ประกาศกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๕๗

---

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืชจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ ตามประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๕๗”

ข้อ ๒ วัตถุประสงค์

๒.๑ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๒ เพื่อให้เกิดความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ ๓ ขอบเขตการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช มีขอบเขตครอบคลุม ดังนี้

๓.๑ การควบคุม...

๓.๑ การควบคุมการเข้าถึงและการใช้งานสารสนเทศ

๓.๑.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

๓.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๓.๑.๓ การควบคุมการเข้าถึงห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑.๔ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑.๕ การควบคุมการเข้าถึงระบบเครือข่าย

๓.๑.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑.๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๓.๑.๘ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

๓.๒ การจัดทำระบบสำรองของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ การกำหนดความรับผิดชอบ

๔.๑ ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูงสุด (CEO) ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

กำหนดให้ผู้อำนวยการศูนย์สารสนเทศ เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

๔.๒ ระดับปฏิบัติ

๔.๒.๑ นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ ผู้รับผิดชอบได้แก่

๔.๒.๑.๑ ศูนย์สารสนเทศ

๔.๒.๑.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๑.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย

๔.๒.๑.๔ ผู้ใช้งาน

๔.๒.๒ นโยบายการจัดทำระบบสำรองของระบบสารสนเทศ ผู้รับผิดชอบได้แก่

๔.๒.๒.๑ ศูนย์สารสนเทศ
๔.๒.๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
๔.๒.๒.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย

๔.๒.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่
๔.๒.๓.๑ ศูนย์สารสนเทศ
๔.๒.๓.๒ ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบจากภายนอก
๔.๒.๓.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่
๔.๒.๔.๑ ศูนย์สารสนเทศ
๔.๒.๔.๒ ส่วนฝึกอบรม สำนักบริหารงานกลาง
๔.๒.๔.๓ หน่วยงานที่ได้รับมอบหมายในการฝึกอบรม
๔.๒.๔.๔ ผู้ดูแลระบบที่ได้รับมอบหมาย
๔.๒.๔.๕ เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๕ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมถึงทบทวนปรับปรุงนโยบายและข้อปฏิบัติอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๕๗" เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช และหน่วยงานภายนอก ต้องถือปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่วันที่ ๒๒ ตุลาคม พ.ศ. ๒๕๕๗ เป็นต้นไป

ประกาศ ณ วันที่ ๒๒ ตุลาคม พ.ศ. ๒๕๕๗

( นายนิพนธ์ โชติบาล )
อธิบดีกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

# เอกสารแนบท้ายประกาศ

# กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๕๗**


# นโยบายและแนวปฏิบัติ
# ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
# ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช
## พ.ศ. ๒๕๕๗

# คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้”และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ศูนย์สารสนเทศ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๕๗ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ และขั้นตอนวิธีปฏิบัติ ที่ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสอดคล้องตามพระราชกฤษฎีกาและประกาศฯ ดังกล่าวข้างต้น เพื่อให้เจ้าหน้าที่และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติต่อไป

# สารบัญ

# นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
# กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

## ๑. วัตถุประสงค์และขอบเขต

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืชจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.๑. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๒. เพื่อให้เกิดความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๓. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืชได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

## ๒. องค์ประกอบของนโยบายในภาพรวม

๒.๑. คำนิยาม

๒.๒. ส่วนที่ ๑ การควบคุมการเข้าถึงและการใช้งานสารสนเทศ

- ๒.๒.๑. การควบคุมการเข้าถึงระบบสารสนเทศ
- ๒.๒.๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- ๒.๒.๓. การควบคุมการเข้าถึงห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย
- ๒.๒.๔. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
- ๒.๒.๕. การควบคุมการเข้าถึงระบบเครือข่าย
- ๒.๒.๖. การควบคุมการเข้าถึงระบบปฏิบัติการ
- ๒.๒.๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
- ๒.๒.๘. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

๒.๓. ส่วนที่ ๒ การจัดทำระบบสำรองของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๒.๔. ส่วนที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒.๕. ส่วนที่ ๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืชแต่ละส่วน ประกอบด้วย วัตถุประสงค์ ผู้รับผิดชอบ รายละเอียดมาตรฐาน แนวทางและขั้นตอนวิธีการปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เพื่อให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ช่วยลดความเสียหายต่อการดำเนินงานขององค์กร และสามารถดำเนินงานได้อย่างมั่นคงและปลอดภัย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ซึ่งเจ้าหน้าที่ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช และหน่วยงานภายนอกที่เกี่ยวข้อง ต้องถือปฏิบัติตามอย่างเคร่งครัด

## คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ประกอบด้วย

**องค์กร** หมายถึง กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**ผู้บริหารระดับสูงสุด** (Chief Executive Officer: CEO) หมายถึง ผู้มีอำนาจสูงสุดของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ได้แก่ อธิบดีกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย ตัดสินใจ และแนะนำแนวทางการดำเนินงานของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง** (Chief Information Officer: CIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

**ศูนย์สารสนเทศ** หมายถึง ศูนย์สารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**ผู้อำนวยการศูนย์สารสนเทศ** หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช และมีอำนาจตัดสินใจเกี่ยวกับระบบเทคโนโลยีสารสนเทศภายในกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**มาตรฐาน** (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

**ขั้นตอนการปฏิบัติ** (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

**แนวทางปฏิบัติ** (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

**ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืชกำหนดไว้ดังนี้

**ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช เช่น ผู้อำนวยการสำนัก/กอง เป็นต้น

**ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

**เจ้าหน้าที่** หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานจ้างเหมา และเจ้าหน้าที่ประจำโครงการต่างๆ ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

**หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

**ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

**สารสนเทศ** (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

**ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

**ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

**ระบบแลน** (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

**ระบบอินเทอร์เน็ต** (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

**ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

**พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร** (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 หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

**สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

**สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีคุณค่าสำหรับองค์กร

**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

**ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

**<u>เหตุการณ์ด้านความมั่นคงปลอดภัย</u>** (Information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

**<u>สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด</u>** (Information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

**<u>จดหมายอิเล็กทรอนิกส์</u>** (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

**<u>รหัสผ่าน</u>** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

**<u>ชุดคำสั่งไม่พึงประสงค์</u>** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

## ส่วนที่ ๑

## นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

### วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานสารสนเทศขององค์กร ป้องกันการบุกรุกผ่านระบบเครือข่าย หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่าย รวมทั้งสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานสนเทศขององค์กรได้อย่างถูกต้อง

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

### ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย
๔. ผู้ใช้งาน

### อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

### ข้อปฏิบัติ

**๑. การควบคุมการเข้าถึงระบบสารสนเทศ**

เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัย มีข้อปฏิบัติ ดังนี้

๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ โดยจำแนกกลุ่มทรัพยากรระบบ การทำงานและสถานที่เก็บหรือประมวลผล และระบุสิทธิ์ในการเข้าถึงสินทรัพย์นั้น

๑.๒ กำหนดสิทธิของผู้ใช้งาน ดังนี้

๑.๒.๑ กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งานแต่ละกลุ่ม ได้แก่

๑.๒.๑.๑ สิทธิอ่านอย่างเดียว
๑.๒.๑.๒ สิทธิการเพิ่มข้อมูล
๑.๒.๑.๓ สิทธิการแก้ไขข้อมูล
๑.๒.๑.๔ สิทธิการลบข้อมูล
๑.๒.๑.๕ สิทธิการอนุมัติ/อนุญาต
๑.๒.๑.๖ ไม่มีสิทธิ

๑.๒.๒ กำหนดการระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย ตามแบบลงทะเบียนผู้ใช้งาน

๑.๓ กำหนดประเภทข้อมูล ลำดับชั้นความลับ ความสำคัญ เวลา และช่องที่เข้าถึง ดังนี้

๑.๓.๑ จัดแบ่งประเภทข้อมูล ออกเป็น

๑.๓.๑.๑ ข้อมูลด้านการบริหาร ได้แก่

๑.๓.๑.๑.๑ นโยบาย

๑.๓.๑.๑.๒ ข้อมูลยุทธศาสตร์

๑.๓.๑.๑.๓ คำรับรองการปฏิบัติราชการ

๑.๓.๑.๑.๔ ข้อมูลบุคลากร

๑.๓.๑.๑.๕ งบประมาณ

๑.๓.๑.๑.๖ การเงินและบัญชี

๑.๓.๑.๒ ข้อมูลด้านการดำเนินงาน ได้แก่

๑.๓.๑.๒.๑ การดำเนินงานตามภารกิจกรมอุทยานแห่งชาติ สัตว์ป่าและพันธุ์พืช

๑.๓.๑.๒.๒ กฎหมาย ระเบียบ

๑.๓.๑.๒.๓ การใช้จ่ายงบประมาณ

๑.๓.๑.๒.๔ ผลการปฏิบัติงาน

๑.๓.๑.๓ ข้อมูลด้านการให้บริการ ได้แก่

๑.๓.๑.๓.๑ ข้อมูลสถิติกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

๑.๓.๑.๓.๒ ข้อมูลวิชาการและองค์ความรู้ด้านการอนุรักษ์ทรัพยากรป่าไม้

๑.๓.๑.๓.๓ ข้อมูลพื้นที่อนุรักษ์

๑.๓.๒ จัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภท ตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ เป็น ๓ ชั้น คือ

๑.๓.๒.๑ ลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๑.๓.๒.๒ ลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๑.๓.๒.๓ ลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๑.๓.๓ จัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภท เป็น ๔ ระดับ คือ

๑.๓.๓.๑ สำคัญมากที่สุด

๑.๓.๓.๒ สำคัญมาก

๑.๓.๓.๓ สำคัญ

๑.๓.๓.๔ ทั่วไป

๑.๓.๔ จัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท

๑.๓.๔.๑ เข้าถึงได้ทุกกลุ่มผู้ใช้งานที่กำหนดไว้

๑.๓.๔.๒ เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง

๑.๓.๔.๓ เข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ

๑.๓.๔.๔ เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ

๑.๓.๕ กำหนดช่องทางในการเข้าถึงข้อมูล

๑.๓.๕.๑ เครือข่ายภายใน (LAN)

๑.๓.๕.๒ อินทราเน็ต (Intranet)

๑.๓.๕.๓ อินเตอร์เน็ต (Internet)

๑.๓.๕.๔ จดหมายอิเล็กทรอนิกส์ (e-mail)

๑.๓.๖ กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล

๑.๓.๖.๑ เวลาราชการ (๘.๓๐ - ๑๖.๓๐ น.)

๑.๓.๖.๒ นอกเวลาราชการ

๑.๓.๖.๓ ช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และ วันหยุดนักขัตฤกษ์)

๑.๓.๖.๔ ช่วงเวลาพิเศษเป็นรายครั้ง

๑.๔ กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ดังนี้

๑.๔.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๑.๔.๒ เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

๑.๔.๓ ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน โดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ

**๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)**

๒.๑ การสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดมาตรการเชิงป้องกัน ดังนี้

๒.๑.๑ มีการเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้งานได้รับทราบ

๒.๑.๒ มีการฝึกอบรมหลักสูตรเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ ให้ทราบถึงภัยและผลกระทบจากการใช้เทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๒.๒ การลงทะเบียนผู้ใช้งานมี ดังนี้

๒.๒.๑ การลงทะเบียนผู้ใช้งาน

๒.๒.๑.๑ ผู้ใช้งานกรอกข้อมูลคำขอตามแบบฟอร์มการขอใช้ระบบเทคโนโลยีสารสนเทศ และยื่นต่อเจ้าหน้าที่หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๒.๑.๒ ผู้ดูแลระบบตรวจสอบและกำหนดสิทธิที่เหมาะสมในการเข้าถึงตามหน้าที่ความรับผิดชอบ หรือตามที่เจ้าของระบบได้มอบหมายสิทธิ

๒.๓ การบริหารจัดการสิทธิของผู้ใช้งาน

๒.๓.๑ ผู้ดูแลระบบ ต้องกำหนดรหัสผู้ใช้ รหัสผ่าน และสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบตามหน้าที่ความรับผิดชอบของแต่ละกลุ่มผู้ใช้งาน เพื่อใช้ในการตรวจสอบยืนยันตัวตนของผู้ใช้งาน

๒.๓.๒ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาควบคุมการใช้งานอย่างรัดกุมเพียงพอ ดังนี้

๒.๓.๒.๑ ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบนั้นๆ

๒.๓.๒.๒ ควบคุมการใช้งานอย่างเข้มงวด กำหนดให้มีการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๒.๓.๒.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๓.๒.๔ มีการเปลี่ยนรหัสผ่านอย่างทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือหากมีความจำเป็นต้องใช้งานเป็นระยะเวลานานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

๒.๓.๓ มีการกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่าย (LAN) ระบบเครือข่ายไร้สาย (Wireless LAN) และระบบอินเตอร์เน็ต โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร และต้องทบทวนสิทธิอย่างสม่ำเสมอ

๒.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๔.๑ เปลี่ยนรหัสผ่านทันทีภายหลังจากได้รับรหัสผ่านชั่วคราว จากการลงทะเบียนผู้ใช้งาน และภายหลังจากการติดตั้งซอฟต์แวร์

๒.๔.๒ ไม่กำหนดรหัสผ่านจากชื่อ นามสกุลตนเอง ชื่อ นามสกุลของบุคคลใกล้ชิด และคำศัพท์จากพจนานุกรม

