สำนักงานคณะกรรมการ
สุขภาพแห่งชาติ

ประกาศสำนักงานคณะกรรมการสุขภาพแห่งชาติ
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานคณะกรรมการสุขภาพแห่งชาติ พ.ศ. ๒๕๖๓

โดยที่เป็นการสมควรกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานและการทำธุรกรรมทางอิเล็กทรอนิกส์ของสำนักงานคณะกรรมการสุขภาพแห่งชาติ (สช.) ให้มีความมั่นคงปลอดภัย น่าเชื่อถือ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานภายในเป็นไปในทิศทางเดียวกัน

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย และเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร เลขาธิการคณะกรรมการสุขภาพแห่งชาติ จึงเห็นควรกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการสุขภาพแห่งชาติ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการสุขภาพแห่งชาติ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการสุขภาพแห่งชาติ พ.ศ. ๒๕๖๓”

ข้อ ๒ ประกาศนี้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ผู้บริหาร บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. มีหน้าที่ต้องปฏิบัติตามแนวนโยบายความมั่นคงปลอดภัยด้านสารสนเทศแนบท้ายประกาศนี้

ข้อ ๔ ผู้บังคับบัญชามีหน้าที่สนับสนุนและกำกับดูแลให้ผู้ที่อยู่ใต้บังคับบัญชาของตนปฏิบัติตามแนวนโยบายความมั่นคงปลอดภัยด้านสารสนเทศโดยเคร่งครัด

ข้อ ๕ ให้เลขาธิการคณะกรรมการสุขภาพแห่งชาติ เป็นผู้รักษาการตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้เลขาธิการวินิจฉัยชี้ขาด คำวินิจฉัยของเลขาธิการให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๑๒ พฤศจิกายน พ.ศ. ๒๕๖๓

(นายประทีป ธนกิจเจริญ)
เลขาธิการคณะกรรมการสุขภาพแห่งชาติ

สำนักงานคณะกรรมการสุขภาพแห่งชาติ (สช.) : ชั้น ๓ อาคารสุขภาพแห่งชาติ ๘๘/๓๙ หมู่ ๔ ซ.ติวานนท์ ๑๔ ถ.ติวานนท์ ต.ตลาดขวัญ อ.เมือง จ.นนทบุรี ๑๑๐๐๐
National Health Commission Office : Floor 3, National Health building, 88/39 Moo 4, Soi Tiwanon 14, Tiwanon Rd., Mueang District, Nonthaburi 11000 Thailand
Tel. +66-2832-9000 Fax. +66-2832-9001 www.nationalhealth.or.th Email : nationalhealth@nationalhealth.or.th

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

(Information Security Policy)

สำนักงานคณะกรรมการสุขภาพแห่งชาติ

พ.ศ. 2563

สารบัญ

หน้าที่

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) ของสำนักงานคณะกรรมการสุขภาพแห่งชาติ พ.ศ.2563

บทนำ

สำนักงานคณะกรรมการสุขภาพแห่งชาติ (สช.) หรือ ต่อไปนี้เรียกว่า "สช." มุ่งเน้นที่จะนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้สนับสนุนการปฏิบัติงานทุกส่วนขององค์กร รวมถึงการให้บริการประชาชนและภาคีเครือข่ายด้วย ดังนั้นจึงได้จัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ขึ้นเพื่อเป็นมาตรฐานและแนวปฏิบัติให้ระบบสารสนเทศของ สช. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคง ปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ทั้งจากภายในและภายนอก ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจก็ตาม อันเป็นการลดความเสียหายต่าง ๆ และรักษาไว้ซึ่งความสามารถในการดำเนินงานได้อย่างมีประสิทธิภาพ

หลักการ

ระบบสารสนเทศ เทคโนโลยี และการสื่อสารที่ทาง สช.ได้จัดเตรียมให้ใช้งานจำเป็นจะต้องมีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินกิจการ ซึ่งการดูแลรักษาและป้องกันมุ่งหมายไปในทางความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการธำรงไว้ซึ่งการรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ โดยอธิบายได้ ดังนี้

การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้สินทรัพย์สามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ์ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งสินทรัพย์นั้นด้วย ดังนั้น ในการรักษาความลับจำเป็นจะต้องมีการควบคุม ทั้งทางกายภาพและทางเทคนิค โดยผู้ที่ไม่มีสิทธิ์จะต้องไม่สามารถเข้าถึงสินทรัพย์นั้นได้ และสินทรัพย์จำเป็นจะต้องมีการจำแนกและกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ที่ถือครองสินทรัพย์ปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น ๆ

ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้สินทรัพย์ถูกเปลี่ยนแปลง แก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิ์ที่จะแก้ไขสินทรัพย์เหล่านั้น ดังนั้นการควบคุมและป้องกันจึงต้องประกอบด้วยการกำหนดสิทธิ์ในการแก้ไข การเข้าถึง และจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีสินทรัพย์และเทคนิคประกอบด้วย

ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้มีสิทธิ์สามารถเข้าใช้งานสินทรัพย์นั้นได้เมื่อยามต้องการใช้งาน ซึ่งมีทั้งในทางกายภาพและทางเทคโนโลยี ได้แก่ การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้นเมื่อผู้ใช้ต้องการจะรับหรือส่ง ระบบจำเป็นที่จะต้องสามารถให้บริการได้ตลอดเวลานั้น เป็นต้น

นอกจากที่กล่าวมาแล้วยังประกอบด้วยเรื่อง ผู้รับผิดชอบต่อการกระทำ (Accountability) ซึ่งหมายถึง สินทรัพย์จำเป็นจะต้องมีผู้รับผิดชอบและสามารถอธิบายได้ถึงผลที่เกิดขึ้นไม่ว่าผลนั้นเกิดจากการกระทำจาก บุคคลหรือสิ่งอื่นใด

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของ สช. เป็นไปอย่างเหมาะสม มีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถดำเนินการได้อย่างต่อเนื่อง รวมถึงป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สช. จึงเห็นสมควรให้กำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีวัตถุประสงค์ ดังนี้

1. เพื่อให้ สช. มีนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยมีความสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่ถูกต้อง
2. เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอ้างอิงตามนโยบายมาตรฐานที่ สช.ปรับใช้ และนโยบายอื่น ๆ ที่เกี่ยวข้อง
3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศและปฏิบัติตามนโยบายอย่างเคร่งครัด
4. เพื่อให้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยสารสนเทศ ของ สช. ต่อไป

ขอบเขต

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้มีผลบังคับใช้กับสารสนเทศของ สช. ผู้ทำหน้าที่ดูแลสินทรัพย์ ผู้ใช้สินทรัพย์ ผู้บริหาร บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. โดยมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลสินทรัพย์จะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของ สช.

นิยาม

1. **สช.** หมายถึง สำนักงานคณะกรรมการสุขภาพแห่งชาติ
2. **ผู้ใช้งาน** หมายถึง คณะกรรมการ ผู้บริหาร บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. รวมถึงนิสิตนักศึกษาฝึกงานที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของ สช. ตามสิทธิ์และหน้าที่ความรับผิดชอบ
3. **คณะกรรมการ** หมายถึง บุคคลผู้ที่ได้รับแต่งตั้งเป็นคณะกรรมการ คณะอนุกรรมการ คณะทำงาน โดยคณะกรรมการสุขภาพแห่งชาติ (คสช.) หรือ สช.
4. **ผู้บริหาร** หมายถึง เลขาธิการและรองเลขาธิการคณะกรรมการสุขภาพแห่งชาติ
5. **บุคลากร** หมายถึง พนักงาน พนักงานโครงการ และบุคคลผู้ที่ สช.ว่าจ้างให้ปฏิบัติงาน ณ สำนักงาน บุคคลผู้ที่ สช.บรรจุและแต่งตั้งเป็นเจ้าหน้าที่ของ สช.
6. **บุคคลภายนอกที่ปฏิบัติงานให้ สช.** หมายถึง บุคคลหรือนิติบุคคลที่ปฏิบัติงาน สช. มอบหมายด้วยวิธีการใด ๆ ได้แก่ การว่าจ้าง การรับข้อตกลง การแต่งตั้ง เป็นต้น ให้ปฏิบัติงานให้ สช.ตามขอบเขตงานที่ได้รับมอบหมาย
7. **ผู้ดูแลระบบเทคโนโลยีสารสนเทศ** หมายถึง บุคลากร หน่วยงานหรือบุคคลภายนอกที่ได้รับมอบหมายจากผู้บริหารให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบงานและเครือข่ายคอมพิวเตอร์
8. **เจ้าของข้อมูล (Information Owner)** หมายถึง ผู้ซึ่งรับผิดชอบข้อมูลของสำนักงานซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้น หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
9. **ข้อมูล (Data)** หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของซีดี (CD) ดีวีดี (DVD) Hard Disk Thumb drive เอกสาร แฟ้ม รายงาน หนังสือ แผนที่ แผนผัง ภาพวาด ภาพถ่าย การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
10. **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
11. **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูลระหว่างระบบคอมพิวเตอร์ ได้แก่ ระบบ LAN (Local Area Network) ระบบ WLAN (Wireless LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเตอร์เน็ต (Internet) เป็นต้น ทั้งที่เชื่อมต่อด้วยสายสัญญาณและไม่ใช้สายสัญญาณในการเชื่อมต่อแต่ใช้เทคโนโลยีการสื่อสารอื่นเพื่อการเชื่อมต่อแทน

12. **ระบบสารสนเทศ (Information System)** หมายถึง ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) สารสนเทศ (Information) เป็นต้น

13. **สินทรัพย์ (Asset)** หมายถึง สิ่งที่มีคุณค่าหรือมูลค่าต่อ สช. และเป็นทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่ สช.เป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งแยกออกเป็นประเภทต่าง ๆ ได้ดังนี้ สารสนเทศ (Information) ซอฟต์แวร์ (Software) ทรัพย์สินที่มีรูปร่าง (Physical Asset) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People)

14. **การเข้าถึง (Access)** หมายถึง การเข้าสถานที่ การใช้งานทางอิเล็กทรอนิกส์ หรือทางกายภาพ รวมถึงการรับรู้ซึ่งข้อมูล สารสนเทศ

15. **การควบคุมการเข้าถึง (Access Control)** หมายถึง การอนุญาต การกำหนดสิทธิ์ การเปลี่ยนแปลง การเพิกถอนหรือการยกเลิกสิทธิ์การเข้าถึง

16. **BYOD (Bring your own device)** หมายถึง การที่นำเอาอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศส่วนบุคคลมาใช้งานที่ สช. หรือเชื่อมต่อกับระบบเครือข่ายของ สช.

17. **อุปกรณ์ประมวลผล (Computing Device)** หมายถึง อุปกรณ์ที่มีหน่วยประมวลผล หน่วยความจำ ส่วนบันทึกข้อมูล ส่วนการเชื่อมต่อเครือข่าย ส่วนรับข้อมูล และส่วนแสดงผล ได้แก่ คอมพิวเตอร์แบบตั้งโต๊ะ เช่น Desktop Computer เป็นต้น และคอมพิวเตอร์แบบพกพา เช่น Notebook, Laptop เป็นต้น

18. **อุปกรณ์เคลื่อนที่ (Mobile Device)** หมายถึง อุปกรณ์ประมวลผลแบบพกพา ที่มีขนาดเล็กสามารถใช้เพียงมือเดียวในการใช้งาน ส่วนของการรับข้อมูลเป็นแบบสัมผัส โดยไม่ต้องใช้ Keyboard และสามารถเชื่อมต่อเครือข่ายแบบไร้สาย เครือข่ายโทรศัพท์ได้ เช่น Smartphone, Tablet เป็นต้น

หมวดที่ 1 การนำอุปกรณ์ส่วนตัวมาใช้ร่วมกับระบบสารสนเทศของสำนักงาน (Bring your own device : BYOD)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยสำหรับการนำอุปกรณ์ส่วนตัวมาใช้ร่วมกับระบบสารสนเทศของสำนักงาน (Bring your own device : BYOD)

ผู้ปฏิบัติ ผู้ใช้งานและส่วนงานที่เกี่ยวข้อง

ข้อปฏิบัติ

1. ไม่อนุญาตให้นำอุปกรณ์ส่วนตัว (Bring your own device : BYOD) มาเชื่อมต่อกับเครือข่ายภายใน รวมทั้งเข้าถึงระบบงานสารสนเทศภายในของ สช. ก่อนได้รับอนุญาตจากผู้บังคับบัญชาและต้องนำอุปกรณ์ส่วนตัวดังกล่าวไปขึ้นทะเบียนกับ สช.
2. ผู้ใช้งานอุปกรณ์ส่วนตัว (Bring your own device : BYOD) ต้องปฏิบัติตามแนวทางปฏิบัติดังนี้
   - 2.1 ผู้ใช้งานต้องอนุญาตให้ สช. ตรวจสอบการใช้งานอุปกรณ์ส่วนตัว (Bring your own device : BYOD) โดยอาจใช้วิธีการตรวจสอบผ่านซอฟต์แวร์บริหารจัดการที่ติดตั้งบนอุปกรณ์ เช่น Mobile Device Management – MDM เป็นต้น หรือตรวจสอบโดยเจ้าหน้าที่ของ สช.
   - 2.2 การเชื่อมต่อเข้าสู่ระบบเครือข่ายและระบบงานของ สช. ต้องดำเนินการผ่านระบบ Virtual Private Network (VPN) ที่ สช. จัดหาให้เท่านั้น
   - 2.3 ผู้ใช้งานมีหน้าที่รับผิดชอบในการปกป้องข้อมูลสำคัญของ สช. ซึ่งบันทึกอยู่บนอุปกรณ์ส่วนตัว (Bring your own device : BYOD) และต้องปฏิบัติตามขั้นตอนการปฏิบัติการรักษาชั้นความลับและระดับชั้นความลับของข้อมูล
   - 2.4 ผู้ใช้งานต้องตั้งค่า Lock screen ด้วย PIN ที่เป็นรหัสที่เดาสุ่มได้ยาก ความยาวอย่างน้อย 4 ตัวเลข หรือใช้วิธีการยืนยันตัวตนก่อนใช้งานเครื่องที่ดีกว่า เช่น Pattern, Password หรือ Fingerprint เป็นต้น และตั้งค่า Automatically Lock Screen Timeout ไม่มากกว่า 15 นาที หรือน้อยที่สุดที่อุปกรณ์สามารถตั้งค่า
   - 2.5 ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมป้องกันไวรัส (Antivirus) ให้กับอุปกรณ์ส่วนตัว (Bring your own device : BYOD) และปรับปรุงฐานข้อมูลของโปรแกรมป้องกันไวรัสให้ทันสมัยเสมอ หากพบว่าโปรแกรมป้องกันไวรัสทำงานผิดพลาด หรือไม่ทำงาน หรือสงสัยว่าอุปกรณ์ส่วนตัว (Bring your own device : BYOD) ติดมัลแวร์ หรือพบข้อมูลภัยคุกคาม ผู้ใช้งานต้องยุติการเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายหรือระบบงานและให้แจ้งส่วนงานที่รับผิดชอบ เพื่อดำเนินการแก้ไขโดยทันที

