การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

1. เพื่อกำหนดการเข้าถึงข้อมูลสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัยด้านสารสนเทศ
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิและการมอบอำนาจของหน่วยงานของรัฐ
3. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
4. เพื่อให้การตรวจสอบและติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

นโยบาย

บุคลากรสำนักงานโครงการ TO BE NUMBER ONE และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

1. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ / เจ้าของข้อมูล ตามความจำเป็นต่อการใช้งานเท่านั้น
2. ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น
3. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึง อย่างสม่ำเสมอ ดังนี้

3.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

3.1.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

3.1.2 กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

3.1.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหนาหน่วยงานหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

3.2 การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

3.2.1 จัดแบ่งประเภทของข้อมูลออกเป็น ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

3.2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

3.2.3 จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง
- ข้อมูลลับ หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
- ข้อมูลใช้งานภายในหน่วยงาน หมายถึง ข้อมูลที่ใช้งานภายในหน่วยงาน และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกหน่วยงาน
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความ มั่นคงปลอดภัย ข้อมูลที่เผยแพร่สู่สาธารณะ ผ่านช่องทางที่เหมาะสมซึ่งองค์กรพิจารณาอนุมัติ หากข้อมูลสูญหายหรือถูกเปิดเผยจะไม่ส่งผลเสียหายต่อองค์กร

3.2.4 จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

3.2.5 รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อย อีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)
- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่ เป็นซอฟต์แวร์มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

4. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

5. เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพ (Physical Access) และจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าวต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากสำนักงานโครงการ TO BE NUMBER ONE และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหายบุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

6. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไข เปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

7. การจัดการสื่อบันทึกข้อมูล (Media Handing)

7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยก/เคลื่อนย้ายได้ (Management of Removable Media) กรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ต้องจัดให้มีกระบวนการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูลและไม่ให้สามารถกู้คืนข้อมูลได้

7.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

7.2.1 ผู้ดูแลระบบ / ผู้ใช้งานต้องทำลายข้อมูลที่เป็นความลับ ที่บันทึกในอุปกรณ์สื่อบันทึกข้อมูลแฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบ หรือเขียนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันการรั่วไหลของข้อมูล หรือป้องกันไม่ให้ข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูล แต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้เครื่องหั่นแผ่น CD/DVD หรือกรรไกตัดทำลาย
ฮารดดิสก์	- ให้การทำลายข้อมูลบน ฮารดดิสก์ ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

7.2.2 กรณีที่จัดเก็บเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใหม่

8.3 การขนย้ายสื่อบันทึก (Physical Media Transfer)

8.3.1 ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ ทำการจะต้องดูแลรักษาความปลอดภัย จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์หรือทำให้เสียหายระหว่างการขนย้าย

8.3.2 ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการ ต้องชดใช้ค่าเสียหาย ไม่ว่าทรัพย์สินนั้นจะชำรุด หรือ สูญหายตามมูลค่าของทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึก
