# นโยบายและแนวปฏิบัติ
## ในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ พ.ศ. 2567

**จัดทำโดย**

กองสื่อสารและสารสนเทศ
สำนักงานสภาเกษตรกรแห่งชาติ

# คำนำ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำเนินงานตามภารกิจของภาครัฐมากขึ้น ทั้งในด้านการบริหาร การตัดสินใจ รวมถึงการกำหนดนโยบายในการขับเคลื่อนพัฒนาประเทศ ประกอบกับการยกระดับภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัล ทำให้หน่วยงานของรัฐต้องปรับตัวและปรับเปลี่ยนกระบวนการคิดการทำงาน ผ่านการใช้เทคโนโลยีสารสนเทศ โดยการสร้างโครงสร้างพื้นฐานด้านดิจิทัลและบูรณาการข้อมูลร่วมกันทั้งภาครัฐและเอกชน เพื่ออำนวยความสะดวกแก่ประชาชน ให้สามารถใช้บริการได้รวดเร็ว มีประสิทธิภาพ โปร่งใสและตรวจสอบได้

ในขณะเดียวกัน การนำเอาเทคโนโลยีสารสนเทศมาใช้กันอย่างแพร่หลาย อาจทำให้เกิดความเสี่ยงจากภัยคุกคามทางไซเบอร์มากขึ้น เช่น การบุกรุกโจมตีผ่านเครือข่ายอินเทอร์เน็ต การก่อกวนทำให้ระบบไม่สามารถใช้งานได้ รวมถึงการขโมยข้อมูลที่เป็นทรัพย์สินหรือความลับทางราชการ ส่งผลต่อความน่าเชื่อถือขององค์กร ซึ่งปัญหาดังกล่าวอาจเกิดจากช่องโหว่ของระบบสารสนเทศ การขาดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจนและการนำมาตรการไปปฏิบัติใช้อย่างมีประสิทธิภาพ

สำนักงานสภาเกษตรกรแห่งชาติ จึงจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖ โดยกำหนดข่อปฏิบัติ มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด รวมถึงให้ผู้ใช้งาน ผู้ดูแลระบบและผู้เกี่ยวข้องกับระบบสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาติ ได้ตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติตามมาตรการที่กำหนด เพื่อให้การดำเนินงานขององค์กรมีมาตรฐาน น่าเชื่อถือ และมีความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศต่อไป

**กองสื่อสารและสารสนเทศ**
**สำนักงานสภาเกษตรกรแห่งชาติ**

# สารบัญ


**บทนำ** 1
1. หลักการและเหตุผล 1
2. วัตถุประสงค์ 1
3. องค์ประกอบของนโยบาย 1
4. การเผยแพร่และทบทวน 2
**คำนิยาม** 3
**โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ** 6
**นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** 7
**หมวด 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ** 7
ส่วนที่ 1 การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) 7
ส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) 9
ส่วนที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) 11
ส่วนที่ 4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control) 14
ส่วนที่ 5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) 17
ส่วนที่ 6 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) 19
ส่วนที่ 7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan Access Control) 21
ส่วนที่ 8 การควบคุมการใช้อินเทอร์เน็ต (Internet) 22
ส่วนที่ 9 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) 23
ส่วนที่ 10 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook) 24
ส่วนที่ 11 การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) 25
ส่วนที่ 12 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) 28
ส่วนที่ 13 การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) 30
ส่วนที่ 14 การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) 32
**หมวด 2 นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล** 34
ส่วนที่ 1 การสำรองข้อมูล (back up) 34
ส่วนที่ 2 การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan) 35
**หมวด 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ** 36
**หมวด 4 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** 37

# บทนำ

**๑. หลักการและเหตุผล**

ตามมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกสกับหนวยงานของรัฐ หรือโดยหนวยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได ตลอดจนมีมาตรฐานเปนที่ยอมรับในระดับสากล

สำนักงานสภาเกษตรกรแห่งชาติ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมายข้างต้น เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในหน่วยงาน และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด สามารถบรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

**๒. วัตถุประสงค์**

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อให้องค์กรมีการกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และกำหนดผู้รับผิดชอบ

๒.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้แก่ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

**๓. องค์ประกอบของนโยบาย**

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาติ อ้างอิงตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖ โดยมีรายละเอียด ดังนี้

- หมวด ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ ประกอบด้วย
  - ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)
  - ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
  - ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
  - ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
  - ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)
ส่วนที่ ๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan Access Control)
ส่วนที่ ๘ การควบคุมการใช้อินเทอร์เน็ต (Internet)
ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)
ส่วนที่ ๑๐ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)
ส่วนที่ ๑๑ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)
ส่วนที่ ๑๒ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
ส่วนที่ ๑๓ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)
ส่วนที่ ๑๔ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

- หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล ประกอบด้วย
  ส่วนที่ ๑ การสำรองข้อมูล (back up)
  ส่วนที่ ๒ การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)
- หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
- หมวด ๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

**๔. การเผยแพร่และทบทวน**

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาติฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยนำออกเผยแพร่ด้วยวิธีการประกาศแจ้งเวียน และนำขึ้นเว็บไซต์ของสำนักงานสภาเกษตรกรแห่งชาติ เพื่อให้บุคลากรของ สกช. และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามแนวนโยบายนี้อย่างเคร่งครัด

# คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **องค์กร** หมายถึง สำนักงานสภาเกษตรกรแห่งชาติ (สกช.)
- **ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)** หมายถึง เลขาธิการสภาเกษตรกรแห่งชาติ
- **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (Ministry Chief Information Officer: MCIO)** หมายถึง รองเลขาธิการสภาเกษตรกรแห่งชาติ ที่ได้รับแต่งตั้งให้ทำหน้าที่และรับผิดชอบในการกำกับดูแล การดำเนินงานด้านเทคโนโลยีสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาติ
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- **ผู้อำนวยการกองสื่อสารและสารสนเทศ** หมายถึง ผู้ที่ได้รับแต่งตั้งให้ทำหน้าที่และรับผิดชอบในการกำกับดูแลกองสื่อสารและสารสนเทศ
- **กองสื่อสารและสารสนเทศ** หมายถึง กองที่ทำหน้าที่วางแผน อำนวยการ ประสานงาน กำกับการและดำเนินการในเรื่องเทคโนโลยีสารสนเทศ และการสื่อสารข้อมูลการรักษาความปลอดภัยทางระบบสารสนเทศ และการสื่อสารข้อมูลให้เป็นไปตามระเบียบปฏิบัติ คำสั่ง และคำชี้แจงของผู้บังคับบัญชา รวมทั้งการจัดทำระเบียบปฏิบัติ คำสั่ง คำแนะนำ ตลอดจนเอกสารที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และการสื่อสาร
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์กร
- **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ ดังนี้
  - ผู้บริหาร หมายถึง เลขาธิการ รองเลขาธิการ ผู้ตรวจการประจำภาค ผู้อำนวยการกองฯ หัวหน้าสำนักงานสภาเกษตรกรจังหวัด
  - ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
  - เจ้าหน้าที่ หมายถึง พนักงาน ลูกจ้าง เจ้าหน้าที่ประจำโครงการ จ้างเหมาเอกชนที่ได้รับมอบหมาย
- **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอก ที่ สกช. อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
- **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น
  - ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
  - ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของหน่วยงาน ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
- **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น
  - พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  - พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
  - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)
  - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
  - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพ

กราฟฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน มาตรฐานที่ใช้ในการรับ - ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP๓ และ IMAP เป็นต้น

- **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการควบคุมการเข้าถึงการใช้งานสารสนเทศสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย
- **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non - Repudiation) และความน่าเชื่อถือ (Reliability)
- **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

# โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ

**วัตถุประสงค์**

เพื่อบริหารจัดการ ปกป้องสินทรัพย์ขององค์กรในด้านสารสนเทศให้มีความมั่นคงปลอดภัย โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย ในการกำหนดนโยบาย ตรวจสอบการทำงานประเมินความเสี่ยง รวมทั้งประสานงานกับหน่วยงานภายนอกหรือผู้ใช้งานสารสนเทศจากภายนอก โดยมีการกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุด (CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (MCIO) ผู้อำนวยการกองสื่อสารและสารสนเทศ ผู้ดูแลระบบที่ได้รับมอบหมาย และผู้ใช้งาน

**ส่วนที่ ๑ ระดับนโยบาย**

๑.๑ ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) ของสำนักงานสภาเกษตรกรแห่งชาติ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (Ministry Chief Information Officer: MCIO) สำนักงานสภาเกษตรกรแห่งชาติ เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแลและควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ ผู้อำนวยการกองสื่อสารและสารสนเทศ สำนักงานสภาเกษตรกรแห่งชาติ เป็นผู้รับผิดชอบในการกำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา จัดทำ ทบทวน วางแผน กำกับดูแล ติดตามการบริหารความเสี่ยง ระบบสารสนเทศ และแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

อนึ่ง หากเกิดความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ ของ สกช. ให้เลขาธิการสภาเกษตรกรแห่งชาติ แต่งตั้งคณะกรรมการ เพื่อการตรวจหาข้อเท็จจริงและดำเนินการตามกฎหมาย ข้อบังคับ ระเบียบที่เกี่ยวข้องต่อไป

**ส่วนที่ ๒ ระดับปฏิบัติงาน**

๒.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบดังนี้

๒.๑.๑ ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศ ให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ ประสานการปฏิบัติงานตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๑.๓ ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ

๒.๑.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery)

๒.๑.๕ ป้องกันและแก้ไขปัญหาการถูกโจมตีหรือการเจาะระบบเครือข่าย ระบบสารสนเทศจากผู้ไม่ประสงค์ดี (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๖ ปฏิบัติงานอื่นตามที่ได้รับมอบหมาย ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๒ ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด

# นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

## หมวด ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

### ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

**วัตถุประสงค์**

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้ไม่ประสงค์ดีหรือโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก พร้อมทั้งตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ผู้ใช้งาน

**แนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ**

๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผล

๑.๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึง อย่างน้อยปีละ ๑ ครั้ง

๑.๓ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศ จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสื่อสารและสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒ การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

การแบ่งประเภทและการจัดลำดับชั้นความลับของข้อมูล จะอ้างอิงจากระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๒.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น
- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินบัญชี ข้อมูลการประเมินผลตามตัวชี้วัด เป็นต้น
- ข้อมูลสารสนเทศด้านการให้บริการ เช่น ข้อเสนอเชิงนโยบายด้านการเกษตร ข้อมูลทะเบียนองค์กรเกษตรกร ปัญหาและความต้องการของเกษตรกรและองค์กรเกษตรกร ข่าวประชาสัมพันธ์ การฝึกอบรม สัมมนา ข้อมูลบันทึกความร่วมมือ เป็นต้น

๒.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ ดังนี้
- ระดับที่ ๑ ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ระดับที่ ๒ ข้อมูลที่มีระดับความสำคัญปานกลาง
- ระดับที่ ๓ ข้อมูลที่มีระดับความสำคัญน้อย

๒.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล ดังนี้
- "ข้อมูลลับที่สุด" หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- "ข้อมูลลับมาก" หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- "ข้อมูลลับ" หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- "ข้อมูลทั่วไป" หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๔ การจัดแบ่งระดับชั้นการเข้าถึง
- ระดับที่ ๑ ระดับชั้นสำหรับผู้บริหารระดับสูง
- ระดับที่ ๒ ระดับชั้นสำหรับผู้ใช้งาน
- ระดับที่ ๓ ระดับชั้นสำหรับผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๕ การกำหนดเวลาในการเข้าถึงข้อมูล
การเข้าถึงข้อมูลระบบสารสนเทศของ สกช. สามารถเข้าถึงได้ทุกวันตลอด ๒๔ ชั่วโมง

**แนวปฏิบัติการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ**

๓ การควบคุมการเข้าถึงระบบสารสนเทศ

๓.๑ ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศ

๓.๒ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๔ จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภารกิจดังนี้

๔.๑ ผู้บริหารระดับสูง

๔.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๓ ผู้ใช้งาน

## ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

**วัตถุประสงค์**

เพื่อบริหารจัดการการเข้าถึงระบบสารสนเทศ และมั่นใจได้ว่าเฉพาะผู้ที่ได้รับสิทธิการเข้าถึงระบบสารสนเทศตามที่กำหนดเท่านั้น สามารถเข้าใช้งานระบบสารสนเทศได้

**ผู้รับผิดชอบ**

๑. หน่วยงานภายใน สกช.
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

**แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน**

๑ การสร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน
- ๑.๑ จัดให้มีการอบรมเพื่อสร้างความรู้ และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคาม และผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง
- ๑.๒ กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศ

๒ การลงทะเบียนผู้ใช้งาน (User Registration)
- ๒.๑ ผู้ดูแลระบบ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับใช้ระบบสารสนเทศ
- ๒.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน
- ๒.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิ
- ๒.๔ ผู้ดูแลระบบต้องชี้แจง และแจ้งผู้ใช้งาน เพื่อให้ผู้ใช้งานทราบถึงสิทธิ หน้าที่รับผิดชอบและมาตรการด้านความมั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศ
- ๒.๕ กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากต้นสังกัด หรือเมื่อมีการลาออก เปลี่ยนแปลงตำแหน่ง โยกย้าย หรือสิ้นสุดการจ้าง

๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)
- ๓.๑ กำหนดระดับสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบ ความจำเป็นในการใช้งาน และทบทวนสิทธิสม่ำเสมอ
- ๓.๒ ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการมอบสิทธิให้แก่ผู้ใช้งาน
- ๓.๓ ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสื่อสารและสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย โดยการให้สิทธิพิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษ จะต้องระงับการใช้งานทันที

๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๔.๑ ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน ส่งมอบให้ผู้ใช้งานเป็นความลับ เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันที

๔.๒ การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้องประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษ อย่างน้อย ๘ หลัก (digits)

๔.๓ กำหนดให้การเข้ารหัสผิดได้ไม่เกิน ๕ ครั้ง กรณีบัญชีผู้ใช้งานไม่สามารถเข้าใช้งานได้เนื่องจากเข้ารหัสผิดเกินจำนวนครั้งที่กำหนดให้ติดต่อผู้ดูแลระบบ และแจ้งความประสงค์ขอตั้งรหัสผ่านใหม่

๔.๔ ให้ผู้ใช้งานเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับแจ้งจากผู้ดูแลระบบทันทีที่เข้าใช้งานเป็นครั้งแรก และต้องเก็บและรักษารหัสผ่านที่ได้รับเป็นความลับ ไม่เปิดเผยต่อผู้อื่น

๔.๕ ไม่ควรจดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือบันทึกไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำ

๔.๖ หากมีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ และหลังจากดำเนินการเรียบร้อยแล้วให้ทำการเปลี่ยนรหัสผ่านทันที

๔.๗ ผู้ใช้งานที่มีสิทธิตามบัญชีผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้ของตนเพื่อเข้าใช้ระบบสารสนเทศ และระบบเครือข่าย และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากบัญชีผู้ใช้งานของตน

๔.๘ กลุ่มผู้ใช้งานที่มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านเดียวกันจะต้องร่วมกันรับผิดชอบหากมีความเสียหาย หรือมีปัญหาเกิดขึ้นกับระบบที่เข้าถึง

๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตจากผู้ที่ไม่สิทธิการเข้าถึง โดยมีแนวปฏิบัติ ดังนี้

๕.๑ จัดทำรายชื่อของผู้ที่ยังมีสิทธิในระบบ พร้อมรายละเอียดสิทธิที่ได้รับของแต่ละบุคคล และจัดส่งรายชื่อนั้นให้กับผู้อำนวยการกองสื่อสารและสารสนเทศ เพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งาน

๕.๒ ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ เปลี่ยนแปลงสิทธิการใช้งานของผู้ใช้งานให้เหมาะสม หรือหากผู้ใช้งานถูกเพิกถอนการอนุญาต ย้าย หรือลาออก ผู้ดูแลระบบต้องถอดถอนสิทธิของผู้ใช้งานนั้นออกจากระบบทันทีที่ได้รับแจ้งจากเจ้าของข้อมูล หรือกองการเจ้าหน้าที่

## ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

**วัตถุประสงค์**

เพื่อกำหนดมาตรการในการใช้งานระบบสารสนเทศและอุปกรณ์ประมวลผลด้านสารสนเทศอย่างเหมาะสมและมีความมั่นคงปลอดภัย

**ผู้รับผิดชอบ**

๑. หน่วยงานภายใน สกช.

๒. ผู้ใช้งาน

**แนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน**

๑ การใช้งานรหัสผ่าน (Password Use)

๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๑.๒ การตั้งรหัสผ่านจะต้องตั้งรหัสให้มีความยากต่อการคาดเดา โดยรหัสผ่านต้องประกอบด้วยตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษ อย่างน้อย ๘ หลัก (Digits)

๑.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ (Save Password)

๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน มีแนวปฏิบัติเพื่อป้องกันผู้ไม่มีสิทธิเข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแล ดังนี้

๒.๑ มีการกำหนดมาตรการป้องกันสินทรัพย์ของ สกช. และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ได้แก่ การจัดการบริเวณล้อมรอบ การควบคุมการเข้าออก การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย

๒.๒ ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน รวมถึงสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

๒.๓ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยการรับ-ส่งข้อมูลสำคัญ หรือ ข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล VPN หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอก

๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) เพื่อไม่ให้อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ รวมถึงกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อไม่มีการใช้งาน โดยมีแนวปฏิบัติ ดังนี้

๓.๑ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๓.๒ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอ เมื่อไม่ใช้งานเกิน ๑๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถใช้งานเครื่องคอมพิวเตอร์ได้

๓.๓ ผู้ใช้งานต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๓.๔ กรณีข้อมูลสำคัญที่บันทึกไว้ในกระดาษ สื่อบันทึกข้อมูล แฟลชไดร์ฟหรือฮาร์ดดิสก์เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๓.๕ การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

| ลำดับ | ประเภทสื่อบันทึกข้อมูล | แนวทางการทำลาย |
|---|---|---|
| ๑ | ฮาร์ดดิสก์ (Hard disk)<br>ฮาร์ดดิสก์ภายนอก (External Hard disk)<br>แฟลชไดรฟ์ (Flash Drive) | ๑. ทำลายข้อมูลตามแนวทางของ DoD ๕๒๒๐.๒๒-M ของกระทรวงกลาโหม USA ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลาย ๆ รอบ<br>๒. ทุบทำลาย หรือบดให้อุปกรณ์เสียหาย ให้ไม่สามารถนำไปใช้ได้ |
| ๒ | แผ่นซีดี/ดีวีดี (CD/DVD) | ใช้วิธีการตัด เผา ทำให้สิ้นสภาพการใช้งาน |
| ๓ | เทป | ใช้วิธีทุบ ทำลายให้เสียหาย |
| ๔ | กระดาษ | ตัดด้วยเครื่องทำลายเอกสาร |

๔ การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

๔.๑ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๔.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน หรือเกิดจากความผิดพลาดใด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๔.๓ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของ สกช. หรือเป็นของบุคคลภายนอก

๔.๔ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแล ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ โอนย้าย หรือทำลาย โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

๔.๕ กรณีข้อมูลส่วนบุคคลที่ สกช. ได้แจ้งวัตถุประสงค์ในการประมวลผลข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลและได้รับความยินยอมแล้ว ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษาใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ สกช. ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับ สกช. ซึ่งอาจแต่งตั้งให้มีผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งาน/เจ้าของข้อมูลส่วนบุคคลทราบ

๔.๖ ห้ามเปิดหรือใช้งานโปรแกรมประเภทการรับส่งข้อมูลภายในเครือข่าย (peer-to-peer) หรือโปรแกรมดาวน์โหลดไฟล์ที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (bitTorrent) อีมูล (eMule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการกองสื่อสารและสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๗ ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิง ในเวลาราชการ

๔.๘ ห้ามใช้สินทรัพย์ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจ

๔.๙ ห้ามใช้ระบบสารสนเทศ เพื่อรบกวนก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจ

๔.๑๐ ห้ามใช้ระบบสารสนเทศเพื่อประโยชน์ทางการค้า

๔.๑๑ ห้ามกระทำการใด ๆ เพื่อการดักจับข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๔.๑๒ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

## ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

**วัตถุประสงค์**

เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาตและควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน ให้มีความมั่นคงปลอดภัย

**ผู้รับผิดชอบ**

๑. หน่วยงานภายใน สกช.
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

**แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย**

๑ การใช้งานบริการเครือข่าย

๑.๑ กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๑.๒ กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศที่ได้รับสิทธิให้เข้าถึงเท่านั้น

๑.๓ กำหนดการใช้งานระบบสารสนเทศของ สกช. โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสื่อสารและสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก (User Authentication for External Connections)

๒.๑ เมื่อผู้ใช้งานที่อยู่ภายนอกและต้องเข้าใช้งานระบบสารสนเทศต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

๒.๒ มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

๒.๓ กรณีบุคคลภายนอกต้องการเข้าสู่ระบบสารสนเทศของ สกช. จากอินเทอร์เน็ตจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสื่อสารและสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

๓.๑ จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่าย โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย ยี่ห้อเครื่องคอมพิวเตอร์ รุ่น หมายเลขเครือข่าย (IP Address) หมายเลขเฉพาะของอุปกรณ์ที่เชื่อมต่อเครือข่าย (Mac Address) สถานที่ติดตั้ง ผู้ใช้งาน

๓.๒ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๓ ต้องใช้อุปกรณ์ป้องกันเครือข่าย (Firewall) ในการกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายได้

๓.๔ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่าย การเชื่อมต่อภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๓.๕ แผนผังระบบเครือข่ายเป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่และทบทวนแผนผังระบบเครือข่าย (Network Diagram) การเชื่อมต่ออุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๔ การป้องกันช่องทางที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

๔.๑ การเข้าถึงช่องทาง (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น

๔.๒ มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

๔.๓ ปิดการใช้งานหรือควบคุมการเข้าถึงช่องทาง (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น

๔.๔ ติดตั้งและตั้งค่าการทำงานของอุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) เพื่อความปลอดภัย

๕ การแบ่งแยกเครือข่าย (Segregation in Networks) กำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้

๕.๑ แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยตามการใช้งาน เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๕.๒ แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๖.๑ จำกัดสิทธิให้กับผู้ดูแลระบบที่ได้รับมอบหมาย มีสิทธิในการเข้าถึงและเชื่อมต่อเข้าสู่ระบบเครือข่าย

๖.๒ ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System)

๖.๓ การเข้าสู่ระบบเครือข่ายขององค์กรต้องเข้าสู่ระบบผ่านช่องทางที่กำหนดไว้เท่านั้น

๖.๔ ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๖.๕ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย

๖.๖ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

(๑) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของ สกช. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) และมีระบบตรวจจับโปรแกรมประสงค์ร้าย (Malware)

(๕) ทบทวนการตั้งค่า (Configuration) ต่าง ๆ ของอุปกรณ์ระบบเครือข่าย เช่น กฎการเข้าถึง (Policy) ช่องทาง (Port) อย่างน้อยปีละ ๑ ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่าการตั้งค่า (Configuration) ต่าง ๆ ต้องแจ้งผู้ดูแลระบบที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๖) หมายเลขเครือข่าย (IP Address) ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

(๗) การใช้งานอุปกรณ์และซอฟต์แวร์หรือเครื่องมือต่าง ๆ (tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบที่ได้รับมอบหมายและจำกัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น

๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ซึ่งมีแนวปฏิบัติในการจัดเส้นทางบนเครือข่าย ดังนี้

๗.๑ ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ โดยกำหนดตารางของการใช้เส้นทางบนระบบเครือข่ายบนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์ป้องกันการบุกรุก (Firewall) หรืออุปกรณ์กระจายสัญญาณข้อมูล (Switch)

๗.๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย (Network Address Translation) เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก และการแปลงชื่อระบบสารสนเทศ (Domain Name Server) เป็นหมายเลขเครือข่าย (IP Address) เพื่อให้ผู้ใช้งานสามารถเข้าใช้งานระบบสารสนเทศได้ง่าย

## ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

**วัตถุประสงค์**

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และควบคุมการใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมที่ใช้งานการปฏิบัติงานของผู้ใช้งาน เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด

**ผู้รับผิดชอบ**

๑. หน่วยงานภายใน สกช.
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. ผู้ใช้งาน

**แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ**

๑ ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๑.๑ กำหนดให้ระบบ ไม่ให้แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนการเข้าสู่ระบบจะเสร็จสมบูรณ์

๑.๒ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการ เช่น การใช้คำสั่ง (Command) การควบคุมทางไกล (Remote Desktop)

๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๒.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศ

๒.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นหรือสอดคล้องกับการปฏิบัติงาน โดยจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกอง หรือผู้ดูแลระบบที่ได้รับมอบหมาย และกำหนดกรอบเวลาการใช้งานที่ชัดเจน และยุติการใช้งานทันที เมื่อพบความผิดปกติหรือหมดช่วงเวลาที่ขออนุญาตไว้

๓ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

กำหนดให้มีการจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมที่ใช้ในการปฏิบัติงานของผู้ใช้งาน เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด โดยมีแนวปฏิบัติ ดังนี้

๓.๑ การใช้งานโปรแกรมอรรถประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๒ โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์การใช้งาน

๓.๓ กำหนดให้มีการตรวจสอบและถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นหรือไม่เกี่ยวข้องกับการปฏิบัติงาน

๔ การกำหนดระยะเวลายุติการใช้งานระบบสารสนเทศ (Session Time - Out)

กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากไม่มีการใช้งานช่วงระยะเวลา ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of Connection Time)

กำหนดให้การจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๑) กำหนดให้มีการจำกัดช่วงระยะเวลาการเชื่อมต่อระบบสารสนเทศ เพื่อให้มีการใช้งานภายในระยะเวลาที่กำหนด เช่น กำหนดให้ใช้งานได้เฉพาะเวลาทำการเท่านั้น

๒) กำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อที่สั้นลงสำหรับระบบสารสนเทศที่มีความสำคัญหรือหลังจากไม่มีการใช้งานช่วงระยะเวลา ๑๕ นาที เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

## ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

**วัตถุประสงค์**

เพื่อป้องกันการเข้าถึงระบบสารสนเทศหรือแอปพลิเคชัน โดยไม่ได้รับอนุญาต

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ผู้พัฒนาหรือผู้รับจ้างให้บริการภายนอก (Outsource)

**แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ**

๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน โดยการเข้าใช้งาน การเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของระบบสารสนเทศและแอปพลิเคชัน ได้กำหนดหลักเกณฑ์การจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ ดังนี้

๑.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานขององค์กร ตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศ

๑.๒ จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ และหากไม่มีการใช้งานนานเกิน ๑๕ นาที ให้ยกเลิกการเชื่อมต่อ

๑.๓ ผู้พัฒนาหรือผู้รับจ้างให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และต้องรักษาความลับไม่เปิดเผยข้อมูลขององค์กร

๑.๔ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้พัฒนาหรือผู้รับจ้างให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศ

๑.๕ ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้พัฒนาหรือผู้รับจ้างให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

๒ ระบบที่มีความสำคัญและส่งผลกระทบสูงหรือระบบซึ่งไวต่อการรบกวน

แยกระบบที่มีความสำคัญออกจากระบบอื่น และจัดให้มีการควบคุมสภาพแวดล้อมโดยเฉพาะ มีรายละเอียด ดังนี้

๒.๑ แยกระบบซึ่งไวต่อการรบกวน ออกจากระบบอื่น

๒.๒ ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

(๑) ระบบมีผลกระทบจะต้องควบคุมการเข้าถึงอุปกรณ์ โดยติดตั้งไว้ในพื้นที่ปลอดภัย

(๒) ติดตามเฝ้าระวังการใช้งานระบบ หากพบเหตุการณ์ผิดปกติและมีผลกระทบให้ระงับการใช้งานทันที

๒.๓ วางแผนการสำรองและทดสอบการกู้คืนระบบ ตามหมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ใช้ปฏิบัติงานจากภายนอก (Mobile Computing and Teleworking)

กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งเกิดจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยผู้ใช้งานต้องปฏิบัติ ดังนี้

๓.๑ การป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ครอบคลุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ได้แก่ Smartphone, Notebook, Tablet หรืออุปกรณ์อื่นใดในลักษณะเดียวกันนี้ โดยกำหนดให้มีการป้องกันการเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เข้ากับเครือข่าย โดยไม่ได้รับอนุญาต

๓.๒ กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และต้องแสดงตัวตนเมื่อเข้าใช้งาน

๔ การปฏิบัติงานจากภายนอก (Teleworking)

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอก กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัย ดังนี้

๔.๑ การปฏิบัติงานจากภายนอก (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ VPN หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอก

๔.๒ การเข้าถึงระบบสารสนเทศขององค์กรจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัว จะต้องติดตั้งโปรแกรมป้องกันไวรัส (anti-virus) ด้วย

๔.๓ การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกได้ จะต้องใช้งานด้วยความระมัดระวัง และออกจากระบบทันทีเมื่อเลิกใช้งาน

๔.๔ ไม่อนุญาตให้ปฏิบัติงานจากภายนอก สำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

๔.๕ การเข้าสู่ระบบสารสนเทศขององค์กรจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยชื่อผู้ใช้งานและรหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๔.๖ ผู้ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของ สกช. โดยไม่ให้บุคคลอื่นสามารถเข้าถึงระบบได้

๔.๗ ผู้ดูแลระบบต้องควบคุมช่องทาง (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๔.๘ ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกแก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต

๔.๙ ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกอย่างน้อยปีละ ๑ ครั้ง

## ส่วนที่ ๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan Access Control)

**วัตถุประสงค์**

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย

**แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย**

๑ เจ้าหน้าที่ของ สกช. ที่ต้องการเข้าถึงระบบเครือข่ายไร้สาย จะต้องลงทะเบียนด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ก่อนเข้าใช้งาน

๒ บุคคลภายนอกที่ต้องการเข้าถึงระบบเครือข่ายไร้สาย จะต้องลงทะเบียนและได้รับอนุญาตจากเจ้าหน้าที่ของ สกช. ที่รับผิดชอบ ซึ่งจะได้สิทธิระยะเวลาการใช้งาน ๒๔ ชั่วโมง หากต้องการใช้งานเป็นช่วงเวลาจะต้องลงทะเบียนกับผู้ดูแลระบบที่ได้มอบหมาย

๓ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๔ ดำเนินการเปลี่ยนชื่อจุดที่ให้บริการสัญญาณไร้สาย (Service Set Identifier: SSID) ที่ถูกกำหนดเป็นค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) มาใช้งาน

๕ ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายของ สกช.

๖ มีการตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

## ส่วนที่ ๘ การควบคุมการใช้อินเทอร์เน็ต (Internet)

**วัตถุประสงค์**

เพื่อให้ผู้ใช้งานได้ตระหนักถึงภัยคุกคามทางไซเบอร์ และสามารถใช้งานอินเทอร์เน็ตในการปฏิบัติงานได้อย่างปลอดภัย

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย

๒. ผู้ใช้งาน

**แนวปฏิบัติการควบคุมการใช้อินเทอร์เน็ต**

๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบอินเทอร์เน็ตเพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่จัดสรรไว้เท่านั้น เช่น อุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) เป็นต้น

๒ ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เว้นแต่มีเหตุผลความจำเป็นและต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสื่อสารและสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓ การใช้งานหรือเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๔ การรับส่งข้อมูลคอมพิวเตอร์ผ่านอินเทอร์เน็ต จะต้องมีการตรวจสอบไวรัส (Virus Scanning) ก่อนการรับส่งข้อมูลทุกครั้ง

๕ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ขององค์กร เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหาย

๖ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๗ ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การปรับปรุง (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๘ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ เป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร การก่อการร้าย หรือเนื้อหาที่มีลักษณะลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบอินเทอร์เน็ต

๙ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ (Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๑๐ ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

## ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

**วัตถุประสงค์**

เพื่อให้ผู้ใช้งาน ได้ทราบหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และเพื่อป้องกันทรัพยากรและสินทรัพย์ขององค์กร ให้มีความมั่นคงปลอดภัย

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ผู้ใช้งาน

**แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล**

๑ เครื่องคอมพิวเตอร์ส่วนบุคคลที่ สกช. อนุญาตให้ผู้ใช้ระบบสารสนเทศใช้งาน เป็นสินทรัพย์ของ สกช. ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๒ โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สกช. ต้องเป็นโปรแกรมที่ สกช. ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย การติดตั้งโปรแกรมเป็นหน้าที่ของผู้ดูแลระบบ ห้ามผู้ใช้งานติดตั้งหรือแก้ไขโปรแกรมด้วยตนเอง

๓ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยผู้ดูแลระบบที่ได้รับมอบหมายหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่ได้ทำสัญญาเท่านั้น การนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกนอก สกช. เพื่อการใดก็ตาม ต้องขออนุมัติเป็นลายลักษณ์อักษรจาก สกช. เท่านั้น

๔ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล

๕ ปรับปรุง (Update) ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๖ กำหนดให้เครื่องคอมพิวเตอร์ล็อกหน้าจอ เมื่อไม่ใช้งานเกิน ๑๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถใช้งานเครื่องคอมพิวเตอร์ได้

๗ ต้องไม่ถอดถอนการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus)

๘ ผู้ใช้งาน มีหน้าที่เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นความลับ ไม่เปิดเผยต่อผู้อื่น

## ส่วนที่ ๑๐ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

**วัตถุประสงค์**

เพื่อให้ผู้ใช้งาน ได้ทราบหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์แบบพกพา และเพื่อป้องกันทรัพยากรและสินทรัพย์ขององค์กร ให้มีความมั่นคงปลอดภัย