หมวดที่ 2 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

วัตถุประสงค์

นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศนี้จัดทำขึ้นเพื่อ

1. กำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศของ สช.
2. ปกป้องข้อมูลและสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

ผู้ปฏิบัติ ผู้ใช้งาน และผู้ที่เกี่ยวข้อง

ข้อปฏิบัติ

1. การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ

1.1 ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนการลงทะเบียนผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

1.2 ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการบริหารจัดการบัญชีชื่อผู้ใช้งาน (User Name)

1.3 ต้องกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ การกำหนดสิทธิ์ หรือการมอบอำนาจเป็นลายลักษณ์อักษร ดังนี้

(1) การกำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องต้องได้รับการควบคุมอย่างเหมาะสมตามความต้องการในการใช้งาน ระดับความสำคัญ ความต้องการข้อกำหนดของกฎหมาย สัญญาต่าง ๆ ที่เกี่ยวข้อง และต้องปฏิบัติตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูล รวมถึงการควบคุมและปกป้องข้อมูลผลลัพธ์ (Output) ที่ได้จากการทำงานของโปรแกรมประยุกต์ หรือแอปพลิเคชัน (Application) อย่างเหมาะสม

(2) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ การระงับสิทธิ์ การมอบอำนาจให้เป็นไปตามการบริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

1.4 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของ สช. นอกเหนือจากสิทธิ์ที่กำหนดไว้จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากผู้มีอำนาจอนุมัติ

1.5 การกำหนดสิทธิ์การเข้าถึงของผู้ใช้งานต้องมีการทบทวนและปรับปรุง อย่างน้อยปีละ 2 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง หรือมีการอัพเกรด (upgrade) ระบบเทคโนโลยีสารสนเทศ เป็นต้น

1.6 การพิสูจน์ตัวตนเพื่อเข้าระบบสารสนเทศที่สำคัญและมีผลกระทบต่อ สช. จะต้องผ่านการประเมินจากส่วนงานที่รับผิดชอบว่าเป็นกระบวนการที่มีความมั่นคงปลอดภัย โดยยึดหลักดังนี้

(1) ไม่แสดงรายละเอียดเกี่ยวกับระบบจนกว่ากระบวนการพิสูจน์ตัวตนเพื่อเข้าสู่ระบบจะเสร็จสิ้น

(2) มีข้อความแสดงเตือนผู้ไม่มีสิทธิ์เข้าถึงระบบงาน

(3) ไม่แสดงข้อความช่วยเหลือใดๆ ซึ่งอาจเป็นข้อมูลให้แก่ผู้ที่ไม่ได้รับอนุญาตหรือผู้ที่ไม่ประสงค์ดี

(4) จำกัดจำนวนครั้งที่อนุญาตให้ Log-on ผิดพลาดได้ พร้อมทั้งทำการหน่วงเวลาระหว่างการ Log-on ที่ผิดพลาดแต่ละครั้ง

(5) บันทึกการ Log-on ที่ถูกต้องและการ Log-on ที่ผิดพลาดเอาไว้เป็นหลักฐานพร้อมทั้งแสดงวันและเวลาล่าสุดของการ Log-on ที่ถูกต้องและการ Log-on ที่ผิดพลาดให้แก่ผู้ใช้งานหลังจากเข้าสู่ระบบได้อย่างถูกต้องแล้ว

(6) ไม่แสดงผลรหัสผ่านบนหน้าจอโดยไม่ปิดบัง (Mask)

(7) ไม่เก็บรักษารหัสผ่านหรือส่งผ่านเครือข่ายในลักษณะ Clear Text

(8) สช. มีสิทธิ์ลงโทษทางวินัยตามระเบียบของ สช. หากระบบคอมพิวเตอร์ของ สช. ได้รับความเสียหาย โดยการติดไวรัสคอมพิวเตอร์ จากการใช้งานระบบสำนักงานเสมือนจากภายนอก สช. ของผู้ใช้งาน

2. การบริหารสิทธิ์ในการใช้งานระบบ

2.1 สิทธิ์ในระบบสารสนเทศที่กำหนด (Assign/Grant) ให้แก่ผู้ใช้งานแต่ละคนนั้น ต้องเหมาะสมกับความต้องการในการใช้งานและเป็นไปตามเอกสารแสดงสิทธิ์การเข้าถึงระบบสารสนเทศ (Access Matrix)

2.2 การกำหนดสิทธิ์ เปลี่ยนแปลง หรือถอดถอนสิทธิ์นั้น ต้องได้รับอนุมัติจากผู้บังคับบัญชาที่มีหน้าที่ดูแลระบบสารสนเทศก่อนจึงจะสามารถกระทำได้

2.3 สิทธิ์พิเศษที่ให้แก่เจ้าหน้าที่ต้องผ่านการอนุมัติจากผู้บังคับบัญชาและเป็นสิทธิ์ชั่วคราวที่มีระยะเวลาจำกัด เมื่อครบกำหนดต้องได้รับการเพิกถอน/ยกเลิกทันที

2.4 การทบทวนสิทธิ์จะต้องมีการดำเนินการอย่างน้อยทุก ๆ 6 เดือน หรือหลังจากมีการเปลี่ยนแปลงสำหรับเจ้าหน้าที่ที่ได้รับสิทธิ์พิเศษหรือมีสิทธิ์ในระบบที่มีความสำคัญจะต้องมีการเพิ่มความถี่ในการทบทวนสิทธิ์มากขึ้น

2.5 กระบวนการและกิจกรรมที่กระทำโดยผู้ใช้งานระบบเทคโนโลยีสารสนเทศต้องถูกบันทึกไว้ทั้งในระบบ (System log) พร้อมทั้งได้รับการควบคุมดูแล (Monitor) โดยผู้ดูแลระบบ (System administrator) และ/หรือผู้จัดการส่วนงานที่เกี่ยวข้องกับการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.1 การให้และการใช้สิทธิ์การเข้าถึงต้องมีการจำกัดและควบคุม ให้สอดคล้องตามบทบาทหน้าที่ความรับผิดชอบที่ได้รับมอบหมายเท่านั้น

3.2 การกำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (Access Matrix) ที่ได้กำหนดไว้

3.3 การควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตตามสิทธิ์ที่ได้รับเท่านั้น เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users) ในกรณีที่มีความจำเป็นต้องการมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานที่เป็นข้อมูลลับ ต้องมีการควบคุมโดยต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร มีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นสภาพ

3.5 การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งานให้ปฏิบัติตามขั้นตอนการปฏิบัติงานการจัดการบัญชีผู้ใช้งาน สิทธิ์การใช้งานทั่วไป และขั้นตอนการปฏิบัติงานการจัดการบัญชีผู้ใช้งาน สิทธิ์การใช้งานระบบ

3.6 สิทธิ์การเข้าถึงของหน่วยงานภายนอก หรือผู้ให้บริการภายนอก (Third Party) ต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการดำเนินงาน หมดสัญญา หรือสิ้นสุดข้อตกลงทันที และต้องมีการปรับปรุงให้เป็นปัจจุบัน

4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลหรือสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

4.1 มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ซึ่งเป็นไปตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

4.2 มีการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของ สช. ในขณะที่ไม่มีผู้ดูแล ดังนี้

(1) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(2) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(3) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(4) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(5) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 15 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(6) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

4.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และผู้ใช้งานต้องออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

4.4 ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 ทั้งนี้ต้องสอดคล้องกับการกำหนดประเภทข้อมูลและการจัดระดับชั้นความลับของข้อมูล (Information Classification, Labeling and Handling)

หมวดที่ 3 การใช้งานระบบสำนักงานเสมือน
แนวทางปฏิบัติการทำงานจากภายนอกที่ตั้ง สช. ผ่านระบบ E-office

วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์การปฏิบัติงานจากภายนอกที่ตั้ง สช. เพื่อควบคุมการเข้าถึงระบบสำนักงานเสมือนและสารสนเทศของ สช. ตามสิทธิ์การเข้าถึงระบบหรือจากผู้ที่ไม่ได้รับการอนุญาต

ผู้ปฏิบัติ ผู้ใช้งาน และผู้ที่เกี่ยวข้อง

ข้อปฏิบัติ

1. **การควบคุมการเข้าถึงระบบสำนักงานเสมือนจากภายนอกที่ตั้ง สช.**
   - 1.1 ในกรณีที่ผู้ใช้บริการการเชื่อมต่อจากภายนอกที่ตั้ง สช. จะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีการควบคุมและตรวจสอบการใช้งาน หรือการเข้าถึงระบบตามสิทธิ์ที่ได้รับอย่างเคร่งครัด
   - 1.2 การเชื่อมต่อจากภายนอกที่ตั้ง สช. จะต้องมีการดำเนินการที่ได้รับการอนุมัติและเชื่อมต่อผ่านระบบเครือข่ายที่มีความปลอดภัย
   - 1.3 สิทธิ์ในการใช้งานเป็นสิทธิ์ที่ สช. จะให้เฉพาะผู้ใช้งานที่ สช.กำหนดเท่านั้น ไม่สามารถถ่ายโอนกันได้
   - 1.4 ผู้ใช้งานที่ได้รับสิทธิ์เข้าใช้งานระบบสารสนเทศ ต้องรับทราบถึงวัตถุประสงค์ วิธีการเข้าถึง และขอบข่ายของการเข้าถึงที่แน่ชัด และต้องได้รับการอนุมัติจากผู้บังคับบัญชาก่อนเข้าใช้งาน
2. **การใช้งานระบบ E-office**
   - 2.1 ต้องระวังในการใช้งานระบบ E-office ไม่ให้เกิดความเสียหายต่อ สช. หรือการใช้งานที่ไม่เหมาะสม
   - 2.2 การใช้งานระบบ E-office ต้องเชื่อมต่อผ่านระบบอินเทอร์เน็ตที่มีการรักษาความปลอดภัย
   - 2.3 ผู้ใช้งานจะต้องถูกกำหนดในการเข้าถึงข้อมูลตามหน้าที่ เพื่อความปลอดภัย
   - 2.4 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลในระบบก่อนนำข้อมูลไปใช้
   - 2.5 ห้ามใช้ซอฟต์แวร์ช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

3. การปฏิบัติงานจากภายนอกที่ตั้ง สช. (Remote Work)

3.1 สช. ต้องกำหนดแนวทางการติดต่อสื่อสารหลักและรอง เมื่อมีการกำหนดให้ปฏิบัติงานจากภายนอกที่ตั้ง สช.

3.2 เจ้าหน้าที่ต้องมีการจัดเตรียมกระบวนการทำงานตามขอบเขตความรับผิดชอบ เมื่อมีการกำหนดให้ปฏิบัติงานจากภายนอกที่ตั้ง สช. และสื่อสารให้ผู้ใช้งานได้รับทราบถึงแนวทางปฏิบัติ

3.3 ผู้ดูแลระบบเทคโนโลยีสารสนเทศและผู้เกี่ยวข้อง ต้องจัดเตรียมระบบสารสนเทศให้รองรับการทำงานจากภายนอกที่ตั้ง สช.

3.4 การเข้าถึงระบบบริหารจัดการสารสนเทศของผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องเชื่อมต่อผ่านระบบเครือข่ายที่มีความปลอดภัย และดำเนินการผ่านระบบ Virtual Private Network (VPN) ที่ สช. จัดหาให้เท่านั้น

3.5 ผู้ใช้งานต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีการควบคุมและตรวจสอบการใช้งาน หรือการเข้าถึงระบบตามสิทธิ์ที่ได้รับอย่างเคร่งครัด

หมวดที่ 4 การทำธุรกรรมอิเล็กทรอนิกส์ และ e-Payment

วัตถุประสงค์

เพื่อให้การทำธุรกรรมอิเล็กทรอนิกส์ของ สช. มีความปลอดภัย น่าเชื่อถือ

ผู้ปฏิบัติ ผู้บริหาร บุคลากร

ข้อปฏิบัติ

1. **การทำธุรกรรมอิเล็กทรอนิกส์**
   - 1.1 การดำเนินการธุรกรรมอิเล็กทรอนิกส์ต้องเชื่อมต่อผ่านระบบอินเทอร์เน็ตที่มีการรักษาความปลอดภัย
   - 1.2 อุปกรณ์คอมพิวเตอร์ที่ใช้ในการดำเนินธุรกรรมอิเล็กทรอนิกส์ต้องมีระบบ Antivirus ป้องกัน
   - 1.3 ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์ ซอฟต์แวร์ที่มีการฝัง Malicious Mobile Code หรือข้อมูลที่มีมัลแวร์ติดตั้ง มาใช้งาน
   - 1.4 ห้ามใช้งานระบบจำรหัสผ่านอัตโนมัติในการทำธุรกรรมอิเล็กทรอนิกส์
   - 1.5 ผู้ใช้งานต้องตรวจสอบที่อยู่เว็บไซต์ในการทำธุรกรรมอิเล็กทรอนิกส์ว่าเป็นที่อยู่ (URL) ที่ถูกต้อง เพื่อป้องกันเว็บไซต์เลียนแบบ (Phishing website)
2. **การทำ e-Payment**
   - 2.1 ผู้ใช้งานต้องตรวจสอบที่อยู่เว็บไซต์ในการทำ e-payment ว่ามีความปลอดภัย มีการเข้ารหัส และมีใบรับรองอิเล็กทรอนิกส์ (SSL Certificate) ที่ถูกต้อง
   - 2.2 ต้องเก็บรักษาบัญชีผู้ใช้งาน e-payment ให้มีความปลอดภัย
   - 2.3 กำหนดรหัสผ่านในการทำ e-payment ให้มีความซับซ้อน ยากต่อการคาดเดา ใช้ตัวอักษรผสมทั้งตัวเล็กและใหญ่ ตัวเลขอารบิก เป็นส่วนประกอบ
   - 2.4 ตรวจสอบความถูกต้อง ครบถ้วน ของข้อมูล ก่อนยืนยัน e-payment

หมวดที่ 5 การใช้ลายเซ็นดิจิทัล (Digital Signature) สำหรับการอนุมัติ

วัตถุประสงค์

เพื่อให้การใช้ลายเซ็นดิจิทัล (Digital Signature) สำหรับการอนุมัติ มีความปลอดภัยน่าเชื่อถือ

ผู้ปฏิบัติ ผู้บริหาร บุคลากร และผู้ที่เกี่ยวข้อง

ข้อปฏิบัติ

1. ต้องมีการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบลายเซ็นดิจิทัล
2. ผู้ใช้ต้องเก็บรักษาบัญชีผู้ใช้งานให้มีความปลอดภัย
3. กำหนดรหัสผ่านในการเข้าระบบ ให้มีความซับซ้อน ยากต่อการคาดเดา ใช้ตัวอักษรผสมทั้งตัวเล็กและใหญ่เป็นส่วนประกอบ
4. ระบบลายเซ็นดิจิทัลต้องมี Log ของการใช้งานลายเซ็นที่เชื่อมโยงกับรายการที่อนุมัติ โดยมีข้อมูลประกอบด้วยข้อมูลเจ้าของลายเซ็นดิจิทัล, วันและเวลาที่ลงลายมือชื่อ, วัตถุประสงค์ในการลงลายมือชื่อ เป็นอย่างน้อย
5. ตรวจสอบความถูกต้องของข้อมูล ก่อนยืนยัน

หมวดที่ 6 การรักษาชั้นความลับและระดับชั้นความลับของข้อมูล

วัตถุประสงค์

เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นๆ ที่มีต่อ สช.

ผู้ปฏิบัติ ผู้บริหาร บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. และผู้ที่เกี่ยวข้อง

ข้อปฏิบัติ

1. ต้องดำเนินการจัดระดับชั้นข้อมูลของข้อมูลหรือสารสนเทศที่อยู่ภายใต้การดูแลของตนเองโดยพิจารณาถึงข้อกำหนดทางด้านกฎหมาย คุณค่า ระดับความสำคัญและระดับความอ่อนไหว เพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต โดยให้ขั้นตอนการปฏิบัติการรักษาชั้นความลับและระดับชั้นความลับของข้อมูล
2. ต้องดำเนินการจัดการข้อมูลหรือสารสนเทศของสำนักงาน เช่น การบ่งชี้ข้อมูลหรือสารสนเทศ การเข้าถึงและการใช้งานข้อมูล การบันทึกข้อมูล การแจกจ่าย การทำลาย เป็นต้น ตามที่ระบุไว้ในขั้นตอนการปฏิบัติการรักษาชั้นความลับและระดับชั้นความลับของข้อมูล

หมวดที่ 7 การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)

วัตถุประสงค์

เพื่อให้บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. รับทราบแนวทางในการคุ้มครองข้อมูลส่วนบุคคลของ สช. ในการจัดเก็บข้อมูลของผู้ใช้งาน

ผู้ปฏิบัติ บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. และผู้ที่เกี่ยวข้อง

ข้อปฏิบัติ

1. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลของผู้ใช้งานต้องดำเนินการจัดเก็บข้อมูลด้วยวิธีที่ไม่ขัดต่อกฎหมาย และจัดเก็บเฉพาะเท่าที่จำเป็นตามหน้าที่และวัตถุประสงค์ในการดำเนินงานของ สช. เท่านั้น ในกรณีจำเป็นที่ต้องใช้ข้อมูลส่วนบุคคลของผู้ใช้งานเพื่อวัตถุประสงค์อื่นต้องดำเนินการแจ้งให้ผู้ใช้งานทราบและให้ความยินยอมก่อนเก็บรวบรวมข้อมูลนั้น เว้นแต่เป็นกรณีที่กฎหมายกำหนด
2. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลของผู้ใช้งานต้องจัดเก็บข้อมูลโดยคำนึงถึงถึงความถูกต้อง ครบถ้วน และความเป็นปัจจุบันของข้อมูลที่จัดเก็บ
3. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลดำเนินการ รวบรวม จัดเก็บ ใช้ ข้อมูลส่วนบุคคลเพียงเท่าที่จำเป็น เช่น ชื่อสกุล ที่อยู่ เลขประจำตัวประชาชน เบอร์โทรศัพท์ อีเมล์ เป็นต้น เพื่อใช้ในการติดต่อให้บริการ ประชาสัมพันธ์ หรือให้ข้อมูลข่าวสารต่าง ๆ รวมทั้งสำรวจความคิดเห็น และหากภายหลังมีการเปลี่ยนแปลงวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคล สช.จะแจ้งให้ผู้ใช้งานทราบ โดยประกาศไว้ในเว็บไซต์ของ สช. และทำการบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐานด้วย
4. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ให้กับบุคคลภายนอกโดยเด็ดขาด เว้นแต่ในกรณีดังนี้จะได้รับอนุญาต หรือได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นการปฏิบัติตามคำสั่งศาล หรือกรณีอื่นที่เป็นไปตามกฎหมาย
5. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลต้องควบคุมผู้ให้บริการภายนอกที่สามารถเข้าถึงหรือดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลให้เก็บรักษาข้อมูลส่วนบุคคลให้เป็นความลับและนำข้อมูลส่วนบุคคลไปใช้นอกเหนือกิจกรรมของ สช.
6. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลอย่างเหมาะสมโดยสอดคล้องกับการรักษาความลับของข้อมูลส่วนบุคคลเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิ์หรือโดยไม่ชอบด้วยกฎหมาย
7. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลจะเปิดเผยนโยบายการคุ้มครองข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ของ สช. และหากเจ้าของข้อมูลประสงค์จะตรวจความมีอยู่ ลักษณะของข้อมูลส่วนบุคคล หรือวัตถุประสงค์ของการนำข้อมูลไปใช้สามารถติดต่อมายัง สช. ได้ผ่านทางโทรศัพท์ของ สช.

8. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลจะเปิดเผยรายละเอียดข้อมูลส่วนบุคคลต่อเมื่อได้รับคำร้องขอจากเจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย โดยการยื่นคำร้องตามหลักเกณฑ์และวิธีการที่ สช. กำหนด เมื่อ สช. ได้รับคำร้องดังกล่าวแล้วจะดำเนินการให้แล้วเสร็จภายในระยะเวลาอันควร ในกรณีที่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย มีการคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆ เช่น การแจ้งดำเนินการปรับปรุงแก้ไขข้อมูล ส่วนบุคคล หรือลบข้อมูลส่วนบุคคล เป็นต้น สช. จะดำเนินตามที่ร้องขอและการบันทึกหลักฐานคำคัดค้านดังกล่าวไว้เป็นหลักฐานด้วย

9. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลในการทำสถิติเกี่ยวกับประชากร เช่น เพศ อายุ อาชีพ ซึ่งอาจจะสามารถเชื่อมโยงกับข้อมูลที่ระบุตัวบุคคลได้นั้น และ หากมีการใช้งานสถิติเกี่ยวกับประชากรเพื่อใช้ในการติดต่อให้บริการ ประชาสัมพันธ์ หรือให้ข้อมูลข่าวสารต่าง ๆ รวมทั้งสำรวจความคิดเห็นในกิจการหรือกิจกรรมของ สช. ห้ามกระทำการใด ๆ แตกต่างจากที่ระบุในวัตถุประสงค์ของการเก็บรวบรวมข้อมูลไว้ตามข้างต้น

10. เจ้าหน้าที่ของ สช. ที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายฉบับนี้ในการคุ้มครองข้อมูลส่วนบุคคลของ สช. ที่ประกาศใช้อย่างเคร่งครัด

หมวดที่ 8 การควบคุมและจัดการสินทรัพย์ดิจิทัล (Digital Asset)

วัตถุประสงค์

เพื่อให้มีการระบุสินทรัพย์ของ สช. และกำหนดหน้าที่ความรับผิดชอบ สำหรับการจัดการอย่างเหมาะสม

ผู้ปฏิบัติ ผู้บริหาร บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. และผู้ที่เกี่ยวข้อง

ข้อปฏิบัติ

1. ต้องทำบัญชีสินทรัพย์ซึ่งรวมถึงครุภัณฑ์คอมพิวเตอร์ ซอฟต์แวร์ ฐานข้อมูล ไฟล์ลิขสิทธิ์ และบัญชีข้อมูลที่เก็บไว้ในสื่อต่าง ๆ ของ สช. และแบ่งประเภท เพื่อใช้กำหนดมูลค่าสินทรัพย์ โดยระบุผู้เป็นเจ้าของสินทรัพย์แต่ละชนิดตามที่กำหนดไว้ และต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนด อย่างน้อยปีละ 1 ครั้ง
2. การใช้งานสินทรัพย์ต้องใช้งานด้วยความระมัดระวัง บำรุงรักษาให้เหมาะสมกับการใช้งาน ตามประกาศ สช.
3. เมื่อสิ้นสุดการจ้างงาน หมดสัญญาหรือสิ้นสุดข้อตกลงต่อกัน ผู้บริหาร บุคลากร และบุคลากรภายนอกที่ปฏิบัติงานให้ สช. ที่ใช้สินทรัพย์อันเป็นสิทธิ์การใช้งานของ สช. ต้องคืนสินทรัพย์ของ สช. ทั้งหมดที่ถือครองให้ครบถ้วน