ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ๒๑ / ๒๕๖๕

เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์

(Information and Cyber Security Policy)

.....

โดยที่เป็นการสมควรปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ให้มีความสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ จึงให้ยกเลิกประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ๔/๒๕๖๔ เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ลงวันที่ ๓๑ มีนาคม พ.ศ. ๒๕๖๔ และให้ใช้นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) แนบท้ายประกาศฉบับนี้แทน

ทั้งนี้ ให้มีผลนับตั้งแต่วันที่ ๑๖ กันยายน พ.ศ. ๒๕๖๕ เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๖๕

(นายสุพจน์ เธียรวุฒิ)

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

นโยบายการปฏิบัติงาน (Policy)

นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์

(Information and Cyber Security Policy)

(PO-S19-002)

แก้ไขครั้งที่ 2

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

Digital Government Development Agency (Public Organization)

การควบคุมเอกสาร

ผู้เรียบเรียง/ผู้จัดทำ	ผู้ตรวจสอบ/ผู้ทบทวน	ผู้อนุมัติ
นางสาววาสนา หมั่นสระเกษ	นางสาวทิสวรรณ ชูปัญญา	นายสุพจน์ เธียรวุฒิ
ผจก. ส่วนพัฒนาองค์กรและบริหารคุณภาพ	ผู้อำนวยการฝ่ายกลยุทธ์องค์กร	ผู้อำนวยการ สพร.

ครั้งที่	วันที่	รายละเอียดการแก้ไข
00	22/04/62	ประกาศใช้ โดยอ้างอิง - ดศ ๐๒๐๗.๔/๑๐๕๕๘ เรื่องแจ้งผลการพิจารณานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพร. - ประกาศ สพร. ที่ ๑๓-๒๕๖๑ เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) - รายงานการประชุมฝ่ายบริหาร สพร. ครั้งที่ ๑๐/๒๕๖๑
01	11/05/64	ประกาศใช้ โดยอ้างอิง - ดศ(สพธอ) ๕๑๑.๙๗/๐๐๙๒ เรื่องแจ้งผลการพิจารณานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (ฉบับทบทวน) - ประกาศ สพร. ที่ ๔-๒๕๖๔ เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy _IS Policy) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
02	16/09/65	ปรับปรุงรายละเอียดเอกสาร - เปลี่ยนชื่อเอกสารจาก “นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy)” เป็น “นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy)” - ปรับปรุงเนื้อหาให้มีความสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

สารบัญ

หัวข้อเรื่อง

หน้า

PO-S19-002 นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์

(Information and Cyber Security Policy)

1. บทนำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือต่อไปนี้เรียกว่า “สำนักงาน” มีวิสัยทัศน์ “***สพร. เป็นกลไก สนับสนุน เชื่อมโยง การขับเคลื่อนรัฐบาลดิจิทัล Enabling Agile Governments”*** อีกทั้งยังมีความมุ่งมั่นและทำงานในเชิงรุก เพื่อยกระดับการบริการด้าน Digital Government ของหน่วยงานภาครัฐ โดยมีภารกิจสำคัญ 9 ด้าน ได้แก่

1) พัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานทางเทคโนโลยีดิจิทัลและระบบการให้บริการหรือแอปพลิเคชันพื้นฐานในส่วนที่เกี่ยวข้องกับรัฐบาลดิจิทัล
2) จัดทำมาตรฐาน แนวทาง มาตรการ หลักเกณฑ์ และวิธีการทางเทคโนโลยีดิจิทัลและกระบวนการดำเนินงานเพื่อให้สามารถเชื่อมโยงข้อมูลและระบบการทำงานระหว่างกันของหน่วยงานได้อย่างมีประสิทธิภาพและมีความสอดคล้องกัน
3) ส่งเสริมและสนับสนุนการบูรณาการและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ การเปิดเผยข้อมูลภาครัฐผ่านเทคโนโลยีดิจิทัล และเป็นศูนย์กลางการแลกเปลี่ยนทะเบียนข้อมูลดิจิทัลภาครัฐเพื่ออำนวยความสะดวกในการให้บริการประชาชนและในการดำเนินงานของหน่วยงานของรัฐ
4) ส่งเสริม สนับสนุนให้หน่วยงานของรัฐให้บริการดิจิทัลแก่ผู้เกี่ยวข้อง
5) พัฒนาบริการดิจิทัลยีดิจิทัลและระบบการให้บริการหรือแอฟพลิเคชันพื้นฐานในส่วนที่เกี่ยวข้องกับรัฐบาลดิจิทัลภาครัฐแบบเบ็ดเสร็จ ณ จุดเดียวที่ประชาชนสามารถเข้าถึงบริการได้อย่างสะดวก รวดเร็ว และมั่นคงปลอดภัย
6) ให้คำปรึกษาและสนับสนุนหน่วยงานของรัฐในการบริหารจัดการโครงการด้านเทคโนโลยีดิจิทัล รวมถึงส่งเสริม สนับสนุน ให้บริการวิชาการ และจัดอบรมเพื่อยกระดับทักษะความรู้ความสามารถของเจ้าหน้าที่ของรัฐด้านรัฐบาลดิจิทัล
7) ศึกษา วิจัย สร้างนวัตกรรม และส่งเสริมและสนับสนุนงานวิชาการ งานวิจัยและนวัตกรรมในการพัฒนารัฐบาลดิจิทัล
8) สนับสนุนการดำเนินงานของหน่วยงานของรัฐที่รับผิดชอบในการจัดทำกรอบการจัดสรรงบประมาณบูรณาการประจำปีที่เกี่ยวกับการดำเนินงานด้านรัฐบาลดิจิทัล ตลอดจนสนับสนุนการติดตาม และประเมินผลการดำเนินงานตามแผนงานและแผนระดับชาติที่เกี่ยวกับรัฐบาลดิจิทัล
9) ดำเนินการอื่นเพื่อพัฒนารัฐบาลดิจิทัลตามที่กฎหมายกำหนดหรือคณะรัฐมนตรีมอบหมาย

ซึ่งถือเป็นองค์ประกอบหลักที่สำคัญของการพัฒนาประเทศไทยไปสู่การเป็น “รัฐบาลดิจิทัล” เพื่อให้สำนักงานปฏิบัติตามภารกิจได้อย่างมีประสิทธิภาพและมีประสิทธิผล ดังนั้นจึงได้จัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) ขึ้นเพื่อเป็นมาตรฐานและแนวปฏิบัติให้ระบบสารสนเทศของสำนักงานเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ทั้งจากภายในและภายนอก ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจก็ตาม อันเป็นการลดความเสียหายต่าง ๆ และรักษาไว้ซึ่งความสามารถในการดำเนินงานได้อย่างมีประสิทธิภาพ

2. หลักการ

ระบบสารสนเทศ เทคโนโลยี และการสื่อสารที่ทางสำนักงานได้จัดเตรียมให้ใช้งานจำเป็นจะต้องมีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินกิจการ ซึ่งการดูแลรักษาและการป้องกันมุ่งหมายไปในทางความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการธำรงไว้ซึ่งการรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ โดยอธิบายได้ ดังนี้

การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้สินทรัพย์สามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งสินทรัพย์นั้นด้วย ดังนั้น ในการรักษาความลับจำเป็นจะต้องมีการควบคุมทั้ง ทางกายภาพและทางเทคนิค โดยผู้ที่ไม่มีสิทธิจะต้องไม่สามารถเข้าถึงสินทรัพย์นั้นได้และสินทรัพย์จำเป็นจะต้องมีการจำแนกและกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ที่ถือครองสินทรัพย์ปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น

ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้สินทรัพย์ถูกเปลี่ยนแปลงแก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิที่จะแก้ไขสินทรัพย์เหล่านั้น ดังนั้นการควบคุมและป้องกันจึงต้องประกอบด้วยการกำหนดสิทธิในการแก้ไข กำหนดสิทธิในการเข้าถึง และจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีสินทรัพย์และทางเทคนิคประกอบด้วย

ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้มีสิทธิสามารถเข้าใช้งานสินทรัพย์นั้นได้เมื่อยามต้องการใช้งาน ซึ่งมีทั้งในทางกายภาพและทางเทคโนโลยี ได้แก่ การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้น เมื่อผู้ใช้ต้องการจะรับหรือส่ง ระบบจำเป็นที่จะต้องสามารถให้บริการได้ตลอดเวลานั้น เป็นต้น

นอกจากที่กล่าวมาแล้วยังประกอบด้วยเรื่อง ผู้รับผิดชอบต่อการกระทำ (Accountability) ซึ่งหมายถึงสินทรัพย์จำเป็นจะต้องมีผู้รับผิดชอบและสามารถอธิบายได้ถึงผลที่เกิดขึ้นไม่ว่าผลนั้นเกิดจากการกระทำจากบุคคลหรือสิ่งอื่นใด

3. วัตถุประสงค์ (Objective)

เพื่อให้ระบบสารสนเทศของสำนักงานเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สำนักงานจึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติ (Procedure) วิธีการปฏิบัติ (Work Instruction) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังนี้

3.1 เพื่อให้สำนักงานมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีความสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่ถูกต้อง

3.2 เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอ้างอิงตามนโยบายมาตรฐานที่สำนักงานปรับใช้ และนโยบายอื่น ๆ ที่เกี่ยวข้อง

3.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้คณะกรรมการ ผู้บริหาร เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบและบุคลากรภายนอกที่ปฏิบัติงานให้สำนักงานตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและปฏิบัติตามอย่างเคร่งครัด

3.4 เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน

3.5 เพื่อใช้เป็นแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศขั้นต่ำ ในการดำเนินการด้านการรักษาความปลอดภัยไซเบอร์ ของสำนักงานและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

4. ขอบเขต (SCOPE)

นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) ฉบับนี้ เป็นการดำเนินการสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระบบบริหารจัดการด้านเทคโนโลยีสารสนเทศ (ISO/IEC 27001) โดยมีผลบังคับใช้กับสารสนเทศของสำนักงาน ผู้ทำหน้าที่ดูแลสินทรัพย์ ผู้ใช้สินทรัพย์ คณะกรรมการ ผู้อำนวยการ เจ้าหน้าที่ ลูกจ้าง และโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับของสำนักงาน โดยมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลสินทรัพย์จะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของสำนักงาน

5. การเผยแพร่และการทบทวน

นโยบายนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบอินทราเน็ต อีเมล หรือช่องทางการสื่อสารอื่นภายในองค์กร เพื่อให้เจ้าหน้าที่ทุกระดับในสำนักงานได้รับทราบ โดยเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด ซึ่งนโยบายนี้ต้องถูกทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

6. คำนิยาม (DEFINITIONS)

คำศัพท์	ความหมาย
สำนักงาน	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
คณะกรรมการ	คณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้อำนวยการ / ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO)	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เจ้าหน้าที่	บุคคลผู้ที่สำนักงานบรรจุและแต่งตั้งเป็นเจ้าหน้าที่
ลูกจ้าง	บุคคลผู้ที่สำนักงานบรรจุและแต่งตั้งเป็นลูกจ้าง โดยมีสัญญาจ้างให้ปฏิบัติงานเป็นการชั่วคราวและมีกำหนดระยะเวลาและสิ้นสุดที่แน่นอน
นิสิตและนักศึกษาฝึกงาน	นิสิตและนักศึกษาที่สำนักงานอนุญาตให้เข้ามาทดลองปฏิบัติงานโดยมีช่วงระยะเวลาที่กำหนดไว้
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน
คณะบริหารระบบบริหารจัดการมาตรฐานของสำนักงาน (Standards Committee)	ผู้ที่ได้รับการแต่งตั้งให้ที่มีหน้าที่รับผิดชอบในการกำกับดูแล การดำเนินของระบบบริหารจัดการมาตรฐานของสำนักงาน รวมทั้งพิจารณา ติดตาม และประเมินผลตามมาตรฐานของสำนักงาน
ผู้ใช้งาน (User)	คณะกรรมการ ผู้อำนวยการ เจ้าหน้าที่ ลูกจ้าง นิสิตและนักศึกษาฝึกงานที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหาร หรือดูแล รักษาระบบสารสนเทศของสำนักงานตามสิทธิและหน้าที่ความรับผิดชอบ
สิทธิของผู้ใช้งาน	สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน ดังนี้ - สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ เจ้าหน้าที่ ลูกจ้าง นิสิตและนักศึกษาฝึกงานทั้งหมดที่ใช้งานระบบสารสนเทศพื้นฐานของสำนักงาน ผู้ใช้งานต้องขออนุญาตจากผู้จัดการส่วน/หัวหน้ากลุ่มงานขึ้นไป โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่สำนักงานกำหนด - สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว

คำศัพท์	ความหมาย
อุปกรณ์สารสนเทศ (Computing Device)	อุปกรณ์ที่มีหน่วยประมวลผล หน่วยความจำ ส่วนบันทึกข้อมูล ส่วนการเชื่อมต่อเครือข่าย ส่วนรับข้อมูล และส่วนแสดงผล ได้แก่ - คอมพิวเตอร์แบบตั้งโต๊ะ เช่น Desktop Computer เป็นต้น - คอมพิวเตอร์แบบพกพา เช่น Notebook, Netbook เป็นต้น รวมถึงอุปกรณ์ต่อพ่วง เช่น Mouse, Keyboard, Monitor เป็นต้น
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
ผู้ให้บริการภายนอก	บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ **หรือ** เป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **หรือ** เป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **หรือ** ข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ **ทั้งนี้** ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์และบริการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
อุปกรณ์เคลื่อนที่ (Mobile Device)	อุปกรณ์สารสนเทศแบบพกพา ที่มีขนาดเล็กสามารถใช้เพียงมือเดียวในการใช้งานส่วนของการรับข้อมูลเป็นแบบสัมผัส โดยไม่ต้องใช้ Keyboard และสามารถเชื่อมต่อเครือข่ายแบบไร้สาย เครือข่ายโทรศัพท์ได้ เช่น Smartphone, Tablet เป็นต้น
เจ้าของข้อมูล (Information Owner)	ผู้ซึ่งรับผิดชอบข้อมูลของสำนักงานซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย
เจ้าของระบบงาน (System Owner)	ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในสำนักงาน
หน่วยงานภายนอก / ผู้ให้บริการภายนอก / บุคคลภายนอก	ลูกค้าหรือผู้ให้บริการภายนอก (Third Party) หรือบุคคลภายนอก ที่ใช้งานระบบสารสนเทศของสำนักงาน ได้เป็นครั้งคราวหรือตามสัญญา
ความมั่นคงปลอดภัยด้านสารสนเทศ	การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความ

คำศัพท์	ความหมาย
(Information Security)	ถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
ข้อมูล (Data)	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ เช่น สื่อสิ่งพิมพ์, รายงาน, หนังสือ, แผนที่, แผนผัง, ภาพวาด, ภาพถ่าย, CD, DVD, Hard disk drive, Flash drive, การบันทึกโดยอุปกรณ์คอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
สื่อสังคมออนไลน์ (Social Media)	สังคมออนไลน์ที่ผู้ใช้อินเทอร์เน็ตสามารถแลกเปลี่ยนประสบการณ์ซึ่งกันและกันโดยใช้สื่อต่าง ๆ เป็นตัวแทนในการสนทนา ได้แก่ - Social Networking เช่น Facebook, Twitter, LinkedIn, Instagram ฯลฯ - Publish เช่น Wikipedia, Tumblr, Online NEWS ฯลฯ - Pictures & Video Sharing เช่น YouTube, Flickr, Photobucket ฯลฯ Instant Messaging เช่น Microsoft Team, Line, Skype ฯลฯ
ระบบเครือข่าย (Network System)	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูลระหว่าง ระบบคอมพิวเตอร์ ได้แก่ ระบบ LAN (Local Area Network) ระบบ WLAN (Wireless LAN) เครือข่าย Intranet และเครือข่าย Intranet เป็นต้น
ระบบ LAN	ระบบเครือข่ายแบบเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันในระยะจำกัด เช่น ในอาคารเดียวกัน หรือบริเวณเดียวกันที่สามารถลากสายถึงกันได้โดยตรง
ระบบเครือข่ายไร้สาย (Wireless LAN : WLAN)	ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ รวมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่าย โดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทน
เครือข่าย Internet	ระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ มีการเชื่อมต่อระหว่างเครือข่ายหลาย ๆ เครือข่ายทั่วโลก
เครือข่าย Intranet	ระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในสำนักงานเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงาน
ระบบสารสนเทศ (Information System)	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น

คำศัพท์	ความหมาย
ระบบงานภายในของสำนักงาน	ระบบงานพื้นฐานของสำนักงานที่อนุญาตให้ผู้ใช้งานสามารถเข้าถึงได้โดยผ่านขั้นตอนและวิธีการที่ปลอดภัยตามที่สำนักงานกำหนด
ระบบบริหารจัดการบริการของสำนักงาน	ระบบงานที่ผู้ใช้งานที่เป็นผู้ดูแลระบบสามารถเข้าถึงหรือควบคุมการให้บริการต่าง ๆ ของสำนักงาน เช่น NetApp, vCenter, SolarWinds เป็นต้น
โปรแกรมประยุกต์ หรือ แอปพลิเคชัน (Application)	โปรแกรมประเภทหนึ่งที่ถูกสร้างขึ้นสำหรับใช้งานเฉพาะทาง ได้แก่ ระบบใบลา ระบบจองห้องประชุม ระบบ MailGoThai และระบบ e-Saraban เป็นต้น
พื้นที่มั่นคงปลอดภัย (Secure Areas)	พื้นที่ที่มีการควบคุมการเข้าถึง และมีระบบป้องกันจากภัยคุกคามต่าง ๆ ได้แก่ ศูนย์คอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบ
การเข้าถึง	การเข้าสถานที่ การใช้งานทางอิเล็กทรอนิกส์หรือกายภาพ รวมถึงการรับรู้ซึ่งข้อมูล
การควบคุมการเข้าถึง	การอนุญาต การกำหนดสิทธิ การเปลี่ยนแปลง การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การตรวจสอบ การอนุมัติ และการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง
สินทรัพย์ (Asset)	สิ่งที่มีคุณค่าหรือมูลค่าต่อสำนักงานและเป็นทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่สำนักงานเป็นเจ้าของ, เช่า, ว่าจ้าง, พัฒนา หรือจัดซื้อ โดยแบ่งแยกออกเป็นประเภทต่าง ๆ ได้ดังนี้ 1) ฮาร์ดแวร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์เครือข่าย และอุปกรณ์ที่เกี่ยวข้อง เป็นต้น 2) ซอฟต์แวร์ (Software) เช่น ระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล เป็นต้น 3) ข้อมูล (Information) เช่น ข้อมูลสำคัญ ข้อมูลส่วนบุคคล ที่จัดเก็บในระบบ การจัดเก็บ log การตั้งค่า Configuration สำคัญ การสำรองข้อมูล เป็นต้น 4) บุคลากร (People) เช่น เจ้าหน้าที่ ลูกจ้าง ผู้รับจ้างภายนอก และผู้ที่เกี่ยวข้อง เป็นต้น 5) ระบบงานบริการ (Service) เช่น บริการจากหน่วยงานภายนอก เป็นต้น
การเปลี่ยนแปลง (Change Management)	กระบวนควบคุมการแก้ไขเปลี่ยนแปลงระบบงานสารสนเทศ การเปลี่ยนแปลงองค์ประกอบของบริการ (CI) การเปลี่ยนแปลงบริการที่อยู่ในความรับผิดชอบของผู้ให้บริการหรือส่วนงานภายในสำนักงาน และการเพิ่มบริการใหม่ของสำนักงาน
การจัดการทรัพยากรระบบ (Capacity Management)	การบริหารจัดการทรัพยากรและการกำหนดค่าขีดความสามารถของเจ้าหน้าที่ แผนการดำเนินงาน และอื่น ๆ

คำศัพท์	ความหมาย
แผนการจัดการทรัพยากรระบบ (Capacity Plan)	แผนการจัดการทรัพยากรระบบของบริการในการติดตามสถานะปัจจุบันของทรัพยากรที่ใช้งาน และวางแผนทรัพยากรสำหรับอนาคตอย่างเพียงพอ
เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)	กรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ซึ่งมีแนวโน้มทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
ความต่อเนื่องในการดำเนินงานของสำนักงาน(Business Continuity Management : BCM)	แนวทางในการบริหารจัดการธุรกิจได้อย่างต่อเนื่อง เมื่อสำนักงานอยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของสำนักงาน ที่สำคัญได้รับการวางแผนความต่อเนื่องในการดำเนินงานของสำนักงาน (Business Continuity Plan หรือ BCP) และแผนสำรองฉุกเฉิน (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม
การประเมินความเสี่ยง	กระบวนการทั้งหมดในการวิเคราะห์และประเมินความเสี่ยง

7. นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy)

แบ่งเป็น 14 หมวด สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระบบบริหารจัดการด้านเทคโนโลยีสารสนเทศ (ISO/IEC 27001) ของสำนักงาน ดังนี้

หมวด 1 นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์

(Information and Cyber Security Policy)

วัตถุประสงค์

นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ (Information and Cyber Security Policy) ฉบับนี้ ถูกจัดทำขึ้น เพื่อกำหนดทิศทางหรือมาตรการ ประเมินความเสี่ยง รับมือ การปฏิบัติตามกรอบความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ ต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบงานสารสนเทศ และการบริหารจัดการ เพื่อผลักดันให้มีการควบคุมภายในด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง (Risk Based Approach) เพื่อสนับสนุนให้ผู้ใช้งานตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ รวมถึงความสำคัญในการบริหารจัดการความเสี่ยงของสำนักงาน

ผู้ปฏิบัติ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์มหาชน) (สพร.) และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน

ข้อปฏิบัติ

1. ผู้อำนวยการเป็นผู้รับผิดชอบความเสี่ยงความเสียหายต่อระบบสารสนเทศของสำนักงาน ซึ่งเกิดจากการละเลย ละเว้นการควบคุมความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์
2. ให้การสนับสนุนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy)
3. ต้องจัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยการประเมินความเสี่ยงดังกล่าวต้องพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจ การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้นตามที่สำนักงานกำหนดไว้

4. ต้องกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น
5. ต้องจัดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจ และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ของสำนักงาน
6. ต้องกำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อรับมือ ตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
7. ต้องประเมินผลสัมฤทธิ์ของนโยบายที่ประกาศใช้ เพื่อนำมาปรับปรุงนโยบาย แผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต
8. นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ ต้องจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์และขอบเขต ต้องได้รับการอนุมัติ เพื่อประกาศใช้และถือปฏิบัติทั่วทั้งสำนักงานโดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของสำนักงานตั้งแต่ คณะกรรมการ ผู้อำนวยการ เจ้าหน้าที่ ผู้ใช้งานและนิสิตนักศึกษาฝึกงาน หน่วยงาน/บุคคลภายนอก (External Party) ที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของสำนักงาน ตลอดจนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน
9. ต้องจัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัยของสำนักงาน
10. ต้องสนับสนุนให้มีการอบรมเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง
11. ต้องมีการกำหนดแผนการตรวจสอบการปฏิบัติตามนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์โดยผู้ตรวจประเมินภายใน หรือผู้ตรวจสอบจากภายนอกอย่างน้อยปีละ 1 ครั้ง และติดตามผลการประเมินเพื่อปรับปรุง ป้องกัน หรือแก้ไขปัญหาที่พบ
12. ต้องมีการนำเสนอผลการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ ต่อผู้อำนวยการ

หมวด 2 โครงสร้างทางด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับสำนักงาน (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับส่วนงานต่าง ๆ ภายในสำนักงาน และเพื่อเป็นแนวทางการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) แบ่งเป็น 2 ส่วน คือ

- การจัดโครงสร้างภายในองค์กร (Internal Organization)
- นโยบายการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอก (Computing Device and Teleworking Policy)

การจัดโครงสร้างภายในองค์กร (Internal Organization)

วัตถุประสงค์

เพื่อกำหนดบทบาทหน้าที่ ความรับผิดชอบในการใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและมีความมั่นคงปลอดภัยทางไซเบอร์

ผู้ปฏิบัติ ผู้บริหารระดับฝ่ายบริหาร

อ้างอิง
1. ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) การจัดแบ่งส่วนงานและขอบเขตหน้าที่ของส่วนงาน ระดับส่วนและกลุ่มงานภายใน
2. หนังสือยินยอมรับเงื่อนไขการใช้งานระบบสารสนเทศของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)

ข้อปฏิบัติ

1. การกำหนดบทบาท และหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยทางไซเบอร์ (Information Security Roles and Responsibilities)

1.1 ต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับเจ้าหน้าที่ในหน่วยงานอย่างเป็นลายลักษณ์อักษร และให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) ที่กำหนดไว้

2. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

2.1 ต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์อย่างชัดเจน เพื่อให้มีการสอบทานระหว่างกันได้

นโยบายการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอก

(Computing Device and Teleworking Policy)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกสำนักงาน

ผู้ปฏิบัติ ผู้ใช้งานและส่วนงานที่เกี่ยวข้อง

อ้างอิง
1. นโยบายในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสม (Acceptable Use Policy)
2. เอกสารประกอบ การทำลายสื่อบันทึกข้อมูลสารสนเทศ
3. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

ข้อปฏิบัติ

1. **อุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ (Computing Device and Mobile Device)**
เพื่อเป็นมาตรการในการควบคุมบริหารจัดการความเสี่ยงสำหรับการใช้งานอุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ของสำนักงาน และของส่วนตัว ต้องปฏิบัติดังนี้

1.1. การใช้งานทั่วไปและการดูแลรักษา

1.1.1 อุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ของสำนักงานถือเป็นสินทรัพย์ของสำนักงาน โดยใช้เพื่อการดำเนินงานของสำนักงานเท่านั้น

1.1.2 ผู้ใช้งานจะต้องทำการลบข้อมูลตามขั้นตอนการปฏิบัติงานการทำลายสื่อบันทึกข้อมูลสารสนเทศก่อนการส่งคืนหรือส่งซ่อมอุปกรณ์สารสนเทศหรืออุปกรณ์เคลื่อนที่ของสำนักงาน

1.1.3 ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์สารสนเทศหรืออุปกรณ์เคลื่อนที่ของสำนักงาน โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

1.1.4 ห้ามมิให้ผู้ใช้งานใช้อุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ของสำนักงานผิดวัตถุประสงค์ และหลีกเลี่ยงการใช้งานในสภาวะแวดล้อมที่มีผลกระทบต่ออุปกรณ์

1.1.5 อนุญาตให้ใช้อุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ส่วนตัวในการเข้าถึงระบบงานภายในของสำนักงานเท่านั้น

1.1.6 ไม่อนุญาตให้นำอุปกรณ์สารสนเทศหรืออุปกรณ์เคลื่อนที่ส่วนตัวในการเข้าถึงระบบบริหารจัดการบริการของสำนักงาน

1.1.7 หากมีความจำเป็นต้องใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์เคลื่อนที่ส่วนตัวมาใช้เชื่อมต่อเครือข่ายภายในของสำนักงาน รวมทั้งเข้าถึงระบบงานภายใน ต้องได้รับการอนุญาตจากผู้บังคับบัญชาและต้องนำอุปกรณ์ส่วนตัวไปขึ้นทะเบียนกับสำนักงาน และต้องปฏิบัติตามขั้นตอนการใช้งานที่สำนักงานกำหนด

1.2. ความปลอดภัยทางด้านกายภาพของอุปกรณ์สารสนเทศของสำนักงาน

1.2.1 ผู้ใช้งานต้องจัดเก็บอุปกรณ์สารสนเทศของสำนักงานในที่ปลอดภัย ไม่วางทิ้งไว้ในที่เสี่ยงต่อการสูญหาย

1.2.2 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ในกรณีที่อุปกรณ์สารสนเทศสูญหายหรือเสียหาย ผู้ใช้งานต้องแจ้งต่อผู้ที่รับผิดชอบหรือผู้บังคับบัญชาทันที

1.2.3 หากผู้ใช้งานพ้นสภาพจากการเป็นผู้ปฏิบัติงานแล้วต้องส่งอุปกรณ์สารสนเทศทั้งหมดที่เคยได้รับ คืนให้แก่สำนักงาน

1.3. การบริหารจัดการข้อมูล

1.3.1 ข้อมูลของสำนักงานที่มีชั้นความลับซึ่งถูกจัดเก็บไว้ในอุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ ทั้งของสำนักงานและของส่วนตัว จะต้องปฏิบัติตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

1.4. การบริหารจัดการรหัสผ่าน (Password)

1.4.1 ผู้ใช้งานต้องปฏิบัติตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy) สำหรับอุปกรณ์สารสนเทศ

1.4.2 ผู้ใช้งานต้องตั้งค่า Lock screen ด้วยรหัสผ่านที่เดาสุ่มได้ยาก เช่น Pattern, Password หรือ Fingerprint เป็นต้น สำหรับอุปกรณ์เคลื่อนที่ และตั้งค่า Automatically Lock Screen Timeout ไม่มากกว่า 1 นาที หรือน้อยที่สุดที่อุปกรณ์สามารถตั้งค่าได้

1.5. การเก็บข้อมูลสำรอง

1.5.1 ผู้ใช้งานต้องปฏิบัติตามนโยบายการสำรองข้อมูล (Back up Policy)

1.6. การป้องกันซอฟต์แวร์ที่ไม่พึงประสงค์ (Malware)

1.6.1 ส่วนงานที่เกี่ยวข้องจะต้องมีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับอุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ของสำนักงาน

1.6.2 ในกรณีที่ผู้ใช้งานนำอุปกรณ์สารสนเทศส่วนตัวมาใช้ในระบบเครือข่ายของสำนักงาน จะต้องรับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ด้วยตนเอง

1.6.3 ห้ามผู้ใช้งานทำการปิด ยกเลิก กระทำการใด ๆ ที่อาจส่งผลต่อระบบการป้องกันไวรัส หรือระบบป้องกันมัลแวร์อื่นใด ที่ติดตั้งอยู่บนอุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่

1.6.4 หากพบว่าโปรแกรมป้องกันไวรัสในอุปกรณ์สารสนเทศหรืออุปกรณ์เคลื่อนที่ ทำงานผิดพลาด หรือไม่ทำงาน หรือสงสัยว่าอุปกรณ์สารสนเทศหรืออุปกรณ์เคลื่อนที่ติดมัลแวร์ หรือพบข้อมูลภัยคุกคาม ผู้ใช้งานต้องยุติการเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายและให้แจ้งส่วนงานที่รับผิดชอบ เพื่อดำเนินการทันที

1.6.5 ต้องตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลต่าง ๆ ได้แก่ External Harddisk, Flash drive ก่อนนำมาใช้งาน

1.6.6 ต้องตรวจสอบไฟล์ที่แนบมากับ E-mail หรือไฟล์ที่ Download มาจากอินเทอร์เน็ตด้วยโปรแกรมตรวจสอบไวรัสก่อนใช้งาน

1.6.7 ไม่ครอบครอง หรือพัฒนาโปรแกรมไวรัส หรือโปรแกรมที่ก่อกวน หรือโปรแกรมที่ส่งผลต่อระบบของสำนักงานหรือองค์กรอื่น ๆ โดยไม่ได้รับอนุญาต

1.6.8 ไม่ติดตั้งหรือใช้งานโปรแกรมเพิ่มเติมโดยไม่ได้รับอนุญาตในอุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ของสำนักงาน

1.6.9 ไม่ติดตั้งหรือใช้งานโปรแกรมที่สุ่มเสี่ยงกับการกระทำผิดกฎหมาย และละเมิดลิขสิทธิ์ในอุปกรณ์สารสนเทศและอุปกรณ์เคลื่อนที่ส่วนตัว

2. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

2.1 การควบคุมการเข้าถึงการปฏิบัติงานภายนอกสำนักงาน

2.1.1 ในกรณีที่ผู้ให้บริการภายนอก (Third Party) มีการ Remote Access เพื่อปฏิบัติงานชั่วคราว ส่วนงานที่รับผิดชอบต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship Policy) โดยควบคุมและตรวจสอบการใช้งาน หรือการเข้าถึงระบบตามสิทธิที่ได้รับอย่างเคร่งครัด

2.1.2 การเชื่อมต่อจากภายนอกสำนักงานจะต้องมีการดำเนินการที่ได้รับการอนุมัติและเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ที่สำนักงานจัดหาให้เท่านั้น

2.1.3 สิทธิในการใช้งาน Remote Access เพื่อปฏิบัติงานชั่วคราวเป็นสิทธิที่สำนักงานจะให้เฉพาะผู้ใช้งาน ผู้ให้บริการภายนอกเป็นการชั่วคราวเท่านั้น ไม่สามารถถ่ายโอนกันได้

2.1.4 ผู้ใช้งานจะต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้ามาใช้งาน Remote Access เข้าสู่ระบบสารสนเทศ ผู้ใช้งานจะต้องระบุวัตถุประสงค์ วิธีการเข้าถึง และขอบข่ายของการเข้าถึงที่แน่ชัด และจะต้องทำการอนุมัติให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น

2.1.5 สำนักงานมีสิทธิเรียกร้องค่าเสียหาย หากระบบคอมพิวเตอร์ของสำนักงานได้รับความเสียหาย โดยการติดไวรัสคอมพิวเตอร์ จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

หมวด 3 นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล
(Human Resource Security Policy)

วัตถุประสงค์

เพื่อให้สำนักงานมีกระบวนการในการคัดเลือกบุคลากร ฝึกอบรมและควบคุมการปฏิบัติงานของบุคลากรในสำนักงานอย่างเหมาะสมตลอดระยะเวลาการจ้างงานและเพื่อให้เข้าใจถึงหน้าที่ความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศของสำนักงาน

ผู้ปฏิบัติ ส่วนบริหารทรัพยากรบุคคล และส่วนงานที่เกี่ยวข้อง

อ้างอิง 1. เอกสารประกอบ ข้อบังคับคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยการบริหารงานบุคคล พ.ศ. 2562
2. การจัดการหน่วยงายภายนอกที่เกี่ยวข้อง (Third party Management)

ข้อปฏิบัติ

1. ก่อนการจ้างงาน

1.1 สำนักงานต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในคุณสมบัติของบุคลากรตามหน้าที่งานที่ได้รับมอบหมาย

1.2 ส่วนบริหารทรัพยากรบุคคล ต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นบุคลากรของสำนักงาน จะต้องมีการตรวจสอบประวัติอาชญากรรม หรืออื่น ๆ ตามเงื่อนไขที่เกี่ยวข้อง

1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

1.3.1 ส่วนบริหารทรัพยากรบุคคล ต้องกำหนดเงื่อนไขการจ้างงาน ที่รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน

1.3.2 ส่วนบริหารทรัพยากรบุคคล ต้องเตรียมข้อมูลที่เกี่ยวข้องกับ นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานเพื่อให้เจ้าหน้าที่และผู้ใช้งานที่เข้ามาใหม่ได้ศึกษาและลงนามรับทราบรวมถึงยอมรับสัญญาในการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายเหล่านั้น

1.3.3 เพื่อให้การบริหารจัดการ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ส่วนบริหารทรัพยากรบุคคล ต้องแจ้งให้ส่วนงานที่รับผิดชอบทราบทันทีเมื่อมีการดำเนินการดังต่อไปนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกหรือการสิ้นสุดการเป็นบุคลากรของสำนักงาน
- การโอนย้ายส่วนงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

1.4 คณะกรรมการ ผู้อำนวยการ เจ้าหน้าที่ และลูกจ้างใหม่ทุกคนที่เข้ามาปฏิบัติงานในสำนักงาน ต้องลงนามรับทราบและยินยอมปฏิบัติตามสัญญาการรักษาข้อมูลที่เป็นความลับของสำนักงาน และเอกสารอื่น ๆ ที่เกี่ยวข้อง ก่อนอนุญาตให้เริ่มงานหรือเข้าถึงและใช้งานข้อมูลสารสนเทศของสำนักงาน

2. ระหว่างการจ้างงาน

2.1 การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่เจ้าหน้าที่และลูกจ้าง (Information Security Education and Training)

2.1.1 ส่วนบริหารทรัพยากรบุคคล ต้องจัดให้มีการอบรมให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศแก่ผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

2.1.2 เจ้าหน้าที่ใหม่และลูกจ้างใหม่ของสำนักงานทุกท่าน ต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการบันทึกการอบรมและเก็บรวบรวมไว้ในระบบ

2.1.3 ส่วนงานที่รับผิดชอบต้องแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงาน

2.2 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process)

สำนักงานจัดให้มีมาตรการดำเนินการกับผู้ฝ่าฝืนหรือละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานที่เป็นความผิดทางวินัยภายใต้ข้อบังคับคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยการบริหารงานบุคคล พ.ศ. 2562

กรณีดำเนินกิจกรรมใด ๆ ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย หากเป็นการปฏิบัติโดยได้รับอนุญาตของสำนักงาน ถือเป็นข้อยกเว้น

3. การเปลี่ยนตำแหน่งหรือการสิ้นสุดการจ้างงาน

3.1 ส่วนงานที่รับผิดชอบ ต้องดำเนินการเปลี่ยนแปลง/เพิกถอน/ยกเลิก/ระงับ สิทธิของผู้ใช้งานที่เกี่ยวกับการใช้งานระบบสารสนเทศเพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะของการว่าจ้าง โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

3.2 เมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน ผู้ใช้งานจะต้องคืนสินทรัพย์อันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของสำนักงาน ได้แก่ อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่สำนักงานทันที

หมวด 4 การบริหารจัดการสินทรัพย์
(Asset Management)

วัตถุประสงค์

เพื่อให้มีการระบุสินทรัพย์ที่สำคัญของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นอย่างเหมาะสม โดยประกอบด้วย

- นโยบายการบริหารจัดการสินทรัพย์ (Asset Management Policy)
- นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)
- นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling Policy)

นโยบายการบริหารจัดการสินทรัพย์
(Asset Management Policy)

วัตถุประสงค์

เพื่อให้มีการระบุสินทรัพย์ที่สำคัญของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์อย่างเหมาะสม

ผู้ปฏิบัติ ผู้จัดการส่วน/หัวหน้ากลุ่มงาน ผู้ที่เกี่ยวข้องและ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน

อ้างอิง 1. เอกสารประกอบ นโยบายในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสม (Acceptable Use Policy)

2. เอกสารประกอบ การจัดการสินทรัพย์ (Asset Management)

ข้อปฏิบัติ

1. หน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

1.1 ต้องทำบัญชีสินทรัพย์ที่สำคัญซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่างๆ ของสำนักงานและแบ่งประเภทให้ชัดเจน เพื่อใช้ในการกำหนดมูลค่าสินทรัพย์ โดยระบุผู้เป็นเจ้าของสินทรัพย์แต่ละชนิดตามที่กำหนดไว้ และต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดอย่างน้อยปีละ 1 ครั้ง

1.2 ต้องมีทะเบียนสินทรัพย์ (Inventory) ที่ระบุสินทรัพย์ของบริการที่สำคัญทางสารสนเทศ และดูแลรักษาทะเบียนสินทรัพย์ให้เป็นปัจจุบัน โดยต้องมีข้อมูลอย่างน้อย ดังนี้

1) ชื่อ/คำอธิบายของสินทรัพย์
2) ฟังก์ชันที่สำคัญของสินทรัพย์ ของบริการที่สำคัญ
3) การระบุและการจัดลำดับความสำคัญของสินทรัพย์
4) เจ้าของและ/หรือผู้ดำเนินการของสินทรัพย์
5) ตำแหน่งทางกายภาพของสินทรัพย์แต่ละรายการ
6) การขึ้นต่อกันของสินทรัพย์ของบริการ

1.3 ต้องระบุขอบเขตเครือข่ายของบริการและ ระบบเชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

1.4 สินทรัพย์ที่เป็นซอฟต์แวร์สำหรับใช้เพื่อการดำเนินงานของสำนักงานซึ่งไม่มีค่าลิขสิทธิ์ หากส่วนงานใดมีการนำมาใช้งาน จะต้องจัดทำทะเบียนการใช้งาน

1.5 อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่สำนักงานเช่ามาใช้งาน ต้องกำหนดให้มีส่วนงานที่รับผิดชอบจัดทำบัญชีรายการของอุปกรณ์ ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่เช่ามาใช้งาน

1.6 การใช้งานสินทรัพย์ต้องใช้งานด้วยความระมัดระวัง บำรุงรักษาให้เหมาะสมกับการใช้งาน ตามประกาศสำนักงาน

1.7 เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลง เจ้าหน้าที่ ลูกจ้าง หรือหน่วยงานภายนอกที่ใช้สินทรัพย์ของสำนักงานต้องคืนสินทรัพย์ของสำนักงานทั้งหมดที่ตนเองถือครองให้ครบถ้วน

นโยบายการจัดชั้นความลับของสารสนเทศ

(Information Classification Policy)

วัตถุประสงค์

เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้น ๆ ที่มีต่อสำนักงาน

ผู้ปฏิบัติ ผู้จัดการส่วน/หัวหน้ากลุ่มงานผู้ที่เกี่ยวข้อง และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน

อ้างอิง เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

ข้อปฏิบัติ

1. **ชั้นความลับของสารสนเทศ (Classification of Information)**

   1.1 การจัดระดับชั้นความลับต้องพิจารณาถึงข้อกำหนดทางด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหว เพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต โดยให้ปฏิบัติตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

   1.2 ต้องกำหนดระดับชั้นความลับของข้อมูล รวมทั้งการจัดเก็บและการใช้งานข้อมูล เป็นลายลักษณ์อักษรและมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ ตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

2. **การบ่งชี้สารสนเทศ (Labeling of Information)**

   2.1 ต้องดำเนินการบ่งชี้ข้อมูลสารสนเทศตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

3. **การจัดการสินทรัพย์สารสนเทศ (Handling of Assets)**

   3.1 การจัดการสินทรัพย์สารสนเทศต้องปฏิบัติตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล
(Media Handling Policy)

วัตถุประสงค์

เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต

ผู้ปฏิบัติ ผู้ใช้งาน

อ้างอิง 1. เอกสารประกอบ นโยบายในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสม (Acceptable Use Policy)
2. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล
3. เอกสารประกอบ การทำลายสื่อบันทึกข้อมูลสารสนเทศ

ข้อปฏิบัติ

1. **การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)**
   - 1.1 ข้อมูลที่มีชั้นความลับ ต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว ตามขั้นตอนการปฏิบัติการทำลายสื่อข้อมูลสารสนเทศ
   - 1.2 ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจากสำนักงาน ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก โดยปฏิบัติตามขั้นตอนการปฏิบัติการทำลายสื่อข้อมูลสารสนเทศ
   - 1.3 ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกนอกสำนักงาน จะต้องได้รับการอนุมัติจากผู้บังคับบัญชาของหน่วยงานที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้ายเพื่อใช้ในการตรวจสอบ
   - 1.4 สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูล
   - 1.5 ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล ให้เป็นไปตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล
   - 1.6 ห้ามไม่ให้นำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ไปใช้เพื่อกิจการอื่นซึ่งไม่เกี่ยวกับภารกิจของสำนักงาน
   - 1.7 ตรวจสอบว่าสื่อบันทึกแบบพกพา และอุปกรณ์คอมพิวเตอร์แบบพกพาทั้งหมด ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของสำนักงาน และบริการของหน่วยงานโครงสร้างที่สำคัญ
   - 1.8 ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนหรือ ข้อมูลในระดับชั้นลับทั้งหมดของบริการที่สำคัญของหน่วยงาน บนสื่อบันทึกข้อมูลแบบถอดได้

2. การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

การทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งาน ต้องปฏิบัติตามขั้นตอนการปฏิบัติงานการทำลายสื่อบันทึกข้อมูลสารสนเทศ

3. ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information Handling Procedures)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ ผู้ใช้งานต้องปฏิบัติตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

4. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ (Security of System Documentation)

4.1 จัดเก็บอย่างมั่นคงปลอดภัย ตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

4.2 มีการกำหนดบุคคลที่มีสิทธิเข้าถึงเอกสารระบบสารสนเทศให้น้อยที่สุด และต้องได้รับการอนุมัติจากเจ้าของระบบงาน

4.3 ไม่จัดเก็บเอกสารระบบสารสนเทศที่มีความสำคัญไว้ในเครือข่ายสาธารณะ หากจำเป็นต้องใช้งานเครือข่ายสาธารณะ จะต้องมีระบบการป้องกันที่เหมาะสม

5. การส่งสื่อบันทึกข้อมูลออกไปภายนอกสำนักงาน (Physical Media Transfer)

5.1 ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้และมีกระบวนการตรวจสอบพนักงานส่งของ

5.2 บรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการส่งโดยเป็นไปตามความเหมาะสม

5.3 ต้องมีการควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต เช่น การเข้ารหัสให้สอดคล้องตามชั้นความลับ

5.4 ส่งด้วยตนเองหรือเจ้าหน้าที่ของสำนักงานและลงบันทึกการรับ-ส่ง เพื่อสามารถตรวจสอบได้

5.5 บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลายส่วนและหลายเส้นทางเพื่อกระจายความเสี่ยง

หมวด 5 การควบคุมการเข้าถึง

(Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์สารสนเทศ สร้างความมั่นคงปลอดภัยให้กับการดำเนินงานของสำนักงาน ประกอบด้วย

- นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information System Access Control Policy)
- นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Policy)
- นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control Policy)

นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(Information System Access Control Policy)

วัตถุประสงค์

นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศนี้จัดทำขึ้นเพื่อ

1. กำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศของสำนักงาน
2. ปกป้องข้อมูลและสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

ผู้ปฏิบัติ ผู้ใช้งาน และส่วนงานที่เกี่ยวข้อง

อ้างอิง 1. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

2. เอกสารประกอบ การสนับสนุนบริการพื้นฐานด้าน IT สำหรับเจ้าหน้าที่

3. เอกสารประกอบ การสนับสนุนบริการพื้นฐานด้าน IT สำหรับบุคคลภายนอก

4. เอกสารประกอบ การจัดการการควบคุม (Controls Management)

ข้อปฏิบัติ

1. การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ

1.1 การเข้าถึงระบบงานภายในของสำนักงานผ่านช่องทาง Web browser จะต้องเข้าผ่านเครือข่าย Intranet ของสำนักงาน หรือผ่าน Virtual Private Network (VPN) ที่สำนักงานจัดหาให้เท่านั้น ยกเว้นระบบเฉพาะที่สำนักงานอนุญาตให้เข้าถึงได้จากเครือข่าย Internet

1.2 การเข้าถึงระบบงานภายในของสำนักงานผ่านช่องทาง Mobile Application หรือ Desktop Application สามารถให้เข้าถึงได้จากเครือข่าย Internet ยกเว้นระบบที่สำนักงานไม่อนุญาตให้เข้าถึงได้จากเครือข่าย Internet

1.3 ต้องกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ การกำหนดสิทธิ หรือการมอบอำนาจเป็นลายลักษณ์อักษร ดังนี้

(1) การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องต้องได้รับการควบคุมอย่างเหมาะสมตามความต้องการในการใช้งาน ระดับความสำคัญ ความต้องการข้อกำหนดของกฎหมาย สัญญาต่าง ๆ ที่เกี่ยวข้อง และต้องปฏิบัติตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล รวมถึงการควบคุมและปกป้องข้อมูลผลลัพธ์ (Output) ที่ได้จากการทำงานของโปรแกรมประยุกต์ หรือ แอปพลิเคชัน (Application) อย่างเหมาะสม

(2) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ การระงับสิทธิ การมอบอำนาจให้เป็นไปตามการบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

1.4 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของสำนักงานนอกเหนือจากสิทธิที่กำหนดไว้จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากผู้มีอำนาจอนุมัติ

1.5 การกำหนดสิทธิการเข้าถึงของผู้ใช้งานต้องมีการทบทวนและปรับปรุง อย่างน้อยปีละ 2 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง หรือมีการ Upgrade ระบบสารสนเทศ เป็นต้น

1.6 การพิสูจน์ตัวตนเพื่อเข้าระบบสารสนเทศที่สำคัญและมีผลกระทบต่อสำนักงานจะต้องผ่านการประเมินจากส่วนงานที่รับผิดชอบว่าเป็นกระบวนการที่มีความมั่นคงปลอดภัย โดยยึดหลักดังนี้

(1) ไม่แสดงรายละเอียดเกี่ยวกับระบบจนกว่ากระบวนการพิสูจน์ตัวตนเพื่อเข้าสู่ระบบจะเสร็จสิ้น

(2) มีข้อความแสดงเตือนผู้ไม่มีสิทธิเข้าถึงระบบงาน

(3) ไม่แสดงข้อความช่วยเหลือใด ๆ 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

2. การบริหารสิทธิในการใช้งานระบบ

2.1 สิทธิในระบบสารสนเทศที่กำหนด (Assign/Grant) ให้แก่ผู้ใช้งานแต่ละคนนั้น ต้องเหมาะสมกับความต้องการในการใช้งานและเป็นไปตามเอกสารแสดงสิทธิการเข้าถึงระบบสารสนเทศ (Access Matrix)

2.2 การกำหนดสิทธิ เปลี่ยนแปลง หรือถอดถอนสิทธินั้น ต้องได้รับอนุมัติจากผู้บังคับบัญชาที่มีหน้าที่ดูแลระบบสารสนเทศก่อนจึงจะสามารถกระทำได้

2.3 สิทธิพิเศษที่ให้แก่เจ้าหน้าที่ต้องผ่านการอนุมัติจากผู้บังคับบัญชาและเป็นสิทธิชั่วคราวที่มีระยะเวลาจำกัด เมื่อครบกำหนดต้องได้รับการเพิกถอน/ยกเลิกทันที

2.4 การทบทวนสิทธิจะต้องมีการดำเนินการอย่างน้อยทุก ๆ 6 เดือน หรือหลังจากมีการเปลี่ยนแปลง สำหรับเจ้าหน้าที่ที่ได้รับสิทธิพิเศษหรือมีสิทธิในระบบที่มีความสำคัญจะต้องมีการเพิ่มความถี่ในการทบทวนสิทธิมากขึ้น

2.5 กระบวนการและกิจกรรมที่กระทำโดยผู้ใช้งานระบบสารสนเทศต้องถูกบันทึกไว้ทั้งในระบบ (System log) พร้อมทั้งได้รับการควบคุมดูแล (Monitor) โดยผู้ดูแลระบบ (System administrator) หรือผู้จัดการส่วน/หัวหน้ากลุ่มงานที่เกี่ยวข้องกับการเข้าถึงระบบสารสนเทศ ตามนโยบายการเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Security Monitoring Policy)

3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.1 การให้และการใช้สิทธิการเข้าถึงต้องมีการจำกัดและควบคุม ให้สอดคล้องตามบทบาทหน้าที่ความรับผิดชอบที่ได้รับมอบหมายเท่านั้น

3.2 การกำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (Access Matrix) ที่ได้กำหนดไว้

3.3 การควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตตามสิทธิที่ได้รับเท่านั้น เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

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

3.5 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งานให้ปฏิบัติตามขั้นตอนการปฏิบัติงานการจัดการบัญชีผู้ใช้งาน สิทธิการใช้งานทั่วไป และขั้นตอนการปฏิบัติงานการจัดการบัญชีผู้ใช้งาน สิทธิการใช้งานระบบ ตามเอกสารการสนับสนุนบริการพื้นฐานด้าน IT สำหรับเจ้าหน้าที่ และตามเอกสารการสนับสนุนบริการพื้นฐานด้าน IT สำหรับบุคคลภายนอก

3.6 สิทธิการเข้าถึงของหน่วยงานภายนอก หรือผู้ให้บริการภายนอก (Third Party) ต่อสารสนเทศและอุปกรณ์สารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการดำเนินงาน หมดสัญญา หรือสิ้นสุดข้อตกลงทันที และต้องมีการปรับปรุงให้เป็นปัจจุบัน

4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

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

4.2 มีการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของสำนักงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(1) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(2) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(3) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(4) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(5) ต้องตั้งค่าให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 10 นาที หรือผู้ใช้งานจะต้องการล็อคหน้าจอคอมพิวเตอร์ด้วยตนเองทุกครั้งเมื่อไม่ได้ใช้งาน

(6) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

4.3 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และผู้ใช้งานต้องออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

4.4 ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 ทั้งนี้ต้องสอดคล้องกับการกำหนดประเภทข้อมูลและการจัดระดับชั้นความลับของข้อมูล ตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control Policy)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

ผู้ปฏิบัติ ผู้ใช้งาน และส่วนงานที่เกี่ยวข้อง

อ้างอิง เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

ข้อปฏิบัติ

1. การควบคุมการเข้าถึงระบบปฏิบัติการของสำนักงาน

1.1 ผู้ดูแลระบบ (system administrator) ต้องจัดการให้เครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไปทุกเครื่องของสำนักงาน ทำงานร่วมกับระบบ Active Directory (AD) และบริหารจัดการให้ระบบ AD สามารถควบคุมเครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไปทุกเครื่องของสำนักงานและกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

1.2 เพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่เหมาะสม และมีการจำกัดสิทธิการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการ โดยพิจารณาตามความเหมาะสมของกลุ่มผู้ใช้งาน

2. ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน โดยมีแนวปฏิบัติ ดังนี้

2.1 การสร้างบัญชีผู้ใช้ใหม่ การแก้ไข หรือยกเลิกบัญชีผู้ใช้ ต้องแจ้งให้ผู้ดูแลระบบดำเนินการ โดยได้รับความเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งาน

2.2 การขอเพิ่ม/เปลี่ยนแปลง/เพิกถอนบัญชีรายชื่อและสิทธิให้มีหลักฐานการร้องขอที่เป็นลายลักษณ์อักษร

2.3 ผู้ใช้งานทุกคนต้องมี User ID ของตนและไม่ซ้ำกับผู้ใช้งานคนอื่น ๆ โดย User ID ที่ออกให้นั้นต้องสามารถตรวจสอบและยืนยันกลับไปยังตัวผู้ใช้งานได้

2.4 ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

3. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

3.1 จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

3.2 กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

3.3 จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

3.4 ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

3.5 ต้องติดตั้งโปรแกรมอรรถประโยชน์ที่มีลิขสิทธิ์ถูกต้องในการใช้งาน

4. การกำหนดเวลาในการใช้งานระบบ

4.1 เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out) ต้องยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม หรือเป็นเวลา 10 นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

4.2 ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) สำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ 3 ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงานตามปกติเท่านั้น

นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
(Application and Information Access Control Policy)

วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของสำนักงานจากผู้ที่ไม่ได้รับอนุญาต

ผู้ปฏิบัติ ผู้ใช้งาน และส่วนงานที่เกี่ยวข้อง

อ้างอิง เอกสารประกอบ นโยบายความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship Policy)

ข้อปฏิบัติ

1. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของสำนักงาน

1.1 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของสำนักงานโดยผู้ให้บริการจากภายนอกต้องดำเนินการตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship Policy)

1.2 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศที่ได้กำหนดไว้

1.3 ระบบที่มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน จะต้องดำเนินการดังนี้

(1) ต้องแยกระบบสำคัญดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อสำนักงาน

(2) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ และไม่อนุญาตให้เข้าถึงระบบผ่านอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอก

หมวด 6 การเข้ารหัสลับข้อมูล
(Cryptography)

วัตถุประสงค์

เพื่อกำหนดแนวทางการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและความเหมาะสม

ผู้ปฏิบัติ ผู้ใช้งาน และส่วนงานที่เกี่ยวข้อง

อ้างอิง 1. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

2.เอกสารประกอบ บริหารจัดการการเข้ารหัสข้อมูล

ข้อปฏิบัติ

1. มาตรการการเข้ารหัสลับข้อมูล (Cryptographic Controls)

1.1 **มาตรการการเข้ารหัสลับข้อมูล**

ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูล และแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ แต่กรณีไม่สามารถเข้ารหัสได้ ต้องควบคุมการเข้าถึงอย่างเหมาะสม

1.2 **การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล**

ต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล โดยให้มีการปฏิบัติตามขั้นตอนการจัดการกุญแจเข้ารหัสลับข้อมูล และให้เป็นไปตามวิธีการดังกล่าวอย่างสม่ำเสมอซึ่งประกอบไปด้วย

1.2.1 ต้องพิจารณาประเภทกลุ่มข้อมูลที่นำมาใช้เข้ารหัสว่าสอดคล้องกับการจัดระดับชั้นความลับของข้อมูล และแนวทางการดำเนินการกำกับข้อมูล

1.2.2 ต้องเลือกใช้การเข้ารหัสข้อมูลให้สามารถดำเนินการได้ 2 แบบดังนี้

- แบบ Symmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสเดียวกัน (Secret Key)
- แบบ Asymmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคู่ (Public/Private Key)

โดยพิจารณาวิธีการเข้ารหัสแต่รูปแบบ อ้างอิง “รูปแบบการเข้ารหัสข้อมูล” รวมทั้ง ใช้อัลกอริทึมที่เหมาะสม

1.2.3 ดำเนินการสร้างกุญแจรหัสจากโปรแกรมที่น่าเชื่อถือ โดยปฏิบัติตามแนวทางการสร้างกุญแจรหัส และการบริหารจัดการกุญแจรหัส (Key Management)

1.2.4 ดำเนินการนำข้อมูลผ่านกระบวนการเข้ารหัส เพื่อนำข้อมูลที่เข้ารหัสไปใช้ตามจุดประสงค์ต่อไป

หมวด 7 นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security Policy)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับกับผู้ใช้งานและผู้ให้บริการภายนอก

ผู้ปฏิบัติ ผู้ใช้งาน และผู้ให้บริการภายนอก

อ้างอิง

1. เอกสารเรื่อง หลักเกณฑ์การเข้า-ออกพื้นที่ศูนย์ข้อมูล (Data Center) และหลักเกณฑ์การนำอุปกรณ์เข้า-ออกพื้นที่ศูนย์ข้อมูล (Data Center)
2. เอกสารประกอบ นโยบายในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสม (Acceptable Use Policy)
3. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล
4. เอกสารประกอบ บริหารอาคารและสถานที่
5. เอกสารประกอบ ตรวจนับ จำหน่ายพัสดุ
6. เอกสารประกอบ คู่มือระบบบริหารจัดการด้านเทคโนโลยีสารสนเทศ (ITMS Manual)
7. เอกสารประกอบ แผนบริหารความต่อเนื่องทางธุรกิจระดับองค์กร (Enterprise Business Continuity Plan)
8. เอกสารประกอบ การจัดการหน่วยงายภายนอกที่เกี่ยวข้อง (Third Party Management)
9. เอกสารประกอบ การพัฒนาบุคลากร (Training and Awareness)

ข้อปฏิบัติ

1. มาตรฐานในการกำหนดบริเวณที่ต้องมีความมั่นคงปลอดภัยด้านสารสนเทศ (Secure Area)

1.1 ข้อกำหนดทั่วไป

1.1.1 ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน

1.1.2 ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย ประกอบด้วย กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกัน ภัยคุกคามจากผู้บุกรุก เป็นต้น

ในพื้นที่ใช้งานระบบสารสนเทศของสำนักงานได้แก่ ห้อง Server/Data Center เพื่อให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัย

1.2 การควบคุมการเข้าออก (Physical Entry Controls)

ส่วนงานที่รับผิดชอบร่วมกับส่วนงานที่เป็นเจ้าของระบบงาน กำหนดมาตรการการควบคุมการเข้าออกในบริเวณพื้นที่ใช้งานระบบสารสนเทศ โดยให้ผ่านเข้าออกได้เฉพาะผู้ใช้งานที่มีสิทธิเท่านั้น ซึ่งมีแนวทางปฏิบัติ ดังนี้

1.2.1 มีการกำหนดสิทธิการเข้าถึงพื้นที่ และมีการทบทวนสิทธิตามรอบ โดยการกำหนดสิทธิต้องระบุเป็นลายลักษณ์อักษร

1.2.2 ระบุตัวผู้ใช้งานและช่วงเวลาที่มีสิทธิผ่านเข้าออกในแต่ละพื้นที่อย่างชัดเจน

1.2.3 ผู้ใช้งานจะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

1.2.4 ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยผู้ให้บริการภายนอก หรือหน่วยงานภายนอกเพื่อป้องกันการเข้าถึงสินทรัพย์ของสำนักงานโดยไม่ได้รับอนุญาต และจัดเป็นบริเวณแยกออกมาต่างหาก ซึ่งเป็นไปตามขั้นตอนการปฏิบัติงานบริหารอาคารและสถานที่

1.2.5 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ให้ปฏิบัติตามประกาศ สพร. เรื่อง หลักเกณฑ์การเข้า-ออกพื้นที่ศูนย์ข้อมูล (Data Center) และหลักเกณฑ์การนำอุปกรณ์เข้า-ออกพื้นที่ศูนย์ข้อมูล (Data Center)

2. ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

2.1 การปฏิบัติงานในพื้นที่สำนักงาน

2.1.1 ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ ได้แก่ เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก ประตูหน้าต่างของสำนักงานต้องปิดล็อคโดยวิธีการที่ปลอดภัย ติดตั้งผนัง ติดตั้งเหล็กดัดล็อคประตูที่ใช้ดอกกุญแจหรือมีระบบ Access Control และปรับปรุงให้มีความเหมาะสมทางสภาวะแวดล้อม ได้แก่ ติดตั้งระบบปรับอากาศ เป็นต้น

2.1.2 ต้องมีการควบคุมการเข้าออกพื้นที่สำนักงานของผู้ติดต่อเฉพาะพื้นที่ที่จัดเตรียมไว้ให้เท่านั้น

2.1.3 ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยผู้ให้บริการภายนอก (Third Party) หรือหน่วยงานภายนอกเพื่อป้องกันการเข้าถึงสินทรัพย์ของสำนักงานโดยไม่ได้รับอนุญาต และจัดเป็นบริเวณแยกออกมาต่างหาก

2.1.4 สำนักงานจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว

2.1.5 ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต”“ห้ามถ่ายภาพหรือวิดีโอ”และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

2.1.6 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้มาติดต่อ หรือผู้ขอเข้าใช้พื้นที่ หรือมิได้เกี่ยวข้องอันใดกับกิจการของสำนักงาน หรือมิได้แจ้งการขอเข้าพื้นที่เป็นการล่วงหน้า ส่วนอาคารสถานที่และยานพาหนะ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนการอนุญาตหรือไม่อนุญาตเข้าพื้นที่

2.2 ข้อปฏิบัติสำหรับผู้ติดต่อจากหน่วยงานภายนอก

2.2.1 ต้องทำการแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประชาชน หรือใบอนุญาตขับขี่ หรือบัตรประจำตัวอื่นใดกับเจ้าหน้าที่เพื่อรับบัตรผู้ติดต่อ (Visitor)

2.2.2 ต้องติดบัตรผู้ติดต่อตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในสำนักงาน

2.2.3 ต้องอยู่ในพื้นที่บริเวณที่จัดไว้ให้ และมีเจ้าหน้าที่คอยดูแลตลอดเวลา

2.2.4 ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่ และเจ้าหน้าที่ต้องตรวจสอบการคืนบัตร

2.2.5 กรณีเข้าพื้นที่มั่นคงปลอดภัย (Secure Area) ผู้มาติดต่อที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ลงในใบนำสินทรัพย์เข้าออกพื้นที่ห้อง Data Center

2.3 ในพื้นที่ที่ต้องการความมั่นคงปลอดภัย (Working in secure areas)

2.3.1 ส่วนงานที่รับผิดชอบต้องกำกับให้มีการกำหนดแนวปฏิบัติของการสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Secure Area) ได้แก่ห้อง Data Center และพื้นที่ปฏิบัติงานของผู้ดูแลระบบ และกำหนดให้มีการนำแนวปฏิบัติไปใช้งานอย่างเคร่งครัด

2.4 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

2.4.1 ส่วนงานที่รับผิดชอบต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึง อาจสามารถเข้าถึงได้ โดยต้องกำหนดพื้นที่การส่งมอบสินค้า และพื้นที่การเตรียม หรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์ ทั้งนี้ให้แยกเป็นสัดส่วนที่ชัดเจน เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศ และข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

2.5 ความปลอดภัยของอุปกรณ์ (Equipment Security)

2.5.1 ผู้ใช้งานต้องจัดตั้งอุปกรณ์ไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

2.5.2 เจ้าของระบบงานต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ ได้แก่ จัดให้มีการซ่อมบำรุงตามรอบที่กำหนดโดยเฉพาะระบบที่มีความสำคัญ เป็นต้น เพื่อให้สามารถใช้งานได้อย่างต่อเนื่องและมีความพร้อมใช้อยู่เสมอ

2.5.3 ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของสำนักงานเมื่อถูกนำไปใช้งานนอกสำนักงาน ตามประกาศสำนักงาน

2.5.4 ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ตามขั้นตอนการปฏิบัติงานการทำลายสื่อบันทึกข้อมูลสารสนเทศ

2.6 ความปลอดภัยของระบบกระแสไฟฟ้าสำรอง (Power Supplies) และระบบป้องกันภัย

2.6.1 ต้องมีระบบไฟฟ้าสำรองอัตโนมัติ เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง และต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาอย่างน้อยปีละ 1 ครั้ง

2.6.2 ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย ได้แก่ ระบบดับเพลิง ระบบแจ้งเตือนอัคคีภัย

2.6.3 ต้องมีการวางแผนและซักซ้อมการปฏิบัติเพื่อรับมือกับเหตุการณ์ฉุกเฉินต่าง ๆ อย่างน้อยปีละ 1 ครั้ง และเป็นไปตามขั้นตอนการเตรียมการของแผนรองรับเหตุการณ์ฉุกเฉิน

2.6.4 ระบบที่สำคัญของสำนักงานจะต้องปฏิบัติตามคู่มือระบบบริหารจัดการด้านเทคโนโลยีสารสนเทศ และแผนบริหารความต่อเนื่องทางธุรกิจระดับองค์กร เพื่อลดผลกระทบที่จะเกิดขึ้นกับการดำเนินงานของสำนักงาน

2.7 ความปลอดภัยของการเดินสายไฟฟ้าหลัก (Main Power Cable) และสายเคเบิลหลัก (Backbone Cable)

2.7.1 การเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงานที่ผ่านเข้ามา ผ่านช่องพิเศษที่จัดไว้ เป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย

2.7.2 การติดตั้งตู้พักสายต้องอยู่ในพื้นที่ที่จำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิเท่านั้น

2.8 ความปลอดภัยของโต๊ะทำงานและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk Clear Screen)

2.8.1 ต้องควบคุมสินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ ฯลฯ ให้ปลอดภัยจากการเข้าถึงโดยผู้ไม่มีสิทธิ

2.8.2 จัดเก็บเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

2.8.3 การทำลายเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูลและขั้นตอนการปฏิบัติการการทำลายสื่อบันทึก

2.8.4 ข้อมูลที่มีความสำคัญมาก รวมถึงข้อมูลในคอมพิวเตอร์ ต้องเคลื่อนย้ายโดยผู้เป็นเจ้าของข้อมูลเท่านั้น ไม่เคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

2.8.5 ข้อมูลที่มีความสำคัญ มีการรักษาความลับต้องมีการเข้ารหัสเมื่อถูกจัดเก็บ

2.8.6 ทุกครั้งที่ออกจากหน้าจอคอมพิวเตอร์ต้องปิดหน้าจอ หรือ log off ออกจากระบบ

2.8.7 ผู้ใช้งานต้องออกจากระบบเมื่อว่างเว้นจากการใช้งาน

2.9 การควบคุมทั่วไป (General Controls)

2.9.1 ส่วนงานที่รับผิดชอบต้องมีการตรวจตราสถานที่ย้ายสินทรัพย์ออก เพื่อให้มั่นใจได้ว่าไม่มีข้อมูลใดหลงเหลืออยู่ และมีการกำหนดความรับผิดชอบในการดูแลให้ครอบคลุมส่วนที่เก็บเอกสาร (ตู้เก็บแฟ้มเอกสาร, ห้องเก็บรักษาแฟ้มข้อมูล, ห้องนิรภัย) และเป็นไปตามขั้นตอนการบริหารสินทรัพย์และการบริหารพัสดุ

2.9.2 การเคลื่อนย้ายสินทรัพย์ของสำนักงาน เจ้าหน้าที่หรือลูกจ้างที่รับผิดชอบในส่วนงานต้องทำเป็นบันทึกและขออนุญาตจากผู้จัดการส่วน/หัวหน้ากลุ่มงานที่เกี่ยวข้องอย่างถูกต้องก่อนการเคลื่อนย้าย

2.9.3 ส่วนงานงานที่รับผิดชอบจะต้องตรวจสอบความพร้อมใช้ของพื้นที่และสินทรัพย์ให้เรียบร้อยปลอดภัย และต้องขนย้ายด้วยความระมัดระวัง

2.9.4 ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลงหรือเคลื่อนย้ายเพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของสำนักงาน

หมวด 8 การบริหารจัดการด้านการดำเนินงาน
(Operations Management)

วัตถุประสงค์

เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์และระบบประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย โดยประกอบด้วย

- นโยบายการเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Security Monitoring Policy)
- นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ (Corporate Antivirus for Computer Policy)
- นโยบายการสำรองข้อมูล (Back up Policy)
- นโยบายการจัดการการเปลี่ยนแปลง (Change Management Policy)
- นโยบายการจัดการทรัพยากรระบบ (Capacity Management Policy)

นโยบายการเฝ้าระวังทางด้านความมั่นคงปลอดภัย
(Security Monitoring Policy)

วัตถุประสงค์

เพื่อเฝ้าระวังกิจกรรมทางด้านความมั่นคงปลอดภัย

ผู้ปฏิบัติ ผู้ใช้งาน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน

อ้างอิง เอกสารประกอบ การประเมินช่องโหว่ (Vulnerability Management)

ข้อปฏิบัติ

1. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging)

ให้บันทึกกิจกรรมการใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้ซึ่งประกอบด้วย

1.1 ชื่อผู้ใช้วัน เวลา และรายละเอียดที่สำคัญ ประกอบด้วย การเข้าระบบและการออกจากระบบ

1.2 บันทึก IP Address และ Protocol ทั้งต้นทางและปลายทาง

1.3 บันทึกของการพยายามเข้าสู่ระบบข้อมูลและทรัพยากรทั้งสำเร็จและไม่สำเร็จ

1.4 บันทึกของการเปลี่ยนค่า Configuration ของระบบ

1.5 บันทึกของการใช้โปรแกรมอรรถประโยชน์และซอฟต์แวร์ประยุกต์ของระบบที่สำคัญ

1.6 มีการแจ้งเตือนเมื่อมีการพยายามเข้าถึงโดยไม่ได้รับอนุญาต

1.7 ต้องมีการตรวจสอบการทำงานของระบบรักษาความมั่นคงปลอดภัยสารสนเทศ

2. การตรวจสอบการใช้งานระบบ (Monitoring System Use)

เพื่อตรวจสอบการทำงานระบบสารสนเทศอย่างสม่ำเสมอ มีแนวทางปฏิบัติดังนี้

2.1 การระบุตัวตนในการเข้าถึง ประกอบด้วย

- ชื่อผู้ใช้
- วัน เวลา และรายละเอียดที่สำคัญ
- ชนิดของเหตุการณ์
- การเข้าถึงไฟล์
- ซอฟต์แวร์หรือโปรแกรมอรรถประโยชน์ที่ใช้

2.2 การดำเนินการเกี่ยวกับสิทธิของผู้ใช้งาน

2.2.1 ตรวจสอบการใช้บัญชีผู้ดูแลระบบหรือเทียบเท่า ได้แก่ Administrator, Root หรือ Supervisor

2.2.2 ตรวจสอบการเปลี่ยนแปลงการให้บริการของระบบสารสนเทศ

2.2.3 ตรวจสอบการเชื่อมต่อการทำงานของอุปกรณ์ภายนอก

2.3 การพยายามเข้าถึงโดยไม่ได้รับอนุญาต

2.3.1 การพยายามเข้าใช้งานของผู้ที่ถูกเพิกถอนสิทธิ

2.3.2 การพยายามเข้าถึงทรัพยากรที่ไม่ได้รับอนุญาต

2.4 การแจ้งเตือนข้อผิดพลาดของระบบ

2.4.1 เปิดการแจ้งเตือนผ่านหน้าจอ

2.4.2 บันทึกกิจกรรมทั้งหมดที่เกิดขึ้นในระบบ

2.4.3 การแจ้งเตือนของระบบบริหารจัดการเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

2.4.4 มีสัญญาณเตือนโดยระบบการควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

2.5 การเปลี่ยนแปลงหรือพยายามเปลี่ยนแปลงการตั้งค่าและการควบคุมระบบรักษาความมั่นคงปลอดภัย

3. การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)

เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาตมีแนวปฏิบัติ ดังต่อไปนี้

3.1 ต้องมีกระบวนการป้องกันการเปลี่ยนแปลงข้อมูล

3.2 ตรวจสอบความจุของพื้นที่ในการจัดเก็บข้อมูลบันทึกเหตุการณ์ให้เพียงพอต่อการดำเนินงานสอดคล้องกับนโยบาย และกฎหมายที่เกี่ยวข้อง

3.3 การสำรองข้อมูลบันทึกเหตุการณ์ จะต้องถูกดำเนินการอย่างเหมาะสม

4. บันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ (Administrator and Operator Logs)

ข้อมูลบันทึกเหตุการณ์ ที่จะบันทึกประกอบด้วย

4.1 บัญชีผู้ใช้งานและผู้ดูแลระบบหรือผู้ปฏิบัติการที่เกี่ยวข้อง

4.2 บันทึกประเภทของข้อมูลและเหตุการณ์ที่เกิดขึ้นของกิจกรรมทั้งหมดในระบบ

5. การบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging)

การบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามความเหมาะสม ดังนี้

5.1 ต้องทบทวนข้อมูลบันทึกเหตุการณ์ที่ผิดพลาดเพื่อความมั่นใจได้มีการดำเนินการแก้ไขข้อผิดพลาดดังกล่าว

5.2 ตรวจสอบกระบวนการแก้ไข เพื่อความมั่นใจว่าปัญหาดังกล่าวได้รับการแก้ไขแล้ว

6. การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

6.1 ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้งานต้องมีการติดตามอย่างเป็นปัจจุบัน จุดอ่อนต่อช่องโหว่ดังกล่าวของสำนักงานต้องมีการประเมิน และมีมาตรการที่เหมาะสมต้องถูกนำมาจัดการกับความเสี่ยงที่เกี่ยวข้อง

6.2 ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน ได้แก่ การเฝ้าระวังภัยคุกคาม การประเมินความเสี่ยงของภัยคุกคาม การปิดช่องโหว่ในระบบ เป็นต้น

6.3 ต้องร่วมกันวิเคราะห์ความเสี่ยงทางเทคนิค และประเมินภัยคุกคามที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศทุก 3 เดือน เป็นอย่างน้อย

6.4 ในกรณีที่มีการร้องขอผลการตรวจสอบช่องโหว่จากลูกค้า หรือบุคคลภายนอกที่ใช้บริการระบบงานสารสนเทศของสำนักงาน ต้องมีการวางแผน รายงานความเสี่ยงที่อาจเกิดขึ้น และขออนุมัติก่อนดำเนินการ

6.5 ในกรณีที่จะทำการปรับปรุงระบบสำคัญ ต้องมีการทดสอบและประเมินก่อนว่าจะไม่ก่อให้เกิดความเสียหายต่อระบบ โดยปฏิบัติตาม นโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy) แต่ถ้าไม่สามารถปรับปรุงได้ ให้พิจารณาดังต่อไปนี้

6.5.1 เปิดการทำงานของระบบเท่าที่จำเป็น

6.5.2 ปรับปรุงหรือเพิ่มระดับด้านความมั่นคงปลอดภัย การเฝ้าระวัง เพื่อตรวจจับหรือป้องกันการโจมตีเครือข่าย

6.5.3 อบรมสร้างความตระหนักเกี่ยวกับช่องโหว่ด้านความมั่นคงปลอดภัย

6.5.4 เก็บบันทึกเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

6.5.5 กระบวนการบริหารจัดการช่องโหว่ ต้องมีการควบคุม ติดตามและประเมิน เพื่อให้มั่นใจว่าการดำเนินเป็นอย่างถูกต้องและเหมาะสม

6.6 ระบบที่มีความเสี่ยงสูงจะต้องมีการดำเนินการปรับปรุงอย่างเร่งด่วน

6.7 ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้งก่อนที่จะมีการทดสอบระบบใหม่หรือมีการเปลี่ยนแปลงระบบที่สำคัญ (ตามความจำเป็น)

6.8 การทดสอบเจาะระบบ และผู้ทดสอบเจาะระบบ (Penetration Tester) ต้องเป็นผู้ที่มีความรู้ความสามารถ ได้รับการรับรองและได้รับประกาศนียบัตรเป็นที่ยอมรับในอุตสาหกรรมและเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ

6.9 การทดสอบเจาะระบบโดยผู้ให้บริการ ต้องอยู่ภายใต้การดูแลของสำนักงานตลอดระยะเวลาดำเนินงาน

6.10 ต้องมีการกำหนดขั้นตอนการติดตามและจัดการช่องโหว่ที่พบ หลังจากดำเนินการทดสอบเจาะระบบของสำนักงาน

7. การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock Synchronization)

การตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานไปยังเครื่องแม่ข่ายที่ให้บริการข้อมูลเวลาโดยการตั้งเวลาของเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงาน โดยการตั้งเวลาด้วย Network Time Protocol (NTP) ไปยังเครื่องแม่ข่ายที่ให้บริการข้อมูลเวลา คือ time.dga.or.th หรือ ตาม Active Directory

นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์

(Corporate Antivirus for Computer Policy)

วัตถุประสงค์

นโยบายนี้ได้ถูกจัดทำขึ้นเพื่อต้องการให้เกิดความมั่นคงปลอดภัยของระบบสารสนเทศสำนักงานช่วยลดภาวะเสี่ยงของปัญหาที่จะเกิดขึ้นกับระบบสารสนเทศทั้งในส่วนของอุปกรณ์และระบบฐานข้อมูลของสำนักงานทำให้การทำงานมีความต่อเนื่องไม่เกิดการหยุดชะงัก

ผู้ปฏิบัติ ผู้ใช้งานและผู้ดูแลระบบ

ข้อปฏิบัติ

1. **แนวทางปฏิบัติการใช้งานระบบป้องกันไวรัส (Corporate Antivirus)**

เพื่อลดความเสี่ยงและปัญหาการติดไวรัสในอุปกรณ์สารสนเทศของสำนักงานต้องปฏิบัติดังต่อไปนี้

1.1 อุปกรณ์สารสนเทศที่เชื่อมต่อกับเครือข่าย Intranet ของสำนักงาน ต้องติดตั้งโปรแกรม Antivirus

1.2 กำหนดให้ส่วนงานที่รับผิดชอบ ร่วมกับส่วนงานที่เกี่ยวข้องเป็นผู้ประสานงานและดำเนินการที่เกี่ยวข้อง ได้แก่

1.2.1 ประเมินและจัดหาจำนวน Licenses ให้เพียงพอต่อการใช้งานของผู้ใช้งาน

1.2.2 ดำเนินการให้การ Update Virus Signature เป็นไปอย่างอัตโนมัติ และจัดทำ Configuration ของระบบ Antivirus ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

1.3 ผู้ใช้งานทุกคนต้องใช้ระบบ Antivirus ตามที่สำนักงานจัดหาให้

1.4 ผู้ดูแลระบบเครื่องแม่ข่ายจะต้องส่งเรื่องขอใช้งาน Antivirus จากส่วนงานที่รับผิดชอบ โดยพิจารณาเป็นรายกรณีไป

1.5 ผู้ใช้งานต้องสำรองข้อมูลสำคัญเก็บไว้ในที่ที่ปลอดภัย โดยสื่อจัดเก็บข้อมูลแบบพกพาหรือพื้นที่จัดเก็บข้อมูลตามที่สำนักงานจัดสรรไว้ให้เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลาย

1.6 ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ระบบ Antivirus ที่ใช้ โดยตรวจสอบการ Update ให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ระบบ Antivirus ได้

1.7 ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ทำงานผิดปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

1.8 ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์ ซอฟต์แวร์ที่มีการฝัง Malicious Mobile Code หรือข้อมูลที่มีมัลแวร์มาติดตั้งใช้งาน

1.9 ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของระบบ Antivirus ที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่สำนักงานจัดหาให้

นโยบายการสำรองข้อมูล

(Backup Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติในการสำรองข้อมูล และป้องกันการสูญหายของข้อมูล

ผู้ปฏิบัติ ผู้ใช้งาน และส่วนงานที่เกี่ยวข้อง

อ้างอิง 1. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

2. เอกสารประกอบ บริหารการเปลี่ยนแปลงและการนำบริการสู่การใช้งาน (Change and Release Management)

3. เอกสารประกอบ การสำรอง/ทดสอบกู้คืนข้อมูล (Backup and Restore testing)

ข้อปฏิบัติ

1. การสำรองข้อมูลจากเครื่องคอมพิวเตอร์สำนักงาน

1.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ โดยเฉพาะข้อมูลที่มีความสำคัญของสำนักงานให้ปฏิบัติตามขั้นตอนการจัดระดับชั้นความลับของข้อมูลอย่างเคร่งครัดการเก็บสำรองข้อมูลและสารสนเทศสำนักงาน

1.2 สำหรับข้อมูลที่สำคัญของระบบบริหารจัดการสารสนเทศ จะต้องมีการจัดเก็บข้อมูลไว้ในที่ตามที่สำนักงานจัดสรรไว้

1.3 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และปฏิบัติตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

1.4 ไม่เก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานไว้บนพื้นที่ตามที่สำนักงานจัดสรรไว้

2. การเก็บสำรองข้อมูลและสารสนเทศสำนักงาน

2.1 ต้องสำรองข้อมูลก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ

2.2 ความถี่ในการสำรองข้อมูลอย่างน้อยสัปดาห์ละ 1 ครั้ง และดำเนินการทดสอบการกู้คืนอย่างน้อยปีละ 1 ครั้ง โดยให้เป็นไปตามเอกสารขั้นตอนการปฏิบัติงานการสำรอง/ทดสอบกู้คืนข้อมูล

2.3 ข้อมูลและสารสนเทศที่มีความสำคัญมากต่อการดำเนินงานของสำนักงาน จะต้องทำการสำรองข้อมูลและทดสอบการกู้คืน เพื่อข้อมูลที่ได้รับการสำรองมีประสิทธิภาพ ประสิทธิผล และมีความพร้อมใช้งาน

2.4 ข้อมูลและสารสนเทศที่สำคัญทั้งหมดของสำนักงาน ต้องมีระบบประมวลผลสำรอง ระบบเครือข่ายสำรอง เพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงานได้ สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้การดำเนินงานของสำนักงานดำเนินต่อไปได้

นโยบายการจัดการการเปลี่ยนแปลง
(Change Management Policy)

วัตถุประสงค์

เพื่อควบคุมการเปลี่ยนแปลงระบบสารสนเทศ และบริการของสำนักงานให้มั่นใจว่าการเปลี่ยนแปลง ปรับปรุง แก้ไขระบบสารสนเทศ และบริการได้รับการควบคุมตลอดระยะเวลาที่มีการเปลี่ยนแปลงรวมถึงลดความเสี่ยงที่อาจเกิดความเสียหายจากการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบสารสนเทศและบริการ

ผู้ปฏิบัติ ผู้ที่ร้องขอการเปลี่ยนแปลง และส่วนงานที่เกี่ยวข้อง

อ้างอิง 1. เอกสารประกอบ บริหารการเปลี่ยนแปลงและการนำบริการสู่การใช้งาน

2. เอกสารประกอบ นโยบายและคู่มือบริหารความเสี่ยง

3. เอกสารประกอบ การกำหนดค่าและการจัดการการเปลี่ยนแปลง (Configuration and Change Management)

ข้อปฏิบัติ

1. ผู้ที่ร้องขอการเปลี่ยนแปลง และส่วนงานที่เกี่ยวข้องต้องปฏิบัติตาม เอกสารขั้นตอนการปฏิบัติงานบริหารการเปลี่ยนแปลงและการนำบริการสู่การใช้งานการเปลี่ยนแปลง โดยอ้างอิงบทบาทหน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารการเปลี่ยนแปลงและการนำบริการสู่การใช้งาน ตารางสิทธิและหน้าที่ของการเปลี่ยนแปลง และเกณฑ์ในการกำหนดประเภทของการเปลี่ยนแปลงและการนำบริการสู่การใช้งาน

2. การดำเนินการเปลี่ยนแปลงต้องดำเนินประเมินความเสี่ยงโดยพิจารณาถึงผลกระทบทุกด้านตามเกณฑ์การประเมินความเสี่ยงของสำนักงานรวมถึงด้านความมั่นคงปลอดภัย ระบุประเภทการเปลี่ยนแปลง กำหนดขั้นตอนการย้อนกลับ (Rollback step) กรณีดำเนินการเปลี่ยนแปลงไม่สำเร็จ ทำการทดสอบเบื้องต้น(กรณีจำเป็น) แจ้งผู้ที่อาจได้รับผลกระทบจากการเปลี่ยนแปลง และขออนุมัติการเปลี่ยนแปลงก่อนดำเนินการทุกครั้ง ตามขั้นตอนการปฏิบัติงานบริหารการเปลี่ยนแปลงและการนำบริการสู่การใช้งานการเปลี่ยนแปลง

นโยบายการจัดการทรัพยากรระบบ

(Capacity Management Policy)

วัตถุประสงค์

เพื่อเป็นแนวทางในการบริหารจัดการทรัพยากรระบบของบริการ เพียงพอตามข้อตกลงระดับการให้บริการ และต่อการให้บริการลูกค้า หรือผู้ใช้งานทั้งในปัจจุบันและในอนาคต

ผู้ปฏิบัติ ส่วนงานที่เกี่ยวข้อง

อ้างอิง เอกสารประกอบ การจัดการทรัพยากรระบบ (Capacity Management)

ข้อปฏิบัติ

1. ต้องดำเนินการวิเคราะห์ข้อมูลที่เกี่ยวข้องกับบริการประกอบด้วยเอกสารคำขอใช้บริการ ข้อมูลการสำรวจความพึงพอใจลูกค้า ข้อมูลการวิจัยตลาด ข้อมูลแนวโน้มค่าใช้จ่ายปีที่ผ่าน รวมถึงพิจารณากฎหมาย กฎระเบียบ ข้อบังคับฯ ที่เกี่ยวข้องกับการดำเนินงานของสำนักงานเพื่อนำมาใช้ในการคาดการณ์และของบประมาณที่ต้องใช้ในการปรับปรุงหรือพัฒนาผลิตภัณฑ์/บริการของสำนักงาน
2. ต้องประเมินงบประมาณที่ใช้ในบริการ และงบประมาณที่ต้องใช้ในการปรับปรุงหรือ พัฒนาผลิตภัณฑ์/บริการของสำนักงาน
3. ต้องวางแผนกับส่วนงานที่เกี่ยวข้องให้เป็นไปตามกรอบงบประมาณที่ได้รับ เพื่อพิจารณากรอบงบประมาณ และข้อมูลทรัพยากรที่ได้รับจากส่วนงานที่เกี่ยวข้อง เพื่อจัดทำแผนการบริหาร/จัดการทรัพยากรของแต่ละบริการ และเสนอผู้มีอำนาจอนุมัติต่อไป
4. ต้องจัดทำแผนการจัดสรรทรัพยากรรายบริการ และนำเสนอผอ. ฝ่าย เพื่อพิจารณาอนุมัติ
5. ต้องจัดทำแผนการจัดการทรัพยากรระบบ (Capacity Plan) รายบริการ และสื่อสารการติดตามการใช้ทรัพยากรของบริการ
6. ต้องนำข้อมูลการเฝ้าระวัง และ Utilization Analysis มาปรับปรุงแผนการจัดการทรัพยากรระบบ (Capacity Plan) รายบริการ
7. ส่วนงานที่รับผิดชอบ พิจารณารายการดังนี้

   7.1 ระดับการใช้งานทรัพยากรระบบอยู่ใน Threshold แผนเพิ่มทรัพยากร

   7.2 เมื่อมีการแจ้งว่าผู้ใช้บริการเดิมต้องการขยายการใช้งานทรัพยากรเป็นจำนวนมากซึ่งเกินกำหนดโควตาที่กำหนดให้

   7.3 เมื่อได้รับการร้องขอ (Customer Requirement) อย่างเป็นทางการ ซึ่งสำนักงานอาจต้องพิจารณากรอบการปรับปรุงประสิทธิภาพของระบบตามกรอบงบประมาณที่สำนักงานได้ร้องขอต่อสำนักงบประมาณ
8. ต้องจัดทำรายงานภาพรวมบริการนำเสนอผู้เกี่ยวข้องและผู้บริหารเพื่อใช้ในการวางแผนทรัพยากร

หมวด 9 การบริหารจัดการด้านการสื่อสาร
(Communication Management)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการบริหารจัดการเครือข่าย และการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกองค์ให้มีความมั่นคงปลอดภัย โดยประกอบด้วย

- นโยบายการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control Policy)
- นโยบายการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (Internet and E-mail Policy)
- นโยบายการใช้สื่อสังคมออนไลน์ (Social Media)
- นโยบายการถ่ายโอนข้อมูลสารสนเทศ (Information Transfer Policy)
- นโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

นโยบายการควบคุมการเข้าถึงระบบเครือข่าย
(Network Access Control Policy)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

ผู้ปฏิบัติ ผู้ใช้งาน และส่วนงานที่เกี่ยวข้อง

อ้างอิง เอกสารประกอบ การเฝ้าระวังและตรวจสอบระบบเครือข่าย (Monitoring)

ข้อปฏิบัติ

1. **กำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational Procedures and Responsibilities)**
   1.1 เจ้าของระบบงานต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานนั้น ๆ โดยมีเนื้อหาที่สำคัญเกี่ยวกับการใช้งาน
   1.2 ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ ต้องปฏิบัติตามขั้นตอนการบริหารจัดการการเปลี่ยนแปลง
   1.3 เจ้าของระบบงานต้องกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานของผู้ที่เกี่ยวข้องไว้อย่างชัดเจน
   1.4 เจ้าของระบบงานต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยตามขั้นตอนการปฏิบัติการแก้ไขเหตุการณ์ไม่พึงประสงค์
   1.5 เจ้าของระบบงานต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

1.6 ผู้ดูแลระบบเครือข่ายต้องรับผิดชอบในการตรวจสอบและดูแลอุปกรณ์ที่เกี่ยวข้องในระบบเครือข่ายทั้งหมด รวมทั้งอุปกรณ์ที่ใช้สำหรับการเข้าถึงระยะไกล (Remote Equipment) และอุปกรณ์ที่อยู่ในพื้นที่ของผู้ใช้งานตามเอกสาร การเฝ้าระวังและตรวจสอบระบบเครือข่าย (Monitoring)

1.7 การดำเนินการใด ๆ ภายในระบบเครือข่าย ต้องอยู่ภายในการควบคุมดูแลและการรับผิดชอบของผู้ดูแลระบบเครือข่าย และต้องรายงานต่อผู้บังคับบัญชา เพื่อควบคุมการใช้งานระบบเครือข่ายให้มีประสิทธิภาพสูงสุด และให้มีความสอดคล้องโดยทั่วกัน

2. การบริหารจัดการเครือข่าย (Network Management)

2.1 อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่าย เพื่อการทำงานภายในสำนักงาน ได้แก่ Router และ Switch มีข้อปฏิบัติดังนี้

2.1.1 อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็นและการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password

2.1.2 การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะสามารถกระทำได้ก็ต่อเมื่อได้รับอนุญาตจากส่วนงานที่รับผิดชอบ

2.1.3 กรณีเชื่อมโยงเครือข่ายโดยพลการแล้วทำให้เกิดความเสียหายกับระบบเครือข่ายจะต้องถูกลงโทษตามที่กำหนดไว้

2.1.4 ผู้ดูแลระบบต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่องและมีความพร้อมใช้อยู่เสมอ

2.1.5 ในระบบที่สำคัญอาจมีการพิจารณาการเข้ารหัสข้อมูลมาใช้ร่วมด้วย

2.1.6 ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

2.2 อุปกรณ์ที่ทำหน้าที่ Remote Access เพื่อการควบคุมระบบจากระยะไกล ได้แก่ Virtual Private Network มีข้อปฏิบัติดังนี้

2.2.1 มีการปรับปรุงช่องโหว่อย่างสม่ำเสมอ และสำรองค่า Configuration ของอุปกรณ์ทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลง หรือตามระยะเวลาที่กำหนด

2.2.2 เมื่อมีการทดสอบการเข้าใช้งานระบบสารสนเทศระยะไกลเสร็จสิ้น ให้ลบบัญชีผู้ใช้งานที่ใช้ในการทดสอบออกจากระบบเพื่อไม่ให้ผู้ไม่มีสิทธิเข้ามาใช้

2.2.3 ไม่มีการตั้งค่า Default Community, Default Username และ Default Password หรือให้ทำการเปลี่ยนค่าดังกล่าวเพื่อความปลอดภัย

2.2.4 กำหนดการพิสูจน์ตัวตน ที่มีความมั่นคงปลอดภัยในการส่งข้อมูล และต้องคงรักษาข้อมูลในการส่งให้มีความสมบูรณ์พร้อมในการใช้งาน

2.2.5 กำหนดให้มีการเข้ารหัสการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

2.2.6 ไม่อนุญาตให้เชื่อมต่อระยะไกลการใช้คำสั่งระบบ (Issuing System Commands) เว้นแต่ได้รับอนุญาตอย่างเป็นทางการจากสำนักงาน

2.2.7 จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

2.3 เครื่องแม่ข่ายและอุปกรณ์ที่ติดตั้งเพื่อการทำงานภายในสำนักงาน มีข้อปฏิบัติดังนี้

2.3.1 ปรับปรุงช่องโหว่อย่างสม่ำเสมอ และมีการสำรองค่า Configuration ของเครื่องแม่ข่ายทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลง หรือตามระยะเวลาที่กำหนด

2.3.2 กำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัย สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย ของบริการที่สำคัญ ที่สอดคล้องกับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2.3.3 กำหนดการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง

2.3.4 กำหนดรอบการปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างเหมาะสมและทันการณ์

2.3.5 ไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

2.3.6 ออกจากระบบทุกครั้งเมื่อเลิกใช้งาน

2.3.7 ผู้ดูแลระบบต้องสำรองข้อมูลและระบบปฏิบัติการ ตามนโยบายการสำรองข้อมูล (Backup Policy) ในหมวด 8 การบริหารจัดการด้านการดำเนินงาน (Operations Management)

2.3.8 อุปกรณ์แม่ข่ายและอุปกรณ์เครือข่ายต้องได้รับการตั้งค่าให้มีความมั่นคงปลอดภัยก่อนนำมาติดตั้งบนระบบเครือข่าย เช่น การกำหนดรหัสผ่านสำหรับบัญชีรายชื่อซึ่งใช้ในการบริการจัดการอุปกรณ์ให้มีความแข็งแกร่ง เปิด Service Port เฉพาะที่จำเป็นต้องใช้งานเท่านั้น เป็นต้น รวมทั้ง กำหนด Access Control List ของตัวอุปกรณ์สื่อสารเพื่อลดช่องโหว่ต่าง ๆ อย่างเหมาะสม

2.4 กำหนดให้มีวิธีปฏิบัติในการเก็บบันทึก Log และตรวจสอบสิ่งผิดปกติต่าง ๆ ภายในระบบเครือข่าย

2.5 การใช้งานเครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องกระทำโดยผู้ดูแลระบบเครือข่ายหรืออยู่ภายใต้การควบคุมดูแลของผู้ดูแลระบบเครือข่ายเท่านั้น และต้องได้รับการอนุมัติจากผู้จัดการส่วน/หัวหน้ากลุ่มงานที่เกี่ยวข้องก่อนทุกครั้ง โดยจะจำกัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น ตามที่กำหนดไว้ในนโยบายการดำเนินการของระบบสารสนเทศ

3. การควบคุมการเข้าถึงระบบเครือข่าย

3.1 ผู้ใช้งานทุกคนจะได้รับสิทธิในการเข้าใช้งานระบบต่าง ๆ รวมถึงระบบเครือข่าย ตามหน้าที่รับผิดชอบเท่าที่จำเป็นเท่านั้น โดยผู้ใช้งานที่ต้องการเข้าถึงระบบใด ๆ และระบบเครือข่าย ต้องดำเนินการขออนุมัติต่อผู้จัดการส่วน/หัวหน้ากลุ่มงานที่เกี่ยวข้องอย่างเหมาะสมทุกครั้ง ทั้งนี้ การพิจารณาให้สิทธิในการเข้าถึงระบบจะต้องสอดคล้องตามนโยบายการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

3.2 ผู้ใช้งานต้องระบุตัวตนผ่านระบบ Active Directory (AD) ของสำนักงานก่อนเข้าใช้งานระบบเครือข่ายของสำนักงานทุกครั้ง

3.3 การเชื่อมต่อเข้าสู่ระบบเครือข่ายของสำนักงานผ่านระบบเครือข่ายไร้สายต้องได้รับการเข้ารหัสอย่างเหมาะสม

3.4 การใช้งานเครือข่ายผู้ใช้งานต้องสามารถเข้าถึงระบบเครือข่าย ระบบเครือข่ายไร้สาย และระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตเข้าถึงเท่านั้น

3.5 กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (Access Matrix) ที่ได้กำหนดไว้

3.6 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) ต้องมีการทบทวนอย่างน้อยปีละ 2 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง

3.7 สิทธิการเข้าถึงของหน่วยงานภายนอก หรือผู้ให้บริการภายนอก (Third Party) ต้องได้รับการถอดถอนเมื่อสิ้นสุดการดำเนินงาน หมดสัญญา หรือสิ้นสุดข้อตกลงทันที และต้องมีการปรับปรุงให้เป็นปัจจุบัน

4. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกสำนักงาน (User Authentication for External Connections)

4.1 ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) เพื่อยืนยันตัวบุคคล ด้วยชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ทุกครั้ง

4.2 ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

5. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

5.1 ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ โดยมีการแสดงตัวตนด้วยชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password)

5.2 มีการควบคุมการใช้งานอย่างเหมาะสม ด้วย MAC address ของอุปกรณ์ที่สำนักงานอนุญาตให้ใช้งานได้

5.3 จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ ผ่าน IP address ที่อนุญาตเท่านั้น

5.4 ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของสำนักงานโดยไม่รับอนุญาต

5.5 ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย เช่น การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานเอง เป็นต้น

5.6 สายสัญญาณที่ใช้ในการเชื่อมต่อการสื่อสาร ทำการเดินในท่อนำสัญญาณอย่างเหมาะสมและมีการจัดหรือรวบสายสัญญาณให้เป็นระเบียบและจัดทำระเบียนสายสัญญาณ (Label)

6. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

6.1 ผู้ดูแลระบบต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ

6.2 บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

6.3 ตรวจสอบและปิดพอร์ตที่ไม่มีการใช้งาน หรือ เลิกใช้งาน หรือ พอร์ตที่ไม่จำเป็น เพื่อลดช่องว่างการเข้าถึงเครือข่าย

6.4 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้โดยจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

7. การแบ่งแยกเครือข่าย (Segregation in Networks)

7.1 ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานให้มีความเหมาะสมตามความต้องการควบคุมความปลอดภัย เพื่อควบคุมการเข้าถึงระบบและเครือข่ายสำคัญให้มีความมั่นคงปลอดภัยในการติดต่อสื่อสาร หรือการส่งผ่านข้อมูล โดยแบ่งออกเป็น 2 เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

7.2 กำหนดให้ให้มีการแยกสภาพแวดล้อมสำหรับระบบสำคัญ (Sensitive system isolation) โดยทำการแยกออกจากระบบอื่น (Segregation in networks)

7.3 กำหนดให้มีการแบ่งแยก และควบคุมเครือข่ายไร้สายกับเครือข่าย LAN ด้วยอุปกรณ์ Firewall เพื่อควบคุมการเข้าถึงที่เหมาะสม

8. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

8.1 ต้องมีการตรวจสอบการเชื่อมต่อเครือข่าย

8.2 จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

8.3 ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

8.4 มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

8.5 ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต โดยจัดให้มีการใช้งาน Firewall เพื่อควบคุมการเข้าใช้งานข้อมูล, แอพพลิเคชัน และ service ต่าง ๆ บนระบบเครือข่ายให้เป็นไปตามที่สำนักงานได้กำหนดไว้เท่านั้น และเพื่อป้องกันการเชื่อมต่อ (Connections) ต่าง ๆ ที่ไม่พึงประสงค์จากภายนอก โดยผู้ดูแลระบบ Firewall มีหน้าที่ในการตรวจสอบ, ดูแล และติดตั้ง Firewall ให้เป็นไปตาม Firewall Rule ที่กำหนดไว้ Firewall Rule ถือเป็นข้อมูลสำคัญซึ่งต้องได้รับการดูแลรักษาอย่างเหมาะสม ทั้งนี้ การดำเนินการเปลี่ยนแปลงใด ๆ ต่อ Firewall Rule จะต้องได้รับการอนุมัติและปฏิบัติตามนโยบายการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศอย่างเหมาะสมทุกครั้ง

9. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

9.1 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

9.2 ต้องมีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย

9.3 กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

10. การควบคุมการเข้าใช้งานระบบจากภายนอก (Remote Access)

10.1 การเข้าสู่ระบบจากภายนอก (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของสำนักงานต้องมีการกำหนดมาตรการรักษาความปลอดภัย

10.2 การเข้าสู่ระบบจากภายนอก (Remote Access) ต้องมีการตรวจสอบข้อมูล และพิสูจน์ตัวตนของผู้ใช้งาน โดย รหัสผ่าน หรือวิธีการเข้ารหัส และมีมาตรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

10.3 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาที่มีอำนาจ และมีการควบคุมอย่างเข้มงวดก่อนเข้าใช้โดยปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

10.4 มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ไม่เปิดพอร์ต (Port) และโมเด็ม (Modem) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น และตัดการเชื่อมต่อเมื่อไม่มีการใช้งาน

นโยบายการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

(Internet and E-mail Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (E-mail) ให้มีการป้องกันการเข้าถึงหรือการเปลี่ยนแปลงแก้ไขข้อความใน E-mail โดยไม่ได้รับอนุญาต และการรักษาข้อมูลและทรัพยากรต่าง ๆ ของสำนักงานให้มีความมั่นคงปลอดภัย

ผู้ปฏิบัติ ผู้ใช้งาน

อ้างอิง 1. เอกสารประกอบ นโยบายในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสม (Acceptable Use Policy)

2. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

ข้อปฏิบัติ

1. การใช้งานอินเทอร์เน็ต

1.1 ห้ามใช้และห้ามเผยแพร่ข้อมูลในเครือข่ายของสำนักงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือข้อมูลที่อาจก่อความเสียหายให้กับสำนักงาน

1.2 ผู้ใช้งานต้องเชื่อมต่ออินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่สำนักงานจัดสรรไว้เท่านั้น

1.3 ในการรับข้อมูลทางอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัสก่อนการใช้งาน

1.4 ผู้ใช้งานจะต้องไม่ Download ซอฟต์แวร์ที่ละเมิดทรัพย์สินทางปัญญา

1.5 ผู้ใช้งานจะถูกกำหนดในการเข้าถึงแหล่งข้อมูลตามหน้าที่ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยของข้อมูล

1.6 ผู้ใช้งานมีหน้าที่ต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้

1.7 ในกรณีที่ผู้ใช้งานพบเว็บไซต์ที่ไม่เหมาะสม เป็นภัยต่อความมั่นคงปลอดภัย ขัดต่อศีลธรรม หรืออาจกระทบต่อความปลอดภัยของสำนักงาน ผู้ใช้งานต้องยกเลิกการติดต่อกับเว็บไซต์ดังกล่าวและแจ้งส่วนงานที่รับผิดชอบทราบทันที

1.8 ในการใช้งาน Social Media หรือ Web board ของผู้ใช้งานเพื่อแลกเปลี่ยนข้อมูลในการปฏิบัติงานสามารถกระทำได้โดยจะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน โดยความคิดเห็นนั้นให้ถือว่าเป็นความคิดเห็นส่วนตัวของผู้ใช้งานไม่ใช่ความคิดเห็นจากสำนักงาน

1.9 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงานการทำลายความสัมพันธ์กับลูกค้าและพันธมิตรธุรกิจ

1.10 หลังใช้งานอินเทอร์เน็ตแล้ว ให้ปิด Web browser เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

2. การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

2.1 ต้องระวังในการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) เพื่อไม่ให้เกิดความเสียหายต่อสำนักงานหรือการใช้งานในทางที่ไม่เหมาะสม

2.2 ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของสำนักงานเพื่องานของสำนักงานเท่านั้น

2.3 ข้อมูลความลับหรือข้อมูลสำคัญที่ต้องส่งออกไปนอกสำนักงานต้องปฏิบัติตามเอกสารประกอบการจัดระดับชั้นความลับของข้อมูล

2.4 ต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ (E-mail) ก่อนทำการเปิด โดยการตรวจสอบไฟล์โดยใช้ ซอฟต์แวร์ป้องกันไวรัส หลีกเลี่ยงในการเปิดไฟล์ที่เป็น Executable file เช่น .EXE, .COM

2.5 ต้องมีความตระหนักในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) อย่างปลอดภัย

2.6 ห้ามใช้ซอฟต์แวร์ช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ

2.7 ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่น เพื่ออ่าน รับ ส่ง ข้อความ เว้นแต่จะได้รับการยินยอมจากเจ้าของ E-mail และให้ถือว่าเจ้าของ E-mail เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ใน E-mail ของตนเอง

2.8 ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของเอกชนในเครือข่ายของสำนักงาน ได้แก่ Hotmail, Yahoo, Gmail เป็นต้น ในการรับส่งข้อมูลสำคัญของสำนักงานเพื่อป้องกันข้อมูลความลับของสำนักงานรั่วไหล

นโยบายการใช้สื่อสังคมออนไลน์

(Social Media)

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงเครือข่ายสังคมออนไลน์ (Social Media) ของสำนักงาน

ผู้ปฏิบัติ ผู้ใช้งาน

ข้อปฏิบัติ

1. การใช้สื่อสังคมออนไลน์ (Social Media)

1.1 ข้อความ ภาพ เสียง วีดิโอคลิป หรือการกระทำการใด ๆ ที่เผยแพร่บน Social Media อันสามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบทั้งทางด้านสังคมและด้านกฎหมาย

1.2 ห้ามมิให้เผยแพร่ข้อมูลบน Social Media ที่เกี่ยวข้องกับกรณีดังต่อไปนี้

1.2.1 ข้อมูลปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือประชาชน หรือความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

1.2.2 ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

1.2.3 ข้อมูลใด ๆ ที่มีลักษณะอันลามก อนาจาร หรือขัดต่อศีลธรรมอันดีงาม

1.2.4 ข้อมูลที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

1.3 การกระทำการใด ๆ ที่เผยแพร่บน Social Media ต้องไม่เป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ต้องให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

1.4 การเผยแพร่ข้อมูลหรือการแสดงความเห็นใด ๆ บน Social Media ที่อาจทำให้ผู้อื่นเข้าใจว่าเป็นความเห็นจากสำนักงาน ผู้เผยแพร่ต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของสำนักงาน เว้นแต่จะเป็นความเห็นของสำนักงานอย่างแท้จริง หรือได้รับการอนุญาตจากผู้มีอำนาจที่เกี่ยวข้อง

1.5 การสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของสำนักงาน ต้องแจ้งให้ผู้อำนวยการหรือผู้บังคับบัญชาทราบ แล้วแต่กรณี และต้องแจ้งรายชื่อของผู้ดูแล Page (Admin) หรือเจ้าของ Account นั้นให้ผู้อำนวยการ หรือผู้บังคับบัญชาทราบ

ด้วย และผู้ดูแลมีหน้าที่ต้องมอบสิทธิในการดูแล Page หรือ Account นั้นคืนแก่สำนักงานเมื่อพ้นจากหน้าที่ที่ต้องดูแลหรือพ้นสภาพจากการเป็นเจ้าหน้าที่ของสำนักงาน

1.6 ห้ามมิให้เผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของสำนักงานบน Social Media ก่อนได้รับการอนุมัติอย่างเป็นทางการจากผู้อำนวยการ

1.7 ผู้ใช้งานจะต้องใช้งาน Social Media ด้วยความระมัดระวัง ดังนี้

1.7.1 ไม่ใช้ Social Media ส่วนบุคคล ในการปฏิสัมพันธ์กับผู้อื่นที่เป็นผู้ใช้บริการ ผู้ให้บริการ หรือผู้รับจ้างที่เกี่ยวข้องกับสำนักงาน

1.7.2 พึงงดเว้นการใช้ Social Media ในการวิพากษ์ วิจารณ์ ตลอดจนแสดงความเห็นในเรื่องที่เป็นข้อมูลภายในสำนักงาน หรืออาจส่งผลกระทบต่อสำนักงานได้

1.7.3 ใช้ตราสัญลักษณ์ (Logo) ของสำนักงานบนรูปประกอบ Profile ของตนได้ หาก Profile นั้นระบุชื่อและนามสกุลจริงอย่างถูกต้อง

1.7.4 ศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Settings” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบทการถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสม นอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลต่อสำนักงานได้ด้วย

1.8 หากพบว่ามีการกระทำใด ๆ บน Social Media ที่อาจก่อให้เกิดความเสียหายหรือความเสื่อมเสียชื่อเสียงแก่สำนักงาน นอกจากสำนักงานจะดำเนินกระบวนการตามกฎหมายที่เกี่ยวข้องกับความผิดนั้นแล้ว สำนักงานจะดำเนินการทางวินัยด้วย

นโยบายการถ่ายโอนข้อมูลสารสนเทศ
(Information Transfer Policy)

วัตถุประสงค์

เพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการถ่ายโอนภายในสำนักงาน หรือที่มีการถ่ายโอนข้อมูลสารสนเทศกับผู้ให้บริการภายนอก (Third Party) หรือหน่วยงานภายนอก โดยผ่านทางช่องทางการสื่อสารทุกชนิด

ผู้ปฏิบัติ ผู้ใช้งาน

อ้างอิง 1. เอกสารประกอบ นโยบายในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสม (Acceptable Use Policy)
2. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

ข้อปฏิบัติ

1. **ผู้ใช้งานจะต้องปฏิบัติตามแนวทางการถ่ายโอนข้อมูลสารสนเทศ** ดังนี้
   - 1.1 ป้องกันการถูกดักจับ คัดลอก แก้ไข และการทำลายข้อมูล
   - 1.2 ป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร (Attachment File) และใส่รหัสลับ
   - 1.3 ใช้เทคนิคการเข้ารหัส เพื่อปกป้องข้อมูลที่เป็นความลับ
   - 1.4 เครื่องถ่ายเอกสารหรือเครื่องพิมพ์ต้องมีการกำหนดรหัสผ่าน เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
   - 1.5 ต้องมีความตระหนักในการสื่อสารถ่ายโอนข้อมูลสารสนเทศ
   - 1.6 สำหรับการใช้เครื่องโทรสาร ผู้ใช้งานต้องมีความตระหนัก ดังนี้
     - 1.6.1 เครื่องโทรสารต้องอยู่ในพื้นที่ควบคุม เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
     - 1.6.2 ตรวจสอบเลขหมายปลายทางให้ชัดเจนก่อนส่งทุกครั้ง
     - 1.6.3 ตรวจสอบความครบถ้วนของเอกสารที่พิมพ์ออกมาทุกครั้ง

2. **ผู้ใช้งานจะต้องจัดทำข้อตกลงในการถ่ายโอนข้อมูลสารสนเทศ ดังนี้**
   - 2.1 กำหนดวิธีการติดต่อสื่อสารข้อมูล และมีการแจ้งให้ผู้รับ-ส่งทราบ
   - 2.2 บันทึกเกี่ยวกับการติดต่อสื่อสารข้อมูลที่สามารถติดตามและสอบกลับได้
   - 2.3 ทำข้อตกลงในการถ่ายโอนข้อมูลต้องคำนึงถึงนโยบาย และกฎหมายที่เกี่ยวข้อง
   - 2.4 ระบุความสำคัญของข้อมูล ตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล
   - 2.5 ส่งข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม ตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

นโยบายการบริหารจัดการรหัสผ่าน

(Password Management Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่าน

ผู้ปฏิบัติ ผู้ใช้งาน และส่วนงานที่เกี่ยวข้อง

ข้อปฏิบัติ

1. การบริหารรหัสผ่าน

1.1 “ชื่อผู้ใช้งานและรหัสผ่าน” ต้องไม่ถูกใช้งานร่วมกันหรือแบ่งปันกันใช้งานไม่ว่ากรณีใด ๆ

1.2 ผู้ใช้งานระบบสารสนเทศจะต้องกำหนดรหัสผ่านให้มีความมั่นคงปลอดภัย (Secure Password) ตามนโยบายการบริหารจัดการรหัสผ่านในกรณีที่ระบบสามารถควบคุมการกำหนดรหัสผ่านให้มีความมั่นคงปลอดภัยได้ ผู้ดูแลระบบ (System Administrator) หรือเจ้าของระบบ (System Owner) ต้องดำเนินการเพื่อให้แน่ใจว่ารหัสผ่านในระบบสอดคล้องตามนโยบายการบริหารจัดการรหัสผ่าน

1.3 ต้องมีกระบวนการที่มั่นคงปลอดภัยในการจัดส่งรหัสผ่าน (System Generated Password) ให้แก่ผู้ใช้งาน

1.4 รหัสผ่านเบื้องต้น (Initial Password) รหัสผ่านมาตรฐาน (Standard Password) และรหัสผ่านปริยาย (Default Password) ของระบบสารสนเทศต้องถูกเปลี่ยนโดย ผู้ดูแลระบบ (System Administrator) หรือเจ้าของระบบ (System Owner) ให้เป็นรหัสผ่านที่มั่นคงในทันทีที่การติดตั้งระบบเสร็จสิ้น

2. การกำหนดคุณภาพรหัสผ่าน

2.1 การกำหนดรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรมชื่อเฉพาะคำที่มีความหมายหรือไม่มีความหมายแต่ทราบโดยทั่วไป และไม่ใช้ข้อมูลที่เกี่ยวข้องกับสำนักงาน หรือเป็นข้อมูลส่วนตัวของผู้ใช้งานซึ่งอาจง่ายแก่การคาดเดา

2.2 ไม่กำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรหรือตัวเลขที่เรียงซ้ำกันเกินกว่า 3 ตัว หรือเรียงกันตามลำดับ เช่น aaaabbbb, 11111111, abcdefg

2.3 รหัสผ่านที่ดีต้องมีลักษณะดังนี้

2.3.1 ความยาวอย่างน้อย 8 ตัวอักษรหรือตามที่ผู้ดูแลระบบกำหนด

2.3.2 ส่วนประกอบของอักษร อักขระพิเศษ หรือตัวเลขประสมกันตามลักษณะดังนี้

(1) ตัวอักษรใหญ่ เช่น A, B, C, ...

(2) ตัวอักษรเล็ก เช่น a, b, c, ...

(3) ตัวเลข เช่น 0, 1, 2, ...

(4) สัญลักษณ์พิเศษ เช่น ! , @, # , $, ...

3. การใช้งานรหัสผ่าน

3.1 ไม่เก็บรหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย

3.2 ต้องพึงระวังผู้อื่นเห็นในขณะที่พิมพ์รหัสผ่าน

3.3 ห้ามใช้งานบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น เว้นแต่จะได้รับอนุญาตจากเจ้าของบัญชี

3.4 เปลี่ยนรหัสผ่านของตนเองที่ได้รับมาจากผู้ดูแลระบบ ไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตาม และไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิมที่ได้รับมา

3.5 ผู้ใช้งานต้องรายงานเหตุการณ์ที่สงสัยว่ามีการเปิดเผยรหัสผ่านไปยังผู้ดูแลระบบ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

3.6 ถ้าผู้ใช้งานไม่สามารถเข้าใช้งานระบบด้วยชื่อผู้ใช้และรหัสผ่านของตนเองได้ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ

4. การเปลี่ยนรหัสผ่าน

4.1 รหัสผ่านของผู้ดูแลระบบควรมีความถี่ในการเปลี่ยนรหัสผ่านให้บ่อยที่สุด

4.2 รหัสผ่านของผู้ใช้งานทั่วไป จะต้องเปลี่ยนทุก 90 วัน

4.3 ห้ามตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม 10 ครั้งล่าสุดที่เคยใช้มาแล้ว

หมวด 10 นโยบายการการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
(Information System Acquisition, Development and Maintenance policy)

วัตถุประสงค์

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

ผู้ปฏิบัติ ส่วนงานที่เกี่ยวข้อง

อ้างอิง 1. เอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

ข้อปฏิบัติ

1. **ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security Requirements of Information Systems)**

   1.1 ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องมีการพิจารณาร่วมกับความต้องการสำหรับระบบใหม่หรือระบบที่มีอยู่แล้ว

   1.2 สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันอย่างเหมาะสมจากการเปิดเผย เปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต

   1.3 สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการส่งข้อมูลซ้ำ โดยปฏิบัติตามเอกสารประกอบ การจัดระดับชั้นความลับของข้อมูล

2. **ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes)**

   2.1 กฎเกณฑ์ในการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดขั้นตอนการปฏิบัติงาน เพื่อเป็นแนวปฏิบัติในสำหรับการพัฒนาระบบของสำนักงาน

   2.2 การเปลี่ยนแปลงระบบ หรือการพัฒนาระบบต้องมีการควบคุม โดยปฏิบัติตามนโยบายการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy) และขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลง

2.3 เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบที่สำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือต่อความมั่นคงปลอดภัยของสำนักงาน

2.4 สำนักงานต้องพิจารณาสภาพแวดล้อมที่เหมาะสมต่อการพัฒนาระบบที่มีความมั่นคงปลอดภัย ได้แก่ พื้นที่ปฏิบัติงานไม่อยู่พื้นที่พลุกพล่าน หรือเข้าถึงได้ง่าย

2.5 การจ้างพัฒนาระบบจากผู้ให้บริการภายนอก ต้องมีการควบคุม เฝ้าระวัง ติดตามการดำเนินงานอย่างใกล้ชิดเพื่อให้เป็นไปตามขอบเขตการดำเนินงาน และสอดคล้องกับนโยบาย ขั้นตอนปฏิบัติของสำนักงานที่กำหนดไว้

2.6 ควรมีการทดสอบการใช้งานระบบ รวมถึงการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชันใหม่

2.7 ต้องมีการควบคุม กำหนดสิทธิการเข้าถึง Source Code อย่างเหมาะสมให้สอดคล้องตามบทบาทหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

2.8 ในกระบวนการพัฒนาระบบสารสนเทศ จะต้องมีระบบการตรวจทานความถูกต้องของข้อมูลที่ดี เพื่อลดความเสี่ยงที่อาจเกิดจากความผิดพลาดในการนำเข้าข้อมูล และความผิดพลาดของข้อมูลที่เกิดจากประมวลผลข้อมูล

2.9 ควรมีการควบคุมและตรวจสอบการทำงานของแอปพลิเคชัน เพื่อป้องกันความเสี่ยงที่อาจเกิดจากการทำงานหรือการประมวลผลข้อมูลที่ผิดพลาดอันจะส่งผลเสียต่อระบบโดยรวม

2.10 ควรจัดทำข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

3. การควบคุมข้อมูลในการทดสอบ (Test Data)

3.1 การป้องกันข้อมูลสำหรับการทดสอบ

ส่วนงานที่รับผิดชอบ และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง

หมวด 11 นโยบายการจัดการผู้ให้บริการภายนอก
(Third Party Management)

วัตถุประสงค์

การใช้บริการจากผู้ให้บริการภายนอก อาจก่อให้เกิดความเสี่ยงได้ ได้แก่ ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต การเกิดภัยคุกคามทางไซเบอร์ เป็นต้น จึงจำเป็นต้องมีการควบคุมผู้ให้บริการภายนอกที่มีการเข้าใช้งานระบบสารสนเทศและการสื่อสารของสำนักงานให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางการคัดเลือกควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก

ผู้ปฏิบัติ เจ้าหน้าที่ที่เกี่ยวข้อง, ผู้ให้บริการภายนอก และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน

อ้างอิง 1. เอกสารประกอบ บริหารงานจัดซื้อ/จัดจ้าง
2. เอกสารประกอบ การให้บริการโดยผู้ให้บริการภายนอก (Third Party Management Procedure)

ข้อปฏิบัติ

1. **นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) ด้านความสัมพันธ์กับผู้ให้บริการภายนอก**
   1.1. ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy)ที่เกี่ยวข้องกับผู้ให้บริการภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณา หรือประเมินความเสี่ยงที่อาจเกิดขึ้น และกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้ผู้ให้บริการภายนอก หรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศขององค์กร
   1.2. ผู้ดูแลระบบและส่วนงานที่รับผิดชอบในประสานงานกับผู้ให้บริการภายนอก ต้องกำกับให้มีการดูแลให้บุคคล หรือผู้ให้บริการภายนอกแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ
   1.3. ควรพิจารณาสร้างกระบวนการการตรวจสอบความถูกต้องของผู้ให้บริการภายนอก เพื่อให้สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ในเงื่อนไขของสัญญา
   1.4. ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

2. การควบคุมการเข้าใช้งานของผู้ให้บริการภายนอก (Third Party)

2.1 ต้องประเมินความเสี่ยงจากการเข้าถึงระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผล และมีมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบได้

2.2 ผู้ให้บริการภายนอก (Third Party) ที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของสำนักงานจะต้องทำเรื่องขออนุมัติจากผู้จัดการส่วน/หัวหน้ากลุ่มงานเจ้าของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าวเป็นลายลักษณ์อักษร ซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

2.2.1 เหตุผลในการขอใช้

2.2.2 ระยะเวลาในการใช้

2.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์เชื่อมต่อเครือข่าย

2.2.4 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

2.3 ผู้ให้บริการภายนอก (Third Party) ไม่ว่าจะปฏิบัติงานอยู่ภายในสำนักงานหรือนอกสำนักงานต้องลงนามในสัญญาการรักษาข้อมูลที่เป็นความลับของสำนักงาน

2.4 เจ้าของระบบมีหน้าที่กำหนดและทบทวนสิทธิของการเข้าใช้งานระบบสารสนเทศเฉพาะบุคคลที่จำเป็นเท่านั้น และมีการทบทวนสิทธิให้เป็นปัจจุบัน

2.5 สำนักงานต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของผู้ให้บริการภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบสารสนเทศ

2.6 สำนักงานมีสิทธิในการตรวจสอบตามสัญญาจ้างเพื่อให้มั่นใจได้ว่าสำนักงานสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.7 ในกรณีที่มีการเปลี่ยนแปลงการดำเนินงาน ผู้ให้บริการจากภายนอกต้องแจ้งให้สำนักงานรับทราบและอนุมัติการเปลี่ยนแปลงนั้น ก่อนการดำเนินงาน เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

2.8 เมื่อสิ้นสุดระยะเวลาการใช้งาน สำนักงานต้องดำเนินการยกเลิกสิทธิในการเข้าถึงแหล่งข้อมูล และแจ้งผู้จัดการส่วน/หัวหน้ากลุ่มงานเจ้าของข้อมูล

2.9 หากพบเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศให้แจ้งไปยังเจ้าของระบบ

2.10 ต้องดำเนินการตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) ที่สำนักงานประกาศไว้อย่างเคร่งครัด

3. การเลือกผู้ให้บริการภายนอก

ต้องปฏิบัติตามขั้นตอนปฏิบัติงานบริหารงานจัดซื้อ/จัดจ้าง

4. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

4.1 ต้องมีการระบุความต้องการด้านความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการที่เกี่ยวกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการสารสนเทศของสำนักงาน

4.2 ต้องระบุการยอมรับนโยบาย กฎหมายที่เกี่ยวข้องและการควบคุมด้านความมั่นคงปลอดภัยของสำนักงาน

4.3 สำนักงานมีสิทธิที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของผู้ให้บริการภายนอก

1. การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Third Party Service Delivery Management)

5.1 ต้องมีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการดำเนินการเป็นไปตามที่กำหนดไว้

5.2 กรณีมีการเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอก ผู้ให้บริการจากภายนอกต้องแจ้งให้สำนักงานรับทราบและอนุมัติการเปลี่ยนแปลงนั้น ก่อนการดำเนินงาน และต้องประเมินความเสี่ยง ตามขั้นตอนการบริหารจัดการการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการดำเนินงานเป็นไปตามขอบเขตที่ได้กำหนดไว้

5.3 กรณีมีการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบัน ต้องมีการสื่อสารให้ผู้ให้บริการภายนอกรับทราบ

หมวด 12 นโยบายการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
(Information Security Incident Management Policy)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศ และภัยคุกคามทางไซเบอร์ของสำนักงาน ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และมีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสำนักงาน

ผู้ปฏิบัติ ผู้พบเหตุ ส่วนงานที่เกี่ยวข้อง และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับของสำนักงาน

อ้างอิง
1. เอกสารประกอบ การจัดการเหตุการณ์ไม่ปกติ (Incident Management)
2. เอกสารประกอบ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan : CSIRT)

ข้อปฏิบัติ

1. กำหนดหน้าที่ความรับผิดชอบการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์อย่างชัดเจน รวมถึงรายละเอียดการติดต่อผู้ที่เกี่ยวข้อง
2. กำหนดขั้นตอนปฏิบัติรับมือเหตุละเมิดด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงาน โดยจำแนกสถานการณ์ เกณฑ์ ขั้นตอนในการเรียกใช้งาน การตอบสนองต่อเหตุการณ์ เพื่อจำกัดขอบเขตผลกระทบของเหตุการณ์ และการเรียกใช้งานกระบวนการกู้คืน
3. กำหนดกระบวนการทบทวน หลังแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ เพื่อป้องกันการเกิดปัญหาซ้ำ
4. ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
5. รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ ต้องมีการกำหนดโครงสร้างการรายงานเหตุการณ์ที่สอดคล้องตามที่กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้อง
6. เรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ ต้องมีการวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด อย่างน้อยปีละ 1 ครั้ง
7. เก็บรวบรวมหลักฐานโดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบสำนักงาน และกฎหมายที่เกี่ยวข้อง

หมวด 13 นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ
(Business Continuity Management Policy)

วัตถุประสงค์

เพื่อเป็นแนวทางในการบริหารจัดการความต่อเนื่องในการดำเนินงานของสำนักงาน เมื่ออยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของสำนักงานที่สำคัญ มีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP) และแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม เพื่อให้การดำเนินงานของสำนักงาน เป็นไปอย่างต่อเนื่อง

ผู้ปฏิบัติ คณะบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย/สร้างความต่อเนื่องทางธุรกิจ และส่วนงานที่เกี่ยวข้อง

อ้างอิง
1. เอกสารประกอบ คู่มือระบบบริหารจัดการด้านเทคโนโลยีสารสนเทศ (ITMS Manual)
2. เอกสารประกอบ แผนบริหารความต่อเนื่องทางธุรกิจระดับองค์กร
3. เอกสารประกอบ แผนการรับมือภัยคุกคามทางไซเบอร์ เบอร์ (Cybersecurity Incident Response Plan : CSIRT)
4. เอกสารประกอบ แผนสื่อสารในภาวะวิกฤต

ข้อปฏิบัติ

1. ขั้นตอนเตรียมการของแผนรองรับเหตุการณ์ฉุกเฉิน

1.1 สำนักงานต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากส่วนงานเจ้าของข้อมูล เจ้าของระบบงาน

1.2 คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ และแผนการรับมือภัยคุกคามทางไซเบอร์ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผน อย่างน้อย ปีละ 1 ครั้ง

1.3 กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ประกอบด้วย

1.3.1 การวิเคราะห์ผลกระทบทางการดำเนินงานของสำนักงาน (Business Impact Analysis)

1.3.2 การประเมินความเสี่ยงและการควบคุม (Risk Analysis & Control)

1.3.3 แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP) แผนการกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan)

1.3.4 การประชาสัมพันธ์และการฝึกอบรมการทดสอบ ปรับปรุงแผนรองรับ

1.4 แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

1.4.1 เพื่อป้องกันผลกระทบและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อการให้บริการของสำนักงาน

1.4.2 เพื่อกำหนดแนวทางในการจัดการต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย

1.4.3 เพื่อให้กระบวนการการดำเนินงานเป็นไปได้อย่างต่อเนื่อง ได้แก่ การสำรองข้อมูล การกู้คืนระบบ เป็นต้น

1.4.4 ต้องมีแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ

2. การตอบสนองต่อเหตุการณ์ฉุกเฉินเพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง

2.1 ระบุขั้นตอนการดำเนินการ ประเมินสถานการณ์เบื้องต้น สถานที่ สาเหตุ และขอบเขต ความเสียหาย เพื่อระงับเหตุการณ์ความเสียหาย และวิธีการดำเนินงานต่าง ๆ ที่เกี่ยวข้อง ได้แก่ แนวทางการเก็บรักษาข้อมูล เอกสาร ความปลอดภัยของผู้ปฏิบัติงาน การเคลื่อนย้ายอพยพพนักงานและผู้ใช้งานและสินทรัพย์ที่จำเป็น

2.2 ระบุแผนปฏิบัติการด้านการติดต่อสื่อสารกำหนดวิธีการสื่อสารและประสานงานกับหน่วยงานหรือบุคคลที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งสถานการณ์ และแนวทางการดำเนินงาน หรือสถานที่ติดต่อฉุกเฉิน รวมทั้งจัดทำรายชื่อหน่วยงาน หรือผู้ที่รับผิดชอบ ในการดำเนินการช่วยเหลือ ยุติเหตุการณ์ความเสียหายทั้งภายในและภายนอกสำนักงาน

2.3 ระบุความต้องการใช้ทรัพยากรต่าง ๆระบุความต้องการทรัพยากรที่มีความจำเป็น งบประมาณ จำนวนแรงงาน สถานที่ ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค อุปกรณ์และเครื่องมือต่าง ๆ ให้ชัดเจน

3. การกลับคืนสู่การทำงานปกติ

3.1 ระบุขั้นตอนการปฏิบัติงานเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ การควบคุมการติดตั้ง การตั้งค่าและทดสอบระบบที่ถูกกู้คืนมาหรือทดแทนใหม่ การรายงานสรุปความเสียหายต่อผู้บังคับบัญชา

3.2 ระบุรายชื่อผู้ที่เกี่ยวข้องจัดทำรายชื่อของหน่วยงาน หรือผู้ที่รับผิดชอบทั้งจากภายในและภายนอก เพื่อการดำเนินการช่วยเหลือ ฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ

3.3 การกำหนดกระบวนการป้องกันและควบคุมความเสี่ยง เพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ความเสียหายในอนาคต

4. การประชาสัมพันธ์ และการฝึกอบรม

4.1 ระบุขั้นตอนและวิธีการประชาสัมพันธ์ให้แก่เจ้าหน้าที่ ผู้ใช้งาน ลูกค้า ผู้ใช้บริการ และจัดฝึกอบรมให้แก่ผู้มีส่วนเกี่ยวข้องให้รับทราบถึงวัตถุประสงค์ ขั้นตอนการปฏิบัติงาน การประสานงาน การติดต่อสื่อสาร แผนการสื่อสารในภาวะวิกฤต ขั้นตอนการรายงาน ระบบรักษาความปลอดภัย และหน้าที่ความรับผิดชอบตามแผนอย่างชัดเจน

5. การทดสอบ ปรับปรุง และสอบทานแผนฉุกเฉิน

5.1 การทดสอบ

5.1.1 กำหนดเวลาการทดสอบแผนกู้คืนที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้นจนสิ้นสุดกระบวนการทดสอบ

5.1.2 กำหนดเหตุการณ์จำลองและรายละเอียดของเหตุการณ์ที่จะใช้ทดสอบต้องระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน

5.1.3 กำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบแผน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่าง ๆ และงบประมาณที่ต้องใช้

5.1.4 กำหนดเกณฑ์การประเมินผลและผู้รับผิดชอบในการประเมินผล เกณฑ์การประเมินผลซึ่งอาจมีความแตกต่างกันไปตามลักษณะของระบบงาน กระบวนการทำงาน และวัตถุประสงค์ของการทดสอบในแต่ละครั้ง

5.1.5 ต้องมีการทดสอบสภาพพร้อมใช้งานระบบสารสนเทศ และระบบสำรอง(ถ้ามี) เพื่อประสิทธิภาพในการให้บริการ และประเมินต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง

5.2 การปรับปรุงและสอบทานแผน

5.2.1 กำหนดเวลา แนวทาง ระยะเวลา และปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

5.2.2 กำหนดผู้รับผิดชอบในการสอบทานแผน เพื่อยืนยันความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผน

5.3 รายละเอียดเพิ่มเติมอื่น ๆ

5.3.1 รายชื่อ ที่อยู่ และหมายเลขโทรศัพท์ของเจ้าหน้าที่และผู้ใช้งานที่มีหน้าที่รับผิดชอบในการปฏิบัติตามแผน

5.3.2 รายชื่อหน่วยงาน สถานที่ตั้ง และหมายเลขโทรศัพท์ของหน่วยงานภายนอกที่เกี่ยวข้อง

5.3.3 รายละเอียดการปฏิบัติตามแผน (Checklist)

5.3.4 รูปแบบรายงานต่าง ๆ ที่จำเป็น

6. สภาพความพร้อมใช้ของอุปกรณ์สารสนเทศ

6.1 ต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งานของระบบสารสนเทศที่มีความสำคัญสูง

6.2 ต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

หมวด 14 นโยบายการปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with Legal Requirements Policy)

วัตถุประสงค์

เพื่อป้องกันการละเมิดตามกฎหมายที่เกี่ยวข้องกับการปฏิบัติงาน ระเบียบ ข้อบังคับ เงื่อนไขในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เพื่อเป็นแนวทางในการปฏิบัติงานของสำนักงานที่สอดคล้องกับมาตรฐาน ข้อกำหนดของกฎหมายตลอดจนนโยบายด้านความมั่นคงปลอดภัย

ผู้ปฏิบัติ ส่วนกฎหมาย ผู้ใช้งานและส่วนงานที่เกี่ยวข้อง

อ้างอิง 1. เอกสารประกอบ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. เอกสารประกอบ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ข้อปฏิบัติ

1. การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย (Identification of Applicable Legislation)

1.1. ส่วนกฎหมาย ต้องระบุข้อกำหนดทางด้านกฎหมาย ระเบียบปฏิบัติ และสัญญาว่าจ้าง รวมทั้งสัญญาที่ทำกับผู้ให้บริการภายนอก (Third Party) หรือบุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานหรือภารกิจของสำนักงาน และบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร

1.2. ปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

2. การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานทรัพย์สินทางปัญญา (Compliance with Intellectual Property Rights (IPR))

2.1 การนำซอฟต์แวร์ของบุคคลที่สามมาใช้ในสำนักงาน ต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ (Licensing Agreement) ถูกต้องตามกฎหมาย

2.2 ผู้ใช้งานซอฟต์แวร์บนระบบสารสนเทศของสำนักงาน ต้องยึดถือและปฏิบัติตามกฎหมายและข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

2.3 ต้องควบคุมการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ โดยมีการบันทึกข้อมูลการใช้งาน เพื่อเก็บเป็นหลักฐาน และมีการตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง ถ้าหากพบว่ามีการละเมิดข้อตกลงจะต้องทำการยกเลิกการติดตั้งหรือลบทิ้งทันที

2.4 ซอฟต์แวร์หรือระบบงานที่พัฒนาขึ้นเพื่อสำนักงาน ถือเป็นสินทรัพย์ของสำนักงาน ทั้งนี้เพื่อเป็นการป้องกันข้อพิพาทในเรื่องกรรมสิทธิของซอฟต์แวร์ที่อาจเกิดขึ้น

2.5 ซอฟต์แวร์ที่ถูกพัฒนาโดยเจ้าหน้าที่หรือลูกจ้าง ถือเป็นสินทรัพย์ของสำนักงาน

2.6 การติดตั้งซอฟต์แวร์ใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการปรับปรุงระบบหรือซ่อมแซมแก้ไขระบบต่าง ๆ จากผู้ให้บริการภายนอกต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

2.7 ถ้ามีการติดตั้งซอฟต์แวร์ใด ๆ ในเครื่องคอมพิวเตอร์ของสำนักงาน โดยไม่ได้รับอนุญาตแล้วเกิดข้อพิพาททางกฎหมาย หรือข้อกำหนดและเงื่อนไขของผู้ผลิตซอฟต์แวร์นั้น ๆ ทาง **“สำนักงานขอสงวนสิทธิที่จะไม่รับผิดชอบในการดำเนินการดังกล่าวไม่ว่าจะกรณีใด ๆ ”**

2.8 ห้ามมิให้ผู้ใช้งานคัดลอก แก้ไข หรือปรับแต่ง ซอฟต์แวร์ที่เป็นสินทรัพย์ของสำนักงาน หรือนำไปให้ผู้อื่นใช้งานโดยไม่ได้รับอนุญาต

3. การป้องกันข้อมูลสำคัญของสำนักงาน (Protection of Organizational Records)

3.1 ข้อมูลสำคัญของสำนักงาน ต้องได้รับการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึง และการเผยแพร่โดยไม่ได้รับอนุญาต

3.2 การปฏิบัติงานต้องสอดคล้องกับกฎหมาย นโยบาย ระเบียบ ข้อบังคับ ของสำนักงาน

4. การป้องกันข้อมูลส่วนบุคคลและการเข้ารหัส

4.1 ผู้ใช้งานและส่วนงานที่เกี่ยวข้อง ต้องศึกษาและปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องกับการป้องกันข้อมูลส่วนบุคคล ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น

4.2 ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนบุคคลของผู้ใช้งาน ได้แก่ ข้อมูลในจดหมายอิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น

4.3 ผู้ดูแลระบบ ต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายภายในประเทศและต่างประเทศ เกี่ยวกับการเข้ารหัสข้อมูล กรณีมีเหตุจำเป็นในการโยกย้ายข้อมูลที่เข้ารหัสไปยังอีกประเทศหนึ่ง ให้ศึกษาและปฏิบัติตามข้อกำหนด หรือกฎหมายของประเทศนั้นด้วย

5. การป้องกันการใช้งานอุปกรณ์สารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)

5.1 อุปกรณ์สารสนเทศของสำนักงานมีไว้เพื่อใช้ในกิจการของสำนักงานเท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บังคับบัญชาที่มีอำนาจ

5.2 ต้องกำหนดให้มีผู้รับผิดชอบรวมถึงส่วนที่รับผิดชอบต้องจัดทำบัญชีรายการของอุปกรณ์สารสนเทศที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้ส่วนจัดซื้อและพัสดุ

5.3 ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของสำนักงาน

5.4 การดำเนินการใด ๆ ที่เป็นการติดตั้งซอฟต์แวร์หรืออุปกรณ์เพิ่มเติมต้องได้รับการอนุมัติจากผู้บังคับบัญชาที่มีอำนาจเป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

5.5 อุปกรณ์สารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนเป็นอย่างน้อย ก่อนการเข้าใช้งานด้วยวิธีการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

6. การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of Cryptographic Controls)

6.11 มาตรการการเข้ารหัสข้อมูล

6.11.1 เจ้าของข้อมูลต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศ เพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้ รวมทั้งต้องสามารถบ่งชี้ตัวตนของเจ้าของหรือผู้ดูแลกุญแจรหัสได้ (Binding keys to identities)

6.11.2 เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง กรณีที่ไม่ทราบหรือต้องการข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติม ให้ติดต่อที่ส่วนงานที่รับผิดชอบ

6.11.3 เจ้าของข้อมูลต้องมีการเข้ารหัสข้อมูลให้สอดคล้องตามชั้นความลับ เมื่อมีการส่งข้อมูลไปยังเครือข่ายสาธารณะ

7. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

7.1 ผู้จัดการส่วน/หัวหน้ากลุ่มงานต้องกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัย ตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยของสำนักงาน

7.2 วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย วัตถุประสงค์ มาตรการ นโยบาย กระบวนการ ขั้นตอนการปฏิบัติ การประเมินความเสี่ยง ต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

7.3 ต้องมีการทบทวนความสอดคล้องทางเทคนิคของระบบอย่างสม่ำเสมอเพื่อพิจารณาความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy)ของสำนักงาน

8. มาตรการการตรวจประเมินระบบสารสนเทศ (Information Systems Audit Controls)

8.1 ต้องมีการวางแผนการตรวจประเมินระบบสารสนเทศ เพื่อให้ลดผลกระทบต่อระบบและกระบวนการดำเนินงานของสำนักงานอย่างน้อยปีละ 1 ครั้ง

9 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of Information Systems Audit Tools)

9.1 ต้องมีแนวทางป้องกันเครื่องมือที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำเครื่องมือไปใช้ในทางที่ผิด และป้องกันการเข้าถึงข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยเครื่องมือ