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ผู้ใช้งาน

**แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา**

๑ เครื่องคอมพิวเตอร์แบบพกพาที่เป็นสินทรัพย์ของ สกช. เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพพร้อมใช้งาน

๒ โปรแกรมที่ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของ สกช. ต้องเป็นโปรแกรมที่ สกช. ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓ ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ลงบนสื่อจัดเก็บข้อมูลที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย หรือกำหนดรหัสการเข้าสื่อบันทึกข้อมูล รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๔ การเคลื่อนย้ายคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือพลัดหลุดมือ เป็นต้น

๕ หลีกเลี่ยงการเก็บเครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทางเพราะอาจถูกกดทับเกิดความเสียหายได้

๖ หลีกเลี่ยงการเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ กรณีต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๗ ปรับปรุง (Update) ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๘ กำหนดให้เครื่องคอมพิวเตอร์ล็อกหน้าจอ เมื่อไม่ใช้งานเกิน ๑๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถใช้งานเครื่องคอมพิวเตอร์ได้

๙ ต้องไม่ถอดถอนการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus)

๑๐ ผู้ใช้งานมีหน้าที่เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นความลับ ไม่เปิดเผยต่อผู้อื่น

## ส่วนที่ ๑๑ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

**วัตถุประสงค์**

เพื่อควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายให้มีความปลอดภัย

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ผู้พัฒนาระบบหรือผู้ให้บริการภายนอก (Outsource)

**แนวปฏิบัติการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย**

๑ ควบคุมการติดตั้งซอฟต์แวร์บนระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบ ดังนี้

๑.๑ ควบคุมการเปลี่ยนแปลงการตั้งค่าต่อระบบสารสนเทศของ สกช. เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

๑.๒ ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้นที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศ

๑.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องแจ้งผู้ดูแลระบบก่อนดำเนินการ

๑.๔ กำหนดให้มีการจัดเก็บชุดคำสั่ง (Source Code) และชุดโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

๑.๕ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ระบบปฏิบัติการ ระบบสารสนเทศ เป็นต้น

๑.๖ วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๑.๗ จัดเก็บซอฟต์แวร์หรือชุดคำสั่ง (Source Code) เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

๒.๑ แจ้งให้ผู้ดูแลระบบที่ได้รับมอบหมาย ได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ (Operating System) เพื่อให้ดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ (Operating System)

๒.๒ วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๓ การพัฒนาซอฟต์แวร์โดยผู้พัฒนาระบบหรือผู้ให้บริการภายนอก (Outsource)

๓.๑ กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้พัฒนาระบบหรือผู้ให้บริการภายนอก (Outsource) และให้ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ ถูกต้องตามกฎหมาย

๓.๒ กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก

๓.๓ กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ก่อนติดตั้ง

๓.๔ ห้ามทดสอบซอฟต์แวร์บนระบบและฐานข้อมูลที่ใช้งานจริง เลือกสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

๔ มาตรการควบคุมผู้พัฒนาระบบหรือผู้ให้บริการภายนอก (Outsource)

๔.๑ ผู้พัฒนาระบบหรือผู้ให้บริการภายนอกที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของ สกช. จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสื่อสารและสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

๔.๓ กำหนดให้ผู้พัฒนาระบบเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้พัฒนาระบบอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๔.๔ การอนุญาตให้ผู้พัฒนาระบบเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสื่อสารและสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๕ ไม่เปิดช่องทาง (Port) และเชื่อมต่อเข้าสู่ระบบระยะไกลทิ้งไว้ โดยไม่จำเป็น และตัดการเชื่อมต่อเมื่อไม่ได้ใช้งาน

๕ มาตรการควบคุมช่องโหว่ทางเทคนิค

๕.๑ กำหนดให้ผู้พัฒนาระบบหรือผู้ให้บริการภายนอก (Outsource) เข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน บริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

(๑) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

(๒) สถานที่ที่ติดตั้ง

(๓) เครื่องแม่ข่ายที่ติดตั้ง

(๔) ผู้ผลิตซอฟต์แวร์

(๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๕.๒ ตรวจสอบ เฝ้าระวังและติดตาม ช่องโหว่ที่เกิดขึ้นของระบบสารสนเทศ และประสานงานผู้เกี่ยวข้อง เพื่อดำเนินการแก้ไขช่องโหว่ตามความเหมาะสมและคำนึงถึงการใช้งานระบบสารสนเทศ

๕.๓ ปิดการใช้งานหรือควบคุมการเข้าถึงช่องทาง (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย

๕.๔ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ชื่อบัญชีผู้ใช้งาน

(๒) วันเวลาที่เข้าถึงระบบ

(๓) วันเวลาที่ออกจากระบบ

(๔) เหตุการณ์สำคัญที่เกิดขึ้น

(๕) การล็อกอิน (log in) ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) การเปลี่ยนการตั้งค่า (Configuration) ของระบบ

(๘) การใช้งานแอปพลิเคชัน (Application)

(๙) การเข้าถึงไฟล์และการกระทำ เช่น เปิด ปิด เขียน อ่าน ลบ เป็นต้น

(๑๐) หมายเลขเครือข่าย (IP address) ที่เข้าถึง

(๑๑) การให้บริการ (Protocol) เครือข่ายที่ใช้

## ส่วนที่ ๑๒ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

**วัตถุประสงค์**

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

**ผู้รับผิดชอบ**

๑. หน่วยงานภายใน สกช.
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. ผู้ใช้งาน

**แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม**

๑ ห้องเครื่องคอมพิวเตอร์ (Data Center)
- ๑.๑ กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงานพื้นที่ควบคุมเฉพาะให้ชัดเจน และควบคุมสิทธิการเข้าถึง
- ๑.๒ กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ดังนี้
  - (๑) ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิการเข้าใช้งานพื้นที่เท่านั้น
  - (๒) ควบคุมการเข้าใช้งานในพื้นที่โดยการลงบันทึกลายนิ้วมือ (Finger Scan) หรือการใช้บัตรเข้าใช้งานในพื้นที่
  - (๓) ติดตั้งกล้องวงจรปิดเพื่อติดตาม/เฝ้าระวังการเข้าพื้นที่ห้องเครื่องคอมพิวเตอร์ (Data Center)
- ๑.๓ จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศให้เพียงพอต่อความต้องการใช้งานและมีความพร้อมในการใช้งาน ดังนี้
  - (๑) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง
  - (๒) ติดตั้งระบบระงับเพลิง
  - (๓) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น
  - (๔) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน
  - (๕) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

๒ การเดินสายไฟ สายสื่อสารและสายเคเบิ้ลอื่น ๆ (Cabling Security)
- ๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงติดตั้งระบบป้องกันที่ปลอดภัย

๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน

๒.๔ ติดป้ายบ่งชี้สายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๒.๕ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๒.๗ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๓ การนำสินทรัพย์ออกไปใช้งานภายนอก (Removal of Property)

๓.๑ ต้องขออนุมัติเป็นลายลักษณ์อักษรจาก สกช. ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือนำไปซ่อมบำรุงภายนอก

๓.๒ ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้สินทรัพย์ดังกล่าวกลับมาตามช่วงเวลาที่กำหนดและตรวจสอบอยู่ในสภาพดี

๓.๓ บันทึกข้อมูลการนำอุปกรณ์ของ สกช. ออกไปใช้งานภายนอก และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

๔ การป้องกันอุปกรณ์ที่ใช้งานภายนอก (Security of Equipment Off Premises)

๔.๑ เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

๔.๒ ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของ สกช. ไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

๕ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

๕.๑ ต้องขออนุมัติเป็นลายลักษณ์อักษรจาก สกช. ในการกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งาน

๕.๒ ต้องทำลายข้อมูลที่สำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

## ส่วนที่ ๑๓ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

**วัตถุประสงค์**

เพื่อให้ผู้ใช้งานได้ตระหนักถึงภัยคุกคามทางไซเบอร์ และสามารถใช้งานอินเทอร์เน็ตในการปฏิบัติงานได้อย่างปลอดภัย

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย

๒. ผู้ใช้งาน

**แนวปฏิบัติการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์**

๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๒ ผู้ดูแลระบบรับเรื่องการขอใช้งานจดหมายอิล็กทรอนิกส์ โดยกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานจดหมายอิเล็กทรอนิกส์รายใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน

๓ กำหนดให้ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) โดยรหัสผ่านต้องประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษอย่างน้อย ๘ หลัก (digits)

๔ กำหนดให้การเข้ารหัสผิดได้ไม่เกิน ๕ ครั้ง กรณีบัญชีผู้ใช้งานไม่สามารถเข้าใช้งานได้เนื่องจากเข้ารหัสผิดเกินจำนวนครั้งที่กำหนด ให้ติดต่อผู้ดูแลระบบ และแจ้งความประสงค์ขอตั้งรหัสผ่านใหม่

๕ เมื่อใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น 'x' หรือ 'O' ในการพิมพ์แต่ละตัวอักษร

๖ ระบบจดหมายอิเล็กทรอนิกส์จะออกจากระบบ (Log out) เพื่อตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาภายใน ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

๗ ผู้ใช้งานควรหลีกเลี่ยงค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๘ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อองค์กร การละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ รวมทั้งไม่อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

๙ ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์

๑๐ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

๑๑ ผู้ใช้งานควรตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ โดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe .bat เป็นต้น

๑๒ ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความ เอกสารแนบ และลิงก์เว็บไซต์ต่าง ๆ ที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๓ ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียง หรือข้อมูลทำให้เกิดความแตกแยกผ่านทางจดหมายอิเล็กทรอนิกส์

๑๔ ผู้ใช้งานควรตรวจสอบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่

## ส่วนที่ ๑๔ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

**วัตถุประสงค์**

๑. เพื่อให้ สกช. มีการกำหนดขอบเขตของการใช้สื่อสังคมออนไลน์ทั้งในระดับตัวบุคคลและระดับองค์กร

๒. เพื่อสร้างและรักษาภาพลักษณ์ของบุคลากรและการดำเนินงานของ สกช.

๓. เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นจากการใช้สื่อสังคมออนไลน์ ต่อองค์กร บุคคลากร รวมถึงผู้มีส่วนได้ส่วนเสีย

๔. เพื่อป้องกันการเปิดเผยข้อมูลความลับของ สกช.

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย

๒. ผู้ใช้งาน

**แนวปฏิบัติการควบคุมการใช้งานเครือข่ายสังคมออนไลน์**

**ส่วนที่ ๑ แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ทั่วไป**

๑ สกช. อนุญาตให้ใช้ระบบเครือข่ายสำหรับเข้าถึงสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมายศีลธรรม และจะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

๒ บุคลากรของ สกช. สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ประชาสัมพันธ์ที่เกี่ยวข้องกับ สกช. ติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ชัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” ข้อความใดเป็น “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่น ๆ และความคิดเห็นดังกล่าวต้องคำนึงถึงประโยชน์สาธารณะด้วย

๓ พึงระมัดระวังการใช้ถ้อยคำและภาษา ที่อาจเป็นการดูหมิ่น ทั้งการหมิ่นประมาทบุคคลอื่น หรือหมิ่นประมาทองค์กรและต้องใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์ ไม่ขัดต่อกฎหมาย

๔ พึงงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะ หรือรูปที่สร้างความเสียหายให้แก่บุคคลอื่น องค์กร และสังคม มาแสดงว่าเป็นรูปของตนเอง

๕ พึงงดเว้นการโพสข้อมูลลามกอนาจาร และอื่น ๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม ได้แก่ การเมือง ศาสนา ชนชาติ เป็นต้น

๖ พึงงดเว้นการอ้างอิงหรือเปิดเผยถึงข้อมูลผู้มีส่วนได้ส่วนเสีย ตลอดจนผู้มีส่วนเกี่ยวข้องอย่างเปิดเผยก่อนได้รับอนุญาต

๗ ผู้ใช้งานต้องตรวจสอบที่มาและความถูกต้องของข้อมูล ก่อนทำการส่งต่อข้อมูล รวมถึงงดเว้นการส่งข้อมูลที่เป็นเท็จ และข้อมูลองค์กรที่มีชั้นความลับ

๘ การเผยแพร่และส่งต่อข้อมูลส่วนบุคคลต้องคำนึงถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล และบทกำหนดโทษตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

๙ หากพบข้อมูลใด ๆ ที่ไม่เหมาะสม หรือไม่ถูกต้อง (ได้แก่ สิ่งที่เป็นลิขสิทธิ์ของผู้อื่น หรือการแสดงความคิดเห็นที่เป็นการหมิ่นประมาท) ต้องดำเนินการลบข้อมูลดังกล่าวออกทันที เพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อ สกช.

**ส่วนที่ ๒ แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับบุคคล**

การนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรใน สกช. มีแนวนโยบายและแนวปฏิบัติดังนี้

๑ กรณีใช้ชื่อบัญชีผู้ใช้งาน (User Account) ที่ระบุถึงต้นสังกัด ผู้ใช้งานพึงใช้ความระมัดระวังในการปฏิบัติตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติของ สกช. ที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย โดยเฉพาะความถูกต้องและการใช้ภาษาที่เหมาะสม

๒ กรณีใช้ชื่อบัญชีผู้ใช้งานที่ระบุถึงตัวตนอันอาจทำให้ผู้ติดตาม (Followers) หรือเพื่อนในเครือข่าย (Friends) เข้าใจได้ว่าเป็นบุคลากรใน สกช. ผู้ใช้งานพึงระมัดระวังการนำเสนอข้อมูลข่าวและการแสดงความคิดเห็นที่อาจนำไปสู่ความเสียหายขององค์กร สังคม และบุคคลอื่น

๓ หากการโพสข้อมูลข่าวสารหรือความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรใน สกช. เกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อองค์กร สังคม และบุคคลอื่น ผู้ใช้งานต้องแสดงความรับผิดชอบต่อองค์กร สังคม และบุคคลอื่นที่ได้รับความเสียหาย ทั้งนี้ ต้องให้ผู้ที่ได้รับความเสียหายได้ มีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

**ส่วนที่ ๒ แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับองค์กร**

การใช้สื่อสังคมออนไลน์เพื่อประชาสัมพันธ์ในระดับองค์กร ต้องที่จะคำนึงถึงรายละเอียดดังนี้

๑ การตั้งค่าบนสื่อสังคมออนไลน์ขององค์กร การใช้ชื่อหรือตราสัญลักษณ์ขององค์กร เพื่อเปิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร หรือการสื่อสารภายในองค์กร จะต้องผ่านการรับทราบและเห็นชอบจากผู้มีอำนาจขององค์กรก่อน

๒ การปกป้องข้อมูลที่เป็นความลับขององค์กร ในกรณีที่มีบัญชีผู้ใช้งานขององค์กร ต้องมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีชั้นความลับ โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และต้องให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วนบุคคลที่ไม่ต้องการเผยแพร่ให้สาธารณะชนรับรู้

๓ การนำเสนอข้อมูลข่าวสารขององค์กรผ่านสื่อสังคมออนไลน์ ต้องเป็นไปตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติขององค์กรที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย

๔ การนำเสนอข้อมูลข่าวสารขององค์กรผ่านสื่อสังคมออนไลน์ ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อมูล ต้องให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

๕ ต้องแยกบัญชีผู้ใช้สื่อสังคมออนไลน์แบบส่วนตัวกับแบบองค์กรที่ทำหน้าที่ประชาสัมพันธ์องค์กรออกจากกัน

๖ หลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง และข้อมูลใด ๆ ขององค์กรหรือที่เกี่ยวข้องกับองค์กรที่ก่อให้เกิดความขัดแย้ง หรือโต้แย้งในสังคม ขัดต่อหลักกฎหมายทั้งในประเทศและในระดับสากล

๗ พึงระวังเรื่องความปลอดภัยระบบ เพื่อป้องกัน รับมือและลดความเสี่ยงจากการถูกโจมตีจากบุคคลภายนอก เช่น การตั้งรหัสผ่านยืนยันตัวตนแบบสองชั้น (๒ Factor Authentication) หลีกเลี่ยงการกดลิงก์จากบัญชีที่ไม่รู้จัก จำกัดสิทธิ์ของผู้ใช้งานแต่ละคนโดยไม่ควรเป็น Full Access ทุกคน เป็นต้น

## หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

### ส่วนที่ ๑ การสำรองข้อมูล (back up)

**วัตถุประสงค์**

๑. เพื่อให้การสำรองข้อมูลมีความเหมาะสมและปลอดภัย ให้ระบบสารสนเทศของ สกช. สามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้มีมาตรฐาน แนวทางปฏิบัติและกำหนดความรับผิดชอบของผู้ดูแลระบบ

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย

๒. ผู้ใช้งาน

**แนวปฏิบัติการรักษาความปลอดภัยและระบบสำรองข้อมูล**

๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดขององค์กร ที่ทำการสำรองข้อมูล (backup) และจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan) อย่างน้อยปีละ ๑ ครั้ง

๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และวางแผนกำหนดความถี่ในการสำรองข้อมูล โดยพิจารณาจากความสำคัญของข้อมูล ความถี่ในการเปลี่ยนแปลงข้อมูล โดยมีรายละเอียดการสำรองข้อมูล ดังนี้

- ๒.๑ ทำการสำรองเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศ
- ๒.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็นการสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)
- ๒.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (latest update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับการกู้คืนระบบ
- ๒.๔ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล เช่น ชื่อข้อมูลที่สำรอง สถานะการสำรองข้อมูล เป็นต้น
- ๒.๕ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการสำรองข้อมูลใหม่โดยทันที
- ๒.๖ จัดให้มีการสำรองข้อมูลของระบบสารสนเทศไว้ที่อุปกรณ์ภายนอก
- ๒.๗ ตรวจสอบการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore)

## ส่วนที่ ๒ การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

**วัตถุประสงค์**

เพื่อจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ เพื่อให้สามารถใช้ระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ผู้ใช้งาน

**แนวปฏิบัติการจัดทำแผนแก้ไขปัญหาจากสถานการณ์และภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ**

๑ จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan) โดยมีรายละเอียดอย่างน้อย ดังนี้

๑.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
๑.๒ กำหนดขั้นตอนปฏิบัติในการกู้คืน (Restore) ระบบสารสนเทศ และระยะเวลาในการกู้คืน
๑.๓ ทดสอบขั้นตอนปฏิบัติในการกู้คืนระบบ
๑.๔ กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายใน และผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อผู้ให้บริการ
๑.๕ สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒ มีการทบทวนเพื่อปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓ กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๔ ดำเนินการซักซ้อมตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (T Contingency Plan) อย่างน้อยปีละ ๑ ครั้ง

## หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

**วัตถุประสงค์**

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคง ปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

**ผู้รับผิดชอบ**

๑. ผู้ดูแลระบบที่ได้รับมอบหมาย

๒. ผู้ตรวจสอบภายใน

**แนวทางปฏิบัติ**

๑ ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศ โดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากหน่วยงานภายนอก อย่างน้อยปีละ ๑ ครั้ง

๒ มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยทุก ๆ ๒ ปี

๒.๓ มีการตรจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้

๒.๔.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

๒.๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รามทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม

๒.๔.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๔.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลการใช้งาน (Log) แสดงการเข้าถึงวันและเวลาที่เข้าถึงระบบ

๒.๔.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

## หมวด ๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

**วัตถุประสงค์**

เพื่อสร้างความรู้ ความเข้าใจให้กับผู้ใช้งาน ได้ตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศอย่างไม่ถูกต้อง และไม่มีความปลอดภัย

**ผู้รับผิดชอบ**

๑. กองสื่อสารและสารสนเทศ

๒. กองการเจ้าหน้าที่

**แนวทางปฏิบัติ**

๑ เผยแพร่ประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้งานและผู้เกี่ยวข้องรับทราบ

๒ จัดฝึกอบรมแนวปฏิบัติตามนโยบาย เพื่อสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากรอย่างเหมาะสม หรืออาจใช้วิธีการเสริมเนื้อหาข้อปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมขององค์กร หรืออาจจัดร่วมกับการสัมมนาอื่น หรืออาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้ อย่างน้อยปีละ ๑ ครั้ง