้บริการภายนอก
- ๕.๒. การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access Delivery and Loading Area)
- ๕.๒.๑. จำกัดการเข้าถึงพื้นที่ หรือบริเวณที่มีการส่งมอบ หรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
  - ๕.๒.๒. จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น
  - ๕.๒.๓. จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในองค์กร
  - ๕.๒.๔. ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน
  - ๕.๒.๕. กำหนดให้มีการลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก ให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร
- ๕.๓. การจัดวางและการป้องกันอุปกรณ์ (Equipment Siting and Protection)
- ๕.๓.๑. ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในหน่วยงานหรือสำนักงานให้น้อยที่สุด
  - ๕.๓.๒. ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอก โดยการหันหน้าจอเข้ามาภายในโดยไม่ให้บุคคลผู้ซึ่งไม่มีสิทธิสามารถมองเห็นหน้าจอ นั้นได้

- ๕.๓.๓ ต้องแยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย
  - ๕.๓.๔ ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสุขภัณฑ์ในบริเวณหรือพื้นที่ห้องควบคุมระบบเครือข่าย ระบบคอมพิวเตอร์ และระบบเครื่องคอมพิวเตอร์แม่ข่าย
  - ๕.๓.๕ ดำเนินการตรวจสอบ สอดส่องระดับอุณหภูมิจ และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบเครือข่าย ระบบคอมพิวเตอร์ และระบบเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว
  - ๕.๓.๖ มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน หรือไฟฟ้ากระชาก
- ๕.๔ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)
- ๕.๔.๑ ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรที่เพียงพอต่อความต้องการใช้งาน เช่น ระบบปรับอากาศ ระบบระบายอากาศ ระบบกระแสไฟฟ้าสำรอง เป็นต้น และต้องมีการตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
  - ๕.๔.๒ ต้องมีการใช้ระบบยูทิลิตี้กับระบบเทคโนโลยีสารสนเทศเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้าและต้องทดสอบระบบยูทิลิตี้อย่างสม่ำเสมอ โดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้
- ๕.๕ การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่น ๆ
- ๕.๕.๑ เจ้าหน้าที่ทุกคนต้องปฏิบัติตามการป้องกันทรัพย์สิน
  - ๕.๕.๒ เจ้าหน้าที่ต้องออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
  - ๕.๕.๓ ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อก และไม่ทิ้งเอกสารสำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของทรัพย์สินของราชการ
  - ๕.๕.๔ ต้องป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน และป้องกันตู้หรือบริเวณที่ใช้ในการรับ-ส่งเอกสารไปรษณีย์ เพื่อความปลอดภัยของข้อมูล
  - ๕.๕.๕ ต้องไม่ให้ผู้ที่มิได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่าง ๆ เช่น เครื่องคอมพิวเตอร์ กล้องดิจิทัล เครื่องพิมพ์ เครื่องถ่ายเอกสาร เครื่องสแกนเอกสาร เป็นต้น โดยมิได้รับอนุญาต
  - ๕.๕.๖ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- ๕.๖ มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์
- ๕.๖.๑ ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์
  - ๕.๖.๒ ต้องลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำลายหรือจำหน่าย
  - ๕.๖.๓ ต้องฟอร์แมต (Format) ฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยการใช้วิธีแบบเขียนทับซ้ำจำนวน ๑ ครั้ง ตามมาตรฐาน NIST ๘๐๐-๘๘ สำหรับข้อมูลที่มีความลับระดับต่ำ หรือแบบเขียนทับซ้ำจำนวน ๓ ครั้ง ตามมาตรฐาน

DoD ๕๒๒๐.๒๒- M สำหรับข้อมูลที่มีความลับระดับปานกลาง หรือแบบเขียนทับซ้ำจำนวน ๗ ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีความลับระดับสูง

- ๕.๖.๔ ลบข้อมูลออกจากฐานข้อมูลที่มีอายุตั้งแต่ ๕ ปีขึ้นไป และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- ๕.๖.๕ ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

## ส่วนที่ ๒

### นโยบายการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย (Network System Control Room Policy)

#### ๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก่ใจ เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะก่อให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้า-ออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่าย

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

#### ๓. คำจำกัดความของผู้เกี่ยวข้อง

- ๓.๑. ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศภายในห้องควบคุมระบบเครือข่าย
- ๓.๒. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์กรที่มีสิทธิในการเข้า-ออกสถานที่ อาคาร ห้องตามที่กำหนด ในทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่
- ๓.๓. ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาติดต่อขอเข้าถึง หรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของห้องควบคุมระบบเครือข่าย

#### ๔. บทบาทและความรับผิดชอบ

- ๔.๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
  - ๔.๑.๑ อนุมัติสิทธิเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
  - ๔.๑.๒ อนุมัติกระบวนการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย
- ๔.๒. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย
  - ๔.๒.๑ ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบเครือข่าย ให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด
  - ๔.๒.๒ ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้า-ออกห้องควบคุมระบบเครือข่าย ต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กรเท่านั้น

#### ๕. แนวปฏิบัติการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย

- ๕.๑. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย และเจ้าหน้าที่องค์กร มีแนวทางปฏิบัติ ดังนี้
  - ๕.๑.๑ ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ควรจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

- ๕.๑.๒ ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น
- ๕.๑.๓ สิทธิ์ในการเข้า-ออกห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย
- ๕.๑.๔ เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบเครือข่าย ตามกระบวนการลงทะเบียนที่ระบุในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน” เป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคน
- ๕.๑.๕ ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกห้องควบคุมระบบเครือข่าย
- ๕.๑.๖ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่าย ก็ต้องมีการควบคุมอย่างรัดกุม
- ๕.๑.๗ กรณีผู้ติดต่อจากหน่วยงานภายนอก มีความจำเป็นต้องเข้าห้องควบคุมระบบเครือข่าย เจ้าหน้าที่ผู้ดูแลระบบขององค์กรจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่อง กำกับดูแลตลอดการปฏิบัติงาน
- ๕.๒ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้
- ๕.๒.๑ ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน หรือ ใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่”
- ๕.๒.๒ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาต เข้า-ออก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน
- ๕.๒.๓ ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในห้องควบคุมระบบเครือข่ายหรือศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๕.๒.๔ ผู้ติดต่อจากหน่วยงานภายนอกต้องมีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารคอยสอดส่องดูแลตลอดเวลา
- ๕.๒.๕ ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อ กับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้า-ออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง
- ๕.๒.๖ เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้า-ออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

๕.๒.๗ เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการ  
ขออนุญาตเข้า-ออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน



## ส่วนที่ ๓

# นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control Policy)

### ๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๓ เจ้าหน้าที่ประจำโครงการขององค์กร

### ๓. แนวปฏิบัติในการควบคุมการเข้าถึงระบบ

- ๓.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์ และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น
- ๓.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
- ๓.๓ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้
- ๓.๔ ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ
- ๓.๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหากเกิดขึ้น

### ๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

- ๔.๑. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าว ต้องมีการจัดเก็บไว้เป็นหลักฐาน
- ๔.๒. เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

๔.๓. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

## ๕. แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้

๕.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ขององค์กร

๕.๑.๑ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

๕.๑.๒ ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิ์จากเจ้าของระบบ สำหรับการใช้งานระบบสารสนเทศและบริการอย่างถูกต้อง มีการอนุมัติรับรองการได้สิทธิ์จากผู้บริหารอย่างชัดเจน

๕.๑.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร

๕.๑.๔ ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิ์การเข้าถึงแก่ผู้ใช้ เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๕.๑.๕ ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นลาออกหรือเปลี่ยนตำแหน่งงาน

๕.๑.๖ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๕.๑.๗ การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๕.๑.๗.๑ เจ้าหน้าที่ใหม่ขององค์กรกรอกข้อมูลคำขอใช้บริการแบบฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เช่น คำขอใช้อินเทอร์เน็ต ระบบอีเมล หรือระบบงานต่าง ๆ

๕.๑.๗.๒ ยื่นคำขอกับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ที่ได้รับมอบหมาย

๕.๑.๘ การให้สิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๕.๑.๘.๑ ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิ์อนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๕.๑.๘.๒ ผู้ดูแลระบบตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

๕.๑.๘.๓ ผู้ดูแลระบบให้สิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม

๕.๑.๙ การแจ้งยกเลิกสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๕.๑.๙.๑ หัวหน้างานหรือผู้บังคับบัญชา แจ้งยกเลิกสิทธิ์การใช้งาน กับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๕.๑.๙.๒ ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

- ๕.๒ กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
- ๕.๓ ผู้ใช้งาน ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด
- ๕.๔ การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน
- ๕.๔.๑ ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ
- ๕.๔.๒ การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
- ๕.๔.๓ การส่งรหัสผ่านให้กับผู้ใช้ให้ใช้วิธีการที่ปลอดภัย และหลีกเลี่ยงการใช้บุคคลที่สาม หรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน
- ๕.๔.๔ กำหนดให้ผู้ใช้ตอบยืนยันการได้รับรหัสผ่าน
- ๕.๔.๕ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ ไม่ได้ป้องกันการเข้าถึง
- ๕.๔.๖ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
- ๕.๔.๖.๑ ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ
- ๕.๔.๖.๒ ต้องควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ๕.๔.๖.๓ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา
- ๕.๔.๖.๔ ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลาสั้นๆ ก็ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน
- ๕.๕ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
- ๕.๕.๑ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ระยะเวลาในการเข้าถึง ช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้
- ๕.๕.๑.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

- ๕.๕.๑.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
  - ๕.๕.๑.๓ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
  - ๕.๕.๑.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL VPN หรือ XML Encryption
  - ๕.๕.๑.๕ ต้องกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
  - ๕.๕.๑.๖ ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
- ๕.๕.๒ เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๒ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- ๕.๖ การบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน
- ๕.๖.๑ ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ
  - ๕.๖.๒ ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ และรหัสผ่านที่กำหนดใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม
  - ๕.๖.๓ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านที่ได้รับทันที
  - ๕.๖.๔ ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
  - ๕.๖.๕ ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่ให้อื่นนำไปใช้ไม่ว่าด้วยเหตุใดๆ ทั้งสิ้น เว้นแต่ กรณีผู้ใช้งานที่มีอำนาจอนุมัติใดๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติราชการอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าวเพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ์ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้วให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที
  - ๕.๖.๖ กำหนดให้รหัสผ่านต้องมีมากกว่า หรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

- ๕.๖.๗ ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕”
  - ๕.๖.๘ ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่
  - ๕.๖.๙ ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
  - ๕.๖.๑๐ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง
  - ๕.๖.๑๑ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์
  - ๕.๖.๑๒ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ
  - ๕.๖.๑๓ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
  - ๕.๖.๑๔ ในกรณีที่ผู้ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที
  - ๕.๖.๑๕ เมื่อมีปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน
  - ๕.๖.๑๖ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึกและประทับตรา“ลับ” และส่งไปยังผู้ใช้งาน และแนบเอกสาร “แนวปฏิบัติสำหรับการบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด
- ๕.๗ การใช้งานรหัสผ่าน
- ๕.๗.๑ เก็บรหัสผ่านไว้เป็นความลับ
  - ๕.๗.๒ หลีกเลี่ยงการบันทึกรหัสผ่านลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่างๆ
  - ๕.๗.๓ เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้
  - ๕.๗.๔ กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวเพียงพอสำหรับจดจำ ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่เป็นตัวเลขทั้งหมด หรือไม่เป็นตัวอักษรทั้งหมด
  - ๕.๗.๕ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว
  - ๕.๗.๖ กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานครั้งแรก
  - ๕.๗.๗ ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ
  - ๕.๗.๘ ไม่ใช้รหัสผ่านร่วมกับผู้อื่น
  - ๕.๗.๙ ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ปฏิบัติงานและในกรณีใช้ส่วนตัว
  - ๕.๗.๑๐ ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว แนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างต้น สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้
- ๕.๘ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน
- ๕.๘.๑ สิทธิ์การเข้าถึงข้อมูลของผู้ใช้ต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด คือ ทุกๆ ๖ เดือน และทุกครั้งที่มีการปรับเปลี่ยน เช่น

- การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง เป็นต้น
- ๕.๘.๒ สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่ เมื่อมีการเคลื่อนย้ายบุคลากรภายในองค์กร
  - ๕.๘.๓ การให้อำนาจสำหรับสิทธิการเข้าถึงพิเศษ ต้องทบทวนบ่อยกว่า คือ ทุก ๓ เดือน
  - ๕.๘.๔ การจัดสรรสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ
  - ๕.๘.๕ ความเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน
- ๕.๙ การป้องกันอุปกรณ์ในกรณีที่ไม่มีผู้ใช้งานที่อุปกรณ์
- ๕.๙.๑ ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงาน
  - ๕.๙.๒ ผู้ใช้งาน ต้องล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน รวมทั้ง Logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อกหน้าจอด้วยโปรแกรม Screen Saver ในระหว่างเวลาพักกลางวันและหลังเลิกงาน
  - ๕.๙.๓ ผู้ดูแลระบบ ต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศของตน โดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

## ๖. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่าย

- ๖.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ ที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
- ๖.๒ การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ต หรืออินทราเน็ต จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และการสื่อสารก่อนที่จะสามารถใช้งานได้ ในทุกกรณี
- ๖.๓ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
- ๖.๔ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน
- ๖.๕ ผู้ดูแลระบบ ต้องจัดให้มีวิธี เพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้
- ๖.๖ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้ทราบทุกครั้ง
- ๖.๗ ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกองค์กร ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet

- Filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย
- ๖.๘ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
  - ๖.๙ การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
  - ๖.๑๐ IP Address ภายในของระบบงานเครือข่ายภายในองค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้เกิดบุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของคุณ์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย
  - ๖.๑๑ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
  - ๖.๑๒ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
  - ๖.๑๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

#### ๗. แนวปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

- ๗.๑ ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน
- ๗.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที
- ๗.๓ ต้องเปิดให้บริการ(Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย
- ๗.๔ ต้องดำเนินการติดตั้งอัปเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น
- ๗.๕ ต้องมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
- ๗.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

## ๘. แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

- ๘.๑. ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน
- ๘.๒. ต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- ๘.๓. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

## ๙. แนวปฏิบัติ การควบคุมการเข้าใช้งานระบบจากภายนอก

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

- ๙.๑. การเข้าสู่ระบบจากระยะไกล (Remote Access) ผู้ระบบเครือข่ายคอมพิวเตอร์ขององค์กรก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
- ๙.๒. วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีและสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
- ๙.๓. ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ
- ๙.๔. ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
- ๙.๕. การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ต(Port) และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

## ๑๐. แนวปฏิบัติการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

- ๑๐.๑ ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ไม่ว่าจะเป็นการเข้าสู่ระบบสารสนเทศทางอินเทอร์เน็ตหรือการเข้าสู่ระบบจากระยะไกล(Remote Access) ต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร อย่างน้อย ๑ วิธี สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ
  - ๑๐.๑.๑ การแสดงตัวตน (Identification) คือ ขั้นตอนที่ใช้แสดงชื่อผู้ใช้ (Username)
  - ๑๐.๑.๒ การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password)



## ส่วนที่ ๔

### นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy)

#### ๑. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการให้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๓ เจ้าหน้าที่ประจำโครงการขององค์กร

#### ๓. แนวปฏิบัติทั่วไป

- ๓.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้
- ๓.๒ การควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก
  - ๓.๒.๑ บุคคลภายนอกที่ต้องการสิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
  - ๓.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้
    - ๓.๒.๒.๑ เหตุผลในการขอใช้
    - ๓.๒.๒.๒ ระยะเวลาในการใช้
    - ๓.๒.๒.๓ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
    - ๓.๒.๒.๔ การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
    - ๓.๒.๒.๕ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล
  - ๓.๒.๓ หน่วยงานภายนอก ที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

- ๓.๒.๔ องค์กรต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำกรควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศที่เข้าไปปฏิบัติงาน
- ๓.๒.๕ เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล
- ๓.๒.๖ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
- ๓.๒.๗ องค์กรมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น
- ๓.๒.๘ ต้องดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

## ส่วนที่ ๕

### นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

#### ๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก่ใจ เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศขององค์กร โดยมีการกำหนดนโยบายและแนวปฏิบัติควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

#### ๓. แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

##### ๓.๑ การใช้งานบริการเครือข่าย

- ๓.๑.๑ ห้ามผู้ใช้งานทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดี แห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือ ความรับผิดชอบขององค์กร
- ๓.๑.๒ องค์กรไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อ หรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร
- ๓.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใด ๆ ในส่วนที่มีใจของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็น การละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์กรไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว
- ๓.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าการพยายามรุกรานเข้าเขตหวงห้ามของทางราชการ
- ๓.๑.๕ องค์กรให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน หรือแจกจ่ายสิทธิ์นี้ให้กับผู้อื่นไม่ได้
- ๓.๑.๖ บัญชีผู้ใช้งาน (User Account) ที่องค์กรให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

- ๓.๑.๗ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- ๓.๑.๘ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา
- ๓.๑.๙ ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างปฏิบัติงาน
- ๓.๒ การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน  
จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวตนบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งาน ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้
- ๓.๒.๑ ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง
- ๓.๒.๒ ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวตนบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้รหัสผ่าน (Password) หรือการใช้สมาร์ตการ์ด
- ๓.๒.๓ จะต้องมีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศ ของหน่วยงาน อย่างน้อย ๑ วิธี
- ๓.๒.๔ ต้องมีการตรวจสอบผู้ใช้งานเมื่อมีการเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต
- ๓.๓ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์กรมีแนวทางปฏิบัติ ดังนี้
- ๓.๓.๑ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น
- ๓.๓.๒ สิทธิ์ในการเข้า-ออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้ากลุ่มงานเทคโนโลยีและเครือข่าย เป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย
- ๓.๓.๓ ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกองค์กร ตามกระบวนการที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”
- ๓.๓.๔ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่ายก็จะต้องมีการควบคุมอย่างรัดกุม
- ๓.๓.๕ การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”
- ๓.๔ ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติ ดังนี้
- ๓.๔.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”
- ๓.๔.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลง

บันทึกการรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออก ตามที่ระบุไว้ในเอกสาร“แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

- ๓.๔.๓ เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน
- ๓.๕ การระบุอุปกรณ์บนเครือข่าย
  - ๓.๕.๑ ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
  - ๓.๕.๒ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่
  - ๓.๕.๓ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
  - ๓.๕.๔ ผู้ขอใช้บริการต้องทำหนังสือเป็นลายลักษณ์อักษรถึงผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง “การขอเชื่อมต่อเครือข่าย” และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น
- ๓.๖ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ
  - ๓.๖.๑ ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย
  - ๓.๖.๒ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์ จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากหัวหน้ากลุ่มงานเทคโนโลยีและเครือข่ายก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา
  - ๓.๖.๓ บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น
  - ๓.๖.๔ ต้องยกเลิกหรือปิดพอร์ต และบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน
- ๓.๗ การแบ่งแยกเครือข่าย
  - ๓.๗.๑ องค์กรแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
  - ๓.๗.๒ องค์กรจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ
  - ๓.๗.๓ องค์กรติดตั้ง Firewall เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี
- ๓.๘ การควบคุมการเชื่อมต่อทางเครือข่าย
  - ต้องควบคุมการเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้
    - ๓.๘.๑ มีการตรวจสอบการเชื่อมต่อเครือข่าย
    - ๓.๘.๒ จำกัดสิทธิ์ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย
    - ๓.๘.๓ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๓.๘.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๓.๘.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๓.๙ การควบคุมการจัดเส้นทางบนเครือข่าย

ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูล หรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๓.๙.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๓.๙.๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓.๙.๓ กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่าย

## ส่วนที่ ๖

### นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

#### ๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

#### ๓. แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

- ๓.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- ๓.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
- ๓.๓ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง
- ๓.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
- ๓.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- ๓.๖ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา
- ๓.๗ ซอฟต์แวร์ที่องค์กรใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว
- ๓.๘ ซอฟต์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น
- ๓.๙ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นขององค์กรเพื่อประโยชน์ทางการค้า
- ๓.๑๐ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์
- ๓.๑๑ ห้ามผู้ใช้ระบบสารสนเทศขององค์กร เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

#### ๔. แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

- ๔.๑ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข
- ๔.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- ๔.๓ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
- ๔.๔ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

#### ๕. แนวปฏิบัติการใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)

- ๕.๑ มีการกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ ระดับสิทธิของผู้ขออนุมัติ และการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน
- ๕.๒ ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน
- ๕.๓ มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้
- ๕.๔ ต้องยกเลิกหรือลบทั้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็น ในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

#### ๖. แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

- ๖.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงาน และอุปกรณ์เครือข่าย มีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๐ นาที
- ๖.๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งาน ช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ
- ๖.๓ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้น สำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

#### ๗. แนวปฏิบัติการป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์

กำหนดมาตรการการบริหารจัดการซอฟต์แวร์ในองค์กร (Software Asset Management SAM)

- กำหนดรายการซอฟต์แวร์ที่ใช้ในธุรกิจ
- ห้ามนำซอฟต์แวร์ที่ไม่ได้รับอนุญาตมาใช้ในองค์กร
- ห้ามดาวน์โหลดโปรแกรมต่างๆ และแจ้งให้ทุกท่านทราบและปฏิบัติตามอย่างเคร่งครัด
- จัดให้มีการจัดซื้อซอฟต์แวร์จากส่วนกลางเพื่อควบคุมและบริหารการจัดซื้อ และการ

จัดเก็บและรักษาเอกสารการอนุญาตให้ใช้สิทธิต่างๆ



- สร้างรายการฐานข้อมูลของซอฟต์แวร์ที่ใช้ในองค์กร และมีการปรับปรุงรายการให้ถูกต้องอย่างสม่ำเสมอ เพื่อทราบถึงรายการของซอฟต์แวร์ที่จำเป็นต้องใช้
- แต่งตั้งผู้รับผิดชอบ เพื่อดูแลและป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ในองค์กร และตรวจสอบอย่างสม่ำเสมอทุกปี

## ส่วนที่ ๗

### นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control)

#### ๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๓ เจ้าหน้าที่ประจำโครงการขององค์กร

#### ๓. แนวปฏิบัติการจำกัดการเข้าถึงระบบสารสนเทศ (Information Access Control)

- ๓.๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการทำงานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติ สำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น
- ๓.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ ที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
- ๓.๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่า ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Login เข้าระบบสารสนเทศอีกครั้ง
- ๓.๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้
  - ๓.๔.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
  - ๓.๔.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
  - ๓.๔.๓ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)
  - ๓.๔.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

- ๓.๔.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- ๓.๔.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระดับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ
- ๓.๕ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ องค์กรได้กำหนดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่องค์กรพัฒนาในรูปแบบของ Webbase Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายใน ซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายดังกล่าว
- ๓.๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้
- ๓.๖.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- ๓.๖.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
- ๓.๖.๓ กำหนดระยะเวลาการใช้งานและระดับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ๓.๖.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น
- ๓.๖.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
- ๓.๖.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

#### ๔. แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

- ๔.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้ยาวนานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๑ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงาน ของสำนักงานตามปกติเท่านั้น
- ๔.๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ
- ๔.๓ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุ และพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้

## ๕. แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน

- ๕.๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ได้แก่ ระบบ GFMS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณการบัญชี การจัดซื้อ-จัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ซึ่งดูแลรับผิดชอบโดยกรมบัญชีกลางจะได้รับการแยกออกจากระบบงานอื่น ๆ ขององค์กร
- ๕.๒ ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

## ๖. แนวปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

- ๖.๑ ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
- ๖.๒ ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
- ๖.๓ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร
- ๖.๔ ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว
- ๖.๕ ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน
- ๖.๖ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์กรต้องการ
- ๖.๗ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล
- ๖.๘ องค์กรไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยองค์กร
- ๖.๙ องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากจากระยะไกล
- ๖.๑๐ องค์กรต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

## ๗ แนวปฏิบัติการควบคุมการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

### ๗.๑ การคัดเลือกผู้ให้บริการ

- มีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงาน ที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ
- มีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

### ๗.๒ การควบคุมผู้ให้บริการ

- ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่ของกรมฯ ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่กรมชลประทาน (onsite service) และให้เจ้าหน้าที่ของกรมฯ ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิดการเชื่อมต่อทันทีที่การให้บริการเสร็จสิ้น เป็นต้น
- กำหนดให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ
- กำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข กำหนดให้มีขั้นตอนในการตรวจรับงานของผู้ให้บริการอย่างชัดเจน

## ส่วนที่ ๘

### นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Policy)

#### ๑. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

#### ๒. ผู้รับผิดชอบ

- ๒.๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒. ผู้ใช้งาน

#### ๓. แนวปฏิบัติทั่วไป

- ๓.๑ เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร
- ๓.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- ๓.๓ ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร
- ๓.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ขององค์กรเท่านั้น
- ๓.๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น
- ๓.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- ๓.๗ ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่
- ๓.๘ ไม่สร้าง Short-cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร
- ๓.๙ ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยปฏิบัติ ดังนี้
  - ๓.๙.๑ ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
  - ๓.๙.๒ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

#### ๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

- ๔.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ
- ๔.๒ ผู้ใช้ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

- ๔.๓ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อกหน้าจอด้วยโปรแกรม Screen Saver เมื่อไม่มีการใช้งานโดยตั้งเวลาประมาณ ๑๐ นาที
- ๔.๔ มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

#### ๕. แนวทางปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้ปฏิบัติตาม แนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

#### ๖. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- ๖.๑ ผู้ใช้ต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ
- ๖.๒ ผู้ใช้มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์
- ๖.๓ ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
- ๖.๔ ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน
- ๖.๕ ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

#### ๗. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

- ๗.๑ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD DVD External Hard Disk เป็นต้น
- ๗.๒ ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
- ๗.๓ ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

ส่วนที่ ๙  
นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา  
(Use of Notebook Computer Policy)

**๑. วัตถุประสงค์**

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

**๒. ผู้รับผิดชอบ**

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ใช้งาน

**๓. แนวปฏิบัติทั่วไป**

- ๓.๑ เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร
- ๓.๒ โปรแกรมที่ได้ถูกติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพา หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- ๓.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น
- ๓.๔ การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น
- ๓.๕ ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ
- ๓.๖ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ ให้มีสภาพเดิม
- ๓.๗ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- ๓.๘ ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้
- ๓.๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่
- ๓.๑๐ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้



- ๓.๑๑ ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์
- ๓.๑๒ การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
- ๓.๑๓ ไม่เคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน
- ๓.๑๔ ไม่ใช่หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
- ๓.๑๕ ไม่ใช่หรือวางเครื่องคอมพิวเตอร์แบบพกพา ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส
- ๓.๑๖ ไม่วางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
- ๓.๑๗ ไม่ติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
- ๓.๑๘ การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบาที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

#### ๔. แนวปฏิบัติการป้องกันความปลอดภัยทางด้านกายภาพ

- ๔.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
- ๔.๒ ผู้ใช้งานไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ
- ๔.๓ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

#### ๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

- ๕.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
- ๕.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตามที่ระบุไว้ใน ข้อ ๕ (๕.๗) “การใช้งานรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- ๕.๓ ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน
- ๕.๔ ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

#### ๖. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตามแนวทางการใช้รหัสผ่านตาม ข้อ ๕ (๕.๗) “การใช้งานรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

## ๗. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- ๗.๑ ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
- ๗.๒ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา
- ๗.๓ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

## ๘. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

- ๘.๑ ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล
- ๘.๒ ผู้ใช้งานต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- ๘.๓ แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ
- ๘.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้นำไปใช้งานได้อีก

## ส่วนที่ ๑๐

### นโยบายการใช้งานอินเทอร์เน็ต (Internet Security Policy)

#### ๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้เกิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ชัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานได้ตามปกติ

#### ๒. ผู้รับผิดชอบ

- ๒.๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๓. ผู้ใช้งาน

#### ๓. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

- ๓.๑. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งาน ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นลายลักษณ์อักษรแล้ว
- ๓.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอัปเดตช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
- ๓.๓. ในการรับ-ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ-ส่งข้อมูลทุกครั้ง
- ๓.๔. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
- ๓.๕. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร
- ๓.๖. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร
- ๓.๗. ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
- ๓.๘. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มี

ลักษณะอันลามก และไม่ทำการเผยแพร่ หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

- ๓.๙. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- ๓.๑๐. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
- ๓.๑๑. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
- ๓.๑๒. ในการเสนอความคิดเห็นผ่านเว็บบอร์ด (Webboard) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับขององค์กร และต้องไม่ใช่ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสียหายต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ
- ๓.๑๓. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

## ส่วนที่ ๑๑

### นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

#### ๑. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

#### ๒. ผู้รับผิดชอบ

- ๒.๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๓. ผู้ใช้งาน

#### ๓. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

- ๓.๑. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
- ๓.๒. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานใหม่และรหัสผ่าน สำหรับการเข้าใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร
- ๓.๓. สำหรับผู้ใช้งานใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
- ๓.๔. การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
- ๓.๕. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น “x” หรือ “o” ในการพิมพ์แต่ละตัวอักษร
- ๓.๖. ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ต้องมีการ Logout ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
- ๓.๗. ผู้ใช้งานไม่ควรตั้งค่าการไปโปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
- ๓.๘. ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน
- ๓.๙. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิด

- ศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร
- ๓.๑๐. ห้ามผู้ใช้งานใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
  - ๓.๑๑. ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น
  - ๓.๑๒. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
  - ๓.๑๓. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น
  - ๓.๑๔. ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
  - ๓.๑๕. ผู้ใช้งานไม่ใช่ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์
  - ๓.๑๖. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
  - ๓.๑๗. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
  - ๓.๑๘. ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
  - ๓.๑๙. ข้อควรระวัง ผู้ใช้ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

## ส่วนที่ ๑๒

### นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

#### ๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการทำงานของระบบเครือข่ายไร้สาย

#### ๒. ผู้รับผิดชอบ

๒.๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

#### ๓. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓.๑. ผู้ใช้งานจะต้องมีบัญชีผู้ใช้งานระบบเครือข่ายขององค์กร จึงจะสามารถใช้งานระบบเครือข่ายไร้สายนี้ได้ กรณีที่องค์กรมีนโยบายในการใช้ชื่อผู้ใช้งานกลาง ให้ผู้ใช้งานติดต่อเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อรับค่า SSID (Service Set Identifier) และ Network Key ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่ายไร้สาย

๓.๒. ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

๓.๓. ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๓.๔. ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๓.๕. ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดายาก เพื่อป้องกันผู้โจมตีไม่สามารถเดาหรือเจาะรหัสได้โดยง่าย

๓.๖. ผู้ดูแลระบบต้องกำหนดค่าใช้ WEB หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

๓.๗. ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

๓.๘. ผู้ดูแลระบบต้องควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน(Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งานตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๓.๙. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ และบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

## ส่วนที่ ๑๓

### นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious Software Protection Policy)

#### ๑. วัตถุประสงค์

เพื่อควบคุม ป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์

#### ๒. ผู้รับผิดชอบ

๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๓ ผู้ใช้งาน

#### ๓. แนวปฏิบัติในการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๓.๑ ก่อนนำซอฟต์แวร์จากภายนอกมาใช้ภายในองค์กร ผู้ใช้งานต้องทำการตรวจสอบซอฟต์แวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้นไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

๓.๒ ผู้ดูแลระบบต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชันล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์

๓.๓ ผู้ดูแลระบบต้องกำหนดให้โปรแกรมค้นหาไวรัสทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะที่มีการใช้ระบบด้วย นอกจากนี้ผู้ดูแลระบบต้องมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ

๓.๔ ผู้ดูแลระบบต้องทำการตรวจทานระบบข้อมูลเพื่อตรวจหาไวรัสและซอฟต์แวร์อันตรายอยู่เป็นประจำ

๓.๕ ผู้ใช้งานต้องตรวจหาไวรัสของไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตก่อนนำไปใช้งาน

๓.๖ ห้ามมิให้เจ้าหน้าที่ดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนาไวรัส หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

๓.๗ ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกองค์กรมาใช้ ผู้ใช้งานสื่อข้อมูลนั้นต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง



## ส่วนที่ ๑๔

### นโยบายป้องกันระบบเครือข่ายและตรวจจัดการบุกรุก (Firewall & IPS Policy)

#### ๑. วัตถุประสงค์

เพื่อควบคุมการใช้งานเครือข่าย และกรองแพ็กเก็ตที่ผ่านเข้ามาในเครือข่ายองค์กร

#### ๒. ผู้รับผิดชอบ

๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

#### ๓. แนวปฏิบัติในการป้องกันระบบเครือข่ายและตรวจจัดการบุกรุก

๓.๑ อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งาน บริการเครือข่ายอื่นๆ ปิดทั้งหมด

๓.๒ ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท Network Scanning Tools เช่น Nmap เป็นต้น

๓.๓ ปิดบริการ รวมทั้งซอฟต์แวร์ที่ไม่จำเป็นบนไฟร์วอลล์

๓.๔ จำกัดบริการเครือข่ายที่ทำงานบนไฟร์วอลล์ให้น้อยที่สุด โดยแยกบริการอื่นๆ เหล่านั้นไปทำงานบนเครื่องอื่น

๓.๕ จำกัดข้อบัญญัติผู้ใช้งานบนเครื่องไฟร์วอลล์ให้น้อยที่สุด และไม่ Run ไฟร์วอลล์โดยใช้ชื่อบัญชีผู้ใช้งานที่เป็น Root หรือ Administrator

๓.๖ เปลี่ยนรหัสผ่านสำหรับ Root หรือ Administrator ที่ผู้ขายกำหนดมาให้ ให้เป็นรหัสอื่นที่ยากต่อการเดา

๓.๗ ต้องใช้ไฟร์วอลล์หลายชนิดร่วมกัน เช่น ไฟร์วอลล์แบบกรองแพ็กเก็ต ไฟร์วอลล์แบบ Proxy เพื่อเป็นการเสริมความมั่นคงปลอดภัยในแง่มุมที่ต่างกัน

๓.๘ ต้องใช้ระบบอื่นทำงานร่วมกับไฟร์วอลล์ ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟร์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) โปรแกรมกรองอีเมล และกรองเว็บ (Anti Spam) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยได้สูงขึ้น

๓.๙ กำหนดกฎในไฟร์วอลล์ให้กรองแพ็กเก็ตที่ไม่ประสงค์ดีออกตามรายการช่องโหว่ที่แพร่ระบาดอยู่ในปัจจุบันเสมอ

๓.๑๐ ป้องกันการเข้าถึงทางกายภาพต่อไฟร์วอลล์ให้มีความแข็งแกร่ง เช่น จัดทำเป็นห้องที่มีการควบคุมการเข้า-ออกอย่างเข้มงวด

๓.๑๑ หมั่นตรวจสอบกฎของไฟร์วอลล์ เพื่อกำจัดกฎที่ไม่มีความจำเป็นทิ้งไป เพื่อเพิ่มประสิทธิภาพของการประมวลผลกฎที่กำหนดไว้ของไฟร์วอลล์

๓.๑๒ เมื่อเพิ่มกฎข้อใหม่เข้าไปในไฟร์วอลล์ ตรวจสอบว่ากฎที่ใส่เข้าไ้ไปนั้นไม่ขัดแย้งกับกฎที่มีอยู่เดิม รวมทั้งทดสอบด้วยว่าไฟร์วอลล์สามารถป้องกันได้จริงตามกฎข้อใหม่นั้น

๓.๑๓ ตรวจสอบว่ากฎที่กำหนดไว้บนไฟร์วอลล์ไม่มีข้อขัดแย้งกับนโยบายความมั่นคงปลอดภัยขององค์กร อย่างน้อยควรทำปีละครั้ง

๓.๑๔ ไม่อนุญาตให้เข้าถึงไฟร์วอลล์จากทางไกลโดยโปรแกรมประเภท Telnet หรือแม้แต่ SSH โดยการเข้าถึงให้ทำได้จากตัวเครื่องไฟร์วอลล์โดยตรง

- ๓.๑๕ สร้างความแข็งแกร่งให้กับระบบปฏิบัติการของไฟร์วอลล์ โดย Update Patch เสมอ
- ๓.๑๖ ตรวจสอบ และติดตั้งโปรแกรมอุดช่องโหว่สำหรับระบบปฏิบัติการของไฟร์วอลล์อย่างสม่ำเสมอ
- ๓.๑๗ ก่อนการอัปเดต หรือแก้ไขช่องโหว่ของไฟร์วอลล์ ให้สำรองข้อมูลแบบ Full Backup ของเครื่องไฟร์วอลล์นั้นเก็บไว้ก่อน หากมีปัญหาจะได้นำกลับมาติดตั้งและใช้งานได้
- ๓.๑๘ ใช้ไฟร์วอลล์ร่วมกับ Router เพื่อป้องกันปัญหา DoS (Denial of Service) และปัญหาการเจาะระบบเข้าสู่ไฟร์วอลล์ได้โดยตรง
- ๓.๑๙ ใช้ไฟร์วอลล์เพื่อกั้นเครือข่ายภายใน ในกรณีที่มีความจำเป็น เช่น เครือข่ายส่วนนั้นอนุญาตให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นในการเข้าถึง
- ๓.๒๐ บันทึกข้อมูล Log ของการเข้าถึงไฟร์วอลล์เก็บไว้ รวมทั้งหากไฟร์วอลล์มีขีดความสามารถในการแจ้งเตือนให้เปิดใช้ขีดความสามารถนี้ด้วย
- ๓.๒๑ ใช้เซิร์ฟเวอร์ เช่น Syslog แยกต่างหากอีกเครื่องหนึ่งจากเครื่องของไฟร์วอลล์ เพื่อเก็บบันทึกข้อมูล Log ของการเข้าถึงไฟร์วอลล์ไว้บนเซิร์ฟเวอร์นั้น ซึ่งจะทำให้การเปลี่ยนแปลงแก้ไขข้อมูล Log โดยผู้บุกรุกทำได้ยากขึ้น
- ๓.๒๒ หากหน่วยงานอื่นต้องการนำระบบขึ้น จะต้องทำเป็นหนังสือผ่านผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร แจ้งเจ้าหน้าที่ให้ดำเนินการเป็นกรณีไป

## ส่วนที่ ๑๕

### นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

#### ๑. วัตถุประสงค์

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๓ ผู้ใช้งาน

#### ๓. แนวปฏิบัติในการคัดเลือกการสำรองข้อมูล

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

- ๓.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละครั้ง
- ๓.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้
  - ๓.๒.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
  - ๓.๒.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
  - ๓.๒.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลสำรองสำเร็จ/ไม่สำเร็จ เป็นต้น
  - ๓.๒.๔ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น
  - ๓.๒.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
  - ๓.๒.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
  - ๓.๒.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

- ๓.๒.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ อย่างน้อยปีละ ๒ ครั้ง
- ๓.๒.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ ตรวจสอบ และทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
- ๓.๒.๑๐ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

#### ๔. แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

- ๔.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียด ดังนี้
  - ๔.๑.๑ มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
  - ๔.๑.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลาสั้น ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้
  - ๔.๑.๓ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
  - ๔.๑.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
  - ๔.๑.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
  - ๔.๑.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น
- ๔.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละครั้ง

#### ๕. แนวปฏิบัติในการสำรองและกู้คืนข้อมูล

เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้กรณีที่เกิดการสูญหาย ไวรัสมัลแวร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยผู้ใช้งานเอง โดยมีมาตรการ ดังนี้

- ๕.๑ การสำรองข้อมูล
  - ๕.๑.๑ ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบ ไม่ต่ำกว่า ๑ ครั้งต่อเดือน
  - ๕.๑.๒ ผู้ดูแลระบบต้องตั้งค่าสำรองข้อมูลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server)

- ๕.๑.๓ ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ ของตนเองตามความเหมาะสม ไม่ต่ำกว่า ๑ ครั้งต่อเดือน
  - ๕.๑.๔ เมื่อองค์กรประกาศให้มีการสำรองข้อมูลเนื่องจากจะได้มีการดำเนินการที่อาจส่งผลกระทบต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ผู้ใช้งานจะต้องทำการสำรองข้อมูลดังกล่าวภายในระยะเวลาที่กำหนด
  - ๕.๑.๕ หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญ ให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)
  - ๕.๑.๖ ผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละหนึ่งครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบบนระบบทดสอบ
  - ๕.๑.๗ ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร และเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย
- ๕.๒ การกู้คืนข้อมูล
- เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลกระทบต่อเครื่องคอมพิวเตอร์ หรือการประมวลผลของคอมพิวเตอร์หยุดทำงานอย่างกะทันหัน หรือเปลี่ยนการทำงานไปจากเดิม ทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลา หรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติ มีมาตรการในการกู้คืนข้อมูล ดังนี้
- ๕.๒.๑ ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา
  - ๕.๒.๒ ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหาย
  - ๕.๒.๓ ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

## ส่วนที่ ๑๖

### นโยบายด้านการปฏิบัติตามข้อบังคับ (Compliance Policy)

#### ๑. วัตถุประสงค์

การปฏิบัติตามข้อบังคับด้านกฎหมาย เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมายที่เกี่ยวข้องกับการดำเนินงานขององค์กร การที่องค์กรทราบถึงข้อกำหนดต่าง ๆ ที่เกี่ยวข้องจะสามารถทำให้องค์กรมีความตระหนักถึงความเสี่ยงที่เกิดขึ้น รวมทั้งวางมาตรการควบคุมที่เหมาะสมได้ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการละเมิดดังกล่าว

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ สำนักกฎหมายและที่ดิน
- ๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๔ เจ้าหน้าที่ที่ได้รับมอบหมาย
- ๒.๕ ผู้ใช้งาน

#### ๓. แนวปฏิบัติในการปฏิบัติตามข้อบังคับ

- ๓.๑ การปฏิบัติตามข้อบังคับด้านกฎหมาย  
บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานคอมพิวเตอร์จะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้นหากผู้ใช้งานคอมพิวเตอร์กระทำผิดตามกฎหมายดังกล่าว องค์กรถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล
- ๓.๒ การปกป้องข้อมูลส่วนบุคคล
  - ๓.๒.๑ ข้อมูลรายละเอียดที่เกี่ยวข้องกับการดำเนินงานขององค์กร ถือเป็นข้อมูลที่มีความสำคัญ เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายตามหน้าที่งาน หรือได้รับอนุญาตจากผู้บริหารเท่านั้น ที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวได้
  - ๓.๒.๒ ข้อมูลส่วนตัวของเจ้าหน้าที่ถือว่าเป็นข้อมูลลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ เช่น เจ้าหน้าที่เอง หรือผู้ทำงานที่มีความเกี่ยวข้องเท่านั้น อย่างไรก็ตาม องค์กรสงวนสิทธิ์ ในการเข้าถึงข้อมูลทั้งหมดที่สร้างและเก็บอยู่ในระบบสารสนเทศขององค์กร
- ๓.๓ ลิขสิทธิ์ซอฟต์แวร์
  - ๓.๓.๑ ห้ามมิให้เจ้าหน้าที่นำซอฟต์แวร์ภายนอกมาใช้ในระบบประมวลผลขององค์กร โดยมีได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในหน่วยงาน โดยผู้บังคับบัญชา ต้องสอบถามกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ในเรื่องลิขสิทธิ์ขององค์กร และความเสี่ยงด้านความปลอดภัยสารสนเทศในการนำซอฟต์แวร์ดังกล่าวมาใช้ตามลำดับ

- ๓.๓.๒ เจ้าหน้าที่ต้องไม่ทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น
- ๓.๓.๓ ซอฟต์แวร์ที่พัฒนาภายในองค์กร ทั้งโดยบุคคลอื่นหรือเจ้าหน้าที่ขององค์กรถือว่าเป็นทรัพย์สินขององค์กร องค์กรไม่อนุญาตให้เจ้าหน้าที่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ ที่เป็นทรัพย์สินขององค์กร โดยไม่ได้รับการอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร
- ๓.๓.๔ ผู้ที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรทั้งหมด ต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด
- ๓.๓.๕ ซอฟต์แวร์ที่ได้จัดซื้อจากภายนอกอาจมีเงื่อนไขในเรื่องลิขสิทธิ์ด้านการใช้งานที่แตกต่างกัน หน่วยงานที่รับผิดชอบด้านการจัดซื้อต้องรับผิดชอบในการศึกษาถึงเงื่อนไขดังกล่าวจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องสร้างความตระหนักถึงผู้ใช้งานซอฟต์แวร์ดังกล่าวได้ทราบถึงเงื่อนไขต่าง ๆ และข้อห้ามที่เกี่ยวข้อง
- ๓.๓.๖ การจัดซื้อหรือใช้ซอฟต์แวร์ของบุคคลอื่นต้องปฏิบัติให้สอดคล้องกับข้อตกลงด้านลิขสิทธิ์ ห้ามนำซอฟต์แวร์ที่ซื้อไปติดตั้งที่เครื่องคอมพิวเตอร์อื่นนอกเหนือจากเครื่องที่ได้มีการติดตั้งแล้วตามข้อตกลงเรื่องลิขสิทธิ์ซอฟต์แวร์
- ๓.๓.๗ ทำการตรวจสอบการใช้งานคอมพิวเตอร์ขององค์กรอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์คอมพิวเตอร์ทุกชนิดเป็นไปตามข้อตกลงด้านลิขสิทธิ์ซอฟต์แวร์
- ๓.๓.๘ เจ้าหน้าที่ที่ฝ่าฝืนละเมิดข้อตกลงด้านลิขสิทธิ์ของเจ้าของซอฟต์แวร์ถือว่าการละเมิดนโยบายความปลอดภัยด้านสารสนเทศขององค์กร ถึงแม้การละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานขององค์กรก็ตาม เจ้าหน้าที่ต้องรับผิดชอบผลเสียหายทั้งหมด

## ส่วนที่ ๑๗

### นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

#### ๑. วัตถุประสงค์

การสอบทานการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มั่นใจว่านโยบายและมาตรฐานต่าง ๆ ด้านความปลอดภัยสารสนเทศมีการปฏิบัติตามอย่างมีประสิทธิภาพ ในทางปฏิบัติ องค์กรจำเป็นต้องมีการตรวจสอบอย่างสม่ำเสมอ ทั้งทางด้านกระบวนการทำงานรวมถึงด้านเทคนิค ทั้งนี้การตรวจสอบมิได้จำกัดเฉพาะหน่วยงานตรวจสอบ หรือคณะทำงานสอบทาน แต่ยังสามารถตรวจสอบภายในโดยหน่วยงานของตนเอง

#### ๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)
- ๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

#### ๓. แนวทางปฏิบัติในการสอบทาน

- ๓.๑ การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
  - ๓.๑.๑ กำหนดให้มีคณะทำงานสอบทาน ระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
  - ๓.๑.๒ ดำเนินการสอบทานระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยด้านสารสนเทศ ว่าสอดคล้องกับนโยบายหรือไม่ โดยรายงานสรุปผลเป็นรายไตรมาส หรืออย่างน้อยทุก ๖ เดือน ให้ CIO ทราบพร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง
  - ๓.๑.๓ หัวหน้างานในแต่ละหน่วยงานต้องรับผิดชอบในการสอบทานอย่างสม่ำเสมอ ถึงการปฏิบัติงานว่าสอดคล้องกับนโยบาย และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยด้านสารสนเทศ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รับผิดชอบในการสนับสนุนด้านการให้คำแนะนำในการปฏิบัติตามข้อกำหนดด้านความปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการปฏิบัติงานดังกล่าว
  - ๓.๑.๔ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายในหน่วยงานภาครัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง
  - ๓.๑.๕ รายการที่สอบทาน
    - ๓.๑.๕.๑ การป้องกันการบุกรุกระบบ
    - ๓.๑.๕.๒ การสำรองข้อมูล
    - ๓.๑.๕.๓ การควบคุมการเข้าห้องควบคุมระบบเครือข่าย



- ๓.๑.๕.๔ การควบคุมผู้เข้า-ออกอาคาร
- ๓.๑.๕.๕ การซ่อมรับสถานการณ์ฉุกเฉิน
- ๓.๒ การกำกับดูแลการปฏิบัติตามด้านเทคนิค
  - ๓.๒.๑ ผู้บริหารต้องกำกับดูแลเพื่อให้มั่นใจว่าเจ้าหน้าที่ที่ทราบถึงความรับผิดชอบด้านการรักษาความปลอดภัยด้านสารสนเทศ และได้มีการปฏิบัติในทางที่เหมาะสม ซึ่งอาจรวมถึงการจัดให้มีมาตรการในการวัดผลการปฏิบัติงานของเจ้าหน้าที่จากการปฏิบัติตามมาตรฐานความปลอดภัยของระบบสารสนเทศ
  - ๓.๒.๒ แผนกด้านตรวจสอบภายใน หรือคณะทำงานสอบทานต้องตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่ รวมทั้งการปฏิบัติตามการควบคุมเหล่านั้น
  - ๓.๒.๓ ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบ และประสิทธิผลของการควบคุมด้านความปลอดภัย
  - ๓.๒.๔ เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ระบบงาน และเอกสาร ที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้อง จากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

ส่วนที่ ๑๘  
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย  
ด้านสารสนเทศ  
(Information Security Awareness Policy)

๑. วัตถุประสงค์

เพื่อเผยแพร่ นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

- ๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๒.๒ สำนักงานเลขาธิการกรม
- ๒.๓ หน่วยงานที่ได้รับมอบหมายในการจัดฝึกอบรม
- ๒.๔ ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๒.๕ เจ้าหน้าที่ที่ได้รับมอบหมาย

๓. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- ๓.๑ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
- ๓.๒ จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน
- ๓.๓ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยการตีพิมพ์ ประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์
- ๓.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

## ภาคผนวก

## การจัดสายการบังคับบัญชา (Lines of authority) เมื่อเกิดเหตุฉุกเฉิน

๑. **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)**
  - ๑.๑ กำหนดนโยบายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
  - ๑.๒ ให้คำปรึกษาแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. **ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร**
  - ๒.๑ มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ
  - ๒.๒ มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุดิบอันตรายเพื่อการระงับเหตุฉุกเฉิน
  - ๒.๓ ประชุมหรือกักตมคณะทำงานบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะทำงานอื่นที่เกี่ยวข้อง
  - ๒.๔ ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม
  - ๒.๕ รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ
๓. **ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่ายและระบบสารสนเทศ**
  - ๓.๑. วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
  - ๓.๒. มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการระงับเหตุฉุกเฉิน จะมาถึงที่เกิดเหตุ
  - ๓.๓. การให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ
  - ๓.๔. ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่
  - ๓.๕. ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น
  - ๓.๖. รายงานให้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์ และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว
  - ๓.๗. กำหนดอัตรากำลังคน วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต
  - ๓.๘. ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ
๔. **ผู้ดูแลระบบเครือข่ายและระบบสารสนเทศ และผู้ช่วยดูแลระบบเครือข่ายและระบบสารสนเทศ (LAN Administrator and Staffs)**
  - ๔.๑. กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง
  - ๔.๒. พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ มาช่วย
  - ๔.๓. ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน
  - ๔.๔. ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดลอม ให้ได้รับความเสียหายน้อยที่สุด
  - ๔.๕. หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ firewall
- ทำการตรวจสอบ virus, worm, spy ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๔.๕ เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

๔.๖ ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่รับจ้างบำรุงรักษาในการกู้ระบบ

๔.๗ ทำการสำรองข้อมูลทุกวัน วันอาทิตย์-วันศุกร์

๔.๘ ทำการสำรองข้อมูลในส่วนของข้อมูล (data) วันเสาร์ทำการสำรองข้อมูลทั้งระบบ

๔.๙ ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, tape backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวข้องกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรอง สำเนาคู่มือ

๔.๑๐ นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

#### ๕. ที่ปรึกษาด้านเทคนิค (เจ้าหน้าที่บริษัทที่รับจ้างบำรุงรักษาระบบ)

๕.๑. ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศ และวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

๕.๒. ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญ หรือหน่วยราชการที่เกี่ยวข้อง

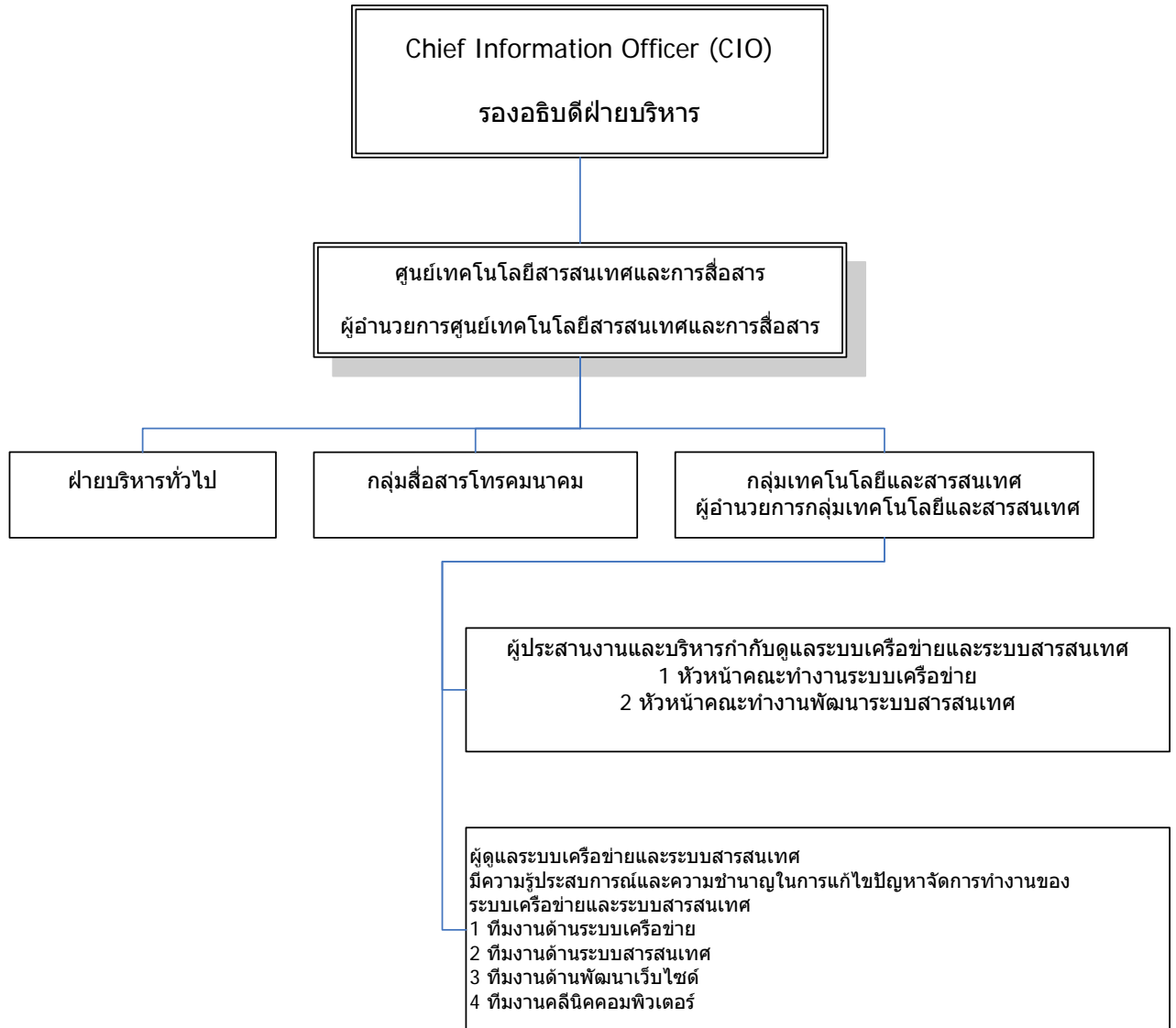
๕.๓. ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

#### ๖. หัวหน้าหน่วยงานที่เกิดเหตุ (On-site manager)

๖.๑. แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

๖.๒ ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสอบสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับชั้น

ผู้รับผิดชอบระบบเครือข่ายและระบบสารสนเทศ  
ตามสายงานการบังคับบัญชา



## แนวปฏิบัติเพื่อการบริหารจัดการการเข้าถึงข้อมูล

๑. ประเภทของข้อมูล แบ่งออกเป็น
  - ข้อมูลตามภารกิจ นโยบาย ยุทธศาสตร์และคำรับรองการปฏิบัติราชการ ได้แก่ ข้อมูลอุทกวิทยา น้ำฝน น้ำท่า ข้อมูลน้ำสถานการณ์น้ำ ข้อมูลโครงการชลประทานต่าง ๆ
  - ข้อมูลเพื่อการสนับสนุน ได้แก่ ข้อมูลงบประมาณ, ข้อมูลการเงินและบัญชี, ข้อมูลพัสดุ ครุภัณฑ์
  - ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลบุคลากร
๒. ลำดับชั้นความลับของข้อมูล แบ่งออกเป็น ๓ ระดับ ดังนี้
  - ระดับชั้นความลับที่สุด คือ ข้อมูลส่วนบุคคล
  - ระดับชั้นความลับปานกลาง คือ ข้อมูลเพื่อการสนับสนุน
  - ระดับชั้นความลับน้อย คือ ข้อมูลตามภารกิจ
๓. ลำดับชั้นการถึงข้อมูล มีดังนี้
  - ผู้บริหาร
  - ผู้ดูแลระบบ
  - ผู้ใช้งานทั่วไปหรือผู้ที่ได้มอบหมาย
  - เจ้าของข้อมูลส่วนบุคคล
๔. กำหนดเวลาที่ได้เข้าถึงข้อมูลสารสนเทศ ให้บริการตลอด ๒๔ ชั่วโมง และจะมีการปรับปรุงให้ทันสมัยตามรอบระยะเวลาที่กำหนด
๕. ช่องทางที่สามารถเข้าถึงระบบ Intranet / Internet