๒.๔.๓ กำหนดรหัสผ่านอย่างน้อย ๘ ตัวอักษร โดยมีการผสมระหว่างตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์

๒.๔.๔ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยทุก ๖ เดือน และไม่ใช่รหัสผ่านเดิมที่เคยใช้งาน

๒.๔.๕ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องใช้วิธีการที่ปลอดภัย ไม่ส่งผ่านบุคคลที่สาม และส่งผ่านจดหมายอิเล็กทรอนิกส์ที่ไม่มีการเข้ารหัสข้อมูลที่ปลอดภัย

๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๒.๕.๑ เจ้าของระบบหรือผู้ดูแลระบบที่ได้รับมอบหมาย ต้องทบทวนความเหมาะสมของสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยทุก ๖ เดือน และเมื่อมีการเปลี่ยนแปลงตำแหน่ง หรือสิ้นสุดหน้าที่ความรับผิดชอบ

๒.๖ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๒.๖.๑ การใช้งานรหัสผ่าน

๒.๖.๑.๑ ต้องเก็บรหัสผ่านไว้เป็นความลับ

๒.๖.๑.๒ ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นจากบุคคลอื่น

๒.๖.๑.๓ เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านอาจรั่วไหลหรือถูกเปิดเผย

๒.๖.๑.๔ กรณีมีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นในการดำเนินงาน ต้องเปลี่ยนรหัสผ่านทันทีหลังจากดำเนินงานเรียบร้อยแล้ว

๒.๖.๑.๕ เมื่อเจ้าหน้าที่ในหน่วยงาน ลาออก เปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบงานสารสนเทศ หรือพ้นจากความรับผิดชอบ ให้หน่วยงานแจ้งผู้ดูแลระบบทันที เพื่อเปลี่ยนสิทธิหรือถอนสิทธิออกจากระบบ ตามความรับผิดชอบทันที

๒.๖.๑.๖ ไม่บันทึกรหัสผ่านไว้ในโปรแกรมหรือการจดจำรหัสผ่านในการ Login อัตโนมัติ

๒.๖.๑.๗ กำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๒.๖.๑.๗.๑ ง่ายต่อการจดจำ

๒.๖.๑.๗.๒ ไม่เกี่ยวข้องกับข้อมูลพื้นฐานที่คนอื่นสามารถคาดเดาได้ง่าย หรือหาได้จากข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ วันเดือนปีเกิด เป็นต้น

๒.๖.๑.๗.๓ ไม่เป็นคำที่อยู่ในพจนานุกรม

๒.๖.๑.๗.๔ มีการผสมระหว่างตัวอักษรพิมพ์ใหญ่พิมพ์เล็ก ตัวเลข และสัญลักษณ์ โดยไม่ใช้คำ ตัวอักษร หรือตัวเลขซ้ำ และมีความยาวอย่างน้อย ๘ ตัวอักษร

๒.๖.๑.๘ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยทุกๆ ๖ เดือนสำหรับผู้ใช้งานทั่วไป และทุกๆ ๓ เดือนสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับสิทธิพิเศษ

๒.๖.๒ การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งานที่อุปกรณ์

๒.๖.๒.๑ ผู้ใช้งานต้องล็อกหน้าจอทุกครั้งเมื่อไม่ใช้งานเครื่องคอมพิวเตอร์และไม่อยู่ที่หน้าจอ หรือตั้งให้มีการล็อกหน้าจออัตโนมัติหลังจากไม่ได้ใช้งานนานเกินกว่า ๑๕ นาที

๒.๖.๒.๒ หลังจากมีการล็อกหน้าจอแล้ว ต้องกำหนดให้ใส่รหัสผ่านให้ถูกต้องก่อนจึงจะสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้

๒.๖.๒.๓ ผู้ใช้งานต้อง Logout ออกจากระบบทันทีเมื่อเลิกใช้งานระบบสารสนเทศ

๒.๖.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ เพื่อควบคุมและป้องกันไม่ให้สินทรัพย์สารสนเทศหรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

๒.๖.๓.๑ การจัดการสภาพแวดล้อมทางกายภาพ

๒.๖.๓.๑.๑ จำแนกและกำหนดพื้นที่การใช้งานและระดับความสำคัญของระบบเทคโนโลยีสารสนเทศ

๒.๖.๓.๑.๒ มีระบบป้องกันการบุกรุกติดตั้งครอบคลุมพื้นที่ที่มีความสำคัญ

๒.๖.๓.๑.๓ มีระบบรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัยดูแลอาคาร และมีการติดตั้งกล้องวงจรปิดเพื่อบันทึกเหตุการณ์ไว้ใช้ในการตรวจสอบภายหลัง

๒.๖.๓.๑.๔ บุคลากรที่ปฏิบัติงานในพื้นที่ต้องปิดล็อกประตูและหน้าต่างทุกครั้งหลังเลิกงาน

๒.๖.๓.๑.๕ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพว่าใช้งานได้ตามปกติอย่างสม่ำเสมอ

๒.๖.๓.๒ การควบคุมการเข้าออกพื้นที่ใช้งาน

๒.๖.๓.๒.๑ จัดทำบันทึกการเข้า-ออก พื้นที่ใช้งานสำหรับบุคคลภายนอกหรือผู้มาติดต่อ

๒.๖.๓.๒.๒ มีเจ้าหน้าที่ดูแลบุคคลภายนอกหรือผู้มาติดต่อในพื้นที่ที่มีความสำคัญทุกครั้งจนเสร็จสิ้นภารกิจ

๒.๖.๓.๒.๓ กรณีบุคคลภายนอกหรือผู้มาติดต่อ ต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเข้ามาในบริเวณพื้นที่ใช้งาน ต้องบันทึกแบบฟอร์มการเข้า-ออก ในรายการอุปกรณ์ด้วยทุกครั้ง

๒.๖.๓.๒.๔ มีการควบคุมการเข้าออกสถานที่ตั้งของระบบเทคโนโลยีสารสนเทศอย่างรัดกุม และอนุญาตให้เฉพาะผู้มีสิทธิและความจำเป็นผ่านเข้าถึงพื้นที่ได้เท่านั้น

๒.๖.๓.๒.๕ กรณีที่ต้องการนำทรัพย์สินสารสนเทศ ออกจากพื้นที่ใช้งาน ต้องขออนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง

๒.๖.๓.๒.๖ จัดให้มีการทบทวนสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๒.๖.๓.๓ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery and Loading Areas)

๒.๖.๓.๓.๑ จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๖.๓.๓.๒ จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๒.๖.๓.๓.๓ จัดพื้นที่หรือบริเวณส่งมอบไว้ต่างหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในองค์กร

๒.๖.๓.๓.๔ ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนจะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

๒.๖.๓.๓.๕ ต้องลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก ให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

๒.๖.๓.๔ การจัดวางและป้องกันอุปกรณ์

๒.๖.๓.๔.๑ ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของระบบเทคโนโลยีสารสนเทศน้อยที่สุด

๒.๖.๓.๔.๒ ต้องแยกอุปกรณ์ที่มีความสำคัญเก็บไว้ในที่ที่มีความปลอดภัย

๒.๖.๓.๔.๓ ไม่นำอาหารและเครื่องดื่ม เข้ามาในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ

๒.๖.๓.๔.๔ ดำเนินการตรวจสอบ ดูแลสภาพแวดล้อม อุณหภูมิ ความชื้น ภายในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายต่ออุปกรณ์ภายในบริเวณดังกล่าว

๒.๖.๓.๔.๕ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรอย่างเพียงพอ ได้แก่ระบบกระแสไฟฟ้าสำรองและป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการเกิดกระแสไฟฟ้าผิดปกติ ระบบปรับอากาศ ระบบระบายอากาศ และระบบควบคุมความชื้น

๒.๖.๓.๔.๖ ต้องตรวจสอบหรือทดสอบการทำงานของระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบต่างๆ สามารถทำงานได้ตามปกติ และลดความเสี่ยงจากการทำงานของระบบล้มเหลว

๒.๖.๓.๕ การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่นๆ

๒.๖.๓.๕.๑ ผู้ใช้งานต้องระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน หรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหาย หรือเสียหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

๒.๖.๓.๕.๒ ผู้ใช้งานต้องเก็บเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลสำคัญไว้ในที่ปลอดภัย เช่น ในตู้หรือโต๊ะที่มีสามารถล็อกได้ และแยกเอกสารสำคัญสำหรับทำลายไว้ต่างหาก เพื่อความปลอดภัยของทรัพย์สินราชการ

๒.๖.๓.๕.๓ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒.๖.๓.๕.๔ ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์และสื่อสารต่างๆ โดยไม่ได้รับอนุญาต

๒.๖.๓.๖ มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

๒.๖.๓.๖.๑ ต้องทำการล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนการส่งซ่อมหรือเปลี่ยนอุปกรณ์

๒.๖.๓.๖.๒ ต้องทำการลบข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการทำลายหรือจำหน่าย

๒.๖.๓.๖.๓ ต้องทำการฟอร์แมตฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยใช้วิธีแบบเขียนทับซ้ำจำนวน ๑ ครั้ง ตามมาตรฐาน NIST ๘๐๐-๘๘ สำหรับข้อมูลที่เป็นชั้นความลับที่ไม่ลับมาก เขียนทับซ้ำจำนวน ๓ ครั้ง มาตรฐาน DoD ๕๒๒๐.๒๒-M สำหรับข้อมูลที่มีชั้นความลับเป็นลับมาก และเขียนทับซ้ำจำนวน ๗ ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลลับมากที่สุด

๒.๖.๓.๖.๔ ลบข้อมูลการดำเนินงานที่มีอายุตั้งแต่ ๕ ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูล และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๒.๖.๓.๖.๕ ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล และเจ้าของข้อมูลในการลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

๒.๖.๓.๗ การรักษาความลับข้อมูล

๒.๖.๓.๗.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและผ่านระบบงานสารสนเทศ

๒.๖.๓.๗.๒ การรับส่งข้อมูลที่เป็นความลับหรือข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption

๒.๖.๓.๗.๓ ผู้ใช้งานสามารถนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๒.๖.๓.๗.๔ กำหนดรหัสผ่านในการเข้าถึงไฟล์ข้อมูลลับ เพื่อป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ใช้งาน

๒.๖.๓.๗.๕ ไม่แชร์ไฟล์ข้อมูลลับบนเครือข่ายเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

๒.๖.๓.๗.๖ ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส และติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ

**๓. การควบคุมการเข้าถึงห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย (Server Room Control)**

๓.๑ การปฏิบัติสำหรับผู้ดูแลระบบและเจ้าหน้าที่ มีดังนี้

๓.๑.๑ ผู้ดูแลระบบต้องตรวจสอบดูแลบุคคลที่มาติดต่อและขออนุญาตเข้ามาภายในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายอย่างตลอดเวลาที่ปฏิบัติงานเคร่งครัด

๓.๑.๒ ผู้ดูแลระบบ ต้องจัดทำทะเบียนผู้สิทธิเข้า-ออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย และกำหนดสิทธิในการเข้า-ออก ห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายเท่านั้น

๓.๑.๓ เจ้าหน้าที่ทุกคนต้องทำบัตรผ่านเพื่อใช้ในการเข้า-ออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑.๔ เจ้าหน้าที่ต้องตรวจสอบอุปกรณ์ที่ผู้ติดต่อนำเข้า-ออกทุกครั้ง

๓.๑.๕ ต้องให้บุคคลที่ผ่านเข้า-ออกลงบันทึกตามแบบฟอร์ม “บันทึกการเข้า-ออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย”

๓.๒ การปฏิบัติสำหรับบุคคลภายนอก มีดังนี้

๓.๒.๑ ผู้ติดต่อจากภายนอกต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารเทศเท่านั้น จึงมีสิทธิในการเข้า-ออกห้องปฏิบัติการเครื่องแม่ข่าย

๓.๒.๒ กรณีที่นำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่ายต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศ

๓.๒.๓ ผู้ติดต่อจากภายนอกต้องลงบันทึกใน บันทึกการเข้า-ออก ห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย ให้ถูกต้องชัดเจน

**๔. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)**

๔.๑ การควบคุมการติดตั้งซอฟต์แวร์

๔.๑.๑ การติดตั้งหรือปรับปรุงซอฟต์แวร์ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศทุกครั้ง และมีผู้ดูแลระบบดูแลตลอดการดำเนินการ

๔.๑.๒ มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศเพื่อป้องกันความเสียหายหรือการหยุดชะงัก

๔.๑.๓ มีการแจ้งให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบ หากจำเป็นต้องปิดระบบสารสนเทศหรือเครื่องคอมพิวเตอร์แม่ข่ายเพื่อปรับปรุง

๔.๑.๔ ต้องทำการทดสอบการทำงานของระบบสารสนเทศหรือซอฟต์แวร์อย่างเพียงพอและรัดกุม รวมทั้งทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งลงบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๔.๒ การพัฒนาระบบสารสนเทศโดยผู้รับจ้างภายนอก

๔.๒.๑ มีการควบคุมโครงการพัฒนาระบบสารสนเทศโดยผู้รับจ้างภายนอก

๔.๒.๒ ต้องระบุผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาระบบสารสนเทศโดยผู้รับจ้างภายนอก

๔.๒.๓ ต้องตรวจสอบโปรแกรมชุดคำสั่งไม่พึงประสงค์ในซอฟต์แวร์ต่างๆ ก่อนทำการติดตั้งในเครื่องคอมพิวเตอร์แม่ข่าย

๔.๓ การควบคุมช่องโหว่ทางเทคนิค

๔.๓.๑ ผู้ดูแลระบบต้องปรับปรุงโปรแกรมจัดการช่องโหว่ต่างๆ (Patch) อย่างสม่ำเสมอ

๔.๓.๒ ต้องมีการควบคุมพอร์ตที่ใช้ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างรอบคอบและรัดกุม โดยเปิดเฉพาะพอร์ตที่จำเป็นต้องใช้เท่านั้น

๔.๔ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) จัดให้มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

๔.๔.๑ ข้อมูลชื่อบัญชีผู้ใช้

๔.๔.๒ ข้อมูลวันเวลาที่เข้าถึงระบบ

๔.๔.๓ ข้อมูลวันเวลาที่ออกจากระบบ

๔.๔.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๔.๔.๕ ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

๔.๔.๖ ข้อมูลการพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

๔.๔.๗ ข้อมูลการเปลี่ยนค่าระบบ (Configuration)

๔.๔.๘ ข้อมูลการใช้งานแอพพลิเคชัน

๔.๔.๙ ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์

๔.๔.๑๐ ข้อมูลหมายเลขอุปกรณ์ (IP Address)

๔.๔.๑๑ ข้อมูลโปรโตคอลที่ใช้งาน

**๕. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)**

๕.๑ การใช้งานบริการเครือข่าย

๕.๑.๑ กำหนดให้ผู้ใช้งานสามารถเข้าถึงได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น

๕.๑.๒ การใช้งานระบบเครือข่ายอินเตอร์เน็ต

๕.๑.๒.๑ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเตอร์เน็ต เพื่อหาประโยชน์ทางธุรกิจส่วนตัว หรือกระทำการใดๆ ที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน

๕.๑.๒.๒ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่ไม่ใช่ของตน โดยไม่ได้รับอนุญาต รวมถึงการเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น

๕.๑.๒.๓ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานและรหัสผ่านเป็นการเฉพาะบุคคลเท่านั้น จะโอนหรือจ่ายแจกสิทธิให้ผู้อื่นไม่ได้ และผู้ใช้งานต้องรับผิดชอบผลต่างๆ อันอาจจะเกิดขึ้นรวมถึงผลเสียต่างๆ ที่เกิดจากบัญชีผู้ใช้งานนั้นๆ เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของบุคคลอื่น

๕.๑.๒.๔ ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

๕.๑.๓ การใช้งานระบบเครือข่ายไร้สาย

๕.๑.๓.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร ต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๕.๑.๓.๒ ผู้ดูแลระบบจัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์ทุกตัวที่เชื่อมต่อกับระบบเครือข่ายไร้สาย ประกอบไปด้วย ชื่อผู้ใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์หรืออุปกรณ์ IP Address MAC Address สถานที่ติดต่อ เบอร์โทรศัพท์ติดต่อ

๕.๑.๓.๓ ผู้ดูแลระบบต้องเปลี่ยนค่ารหัสผู้ใช้และรหัสผ่านในการเข้าตั้งค่าการทำงานของอุปกรณ์ไร้สายที่ติดตั้งมาจากผู้ผลิต เพื่อป้องกันการโจมตี

๕.๑.๓.๔ ต้องใช้การเข้ารหัสข้อมูลระบบเครือข่ายไร้สาย เพื่อให้ข้อมูลมีความปลอดภัย

๕.๑.๓.๕ มีการใช้ MAC Address ตามที่กำหนดไว้ในการตรวจสอบอุปกรณ์ที่มีสิทธิเข้าถึงระบบเครือข่ายไร้สาย และใช้รหัสผู้ใช้และรหัสผ่านเพื่อยืนยันตัวบุคคลในการใช้งาน

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร

๕.๒.๑ ผู้ใช้งานต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

๕.๒.๒ มีการตรวจสอบผู้ใช้งานก่อนทุกครั้งในการอนุญาตให้เข้าถึงระบบสารสนเทศ โดยมีการยืนยันตัวบุคคลว่าเป็นผู้ใช้งานจริงด้วยรหัสผ่าน

๕.๒.๓ การเข้าสู่ระบบสารสนเทศขององค์กรผ่านอินเตอร์เน็ต ต้องได้รับอนุญาตจากศูนย์สารสนเทศ

๕.๒.๔ การใช้งานระบบสารสนเทศขององค์กรผ่านอินเตอร์เน็ต ต้องมีการเข้ารหัสที่เป็นมาตรฐานสากลเพื่อความมั่นคงปลอดภัย เช่น VPN หรือ SSL เป็นต้น

๕.๓ การระบุอุปกรณ์บนระบบเครือข่าย

๕.๓.๑ ผู้ดูแลระบบจัดทำบัญชีของเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่เชื่อมต่อกับเครือข่าย ประกอบไปด้วย ชื่อผู้ใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์หรืออุปกรณ์ IP Address MAC Address สถานที่ติดตั้ง เบอร์โทรศัพท์ติดต่อ

๕.๓.๒ การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายจะต้องได้รับการอนุมัติจากผู้บังคับบัญชาและได้รับความเห็นชอบจากศูนย์สารสนเทศก่อนติดตั้ง

๕.๓.๓ มีการใช้ไฟร์วอลล์กำหนดหมายเลขอุปกรณ์ (IP Address) ในการเข้าถึงเครือข่ายขององค์กร กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องระบุหมายเลขอุปกรณ์ว่าสามารถเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๕.๔.๑ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่าย ในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงค่าระบบโดยบุคคลที่ไม่มีสิทธิ

๕.๔.๒ ต้องมีการป้องกัน IP Address ภายในระบบเครือข่ายขององค์กรจากการมองเห็นจากภายนอก เพื่อป้องกันไม่ให้ภายนอกรู้ถึงโครงสร้างระบบเครือข่ายภายใน

๕.๔.๓ การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ซึ่งเป็นช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัย ต้องได้รับอนุมัติสิทธิจากผู้อำนวยการศูนย์สารสนเทศทุกครั้ง มีการควบคุมอย่างเข้มงวดโดยระบุหมายเลขอุปกรณ์ที่ใช้ในการเข้าระบบ และเมื่อเลิกใช้งานแล้วต้องยกเลิกสิทธิดังกล่าวทันที

๕.๔.๔ การเปิดพอร์ตใดๆ ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่เปิดพอร์ตทิ้งไว้โดยไม่จำเป็น

๕.๔.๕ ต้องมีการควบคุมพอร์ตที่ใช้ในการเข้าสู่ระบบเครือข่ายอย่างรอบคอบและรัดกุมอย่างสม่ำเสมอ

๕.๕ การแบ่งแยกเครือข่าย

๕.๕.๑ มีการแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย (VLAN) ตามอาคารต่างๆ เพื่อความสะดวกในการควบคุมและบริหารจัดการ

๕.๕.๒ มีการแบ่งแยกเครือข่ายภายใน เครือข่ายภายนอก และ Demilitarized Zone เพื่อความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย

๕.๖.๑ ระบบเครือข่ายทั้งหมด ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือทำ Packet Filtering เช่น Firewall หรืออุปกรณ์อื่นๆ

๕.๖.๒ ผู้ดูแลระบบ ต้องจำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

๕.๖.๓ การเข้าสู่ระบบเครือข่ายภายใน โดยผ่านอินเตอร์เน็ตต้องได้รับอนุมัติจากผู้อำนวยการศูนย์สารสนเทศก่อนทุกครั้ง และต้องมีการ Login ผ่านช่องทางที่ปลอดภัยเพื่อยืนยันพิสูจน์ตัวตน

๕.๖.๔ การเข้าสู่ระบบเครือข่ายไร้สาย ผู้ใช้งานต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์สารสนเทศ ตามความจำเป็นในการใช้งาน

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย

๕.๗.๑ กำหนดผู้รับผิดชอบในการปรับปรุง แก้ไข หรือเปลี่ยนแปลงค่าระบบต่างๆ ของระบบเครือข่ายและอุปกรณ์ที่ใช้เชื่อมต่อกับระบบเครือข่าย และมีการทบทวนค่าระบบต่างๆ อย่างสม่ำเสมอ

๕.๗.๒ ผู้ดูแลระบบต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน และจำกัดสิทธิในการใช้บริการเครือข่าย เพื่อควบคุมให้ผู้ใช้งานสามารถใช้งานได้เฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

**๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)**

๖.๑ การควบคุมการเข้าใช้งานระบบปฏิบัติการ

๖.๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๖.๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ ตามข้อ ๒.๖ “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

๖.๑.๓ ผู้ใช้งานต้องทำการล็อกหน้าจอหรือตั้ง Screen Saver เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ และเมื่อกลับมาใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๖.๑.๔ ผู้ใช้ต้องทำการ Logoff ออกจากระบบปฏิบัติการหรือปิดเครื่องทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่เครื่องเป็นเวลานาน

๖.๑.๕ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้งานรหัสผู้ใช้และรหัสผ่านของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๖.๑.๖ ซอฟต์แวร์ที่องค์กรมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความรับผิดชอบ และไม่ให้ผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากตรวจพบถือเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๖.๑.๗ ซอฟต์แวร์ที่ศูนย์สารสนเทศติดตั้งไว้ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข ก่อนได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศ

๖.๒ การระบุและยืนยันตัวบุคคลของผู้ใช้งาน (User Identification and Authentication)

๖.๒.๑ ผู้ใช้งานต้องทำการแสดงและพิสูจน์ยืนยันตัวบุคคลด้วยรหัสผู้ใช้และรหัสผ่านก่อนการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวผู้ใช้งานมีปัญหา ต้องแจ้งให้ผู้ดูแลระบบทราบและแก้ไข

๖.๒.๒ ผู้ใช้งานที่เป็นเจ้าของรหัสผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดจากการใช้งานรหัสผู้ใช้งานของระบบเทคโนโลยีสารสนเทศ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๖.๓ การบริหารจัดการรหัสผ่าน เป็นไปตามข้อ ๒. “การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน”

๖.๔ การควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

๖.๔.๑ การติดตั้งซอฟต์แวร์อื่นๆ ที่มาจากแหล่งภายนอก ต้องได้รับอนุญาตจากผู้บังคับบัญชาก่อน

๖.๔.๒ ต้องจัดเก็บโปรแกรมอรรถประโยชน์แยกจากซอฟต์แวร์สำหรับระบบงานสารสนเทศ

๖.๔.๓ มีการจำกัดผู้ได้รับอนุญาตและสิทธิการใช้งานโปรแกรมอรรถประโยชน์

๖.๔.๔ ต้องยกเลิกหรือถอดถอนโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นสำหรับผู้ใช้งาน รวมถึงต้องป้องกันไม่ใช้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมเหล่านั้นได้

๖.๔.๕ ตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสารสนเทศอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบโดยไม่ได้รับอนุญาต

๖.๔.๖ ซอฟต์แวร์ที่ติดตั้งต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกซอฟต์แวร์ต่างๆและนำไปติดตั้งหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๖.๕ การกำหนดเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน (Session Time-out)

๖.๕.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๐ นาที

๖.๕.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานการเงินและบัญชี ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖.๖ การจำกัดเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๖.๖.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานระบบสารสนเทศแต่ละครั้งไม่เกิน ๓ ชั่วโมง โดยจะต้องระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ และหากไม่มีการใช้งานนานเกิน ๑๐ นาที ต้องยกเลิกการเชื่อมต่อระบบ

๖.๖.๒ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) มีการจำกัดระยะเวลาเชื่อมต่อที่สั้นขึ้น

**๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Access Control)**

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๗.๑.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานขององค์กร ตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบงานและข้อมูลต่างๆ

๗.๑.๒ ต้องจำกัดเวลาการเชื่อมต่อระบบสารสนเทศต่างๆ และหากไม่มีการใช้งานนานเกิน ๑๐ นาที ต้องยกเลิกการเชื่อมต่อระบบ

๗.๑.๓ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ ให้เป็นไปตามข้อกำหนดการรักษาความลับข้อมูล

๗.๑.๔ มีมาตรการตรวจสอบข้อมูลที่นำออกจากระบบว่ามีความถูกต้องและสมบูรณ์ก่อนนำไปใช้งาน

๗.๑.๕ ผู้รับจ้างพัฒนาระบบต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร

๗.๑.๖ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้รับจ้างพัฒนาระบบจากภายนอกให้มีสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้รับจ้างพัฒนาระบบจากภายนอกทุกครั้ง

๗.๒ การบริหารจัดการระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร

๗.๒.๑ ต้องมีการระบุระดับความสำคัญของระบบซึ่งไวต่อการรบกวน และแยกระบบดังกล่าวไว้ในสภาพแวดล้อมของตนเองโดยเฉพาะ

๗.๒.๒ มีการสำรองและทดสอบการกู้คืนระบบ ตามข้อปฏิบัติการสำรองและกู้คืนระบบสารสนเทศ

๗.๒.๓ มีการประเมินความเสี่ยง ตามเอกสาร การบริหารจัดการความเสี่ยงด้านสารสนเทศ

๗.๒.๔ มีการควบคุมการเข้าใช้งานระบบดังกล่าว ตามข้อกำหนดการบริหารจัดการการเข้าถึงของผู้ใช้งาน

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อดูแลรักษาความปลอดภัยในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ดังนี้

๗.๓.๑ ข้อปฏิบัติทั่วไป

๗.๓.๑.๑ เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เป็นทรัพย์สินขององค์กร ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานขององค์กรเท่านั้น

๗.๓.๑.๒ โปรแกรมที่ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรมีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้ง แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๗.๓.๑.๓ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๗.๓.๑.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์และอุปกรณ์ และรักษาสภาพให้มีสภาพเดิมอยู่เสมอ

๗.๓.๑.๕ กรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาหรืออุปกรณ์สื่อสารเคลื่อนที่ ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาหรืออุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่อาจเกิดจากการกระทบกระเทือน

๗.๓.๑.๖ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ซึ่งอาจทำให้เป็นรอยขีดข่วนหรือแตกเสียหาย

๗.๓.๑.๗ การเช็ดทำความสะอาดจอภาพต้องเช็ดอย่างเบามือ และไปในทางเดียวกันห้ามหมุนวน เนื่องจากจะทำให้หน้าจอเป็นรอยขีดข่วนได้

๗.๓.๑.๘ หากมีการนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินขององค์กรมาใช้งานกับระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากศูนย์สารสนเทศก่อนการใช้งาน

๗.๓.๒ การป้องกันความปลอดภัยด้านกายภาพ

๗.๓.๒.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

๗.๓.๒.๒ ไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละออง สูง และต้องระวังป้องกันการตกกระทบ

๗.๓.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ เป็นไปตามข้อ ๔. “การควบคุมการเข้าถึงระบบปฏิบัติการ”

๗.๓.๔ การใช้รหัสผ่าน เป็นไปตาม ข้อ ๒.๖.๑ “การใช้งานรหัสผ่าน”

๗.๓.๕ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๗.๓.๕.๑ ผู้ใช้งานต้อง update ระบบปฏิบัติการ เว็บเบราเซอร์ และโปรแกรมอรรถประโยชน์ต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ในการโจมตีจากภัยคุกคามต่างๆ ที่เกิดขึ้นจากซอฟต์แวร์

๗.๓.๕.๒ ห้ามปิดหรือยกเลิกระบบป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

๗.๓.๕.๓ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดไวรัสหรือมีโปรแกรมชุดคำสั่งไม่พึงประสงค์ ห้ามเชื่อมต่อเครื่องต้องสงสัยนั้นกับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ไปยังเครื่องอื่นๆ ในเครือข่าย

๗.๓.๖ การสำรองข้อมูลและกู้คืนระบบ

๗.๓.๖.๑ ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ขององค์กร ด้วยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

๗.๓.๖.๒ ผู้ใช้งานต้องเก็บรักษาสื่อสำรองข้อมูล ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๗.๓.๖.๓ แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

๗.๓.๖.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ได้ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๗.๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๗.๔.๑ การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ซึ่งเป็นช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัย ต้องได้รับอนุมัติสิทธิจากผู้อำนวยการศูนย์สารสนเทศทุกครั้ง มีการควบคุมอย่างเข้มงวดโดยระบุหมายเลขอุปกรณ์ที่ใช้ในการเข้าระบบ และเมื่อเลิกใช้งานแล้วต้องยกเลิกสิทธิดังกล่าวทันที

๗.๔.๒ ผู้ใช้งานระบบจากระยะไกล ต้องทำการระบุและพิสูจน์ตัวตนก่อนเข้าใช้งานทุกครั้ง

๗.๔.๓ ไม่อนุญาตให้ครอบครัวหรือเพื่อนของผู้ใช้งานจากระยะไกลเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลขององค์กร

๗.๔.๔ เครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการเชื่อมต่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกล ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสหรือโปรแกรมชุดคำสั่งไม่พึงประสงค์

**๘. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)**

๘.๑ การใช้งานสำหรับผู้ใช้งาน

๘.๑.๑ ผู้ใช้งานต้องกรอกแบบฟอร์มคำขอใช้จดหมายอิเล็กทรอนิกส์ขององค์กร และยื่นคำขอกับเจ้าหน้าที่ศูนย์สารสนเทศที่ได้รับมอบหมาย เพื่อดำเนินการกำหนดชื่อบัญชีผู้ใช้งานและรหัสผ่าน

๘.๑.๒ เมื่อเข้าสู่ระบบครั้งแรก ต้องเปลี่ยนรหัสผ่านโดยทันที โดยใช้รหัสผ่านที่มีคุณภาพตามข้อ ๒.๖.๑.๗ “การกำหนดรหัสผ่านที่มีคุณภาพ”

๘.๑.๓ ไม่บันทึกหรือเก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ หรือเก็บไว้ในที่สังเกตเห็นได้

๘.๑.๔ ห้ามใช้ e-mail เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย กระทบต่อการดำเนินงานขององค์กร และรบกวนผู้ใช้งานอื่น

๘.๑.๕ ไม่ใช้ e-mail ของผู้ใช้งานอื่นเพื่ออ่าน รับส่งข้อความ ข้อมูล ยกเว้นแต่จะได้รับความยินยอมจากเจ้าของ และให้ถือว่าเจ้าของ e-mail นั้นเป็นผู้รับผิดชอบต่อการใช้งานต่างๆ จาก e-mail ของตน

๘.๑.๖ ผู้ใช้งาน e-mail ขององค์กรเพื่อติดต่องานของราชการเท่านั้น ห้ามใช้เพื่อประโยชน์ทางธุรกิจส่วนตัวหรือเป็นไปในเชิงพาณิชย์

๘.๑.๗ ผู้ใช้งานต้องตรวจสอบไฟล์แนบใน e-mail ก่อนทำการเปิดทุกครั้งโดยใช้โปรแกรมป้องกันไวรัส เพื่อป้องกันการเปิด executable file

๘.๑.๘ ผู้ใช้งานต้องลบ e-mail ที่ไม่จำเป็นต้องใช้งานออกจากระบบเพื่อรักษาเนื้อที่ในระบบตามที่ได้จำกัดไว้

๘.๑.๙ หลังใช้งานเสร็จ ต้องออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

## ส่วนที่ ๒

## นโยบายการจัดทำระบบสำรองของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

### วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย ถูกทำลาย หรือถูกเปลี่ยนแปลง จากไวรัสคอมพิวเตอร์ โปรแกรมชุดคำสั่งไม่พึงประสงค์ ผู้บุกรุกทำลาย โดยสามารถนำกู้ข้อมูลที่มีปัญหากลับมาใช้งานได้

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการสำรองข้อมูลเพื่อความมั่นคงปลอดภัยด้านสารสนเทศ

### ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

### อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

### ข้อปฏิบัติ

๑. การคัดเลือกและจัดทำระบบสำรอง
   ๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดขององค์กร และกำหนดระบบสารสนเทศที่ต้องจัดทำระบบสำรอง
   ๑.๒ กำหนดรายละเอียดของระบบสารสนเทศที่ต้องสำรองข้อมูลไว้อย่างน้อย ดังนี้
      ๑.๒.๑ ข้อมูลของระบบสารสนเทศ (Database)
      ๑.๒.๒ ข้อมูลการตั้งค่าต่างๆของระบบ (Configuration)
      ๑.๒.๓ ระบบปฏิบัติการ
      ๑.๒.๔ ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ
   ๑.๓ กำหนดขั้นตอนและความถี่ในการสำรองและการกู้คืนข้อมูลอย่างถูกต้องและชัดเจน
   ๑.๔ กำหนดรูปแบบการสำรองข้อมูลตามความเหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น Full Backup หรือ Incremental Backup
   ๑.๕ ทำการสำรองข้อมูลตามชนิด ความถี่ และรูปแบบที่ได้กำหนดไว้ และตรวจสอบว่าข้อมูลที่ได้สำรองนั้นมีความสมบูรณ์
   ๑.๖ บันทึกรายละเอียดการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วันเวลา ชื่อข้อมูลที่ทำการสำรอง และผลการดำเนินการ
   ๑.๗ จัดเก็บข้อมูลที่ได้สำรองไว้ในสถานที่ปลอดภัย มีการระบุรายละเอียดของข้อมูลที่สำรองบนสื่อเก็บข้อมูลอย่างชัดเจน
   ๑.๘ มีการเข้ารหัสข้อมูลสำหรับข้อมูลลับที่ได้สำรองเก็บไว้

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๑ มีการประเมินความเสี่ยง สำหรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและทำให้เกิดการหยุดชะงัก ตามเอกสาร “การบริหารจัดการความเสี่ยงด้านสารสนเทศ”

๒.๒ มีการจัดทำแผนบริหารความเสี่ยงเพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติตามเอกสาร “แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ (IT Contingency Plan)”

๒.๓ จัดทำแผนกู้คืนระบบเมื่อเกิดสถานการณ์ฉุกเฉิน ตามเอกสาร “แผนบริหารความต่อเนื่อง” โดยมีรายละเอียด ดังนี้

๒.๓.๑ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๓.๒ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบ

๒.๓.๓ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๒.๔ มีขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้

๒.๕ มีการสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๓. การกำหนดหน้าที่ความรับผิดชอบของบุคลากร เป็นไปตามเอกสาร “แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ” และ “แผนบริหารความต่อเนื่อง”

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑ ตรวจสอบว่าการสำรองข้อมูลนั้น สำเร็จครบถ้วน

๔.๒ ทดสอบการกู้คืนข้อมูลที่สำรองไว้ ว่าสามารถกู้คืนได้อย่างครบถ้วนและสามารถใช้งานได้ตามปกติ

๕. ระยะความถี่ของการปฏิบัติ

๕.๑ ความถี่ในการสำรองข้อมูลของระบบสารสนเทศ ขึ้นอยู่กับความสำคัญของระบบสารสนเทศ และสภาพการเปลี่ยนแปลงข้อมูล โดยระบบที่มีความสำคัญมาก หรือมีการเปลี่ยนแปลงข้อมูลบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๕.๒ ทำการทดสอบการกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง

๕.๓ มีการทบทวนและปรับปรุงการบริหารจัดการความเสี่ยงด้านสารสนเทศ แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ และ แผนบริหารความต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง

## ส่วนที่ ๓

## นโยบายการตรวจสอบและประเมินความเสี่ยง

### วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศขององค์กร เพื่อให้มั่นใจว่านโยบายและมาตรฐานต่างๆ ด้านความมั่นคงปลอดภัยสารสนเทศได้มีการปฏิบัติตามอย่างมีประสิทธิผล

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

### ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ
๒. ผู้ตรวจสอบภายใน
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

### อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

### ข้อปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๒. ตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายในขององค์กร เพื่อให้ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๓. การประเมินความเสี่ยงด้านสารสนเทศเป็นไปตามเอกสาร “การบริหารจัดการความเสี่ยงด้านสารสนเทศ”

๔. การตรวจสอบและประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยครอบคลุมหัวข้อต่อไปนี้

๔.๑ การบริหารจัดการสินทรัพย์ ตรวจสอบบัญชีรายการสินทรัพย์และสภาพการพร้อมใช้งาน

๔.๒ การควบคุมการเข้าถึงและการใช้งานสารสนเทศ ตรวจสอบว่ามีความเหมาะสมเพียงพอเป็นไปตามแนวปฏิบัติที่กำหนดไว้ เพื่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๔.๓ การสำรองและกู้คืนข้อมูล ตรวจสอบข้อมูลที่ได้มีการสำรองและมีการทดสอบการกู้คืน

๔.๔ การพัฒนา จัดซื้อจัดหาระบบเทคโนโลยีสารสนเทศ เพื่อตรวจสอบการจัดหาระบบเทคโนโลยีสารสนเทศเป็นไปตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการพัสดุ พ.ศ. ๒๕๓๕ และฉบับแก้ไขเพิ่มเติม

๔.๕ การเตรียมความพร้อมรับมือกับสถานการณ์ฉุกเฉิน ตรวจสอบการซ้อมรับสถานการณ์ต่างๆ ตามเอกสาร “แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ (IT Contingency Plan)”

๕. เครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัย ที่จำเป็นต้องใช้ ต้องได้รับการปกป้องจากการลักลอบใช้งานโดยไม่ได้รับอนุญาตหรือใช้ในทางที่ผิดวัตถุประสงค์ รวมถึงมีการควบคุมจำกัดการเข้าถึงข้อมูลเฉพาะผู้ที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

๖. เมื่อดำเนินการตรวจสอบและประเมินการรักษาความความมั่นคงปลอดภัยแล้ว ต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงขององค์กรทราบ พร้อมทั้งเสนอแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าการรักษาความมั่นคงปลอดภัยด้านสารสนเทศยังมีจุดบกพร่อง

## ส่วนที่ ๔

## นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

### วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้บุคลากรขององค์กร ได้รับทราบ เข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้องเหมาะสม

### ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ
๒. ส่วนฝึกอบรม สำนักบริหารงานกลาง
๓. หน่วยงานที่ได้รับมอบหมายในการฝึกอบรม
๔. ผู้ดูแลระบบที่ได้รับมอบหมาย
๕. เจ้าหน้าที่ที่ได้รับมอบหมาย

### อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

### ข้อปฏิบัติ

๑. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมขององค์กร

๒. เผยแพร่ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย และมีการเปลี่ยนเกร็ดความรู้อยู่เสมอ ผ่านทางการติดประกาศประชาสัมพันธ์ แผ่นพับ และผ่านเว็บไซต์ขององค์กร

๓. จัดทำคู่มือการใช้ระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย และให้มีการเผยแพร่ทางหนังสือเวียนและทางเว็บไซต์ขององค์กร

๔. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน