BIG DATA INSTITUTE

ประกาศสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
เรื่อง นโยบายธรรมาภิบาลข้อมูล

ด้วยพระราชบัญญัติการบริการงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ บัญญัติให้หน่วยงานของรัฐ ต้องจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ ๑๒ มีนาคม พ.ศ. ๒๕๖๓

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. ๒๕๖๖ ประกอบกับมติที่ประชุมคณะทำงานธรรมาภิบาลข้อมูลและกำกับดูแลการปฏิบัติตามกฎหมายที่เกี่ยวข้อง ครั้งที่ ๑/๒๕๖๗ เมื่อวันที่ ๒๑ มิถุนายน ๒๕๖๗ จึงประกาศนโยบายธรรมาภิบาลข้อมูล เพื่อใช้สำหรับยึดถือปฏิบัติภายในสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) รายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๔ กรกฎาคม พ.ศ.๒๕๖๗

(นางสาวธีรณี อจลากุล)
ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่

เอกสารแนบท้ายประกาศสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
เรื่อง นโยบายธรรมาภิบาลข้อมูล ลงวันที่ 4 กรกฎาคม พ.ศ.2567

นโยบายธรรมาภิบาลข้อมูล
(Data Governance Policy)

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

เวอร์ชัน 1.0

สารบัญ

1. บทนำ 3
2. วัตถุประสงค์ 3
3. นิยาม 3
4. โครงสร้างธรรมาภิบาลข้อมูล 5
5. นโยบายธรรมาภิบาลข้อมูล 7
   5.1 นโยบายทั่วไป 7
   5.2 กระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes) 9
6. การจัดเก็บข้อมูลและทำลายข้อมูล 10
   6.1 นโยบายการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Policy) 10
   6.2 แนวปฏิบัติการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Guideline) 11
7. การใช้ข้อมูล (Data Usage) 13
   7.1 นโยบายการใช้ข้อมูล (Data Usage Policy) 13
   7.2แนวปฏิบัติการใช้ข้อมูล (Data Usage Guideline) 14
8. การจำแนกข้อมูล (Data Classification) 15
   8.1 นโยบายการจำแนกข้อมูล (Data Classification Policy) 15
   8.2 แนวปฏิบัติการจำแนกข้อมูล (Data Classification Guideline) 21
9. การรักษาความปลอดภัยทางข้อมูลสารสนเทศ (Information Security) 23
   9.1 นโยบายการรักษาความปลอดภัยทางข้อมูลสารสนเทศ (Information Security Policy) 23
   9.2 แนวปฏิบัติการรักษาความปลอดภัยทางข้อมูลสารสนเทศ (Information Security Guideline) 26
10. การบูรณาการและแลกเปลี่ยนข้อมูล (Data Exchange) 29
   10.1 นโยบายการบูรณาการและแลกเปลี่ยนข้อมูล (Data Exchange Policy) 29
   10.2 แนวปฏิบัติการบูรณาการและแลกเปลี่ยนข้อมูล (Data Exchange Guideline) 29
11. การสำรองและกู้คืนข้อมูล (Data Backup & Recovery) 31
   11.1 นโยบายการสำรองและกู้คืนข้อมูล (Data Backup & Recovery Policy) 31
   11.2 แนวปฏิบัติการสำรองและกู้คืนข้อมูล (Data Backup & Recovery Guideline) 31
12. การประเมินผลธรรมาภิบาลข้อมูล (Data Governance Assessment) 34

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

1. บทนำ

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (สขญ.) จัดตั้งขึ้นเพื่อตอบสนองการดำเนินงานตามแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) และรองรับการให้บริการด้านการพัฒนาเจ้าหน้าที่และการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) ของภาครัฐ ตามยุทธศาสตร์ชาติยุทธศาสตร์ที่ 6 ด้านการปรับสมดุลและการพัฒนาระบบบริหารจัดการภาครัฐ ที่กำหนดให้มีระบบการบริหารจัดการข้อมูลที่มีความเชื่อมโยงระหว่างหน่วยงาน และแหล่งข้อมูลต่าง ๆ ไปสู่การวิเคราะห์การจัดการข้อมูลขนาดใหญ่ โดยมีวัตถุประสงค์เพื่อส่งเสริมให้เกิดวัฒนธรรมการวิเคราะห์และใช้ประโยชน์ข้อมูลขนาดใหญ่เพื่อประกอบการตัดสินใจ (Data-Driven Decision) สกัดข้อมูลเชิงลึกในการดำเนินงาน (Insight to Operation) และช่วยเหลือให้หน่วยงานภาครัฐสามารถให้บริการประชาชนได้อย่างเป็นรูปธรรม

การดำเนินงานของ สขญ. ได้มีส่วนเข้าไปเกี่ยวข้องกับข้อมูลจากหลากหลายหน่วยงาน ทั้งข้อมูลที่เปิดเผยได้ และไม่สามารถเปิดเผยได้ เป็นข้อมูลที่มีความอ่อนไหว หรือเป็นข้อมูลที่เป็นความลับของทางราชการที่ต้องมีการบริหารจัดการสิทธิการเข้าถึงข้อมูล ดังนั้นจึงจำเป็นต้องมีการวางกรอบนโยบาย ธรรมาภิบาล (Data Governance) ในการจัดเก็บ จัดการดูแล นำไปใช้ ประมวลผล แลกเปลี่ยนและเผยแพร่ข้อมูล ให้เป็นไปอย่างมีระบบ มีการกำหนดนโยบายและแนวทางในการปฏิบัติที่ชัดเจน สอดคล้องตามมาตรฐาน ตามความถูกต้องเหมาะสม และตามกฎระเบียบ ข้อบังคับ หรือกฎหมายที่เกี่ยวข้องกับข้อมูลหรือกระบวนการต่างๆ กรอบนโยบายธรรมาภิบาลข้อมูลและแนวปฏิบัตินี้ฝ่ายต่างๆ และเจ้าหน้าที่ทุกคนของ สขญ. ต้องนำไปใช้ได้อย่างเหมาะสม โดยเข้าใจถึงสิทธิ หน้าที่ และความรับผิดชอบของการมีส่วนได้ส่วนเสียในข้อมูล รวมทั้งเป็นต้นแบบการดูแลข้อมูล และส่งเสริมความเชื่อมั่นของ สขญ.

2. วัตถุประสงค์

2.1 เพื่อให้การบริหารจัดการข้อมูลของ สขญ. สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

2.2 เพื่อใช้เป็นกรอบและแนวทางสำหรับผู้บริหาร เจ้าหน้าที่ สขญ. และผู้ที่เกี่ยวข้อง ในการบริหารจัดการข้อมูลของหน่วยงาน

3. นิยาม

3.1 BDI หรือ สขญ. หมายถึง สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

3.2 ข้อมูล (Data) หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

3.3 ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคลและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

3.4 หมวดหมู่ของข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น ๔ หมวดหมู่ ดังนี้ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และ ข้อมูลสาธารณะ

3.5 การจัดชั้นความลับของข้อมูล คือ การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

3.6 วงจรชีวิตของข้อมูล (Data Life Cycle) คือ ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูล

3.7 ระบบคอมพิวเตอร์แม่ข่าย คือ เครื่องคอมพิวเตอร์ประมวลผลระดับสูง ที่มีเสถียรภาพ ทั้งในด้านการบริหารจัดการหน่วยจัดเก็บข้อมูล หน่วยความจำ การเชื่อมต่อระบบเครือข่าย และการใช้พลังงานไฟฟ้า โดยทำงานในการให้บริการระบบโปรแกรมประยุกต์ (Application) ระบบข้อมูลสารสนเทศ (MIS) และระบบฐานข้อมูล (Database) แก่ผู้ใช้งาน (User) ผ่านเว็บไซต์ (Website) หรือโปรแกรมคอมพิวเตอร์ลูกข่าย (Client Server Software) บนระบบเครือข่ายภายใน (Intranet) และระบบเครือข่ายอินเทอร์เน็ต (Internet)

3.8 การสำรองข้อมูลสารสนเทศ (Backup) คือ กระบวนการจัดเก็บข้อมูลของเครื่องคอมพิวเตอร์ทั้งระบบปฏิบัติการ (Operation System) ข้อมูลการตั้งค่า (Configuration Data) และข้อมูลอื่น ๆ (Data) โดยการคัดลอกข้อมูลของเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ในปัจจุบัน บนสื่อบันทึกข้อมูลภายนอกเครื่องคอมพิวเตอร์ เพื่อป้องกันข้อมูลเสียหาย (Data Corruption) และข้อมูลสูญหาย (Data Deletion / Data Loss) จากความตั้งใจหรือความประมาทของผู้ใช้งาน รวมถึง การเกิดภัยพิบัติ (Disaster) ที่มีผลกระทบต่อเครื่องคอมพิวเตอร์ดังกล่าว

3.9 การกู้คืนข้อมูลสารสนเทศ (Recovery) คือ กระบวนการแก้ไขปัญหาที่เกิดกับข้อมูลของเครื่องคอมพิวเตอร์ จากสื่อบันทึกข้อมูลที่สำรองข้อมูลสารสนเทศ

3.10ผู้รับผิดชอบข้อมูล หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย ผู้รับผิดชอบข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำดาตาคลีนซิ่ง (Data Cleansing)

3.11ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือ ที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

3.12การประมวลผลข้อมูล หมายถึง การปฏิบัติการหรือส่วนหนึ่งของการปฏิบัติการซึ่งได้กระทำต่อข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การดัดแปลง ปรับเปลี่ยน การกู้คืน การให้คำปรึกษา การใช้ การเปิดเผยโดยการส่ง การแพร่กระจาย หรือทำให้มีอยู่ การจัดวางให้ถูกตำแหน่งหรือการรวม การจำกัด การลบ และการทำลาย

3.13ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3.14ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” โดยที่ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

4. โครงสร้างธรรมาภิบาลข้อมูล

เพื่อแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล และแสดงถึงสิทธิ์ในการสั่งการตามลำดับขั้น จำเป็นต้องกำหนดโครงสร้างเจ้าหน้าที่ที่รับผิดชอบในธรรมาภิบาลข้อมูล องค์ประกอบสำคัญหนึ่งในโครงสร้าง ได้แก่ คณะกรรมการธรรมาภิบาลข้อมูล (Data Council) และคณะทำงานด้านธรรมาภิบาลข้อมูล ซึ่งมีอำนาจหน้าที่ ดังนี้

1) กำหนดหลักเกณฑ์และวางแนวทางในการจัดเก็บ การประมวลผลและการเผยแพร่ข้อมูล เพื่อเตรียมความพร้อมด้านความมั่นคงปลอดภัยของข้อมูลของ สขญ.

2) กำหนดหลักเกณฑ์ แนวทาง ตลอดจนพิจารณาให้ความเห็นชอบรับรอง แนวปฏิบัติวิธีการดำเนินงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและสารสนเทศภายใต้การดำเนินการของ สขญ.

3) กำหนดหลักเกณฑ์การพิจารณาการเปิดเผยข้อมูล และระดับชั้นความลับที่ สขญ. ถือครองและประมวลผลข้อมูล เพื่อให้บริการแก่บุคคลภายใน และหน่วยงานภายนอกของ สขญ.

4) ติดตามการจัดเก็บข้อมูล การจัดทำบัญชีข้อมูล (Data catalog) และการจัดระดับความสำคัญของข้อมูลภายในของ สขญ.

5) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมาย

เจ้าหน้าที่ที่เกี่ยวข้องในโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ แบ่งออกเป็น 3 ส่วน ประกอบด้วย (1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) (2) ทีมบริกรข้อมูล (Data Steward Team) หรือฝ่ายเทคโนโลยีสารสนเทศ และ (3) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)

(1) <u>คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)</u>

คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ประกอบไปด้วย ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) และตัวแทนจากฝ่ายต่างๆ ของ สขญ.

ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ทำหน้าที่ กำหนดวิสัยทัศน์ ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) มีหน้าที่นำข้อมูลและวิเคราะห์ข้อมูลของหน่วยงานเพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานมีคุณค่า และเกิดประโยชน์สูงสุดต่อหน่วยงาน นอกจากนี้ยังต้องวิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการธรรมาภิบาลข้อมูลให้มีคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูลของหน่วยงาน และนำแนวปฏิบัติและมาตรฐานของหน่วยงานไปปรับปรุงข้อมูลและยุทธศาสตร์ของประเทศ โดยในส่วนของการทำงานในระดับประเทศ ผู้บริหารข้อมูลระดับสูง จะต้องทำหน้าที่เป็นตัวกลางระหว่างหน่วยงานในการแลกเปลี่ยน เชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงาน รวมถึงส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหาเพื่อแก้ไขจนสามารถลดปัญหาของประเทศที่เกิดขึ้นในปัจจุบัน และลดความเสี่ยงของปัญหาที่อาจเกิดขึ้นในอนาคตได้ พร้อมทั้งต้องวิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูลให้ตอบสนองความต้องการของประชาชนด้วย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) เป็นผู้บริหารที่มีบทบาทสูงสุดในการทำให้หน่วยงานมีความปลอดภัยเพียงพอ สำหรับการทำงานทั้งด้านการบริหารจัดการดูแล และด้านข้อมูล ทำให้เกิดการเชื่อมต่อระหว่างหน่วยงาน ตัวอย่างเช่น หน่วยงานไม่มีความกังวลเกี่ยวกับช่องโหว่ด้านความปลอดภัย ทำให้การทำงานของหน่วยงานเป็นไปได้อย่างราบรื่น ดังนั้นการมีผู้บริหารด้านการรักษาความปลอดภัยระดับสูงที่ดี สามารถลดความหวาดระแวงในการทำงานระหว่างส่วนงานต่าง ๆ ทำให้เพิ่มมูลค่าให้กับหน่วยงานภาครัฐได้ ดังนั้นหน้าที่หลักของผู้บริหารด้านการรักษาความปลอดภัยระดับสูง คือ การปรับปรุงความมั่นคงทางกายภาพและความปลอดภัยด้านเทคโนโลยีให้มากขึ้น รวมถึงต้องมีทำงานร่วมกับผู้บริหารอื่น ๆ ในการตัดสินใจเกี่ยวกับลำดับความสำคัญของความต้องการด้านความปลอดภัยเพื่อกำหนดเป้าหมายและวัตถุประสงค์ของการป้องกันหน่วยงานเพื่อให้สอดคล้องกับแผนกลยุทธ์ของหน่วยงาน นอกจากนี้ยังต้องดูแลเครือข่ายของคณะกรรมการ ผู้บริหาร ผู้จัดการ และเจ้าหน้าที่รักษาความปลอดภัยและทำงานร่วมกับหน่วยงานด้านความมั่นคงในท้องถิ่น และหน่วยงานรักษาความปลอดภัยอื่น ๆ

(2) <u>ทีมบริกรข้อมูล (Data Steward Team)</u>

ทีมบริกรข้อมูล (Data Steward Team) ประกอบไปด้วย หัวหน้าบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดธรรมาภิบาลข้อมูลที่ดีภายในหน่วยงาน ทีมบริกรข้อมูลรับคำสั่งโดยตรงจากคณะกรรมการธรรมาภิบาลข้อมูล ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูล โดยบริกรข้อมูลด้านธุรกิจเป็นผู้ให้การสนับสนุนด้านธุรกิจ ขณะที่บริกรข้อมูลด้านเทคนิคเป็นผู้ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ

หัวหน้าบริกรข้อมูลทำหน้าที่เป็นผู้ควบคุมและสั่งการภายในทีมบริกรข้อมูล และเป็นหนึ่งในคณะกรรมการธรรมาภิบาลข้อมูล

บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) คือ บุคคลที่ทำหน้าที่รับผิดชอบในการนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล สถาปนิกข้อมูล (Data Architects) และนักวิเคราะห์ระบบ (System Analyst) ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ บริกรข้อมูลด้านธุรกิจมักจะเป็นบุคคลที่มาจากฝ่ายธุรกิจแต่มีความเข้าใจด้านเทคโนโลยีสารสนเทศ

บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) คือ บุคคลที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามเมทาดาตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูลความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค ทั้งนี้ บริกรข้อมูลด้านเทคนิคมักจะเป็นบุคคลฝ่ายเทคโนโลยีสารสนเทศแต่มีความเข้าใจเกี่ยวกับธุรกิจ

บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) คือ บุคคลที่ทำหน้าที่ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล นอกจากนี้หน่วยงานอาจจะกำหนดบริกรข้อมูลด้านอื่น ๆ เพื่อดูแลเรื่องต่าง ๆ โดยเฉพาะ เช่น บริกรข้อมูลด้านความมั่นคงปลอดภัย บริการข้อมูลด้านการอบรมและให้ความรู้

(3) <u>ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)</u>

นอกเหนือจากคณะกรรมการธรรมาภิบาลข้อมูลและทีมบริกรข้อมูล ยังมีผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders) อื่น ๆ ซึ่งทำหน้าที่ให้การสนับสนุนธรรมาภิบาลข้อมูลต่อทีมบริกรข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล ประกอบไปด้วย ผู้รับผิดชอบข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users)

ผู้รับผิดชอบข้อมูล (Data Owners) คือ บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย ผู้รับผิดชอบข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำดาตาคลีนซิ่ง (Data Cleansing) นอกจากนี้ยังหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล ผู้รับผิดชอบข้อมูลมักจะอยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานบุคคลเป็นผู้รับผิดชอบข้อมูลบุคคล ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานการเงินเป็นผู้รับผิดชอบข้อมูลการเงิน

ทีมบริหารจัดการข้อมูล (Data Management Team) มีหน้าที่หลักในการบริหารจัดการข้อมูล ซึ่งมักจะเป็นเจ้าหน้าที่ภายในฝ่ายเทคโนโลยีสารสนเทศของหน่วยงาน ประกอบด้วย สถาปนิกข้อมูล (Data Architects) นักจัดการฐานข้อมูล (Database Administrators - DBA) นักวิเคราะห์ข้อมูล (Data Analysts) และนักวิทยาการข้อมูล (Data Scientists) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ทีมบริหารจัดการข้อมูลสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA

ผู้สร้างข้อมูล (Data Creators) คือ บุคคลที่ทำหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

ผู้ใช้ข้อมูล (Data Users) คือ บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

5. นโยบายธรรมาภิบาลข้อมูล

5.1 นโยบายทั่วไป

แนวทางการดำเนินงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลในภาพรวม ให้เป็นไปด้วยความเรียบร้อย ถูกต้อง รวมทั้งสอดคล้องกับกฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้อง ประกอบด้วย

1) กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคล ตามโครงสร้างธรรมาภิบาลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร

2) กำหนดกลุ่มบุคคลหรือบุคคลภายในหน่วยงานเป็นผู้รับผิดชอบข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ

3) กำหนดให้มีการวัดผลการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล อย่างน้อยปีละ 1 ครั้ง โดยมีอย่างน้อยในเรื่องดังต่อไปนี้ (1) การประเมินความพร้อมธรรมาภิบาลข้อมูล (ดูรายละเอียดเพิ่มเติมในหัวข้อการประเมินผลธรรมาภิบาลข้อมูล) และ (2) การประเมินความมั่นคงปลอดภัยของข้อมูล

4) กำหนดให้มีการติดตาม และรายงานผลการดำเนินงาน อย่างน้อยปีละ 1 ครั้ง เพื่อนำไปปรับปรุงกระบวนการธรรมาภิบาลข้อมูลให้มีประสิทธิภาพมากขึ้น

5) กำหนดให้มีการตรวจสอบความสอดคล้องกัน ระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้เสีย อย่างน้อยปีละ 1 ครั้ง

6) นโยบายข้อมูลต้องจัดทำเป็นลายลักษณ์อักษร และต้องได้รับการอนุมัติ เพื่อประกาศใช้และถือปฏิบัติทั่วทั้งหน่วยงาน โดยให้มีผลบังคับใช้กับเจ้าหน้าที่ในทุกระดับชั้นของหน่วยงาน ตลอดจนหน่วยงาน/บุคคลภายนอก ที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของหน่วยงาน

7) กำหนดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต (อ้างอิงตามนโยบายความมั่นคงปลอดภัยสารสนเทศของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) หรือเป็นไปตามมาตรฐานสากล)

8) กำหนดให้มีมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน (อ้างอิงตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) สพร. และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

9) กำหนดให้มีแนวปฏิบัติเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายข้อมูล

10) กำหนดให้มีการเผยแพร่ประชาสัมพันธ์นโยบายข้อมูลให้กับบุคคลหรือหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อให้มีความรู้ความเข้าใจต่อการปฏิบัติตามนโยบายข้อมูล

11) กำหนดให้มีการตรวจสอบการปฏิบัติตามนโยบายข้อมูลโดยผู้ตรวจประเมิน ตามที่คณะกรรมการธรรมภิบาลข้อมูลของ สขญ. กำหนด และติดตามผลการประเมินเพื่อปรับปรุง ป้องกัน หรือแก้ไขปัญหาที่พบอย่างต่อเนื่อง

12) กำหนดให้มีการทบทวนนโยบายข้อมูล รวมถึงการรักษาความมั่นคงปลอดภัยเกี่ยวกับข้อมูลอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และปรับปรุงอย่างต่อเนื่อง

13) กำหนดให้มีมาตรฐานหรือวิธีปฏิบัติที่เกี่ยวกับข้อมูล เช่น มาตรฐานการจัดชั้นความลับของข้อมูล เพื่อจัดลำดับความสำคัญของข้อมูลให้มีความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม เป็นต้น

14) กำหนดให้แจ้งความมีอยู่ และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล ให้แก่คณะกรรมการธรรมาภิบาลข้อมูล ได้ทราบและดำเนินการตามกระบวนการธรรมาภิบาลข้อมูล

15) สนับสนุนให้มีการฝึกอบรมหรือมีแหล่งให้ความรู้เพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลภาครัฐ และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและวงจรชีวิตของข้อมูล โดยจัดให้มีการทดสอบวัดความรู้ด้านธรรมาภิบาลข้อมูลอย่างน้อยปีละ 1 ครั้ง

16) จัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล

5.2 กระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes)

การดำเนินงานธรรมาภิบาลข้อมูล เป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการธรรมาภิบาลข้อมูลเริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่อง ดังนี้

รูปที่ ๑๑ กระบวนการธรรมาภิบาลข้อมูลภาครัฐ

๑) <u>การวางแผน (Plan)</u>

การวางแผนเริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนด กฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่าง ๆ เพื่อใช้ในธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล หลังจากที่ได้มีการกำหนดวิสัยทัศน์และประเด็นปัญหาที่ชัดเจนแล้ว ขั้นตอนถัดไป คือ การกำหนดขอบเขตการดำเนินการ ระยะเวลาดำเนินการบุคคลที่เกี่ยวข้อง และต้นทุนที่ใช้ในการดำเนินงาน หลังจากนั้นนำแผนงาน กฎระเบียบ และนโยบายที่เกี่ยวข้องไปประกาศใช้อย่างเป็นทางการ

๒) <u>การปฏิบัติ (Do)</u>

การปฏิบัติในที่นี้อ้างถึงการดำเนินการใด ๆ ของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ เช่น สถาปนิกข้อมูล นักออกแบบข้อมูล นักจัดการฐานข้อมูลวิศวกรข้อมูล นักวิเคราะห์ข้อมูล นักวิทยาการข้อมูล ผู้รับผิดชอบข้อมูล ผู้รับผิดชอบข้อมูลส่วนบุคคลผู้สร้างข้อมูล ผู้บริหาร ผู้ใช้ข้อมูล ซึ่งต้องดำเนินการให้สอดคล้องกับกฎระเบียบ นโยบายมาตรฐาน และแนวปฏิบัติที่ได้กำหนดไว้ ขณะที่บริกรข้อมูลจะให้ความรู้และสนับสนุนให้บุคคลที่เกี่ยวข้องสามารถปฏิบัติตามกฎระเบียบเหล่านั้น ทั้งนี้ รายงานความก้าวหน้า ผลการปฏิบัติงานและประเด็นปัญหาที่พบระหว่างปฏิบัติงานจะถูกรายงานไปยังคณะกรรมการธรรมาภิบาลข้อมูล

๓) <u>การตรวจสอบ วัดผล และรายงาน (Check, Measure and Report)</u>

ในการตรวจสอบบริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจากนั้นรายงานผลความสอดคล้อง คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูลไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบ

๔) <u>การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)</u>

ธรรมาภิบาลข้อมูลภาครัฐเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่องตลอดระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ทั้งนี้สภาพแวดล้อมหรือกฎหมายที่เปลี่ยนแปลง รายการความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย รวมไปถึงผลการตรวจสอบเช่น รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูล จะถูกใช้สำหรับการปรับปรุงกระบวนการธรรมาภิบาลข้อมูลภาครัฐ นโยบาย กฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ

ข้อกฎหมายและเอกสารอ้างอิง

1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

3) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

4) ประกาศ สพร. ที่ 3/2564 เรื่อง มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (มสพร. 1-2564)

5) ประกาศ สพร. ที่ 4/2564 เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศของ สพร.

6) ชุดเอกสารแม่แบบ (template) สำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลภาครัฐ (Version 1.0) จัดทำโดย สพร.

6. การจัดเก็บข้อมูลและทำลายข้อมูล

6.1 นโยบายการจัดเก็ข้อมูลและทำลายข้อมูล (Data Storage and Destruction Policy)

1) กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

2) กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

3) กำหนดสิทธิ์การเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

4) จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน โดยจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ

5) ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากผู้รับผิดชอบข้อมูล ผู้ควบคุมหรือหน่วยงานที่จัดเก็บต้องดำเนินการลายให้เร็วที่สุด โดยต้องไม่ขัดต่อข้อตกลงระหว่างผู้รับผิดชอบข้อมูลกับผู้ควบคุม หรือไม่ขัดต่อข้อกฎหมายใดๆ

6) กำหนดแนวปฏิบัติในการทำลายข้อมูล เมื่อข้อมูลไม่มีการใช้งานหรือมีการเก็บเกินระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบ

7) สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูล ให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน

8) การรับเข้าและการจัดเก็บข้อมูล ข้อมูลของเจ้าหน้าที่นั้นจะเกิดจากการสมัครเข้าทำงานของเจ้าหน้าที่ ข้อมูลเจ้าหน้าที่จะมีการจัดเก็บโดยอัตโนมัติลงระบบฝ่ายบุคคลของหน่วยงาน ซึ่งมีการจำกัดสิทธิ์การเข้าถึง

9) การรับเข้าและการจัดเก็บข้อมูล ข้อมูลจากลูกค้านั้นจะเกิดจากการได้รับข้อมูลจากองค์กรภายนอก เมื่อได้รับข้อมูลจากหน่วยงานภายนอกหรือจากทางลูกค้า จะต้องมีการขึ้นทะเบียนชุดข้อมูลบนระบบ CKAN Data Catalog ของหน่วยงานและทำการจัดเก็บข้อมูลใน One Drive/SharePoint/Microsoft Teams ของโครงการที่เกี่ยวข้อง ซึ่งจะมีการจำกัดสิทธิ์การเข้าถึงข้อมูล

10) การเข้าถึงข้อมูล ข้อมูลที่เจ้าหน้าที่ท่านอื่นๆ จะสามารถเข้าถึงได้นั้น จะประกอบด้วย ชื่อ นามสกุล ชื่อเล่น เบอร์โทรศัพท์ ตำแหน่ง และส่วนงาน หากต้องการเข้าถึงข้อมูลอื่นๆ ของเจ้าหน้าที่จะต้องดำเนินการขอสิทธิ์การเข้าถึงจากฝ่ายบุคคลเป็นอันดับแรก

11) การส่งต่อข้อมูลทั้งภายในและภายนอกองค์กร ต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ และหลักเกณฑ์ในการบริหารจัดการและใช้งานข้อมูลตามชั้นความลับข้อมูลอิเล็กทรอนิกส์

12) การทำลายข้อมูล ข้อมูลเจ้าหน้าที่จะถูกจัดเก็บ เมื่อเจ้าหน้าที่ลาออกหรือพ้นสภาพจากการเป็นเจ้าหน้าที่ หากหมดความจำเป็นในการเก็บรักษาข้อมูลเจ้าหน้าที่ บริษัทอาจทำลาย ลบ นำออกจากระบบภายในระยะเวลา 5 ปี หลังจากที่เจ้าหน้าที่ได้พ้นสภาพการเป็นเจ้าหน้าที่

13) การทำลายข้อมูล ข้อมูลลูกค้า ถ้าเป็นข้อมูลอ่อนไหวหรือข้อมูลส่วนบุคคล จะถูกจัดเก็บไม่เกิน 90 วัน ก่อนที่ทางบริษัทจะทำลายข้อมูล เมื่อปิดโครงการ หรือตามข้อกำหนดสัญญากับทางลูกค้า ส่วนของข้อมูลเปิดจะยังสามารถใช้งานได้ปกติ หรือ ตามข้อกำหนดของลูกค้า

14)การจัดการและจัดเก็บระบบกล้องรักษาความปลอดภัย (Security CCTV)

- การรับเข้าและการจัดเก็บข้อมูล เมื่อมีการเกิดของข้อมูล CCTV ซึ่งเกิดจากการบันทึกภาพในขณะที่มีการใช้งานกล้อง CCTV โดย ข้อมูลเหล่านี้จะมีการจัดเก็บโดยอัตโนมัติลงอุปกรณ์บันทึกข้อมูลที่หน่วยงาน ซึ่งหน่วยงานจะทำการจัดเก็บถาวรข้อมูล CCTV ไว้ตามเท่าที่จำเป็น โดยจะยึดจากหลักเกณฑ์ต่าง ๆ ดังนี้ เช่น เพื่อการคุ้มครองชีวิต ร่างกาย สุขภาพ ความปลอดภัยส่วนบุคคลและทรัพย์สินต่าง ๆ เป็นต้น
- การเข้าถึงข้อมูล คือ เมื่อต้องการใช้ข้อมูล CCTV จะต้องติดต่อและได้รับการอนุมัติจาก Information Security Officer (ISO) โดยทั่วไปจะใช้ในกรณี เช่น ทรัพย์สินภายในพื้นที่สำนักงานศูนย์หาย มีการแจ้งว่ามีการลักลอบเข้าพื้นที่ของหน่วยงานโดยพลการ เป็นต้น
- การส่งต่อข้อมูลระบบกล้องรักษาความปลอดภัย ต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ
- การทำลายข้อมูล หากหมดความจำเป็นในการเก็บรักษาข้อมูล CCTV บริษัทจะต้องทำลาย ลบ นำออกจากระบบภายในระยะเวลา 90 วันนับจากวันที่มีการบันทึก

6.2 แนวปฏิบัติการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Guideline)

1) กำหนดให้ผู้รับผิดชอบข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน

2) กำหนดให้ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร

3) กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบได้แก่ ผู้รับผิดชอบข้อมูล บริกรข้อมูลด้านเทคนิค และบริกรข้อมูลด้านธุรกิจ โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

4) ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งผู้รับผิดชอบข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยทำการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

- ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น
- ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้
    i. เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน
    ii. เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้

5) กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

6) ในการจัดเก็บข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และไม่เก็บรวบรวมข้อมูลส่วนบุคคลดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากผู้รับผิดชอบข้อมูล

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลอื่นใดซึ่งกระทบต่อผู้รับผิดชอบข้อมูลในทำนองเดียวกันตามที่หน่วยงานกำหนด

7) กำหนดให้การยกเลิกการจัดเก็บข้อมูลกรณีผู้รับผิดชอบข้อมูลถอนความยินยอม ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

8) ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อยดังนี้

- เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้

- มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้

- การจัดเก็บข้อมูล ระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server NAT และอื่น ๆ

9) กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

10) กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บ เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต หากประชุมภายในองค์กรทุกคนสามารถเข้าถึงได้ และส่งต่อได้ แต่หากเป็นการประชุมโครงการหรือกับหน่วยงานภายนอก เจ้าหน้าที่จำเป็นที่จะต้องขออนุญาตผู้บริหารฝ่ายหรือโครงการเฉพาะก่อน โดยอ้างอิง SP-006-DOCP_Document control policy

11) กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด ต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

12) ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงานสำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

13) กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ 1 ครั้ง

ข้อกฎหมายและเอกสารอ้างอิง

1) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

3) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5) SP- ACLP-001_Access Control Management

7. การใช้ข้อมูล (Data Usage)

7.1 นโยบายการใช้ข้อมูล (Data Usage Policy)

1) ผู้รับผิดชอบข้อมูลจะเป็นผู้พิจารณาระดับการรักษาความปลอดภัยและเงื่อนไขการเข้าใช้งานชุดข้อมูลนั้น ๆ โดยที่ผู้บริหารข้อมูลจะต้องแน่ใจว่าเงื่อนไขต่าง ๆ ได้มีการสื่อสารออกไปอย่างชัดเจนไปยังผู้ใช้งานข้อมูลภายใน สขญ.

2) ผู้รับผิดชอบข้อมูลจะต้องไม่ปฏิเสธคำร้องขอการใช้ข้อมูลจากผู้ใช้งานข้อมูลภายใน BDI เว้นเสียแต่ว่า

- ข้อมูลนั้นมีชั้นความลับและการร้องขอข้อมูลของผู้ใช้งานไม่มีเหตุผลที่ชอบธรรมหรือไม่สมเหตุสมผล

- การแบ่งปันข้อมูลเป็นสิ่งต้องห้ามอย่างชัดเจนตามกฎหมาย หรือข้อตกลงในการได้มาของข้อมูล

3) มีการกำหนดแนวทางการขอสิทธิในการใช้ข้อมูลที่ชัดเจน ผู้ใช้งานข้อมูลจะต้องขออนุมัติจากผู้รับผิดชอบข้อมูลหรือผู้บริหารจัดการข้อมูลในการเข้าถึงข้อมูลที่เป็นความลับ ซึ่งในคำร้องขอการเข้าถึงข้อมูลนั้นผู้ใช้งานข้อมูลจะรวมถึง

- ขอบเขตและความละเอียดของข้อมูลที่ร้องขอ เช่น ช่วงเวลาที่ต้องการใช้ข้อมูล
- วัตถุประสงค์ในการร้องขอข้อมูล
- ความถี่ในการเข้าใช้งานข้อมูล (เช่น เป็นครั้งคราวหรือใช้ประจำ)

4) มีแนวทางการขอสิทธิและเข้าถึงข้อมูลที่สะดวก รวดเร็ว ภายใต้กรอบการกำกับดูแลที่เหมาะสมและช่วยให้ผู้บริหารจัดการข้อมูลสามารถติดตามและประเมินความคุ้มค่าของข้อมูลที่มีการป้องกันความเสี่ยงการรั่วไหลของข้อมูลหรือใช้ไม่ตรงตามวัตถุประสงค์

5) ผู้บริหารจัดการข้อมูลจะต้องมั่นใจว่าข้อมูลที่แบ่งปันกันทั้งหมดนั้นถูกต้อง ทันสมัย และมีความพร้อม ตามเวลาที่กำหนดและจะต้องแจ้งให้ผู้ใช้งานข้อมูลทราบถึงคุณภาพของข้อมูลและข้อจำกัดของชุดข้อมูลก่อนที่จะให้ชุดข้อมูลกับผู้ใช้งาน

6) ผู้บริหารจัดการข้อมูลจะต้องสื่อสารกับผู้ใช้งานข้อมูลภายใน BDI ถึงระยะเวลาโดยประมาณในการตอบสนองต่อการร้องข้อการเข้าถึงข้อมูล

7) ผู้ใช้งานข้อมูลจะต้องปฏิบัติตามนโยบายที่กำหนดโดยเจ้าข้องข้อมูลและหน่วยงานภาครัฐอื่น ๆ ที่ให้ข้อมูลสำหรับการใช้งานชุดข้อมูลนั้น ๆ โดย

- ผู้ใช้งานข้อมูลควรใช้ข้อมูลตามวัตถุประสงค์ที่ได้รับอนุมัติจากผู้รับผิดชอบข้อมูลเท่านั้น ถ้ามีการใช้งานเพื่อวัตถุประสงค์อื่นจะต้องขออนุมติอีกครั้ง
- ผู้ใช้งานข้อมูลจะต้องไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาตจากแหล่งข้อมูล เว้นแต่จะได้รับอนุญาติหรือเป็นไปตามที่กฎหมายกำหนด หรือข้อมูลนั้น ๆ ได้รับอนุมัติล่วงหน้าไว้แล้ว เพื่อวัตถุประสงค์การใช้งานดังกล่าวจากแหล่งข้อมูล

7.2 แนวปฏิบัติการใช้ข้อมูล (Data Usage Guideline)

1) ผู้ร้องขอใช้ข้อมูลขออนุมัติไปยังคณะผู้บริหารข้อมูล โดยระบุขอบเขตและความละเอียดของข้อมูลที่ร้องขอ อย่างน้อยต้องมีวัตถุประสงค์ ความถี่ ระยะเวลาที่ต้องใช้

2) สำหรับข้อมูลจากหน่วยงานอื่น ที่ สขญ. เป็นเพียงผู้ประมวลผลข้อมูล ให้ยึดตามนโยบายและแนวปฏิบัติของเจ้าข้องข้อมูล และผู้บริหารข้อมูลของข้อมูลนั้นๆ

3) ผู้บริหารข้อมูลและผู้รับผิดชอบข้อมูลพิจารณาความเหมาะสมของวัตถุประสงค์ สิทธิ และชั้นความลับ รวมไปถึงเงื่อนไขการเข้าใช้งานชุดข้อมูลนั้น ๆ (ถ้ามี)

4) ให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงข้อมูล (Access Control Management) ในการควบคุมสิทธิ์ในการเข้าถึงทรัพยากรข้อมูล

5) หากโดยสิทธิ ผู้ร้องขอไม่สามารถเข้าถึงข้อมูลที่ร้องขอได้ และผู้ร้องขอจำเป็นต้องใช้ข้อมูลดังกล่าว เพื่อการปฏิบัติงาน ให้ส่งผ่านคำขอไปยังคณะทำงานฯ เพื่อเสนอขออนุมัติการใช้ข้อมูล

6) หากพิจารณาแล้ว สามารถใช้ข้อมูลได้ ให้ผู้บริหารข้อมูลกำหนดสิทธิตามระบบ และทำความเข้าใจ ถึงข้อควรระวังในการใช้ข้อมูลให้กับผู้ร้องขอ

7) ผู้บริหารข้อมูลปรับปรุงเมทาดาตาเพื่อบันทึกเพิ่มผู้ใช้ข้อมูลชุดนี้ต่อไป

8) ทำการวัดและประเมินผลกระบวนการใช้ข้อมูล และรวบรวมข้อมูลเชิงสถิติเพื่อปรับปรุงประสิทธิภาพของกระบวนการในรายปีต่อไป

เอกสารเพิ่มเติม

1) SP-ACLP-001_Access Control Management
2) GL-CSOG-001_Customer Service Operation Guidelines
3) SP-PROJ-005_Project Management Policy

8. การจำแนกข้อมูล (Data Classification)

8.1 นโยบายการจำแนกข้อมูล (Data Classification Policy)

1) กำหนดบุคคลหรือกลุ่มบุคคลภายในหน่วยงานเป็นผู้รับผิดชอบข้อมูล เพื่อทำหน้าที่ในการจำแนกประเภทของข้อมูล

2) กำหนดให้มีการระบุเกณฑ์มาตรฐานการจำแนกข้อมูลและประกาศใช้ให้เป็นไปในทิศทางเดียวกันทั้งหน่วยงาน

3) มีการประเมินระดับผลกระทบและความเสี่ยงที่จะมีต่อหน่วยงานหากชุดข้อมูลเกิดการรั่วไหลหรือถูกเปิดเผยโดยไม่ได้รับการยินยอม เพื่อใช้เป็นเกณฑ์ในการระบุหมวดหมู่และประเภทชั้นความลับ

4) กำหนดให้มีการติดป้ายกำกับชุดข้อมูล (Labeling/Tagging Dataset) เมื่อได้รับการประเมินและมั่นใจได้ว่ามีการระบุหมวดหมู่และประเภทชั้นความลับอย่างเหมาะสม

5) กำหนดให้มีการจัดทำแนวปฏิบัติการจัดการชุดข้อมูลที่ได้รับการจัดหมวดหมู่และชั้นความลับตามแนวทางที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการเข้าถึงข้อมูล

6) กำหนดให้มีการกำกับติดตามอย่างต่อเนื่อง และมีการวัดผลการดำเนินงานและความสำเร็จของการจำแนกข้อมูล โดยตรวจสอบความปลอดภัยและรูปแบบการเข้าถึงระบบและข้อมูล

องค์กรกำหนดให้มีการจำแนกชั้นความลับของข้อมูลออกเป็น 4 ประเภท ดังนี้

Top Secret (ลับที่สุด)	**นิยาม**
	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด ซึ่งผู้รับผิดชอบข้อมูลต้องจำกัดไม่ให้มีการเปิดเผยข้อมูลดังกล่าวอย่างเคร่งรัด และจำกัดเฉพาะเจ้าหน้าที่ที่กำหนดโดยนโยบายเท่านั้นในการเข้าถึงประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด
	คุณลักษณะ:
	• มีความสำคัญต่อองค์กรในระดับสูงมาก • หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อองค์กรในระดับสูงมาก • เกี่ยวข้องกับแผนกลยุทธ์ และทิศทางหลักในการดำเนินธุรกิจ • มีความสำคัญอย่างมากต่อความสำเร็จทางเทคนิค หรือทางการเงินของสินค้า • จำเป็นต้องมีมาตรการควบคุมการเผยแพร่ข้อมูลที่เข้มงวด โดยพิจารณาจำกัดรายชื่อผู้ได้รับอนุญาตให้เข้าถึงข้อมูลอย่างรอบคอบ • ข้อมูลส่วนบุคคลแบบอ่อนไหว ตามมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
	ตัวอย่าง:
	• แผนการควบรวมกิจการ กลยุทธ์การลงทุน กลยุทธ์ทางการตลาด • ข้อมูลสำคัญขององค์ประกอบ วัสดุ และเทคโนโลยีในการผลิต • แผนกลยุทธ์ และทิศทางในการดำเนินธุรกิจ • ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวิภาพ
Secret (ลับมาก)	**นิยาม**
	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งผู้รับผิดชอบข้อมูลต้องจำกัดให้มีการเปิดเผยเฉพาะกลุ่มเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น
	คุณลักษณะ:
	• มีความสำคัญต่อองค์กรในระดับสูง • หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อองค์กร • เกี่ยวข้องกับทิศทางการปฏิบัติงานขององค์กร (มีผลเฉพาะในช่วงระยะเวลาหนึ่ง) • มีความสำคัญต่อความสำเร็จทางเทคนิค หรือทางการเงินของสินค้า • จำเป็นต้องมีมาตรการควบคุมการเผยแพร่ข้อมูลที่เข้มงวด โดยจำกัดการเข้าถึงให้กับกลุ่มบุคคลบางกลุ่มเท่านั้น และต้องได้รับการปกป้องอย่างเหมาะสม • ข้อมูลส่วนบุคคลทั่วไป
	ตัวอย่าง:
	• ข้อมูลเกี่ยวกับรายได้ ต้นทุน กำไร หรือข้อมูลทางการเงินอื่นๆ • แผนการปฏิบัติงาน แผนผลิตภัณฑ์ ข้อกำหนดทางการตลาด • ข้อมูลสำคัญขององค์ประกอบ วัสดุ เทคโนโลยี งานวิจัยและการพัฒนาของผลิตภัณฑ์ต่างๆ • ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติงาน แผนงานของโครงการ งานออกแบบ และข้อกำหนดต่างๆ • เอกสารเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ (ISMS related documents) • ข้อมูลเกี่ยวกับลูกค้า และพันธมิตรทางธุรกิจ • ข้อมูลส่วนตัวของเจ้าหน้าที่

Confidential (ลับ)	**นิยาม**
	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ โดยรวมถึงข้อมูลภายในองค์กร ซึ่งสามารถเปิดเผยให้แก่เจ้าหน้าที่ของ สขญ.
	คุณลักษณะ:
	● ข้อมูลทางธุรกิจ ข้อมูลที่ใช้งานภายในองค์กร และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกองค์กร ● หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อองค์กรในระดับต่ำ หรืออาจจะไม่มีผลกระทบใดๆ ● ไม่ควรทำสำเนา หรือนำออกจากองค์กรโดยไม่ได้รับอนุญาต ● เป็นชั้นความลับปริยายขององค์กร (Default)
	ตัวอย่าง:
	● ข้อมูลทางธุรกิจ ● นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ● ประกาศภายในองค์กร บันทึกข้อความภายในองค์กร รายงานของโครงการ บันทึกการประชุม
Public (สาธารณะ)	**นิยาม**
	ข้อมูลที่สามารถนำไปเปิดเผยนอกองค์กรและสาธารณะ โดยไม่มีความเสี่ยงหรือมีความเสี่ยงน้อยที่องค์กรรับได้
	คุณลักษณะ:
	● ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัยเป็นพิเศษ หรือ ● ข้อมูลสำหรับการเผยแพร่ต่อสาธารณะ ผ่านช่องทางที่เหมาะสมซึ่งองค์กรพิจารณาอนุมัติแล้ว ● หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะไม่ส่งผลเสียหายใดๆ ต่อองค์กร ● อาจต้องได้รับการปกป้องให้มีความถูกต้องและสมบูรณ์ครบถ้วน
	ตัวอย่าง:
	● ข้อมูลบนเว็บไซต์ ● ข้อมูลจากการแถลงข่าว หรือรายงานประจำปีขององค์กร

หลักเกณฑ์ในการบริหารจัดการและใช้งานข้อมูลตามชั้นความลับ

เอกสารตีพิมพ์

ลับมาก	ลับ	ใช้ภายใน	สาธารณะ
การระบุชั้นความลับของข้อมูล			
ระบุคำว่า “ลับมาก” และชื่อผู้เป็นเจ้าของข้อมูล - ทุกหน้าเอกสาร หากเป็นเอกสารแยกแผ่นหรือไม่ได้รับการเข้าเล่ม - บนปก หรือหน้าแรกของเอกสาร หากได้รับการเข้าเล่ม	ระบุคำว่า “ลับ” และชื่อฝ่ายที่เป็นเจ้าของข้อมูล - ทุกหน้าเอกสาร หากเป็นเอกสารแยกแผ่นหรือไม่ได้รับการเข้าเล่ม - บนปก หรือหน้าแรกของเอกสาร หากได้รับการเข้าเล่ม	ไม่จำเป็นต้องเขียนระบุ (แต่แนะนำให้ระบุคำว่า “ใช้ภายใน”)	ระบุคำว่า “สาธารณะ” บนปก หรือหน้าแรกของเอกสาร
การเข้าถึงเอกสาร			
บุคคลที่ได้รับการระบุชื่อเท่านั้น (เจ้าของข้อมูลเป็นผู้กำหนดรายชื่อที่สามารถตรวจสอบได้ โดยสำเนาทุกฉบับที่แจกจ่ายออกไปต้องได้รับการระบุหมายเลขกำกับ)	กลุ่มบุคคลที่ได้รับอนุญาตจากหัวหน้าฝ่ายที่เป็นเจ้าของข้อมูล	ใช้งานได้ภายในองค์กรเท่านั้น (อ้างอิงตามหลักการ “Need to Know”)	ไม่มีข้อจำกัด
การเก็บรักษา			
เก็บรักษาในตู้เอกสารที่ปิดล็อคเมื่อไม่ได้ใช้งาน	เก็บรักษาในตู้เอกสารที่ปิดล็อคเมื่อไม่ได้ใช้งาน	เอกสารต้นฉบับต้องได้รับการเก็บรักษาอย่างดี ไม่ให้เกิดความเสียหาย	เอกสารต้นฉบับต้องได้รับการเก็บรักษาอย่างดี ไม่ให้เกิดความเสียหาย
การทำสำเนาเอกสาร			
- ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอ - สำเนาต้องได้รับการระบุชื่อผู้ที่ได้รับอนุญาตให้ใช้งาน	- ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอ - สำเนาต้องได้รับการระบุชื่อผู้ที่ได้รับอนุญาตให้ใช้งาน	อนุญาตให้ทำสำเนาได้เพื่อใช้ในการปฏิบัติงานเท่านั้น	ไม่มีข้อจำกัด
การส่งเอกสาร (ภายในองค์กร)			
สอดในซองปิดผนึก และระบุคำว่า “ลับมาก” และชื่อ-ที่อยู่ผู้รับบนหน้าซอง	สอดในซองปิดผนึก และระบุคำว่า “ลับ”และชื่อ-ที่อยู่ผู้รับบนหน้าซอง	ควรมีปกเอกสารเพื่อปกปิดข้อมูลอย่างมิดชิด	ไม่มีข้อจำกัด
การส่งเอกสาร (ภายนอกองค์กร)			

ลับมาก	ลับ	ใช้ภายใน	สาธารณะ
สอดในซอง 2 ชั้น และใช้บริการไปรษณีย์ลงทะเบียน หรือบริษัทขนส่งที่เชื่อถือได้ - ซองชั้นในระบุคำว่า "SECRET" และปิดผนึกด้วยเทปกาว หรือวัสดุที่สามารถป้องกันการลักลอบเปิดอ่านได้ - ซองชั้นนอกต้องถูกปิดผนึกพร้อมทั้งระบุชื่อ-ที่อยู่ของผู้รับและผู้ส่ง	สอดในซอง 2 ชั้น และใช้บริการไปรษณีย์ลงทะเบียน หรือบริษัทขนส่งที่เชื่อถือได้ - ซองชั้นในระบุคำว่า "CONFIDENTIAL" และปิดผนึกด้วยเทปกาว หรือวัสดุที่สามารถป้องกันการลักลอบเปิดอ่านได้ - ซองชั้นนอกต้องถูกปิดผนึกพร้อมทั้งระบุชื่อ-ที่อยู่ของผู้รับ และผู้ส่ง	สอดซองปิดผนึก และระบุชื่อ-ที่อยู่ของผู้รับ	ไม่มีข้อจำกัด
การส่งโทรสาร			
- ตรวจสอบเลขหมายปลายทางให้ถูกต้อง - โทรศัพท์แจ้งให้ผู้รับทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้งยืนยันเมื่อได้รับเอกสารแล้ว	- ตรวจสอบเลขหมายปลายทางให้ถูกต้อง - โทรศัพท์แจ้งให้ผู้รับทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้งยืนยันเมื่อได้รับเอกสารแล้ว	- ตรวจสอบเลขหมายปลายทางให้ถูกต้อง - โทรศัพท์แจ้งให้ผู้รับทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้งยืนยันเมื่อได้รับเอกสารแล้ว	ไม่มีข้อจำกัด
การรับโทรสาร			
รอรับเอกสารที่เครื่องโทรสารทุกครั้ง (ต้องส่งผ่านเครื่องโทรสาร ห้ามส่งผ่าน Fax pool)	รอรับเอกสารที่เครื่องโทรสารทุกครั้ง (ต้องส่งผ่านเครื่องโทรสาร ห้ามส่งผ่าน Fax pool)	รอรับเอกสารที่เครื่องโทรสารทุกครั้ง	ไม่มีข้อจำกัด
การทำลายเอกสาร			
ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร หรือฉีกเป็นชิ้นเล็กๆ	ไม่มีข้อจำกัด

ข้อมูลอิเล็กทรอนิกส์

ลับมาก	ลับ	ใช้ภายใน	สาธารณะ
การระบุชั้นความลับเมื่อใช้งานข้อมูลกับแอพพลิเคชั่น หรือบนจอแสดงผล			
ระบุคำว่า “ลับมาก” ที่ด้านล่างของหน้าจอ (ควรระบุชื่อเจ้าของข้อมูลด้วยหากสามารถกระทำได้)	ระบุคำว่า “ลับ”ที่ด้านล่างของหน้าจอ (ควรระบุชื่อฝ่ายที่เป็นเจ้าของข้อมูลด้วยหากสามารถกระทำได้)	ไม่จำเป็นต้องระบุ (แต่แนะนำให้ระบุคำว่า “ใช้ภายใน”)	ควรระบุคำว่า “สาธารณะ”ที่ด้านบนของหน้าจอ (ระบุหรือไม่ระบุก็ได้)
การระบุชั้นความลับเมื่อใช้งานข้อมูลกับสื่อที่สามารถแลกเปลี่ยนข้อมูลได้			
ระบุคำว่า “ลับมาก” และเจ้าของข้อมูลบนสื่อบันทึกข้อมูล	ระบุคำว่า “ลับ” และฝ่ายที่เป็นเจ้าของข้อมูลบนสื่อบันทึกข้อมูล	ไม่จำเป็นต้องระบุ (แต่แนะนำให้ระบุคำว่า “ใช้ภายใน” บนสื่อบันทึกข้อมูล)	ไม่มีข้อจำกัด
การเข้าถึง และการทำสำเนาข้อมูล			
บุคคลที่ได้รับการระบุชื่อเท่านั้น (เจ้าของข้อมูลเป็นผู้กำหนดรายชื่อที่สามารถตรวจสอบได้)	กลุ่มบุคคลที่ได้รับอนุญาตจากหัวหน้าฝ่ายที่เป็นเจ้าของข้อมูล	ใช้งานได้ภายในองค์กรเท่านั้น (อ้างอิงตามหลักการ “Need to Know”)	ไม่มีข้อจำกัด
การเก็บรักษาบนสื่อที่ไม่สามารถเคลื่อนย้ายได้ (ที่ได้รับการควบคุมการเข้าถึง)			
ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล
การเก็บรักษาบนสื่อที่ไม่สามารถเคลื่อนย้ายได้ (ที่ไม่ได้รับการควบคุมการเข้าถึง)			
เข้ารหัสข้อมูล	เข้ารหัสข้อมูล	ควรจะเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล
การเก็บรักษาบนสื่อที่สามารถเคลื่อนย้ายได้			
เข้ารหัสข้อมูล	เข้ารหัสข้อมูล	ควรจะเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล
การสั่งพิมพ์ข้อมูล			
ต้องพิมพ์ข้อมูลด้วยเครื่องพรินเตอร์ที่กำหนด และมีผู้รอรับเอกสารที่เครื่องทุกครั้ง	ต้องพิมพ์ข้อมูลด้วยเครื่องพรินเตอร์ที่กำหนด และมีผู้รอรับเอกสารที่เครื่องทุกครั้ง	ต้องพิมพ์ข้อมูลด้วยเครื่องพรินเตอร์ที่กำหนด	ไม่มีข้อจำกัด
การส่งข้อมูลผ่านเครือข่ายสาธารณะ			
เข้ารหัสข้อมูล	เข้ารหัสข้อมูล	ควรจะเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล
การส่งข้อมูลบนระบบเครือข่ายภายใน/ส่วนตัว			
เข้ารหัสข้อมูล	ควรจะเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล
การทำลายข้อมูล			
ด้วยวิธีที่มั่นคงปลอดภัย (Secure deleted)	ด้วยวิธีที่มั่นคงปลอดภัย (Secure deleted)	ลบไฟล์ด้วยวิธีการปกติ	ไม่มีข้อจำกัด
การทำลายสื่อบันทึกข้อมูล			
เจ้าของข้อมูลต้องเฝ้าดูให้แน่ใจว่าสื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม	เจ้าของข้อมูลต้องเฝ้าดูให้แน่ใจว่าสื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม	ทำลายด้วยวิธีการปกติ	ไม่มีข้อจำกัด

8.2 แนวปฏิบัติการจำแนกข้อมูล (Data Classification Guideline)

1) ทำการกำหนดนโยบายการจัดประเภทข้อมูล ได้แก่ วัตถุประสงค์ ขั้นตอนการทำงาน รูปแบบและระดับการจำแนกข้อมูล เจ้าของ และการจัดการข้อมูล

2) จัดทำเกณฑ์สำหรับการระบุหมวดหมู่และระบุชั้นความลับของข้อมูลเพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้อง ซึ่งควรพิจารณาจากกฎหมายหลักที่เกี่ยวข้องกับเกณฑ์การจัดหมวดหมู่ ทั้งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 พระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และมาตรฐานการจำแนกข้อมูลของ สพร.

3) กรณีที่ สขญ. เป็นผู้ประมวลผลข้อมูล ไม่ได้เป็นเจ้าของและผู้รับผิดชอบข้อมูล ให้ระบุชั้นความลับของข้อมูล และการเข้าถึงข้อมูลตามนโยบายของเจ้าของข้อมูลเป็นผู้ระบุ หากยังไม่มีการจัดชั้นความลับกับข้อมูลดังกล่าว ให้ สขญ. หารือร่วมกับหน่วยงานเจ้าของข้อมูล และผู้รับผิดชอบข้อมูล เพื่อระบุชั้นความลับของข้อมูลนั้น ก่อนการดำเนินการใดๆ

4) สร้างชุดคำถาม จำแนก หมวดหมู่ และชั้นความลับข้อมูลให้อยู่ในรูปแบบของแผนผังการตัดสินใจ (Decision Tree) เพื่อให้ทุกส่วนงานในหน่วยงาน สามารถใช้แผนผังดังกล่าวเป็นเครื่องมือระบุหมวดหมู่และชั้นความลับได้อย่างสอดคล้องกันภายในหน่วยงานดังตัวอย่างรูปที่ 1

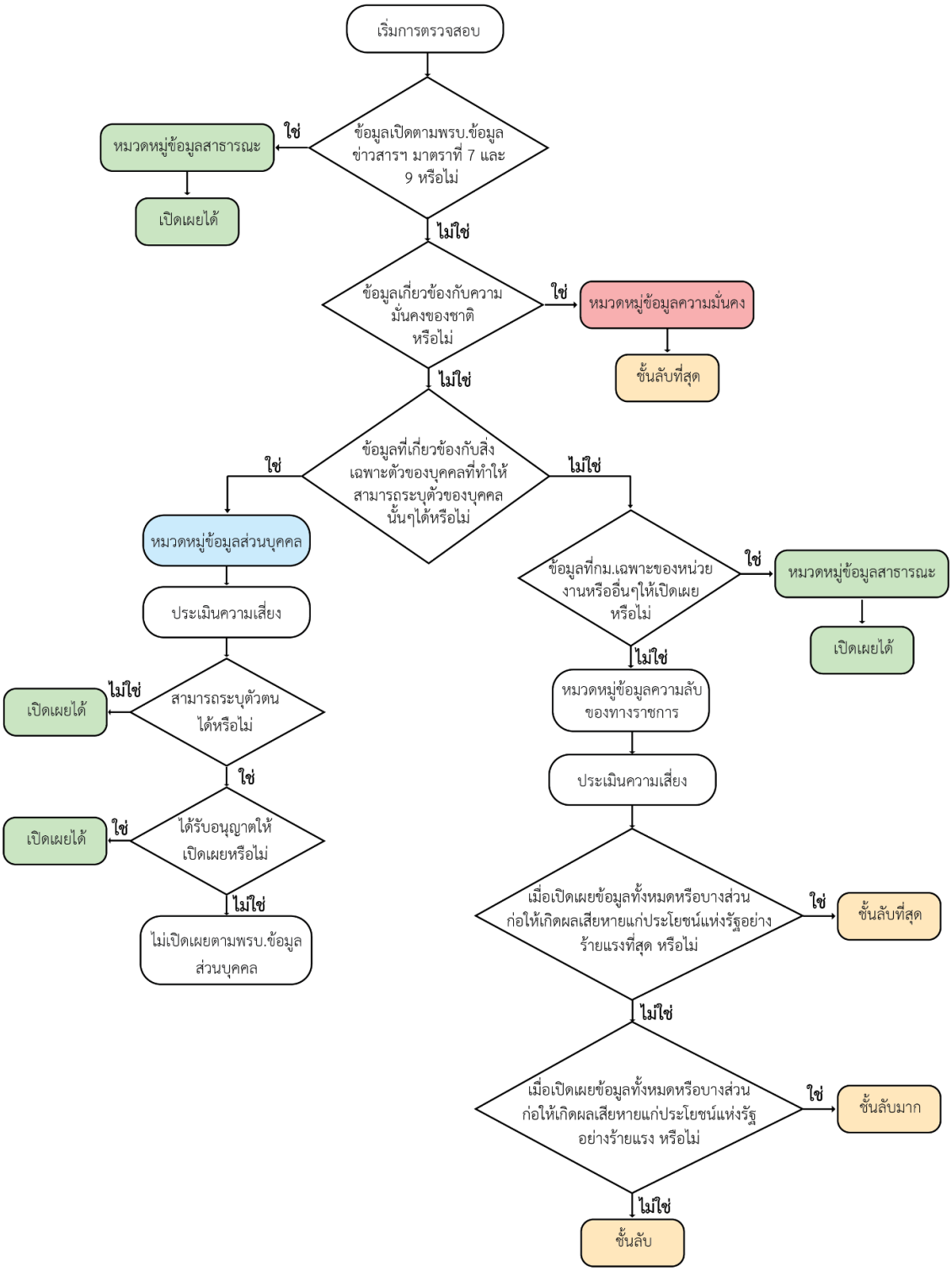
5) รวบรวมชุดข้อมูลของหน่วยงานมาจัดทำบัญชีรายการข้อมูลเพื่อทำการระบุหมวดหมู่และระดับชั้นความลับของข้อมูลตามเกณฑ์ที่หน่วยงานกำหนด

6) เพิ่มป้ายกำกับโดยการติดแท็กข้อมูลสำหรับข้อมูลที่มีการระบุหมวดหมู่ไว้

7) ใช้ผลลัพธ์จากการจำแนกข้อมูลมาปรับปรุงความปลอดภัยและข้อปฏิบัติต่าง ๆ เช่น การกำหนดสิทธิการเข้าถึงข้อมูลตามระดับการจำแนก โดยการจัดการชุดข้อมูลดังกล่าวควรครอบคลุมหัวข้อดังต่อไปนี้

- สิทธิการเข้าถึงข้อมูล (Access Control)
- การคัดลอก หรือการพิมพ์ข้อมูล (Copying/Printing)
- ระบบการป้องกันเครือข่าย หรือเน็ตเวิร์คจากผู้ใช้ภายนอก (Network Security)
- ระบบการรักษาความปลอดภัย (Security System)
- การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)
- การเข้าถึงข้อมูลจากระยะไกล (Remote Access)
- การจัดเก็บข้อมูล (Storage)
- การควบคุมการขนส่ง หรือโอนถ่ายข้อมูล (Transmission)
- ระบบสำรองและกู้คืนข้อมูล (Backup and Disaster Recovery)
- การทำลายข้อมูล (Data Destruction and Disposal)

8) ติดตาม ทบทวน ปรับปรุง อย่างต่อเนื่อง ให้มีการจำแนกข้อมูลได้อย่างถูกต้องและเป็นมาตรฐาน



รูปที่ 1 แผนผังการตัดสินใจ (Decision Tree) สำหรับการจำแนกหมวดหมู่ และชั้นความลับข้อมูล

ข้อกฎหมายและเอกสารอ้างอิง

1) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540

2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

4) มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) DGA Community Standard ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ GOVERNMENT DATA CATALOG GUIDELINE เวอร์ชัน 1.0 หัวข้อการจัดหมวดหมู่ตามธรรมาภิบาลข้อมูลภาครัฐ (Data Classification) หน้า 27

เอกสารเพิ่มเติม

SP-ACLP-001_Access Control Management

9. การรักษาความปลอดภัยทางข้อมูลสารสนเทศ (Information Security)

9.1 นโยบายการรักษาความปลอดภัยทางข้อมูลสารสนเทศ (Information Security Policy)

1) ต้องมีการกำหนดผู้รับผิดชอบด้านความปลอดภัยทางข้อมูลสารสนเทศ มีการแบ่งแยกหน้าที่และความรับผิดชอบให้ชัดเจนในการปฏิบัติงานเพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงแก้ไขระบบการรักษาความปลอดภัยทางข้อมูลสารสนเทศ

- ผู้อำนวยการ มีหน้าที่ดูแล ให้การสนับสนุนด้านทรัพยากรที่จำเป็นต่อระบบความมั่นคงปลอดภัยสารสนเทศ ประกาศ และสื่อสารให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่สำนักงานกำหนด
- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่อนุมัติการใช้งานนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ในกรณีพบความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อยู่ในระดับที่สำนักงานยอมรับไม่ได้ และมีข้อจำกัดหรือเหตุผลทำให้ไม่สามารถแก้ไขและควบคุมความเสี่ยงนั้นได้ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเป็นผู้พิจารณายอมรับความเสี่ยงนั้น หรือเสนอแนะแนวทางอื่นในการแก้ไข โดยคำนึงถึงผลกระทบที่อาจจะเกิดขึ้น
- กรณีมีผู้ปฏิบัติงานฝ่าฝืนนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ละเมิดทรัพย์สินทางปัญญาหรือกฎหมายลิขสิทธิ์ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงพิจารณาดำเนินการทางวินัย เรียกค่าเสียหาย หรือดำเนินคดีตามกฎหมาย
- กรณีพบผู้ปฏิบัติงานกระทำการด้านสารสนเทศในลักษณะอันอาจก่อให้เกิดความเข้าใจผิดต่อภาพลักษณ์หรือความเสียหายต่อสำนักงาน ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงพิจารณาสั่งการระงับ ยกเลิก หรือดำเนินการใด ๆ
- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่กำกับ ดูแลติดตาม ให้คำแนะนำในการจัดทำและทบทวนนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- คณะกรรมการบริหารเทคโนโลยีสารสนเทศ มีหน้าที่กำกับ ดูแล ติดตามให้คำแนะนำในการจัดทำและเห็นชอบนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- คณะทำงานย่อยระบบมาตรฐาน ISO 27001 มีหน้าที่จัดทำทบทวน และดำเนินงานที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักงาน เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ

- ผู้ปฏิบัติงาน มีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงดูแลรักษาและระมัดระวังการใช้สินทรัพย์ของสำนักงาน โดยต้องมีความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

2) กำหนดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยมีแผนการจัดการความเสี่ยง ซึ่งกำหนดเกณฑ์ในการประเมิน การแก้ไข และยอมรับความเสี่ยง เพื่อลดโอกาสในการสูญเสียความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของสินทรัพย์ของสำนักงาน

3) สร้างความรู้และความตระหนักในการใช้งานระบบสารสนเทศอย่างมั่นคงปลอดภัยแก่ผู้ใช้งาน ผู้ปฏิบัติงาน โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่เอกสารที่เกี่ยวข้องผ่านระบบเว็บไซต์ภายในของสำนักงาน รวมถึงสื่อสารนโยบายด้านความมั่นคงปลอดภัยสารสนเทศให้ผู้ให้บริการภายนอกทราบในเรื่องที่เกี่ยวข้อง

4) กำหนดให้มีการบริหารจัดการสินทรัพย์ โดยการจัดทำมาตรการควบคุม การใช้งานสินทรัพย์ที่เหมาะสมตลอดวงจรชีวิตของสินทรัพย์ตั้งแต่การจัดหาการลงทะเบียน การควบคุมการตั้งค่าด้านความมั่นคงปลอดภัย มาตรการป้องกันด้านความมั่นคงปลอดภัยที่เหมาะสมเพียงพอ การบำรุงรักษา การจำหน่าย และการทำลายสินทรัพย์ ตามลำดับชั้นความลับของข้อมูลที่อยู่ในสินทรัพย์นั้น ๆ

5) กำหนดให้มีการบริหารจัดการเอกสารที่เกี่ยวข้องกับการปฏิบัติงานภายในของสำนักงาน ได้แก่ นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ขั้นตอนการปฏิบัติงาน วิธีปฏิบัติงาน เอกสารสนับสนุนการทำงาน คู่มือการตั้งค่าระบบสารสนเทศ และบันทึกต่าง ๆ โดยเอกสารจะถูกกำหนดรหัสและควบคุม ตั้งแต่การขึ้นทะเบียนเอกสารใหม่ การทบทวนและอนุมัติก่อนการใช้งาน การแก้ไขเอกสาร การเผยแพร่เอกสาร การยกเลิกเอกสาร และการทำลายเอกสารที่เลิกใช้งาน

6) กำหนดให้มีการควบคุมการเข้าถึงระบบสารสนเทศแก่ผู้ใช้งาน ตั้งแต่การลงทะเบียน การกำหนดสิทธิ การเพิกถอนสิทธิ การทบทวนสิทธิการใช้งาน รวมถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลในส่วนที่ไม่พึงเปิดเผยภายใต้บทบัญญัติของกฎหมาย

7) กำหนดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานครอบคลุมในเรื่องดังนี้ การจัดทำขั้นตอนปฏิบัติงาน การป้องกันมัลแวร์ การควบคุมการใช้งานซอฟต์แวร์ การบริหารจัดการช่องโหว่ และการตรวจสอบระบบสารสนเทศ

8) กำหนดให้มีการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม และมาตรการเกี่ยวกับการเข้าถึงทางกายภาพและสภาพแวดล้อมสำหรับพื้นที่สำนักงาน พื้นที่จัดส่งและรับของ พื้นที่มั่นคงปลอดภัย

9) กำหนดให้มีการบริหารจัดการการเปลี่ยนแปลงขององค์กรกระบวนการทางธุรกิจ สินทรัพย์และระบบประมวลผลข้อมูลสารสนเทศ ที่มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการวางแผน การจัดลำดับความสำคัญ ประเมินผลกระทบ การอนุมัติจากผู้มีอำนาจ การมอบหมาย ทดสอบ บันทึก และดำเนินการอย่างเหมาะสม เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล

10) กำหนดให้มีการบริหารจัดการการสำรองข้อมูลสำหรับระบบสารสนเทศ เพื่อป้องกันข้อมูลจากการสูญหาย ถูกทำลาย จากเหตุการณ์ไม่พึงประสงค์หรือเหตุการณ์ที่ไม่คาดคิด เพื่อให้ระบบสารสนเทศของสำนักงานสามารถให้บริการได้อย่างต่อเนื่อง

11) กำหนดให้มีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบสารสนเทศ เช่นกิจกรรมของผู้ดูแลระบบและผู้ใช้งาน ความผิดปกติหรือข้อผิดพลาดของระบบสารสนเทศ การใช้งานต่าง ๆ เป็นต้น ทั้งนี้ เหตุการณ์ที่บันทึกต้องได้รับการปกป้องจากการเปลี่ยนแปลงเพื่อทำลายและการเข้าถึงโดยไม่ได้รับอนุญาต โดยต้องมีการตรวจสอบและวิเคราะห์เหตุการณ์ที่บันทึกอย่างสม่ำเสมอ เพื่อป้องกันเหตุการณ์ไม่พึงประสงค์หรือภัยคุกคามที่อาจส่งผลกระทบต่อสำนักงาน

12) กำหนดให้มีการควบคุมการสื่อสาร และการส่งข้อมูลผ่านระบบเครือข่ายของสำนักงาน เพื่อป้องกันการเข้าถึงระบบสารสนเทศของสำนักงานจากผู้ที่ไม่ได้รับอนุญาต ป้องกันภัยคุกคามที่อาจก่อให้เกิดผลกระทบต่อสำนักงาน รวมถึงควบคุมการเข้าถึงการใช้งานระบบเครือข่ายเพื่อปฏิบัติงานจากภายนอกสำนักงานให้มีความมั่นคงปลอดภัย

13) กำหนดให้มีการพิจารณาด้านความมั่นคงปลอดภัยสารสนเทศในกระบวนการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ โดยมีการศึกษาความเป็นไปได้ การวิเคราะห์ผลกระทบ และการตรวจสอบระบบสารสนเทศให้มั่นใจว่าเป็นไปตามข้อกำหนดก่อนการโอนย้ายขึ้นสู่สภาพแวดล้อมการใช้งานจริง เพื่อป้องกันผลกระทบต่อการปฏิบัติงานหรือต่อภารกิจของสำนักงาน

14) กำหนดให้มีการใช้งานการเข้ารหัสเพื่อให้มีการปกป้องข้อมูลสำคัญขององค์กร และต้องมีการบริหารจัดการกุญแจในการเข้ารหัสด้วยวิธีการที่เหมาะสมและปลอดภัยเพียงพอในการปกป้องการเข้าถึงกุญแจโดยไม่ได้รับอนุญาต หรือการใช้งานอย่างไม่เหมาะสม

15) กำหนดให้มีการบริหารจัดการการให้บริการโดยหน่วยงานภายนอกโดยกำหนดระเบียบข้อบังคับ หลักเกณฑ์ และแนวปฏิบัติในการดำเนินงาน เพื่อใช้ในการติดตาม ทบทวน บริหารจัดการการเปลี่ยนแปลงการให้บริการ และตรวจประเมินการส่งมอบบริการของหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อควบคุมการเข้าถึงหรือใช้งานข้อมูลและระบบสารสนเทศของสำนักงาน ให้เป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

16) กำหนดให้มีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด โดยมีการกำหนดหน้าที่ของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการเฝ้าระวังการรายงานเหตุการณ์ การวิเคราะห์ การเก็บรวบรวมหลักฐาน การแก้ปัญหา และการบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น เพื่อให้เกิดการตอบสนองอย่างรวดเร็ว มีประสิทธิภาพและประสิทธิผล เป็นระเบียบแบบแผน และนำความรู้ที่ได้รับจากการวิเคราะห์และแก้ปัญหาไปใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ในอนาคต

17) กำหนดให้มีการปฏิบัติตามข้อกฎหมาย ระเบียบข้อบังคับ ข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มาตรฐาน และข้อกำหนดด้านความมั่นคงปลอดภัยที่สำนักงานกำหนด โดยมีการสื่อสารกับผู้ปฏิบัติงานให้รับทราบและเข้าใจ รวมทั้งมีการทบทวนและตรวจสอบการปฏิบัติตามนโยบายที่สำนักงานกำหนด

18) กำหนดให้มีการประเมินผลการปฏิบัติงานและการตรวจประเมินระบบมาตรฐานภายในโดยกำหนดให้มีการตรวจประเมินและวัดผลการปฏิบัติงานตามกฎหมาย ระเบียบ ข้อบังคับที่สำนักงานกำหนด รวมถึงมาตรฐานต่าง ๆ ที่จำเป็นต่อการดำเนินงานของสำนักงาน เพื่อมั่นใจถึงประสิทธิภาพในการปฏิบัติงานและความมั่นคงปลอดภัยในข้อมูล รวมถึงระบบสารสนเทศของสำนักงาน

19) ทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงานตามรอบเวลาที่กำหนดไว้อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

20) กำหนดให้มีการแก้ไขและปรับปรุงการปฏิบัติงานที่ไม่สอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการกำหนดกระบวนการในการทบทวน การระบุสาเหตุ การแก้ไขหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การทบทวนประสิทธิผลของปฏิบัติการแก้ไข รวมถึงการจัดเก็บเอกสารที่เกี่ยวข้อง เพื่อให้เกิดการพัฒนาอย่างต่อเนื่องและมีประสิทธิภาพ

ทั้งนี้ องค์กรได้กำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศฉบับย่อยออกเป็นทั้งหมด 5 ฉบับดังต่อไปนี้ เพื่อสามารถระบุรายละเอียดของความต้องการด้านความมั่นคงปลอดภัยสารสนเทศได้ชัดเจนยิ่งขึ้น

1. นโยบายการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control Policy)
2. นโยบายความมั่นคงปลอดภัยของการปฏิบัติงานและเครือข่าย (Communication and Operation Security Policy)
3. นโยบายความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security Policy)
4. นโยบายการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Policy)
5. นโยบายการใช้สารสนเทศขององค์กร (Acceptable Use Policy)

9.2 แนวปฏิบัติการรักษาความปลอดภัยทางข้อมูลสารสนเทศ (Information Security Guideline)

1) เจ้าของระบบ/ผู้ดูแลระบบ มีหน้าที่ความรับผิดชอบดังต่อไปนี้

- ปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ที่เจ้าของระบบกำหนดไว้
- สามารถยุติการทำงานของระบบสารสนเทศ ซึ่งพบว่าเป็นภัยต่อความมั่นคงปลอดภัยหรือสร้างภาระให้ระบบสารสนเทศของ BDI โดยไม่จำเป็นต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของภัยหรือภาระนั้น และทำรายงานให้ผู้บังคับบัญชารับทราบ
- สามารถยุติการทำงานของระบบสารสนเทศที่เปิดใช้โดยไม่ได้รับอนุญาต โดยไม่ต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของระบบงานนั้น และทำรายงานให้ผู้บังคับบัญชารับทราบ
- แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบ เพื่อบำรุงรักษาปรับปรุงหรือเปลี่ยนแปลงระบบ ซึ่งส่งผลให้ต้องหยุดบริการในช่วงเวลาหนึ่ง ยกเว้นในกรณีฉุกเฉิน ผู้ดูแลระบบมีสิทธิปิดระบบทันทีและจะต้องพยายามให้ผู้ใช้งานสามารถเก็บบันทึกข้อมูลได้อย่างสมบูรณ์ก่อนที่จะดำเนินการปิดระบบ และทำรายงานให้ผู้บังคับบัญชารับทราบ
- สามารถจำกัดหรือระงับสิทธิของผู้ใช้งานระบบอย่างไม่เหมาะสม และแจ้งให้ผู้บังคับบัญชารับทราบ เพื่อแจ้งไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อตั้งคณะกรรมการพิจารณาสอบสวนหรือลงโทษตามความเหมาะสม
- จะต้องรับผิดชอบในการปรับปรุงข้อมูลที่เกี่ยวข้องกับการดำเนินงานเมื่อมีการเปลี่ยนแปลงใด ๆ เกิดขึ้น
- ติดตาม กำชับการใช้งาน และปรับปรุงฐานข้อมูลของผู้ใช้งาน ให้ถูกต้องเป็นปัจจุบันอยู่เสมอ รวมทั้งต้องลบบัญชีผู้ใช้งานของผู้ที่หมดสิทธิในการใช้งานระบบออกจากฐานข้อมูล
- ต้องติดตามข่าวสาร ภาวะภัยคุกคาม ช่องโหว่ของระบบสารสนเทศ และต้องปรับปรุงดูแลระบบเพื่อลดความเสี่ยงของการถูกบุกรุกอย่างสม่ำเสมอ

- ต้องขออนุญาตผู้บังคับบัญชาในกรณีที่มีการประเมิน ตรวจสอบ ทดสอบหาจุดอ่อนช่องโหว่อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศและทำการแก้ไขอย่างรวดเร็ว

- ต้องรายงานผู้บังคับบัญชาในกรณีที่ตรวจพบหรือได้รับรายงานจากผู้ใช้งานหรือสงสัยว่าระบบ สารสนเทศที่รับผิดชอบโดยตรงหรือระบบที่เกี่ยวข้องอื่นใดของ BDI ถูกละเมิดทางด้านความมั่นคงปลอดภัย

- การเพิ่มหรือลดสิทธิในการเข้าถึงระบบใด ๆ ให้ปฏิบัติตามเอกสารกระบวนการที่เจ้าของระบบกำหนดอย่างเคร่งครัด พร้อมทั้งทบทวนความเหมาะสมของมาตรการที่นำมาใช้ในระบบอย่างสม่ำเสมอ

- ต้องสมัครเป็นสมาชิกเพื่อรับข่าวสารแจ้งเตือนเกี่ยวกับช่องโหว่ด้านความมั่นคงปลอดภัยและเข้าร่วมการประชุมหรือสัมมนาที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

2) ผู้รับผิดชอบข้อมูล มีสิทธิหน้าที่ความรับผิดชอบ ดังต่อไปนี้

- อนุมัติและตรวจทานเพื่อให้มั่นใจว่าสิทธิของผู้ใช้งานถูกต้องเหมาะสม

- กำหนดระดับชั้นความปลอดภัยให้กับข้อมูล

- ตรวจทานระดับชั้นความปลอดภัยของข้อมูลเพื่อให้มั่นใจว่ายังเป็นไปตามความต้องการของการปฏิบัติงาน และมีความเหมาะสมและสอดคล้องกับระดับความปลอดภัยนั้น ๆ

- ตรวจสอบให้มั่นใจว่าข้อมูลที่ได้มีการระบุหรือแสดงระดับความปลอดภัยตามที่ได้จัดระดับไว้อย่างถูกต้องและเหมาะสม ไม่ว่าจะอยู่ในรูปแบบหรือสื่อประเภทใดก็ตามกำหนดพื้นฐานการรักษาความปลอดภัยในการเข้าถึงข้อมูลของหน่วยงาน

3) ผู้ใช้งาน มีสิทธิหน้าที่ความรับผิดชอบ ดังต่อไปนี้

- สามารถเข้าถึงข้อมูล ข่าวสาร ที่มิใช่ข้อมูลและสารสนเทศที่กำหนดชั้นความลับยกเว้น ในกรณีที่ได้รับอนุญาตสิทธิเป็นลายลักษณ์อักษรตามที่กำหนดไว้ในเอกสารระเบียบการปฏิบัติงาน เรื่องการจัดระดับชั้นความลับข้อมูลและสารสนเทศ

- ต้องช่วยกันรักษาอุปกรณ์ต่าง ๆ ไม่ให้เกิดความเสียหายหากมีความเสียหายจากอุบัติเหตุหรือภัยต่าง ๆ ผู้ใช้งานต้องแจ้งผู้ดูแลระบบ และผู้บังคับบัญชารับทราบทันที

- พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ขนาดใหญ่โดยไม่จำเป็น ไม่ส่งหรือกระจายส่งต่อไปรษณีย์อิเล็กทรอนิกส์ในลักษณะจดหมายลูกโซ่ ฯลฯ

- ต้องให้ข้อมูลประจำตัวที่ถูกต้องสำหรับการเปิดบัญชีผู้ใช้งาน (User ID หรือ Login Account)

- ต้องรับผิดชอบในการเลือกรหัสผ่าน (Password) ที่ปลอดภัยตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

- ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาด มิฉะนั้น ผู้ใช้งานอาจมีความผิดทางวินัยและต้องรับผิดชอบต่อปัญหาที่เกิดขึ้น เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย ฯลฯ

- ต้องแจ้งต่อผู้ดูแลระบบและผู้บังคับบัญชาโดยทันทีในกรณีตรวจพบ หรือสงสัยว่ามีการนำบัญชีผู้ใช้งานของตนหรือของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาต หรือใช้งานในทางมิชอบและพบเห็นพฤติกรรมการล่วงละเมิดความมั่นคงปลอดภัยทุกอย่างในระบบ

- ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

- ไม่ล่วงล้ำเข้าในบริเวณพื้นที่ใช้งานระบบสารสนเทศที่ไม่ได้รับอนุญาต

- ต้องใช้ระบบในลักษณะที่ถูกต้องตามกฎหมาย ไม่ละเมิดสิทธิและไม่ก่อความเดือดร้อนหรือความเสียหายแก่บุคคลหรือองค์กรอื่น
- ไม่ติดตั้งหรือเปิดให้บริการระบบเครือข่ายบนเครื่องของรัฐสภาเพื่อทำธุรกิจส่วนตัว
- ต้องคืนสินทรัพย์ของรัฐสภาอันเกี่ยวกับการปฏิบัติหน้าที่ในทันทีที่พ้นหน้าที่ เช่น อุปกรณ์ระบบ สารสนเทศข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า - ออก ฯลฯ
- แจ้งให้ผู้ดูแลระบบและผู้บังคับบัญชาหน่วยงานทราบทันทีในกรณีที่มีการเคลื่อนย้ายถอดถอนอุปกรณ์ระบบสารสนเทศ
- แจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยให้กับผู้ดูแลระบบทันที ในกรณีที่มีเหตุการณ์บุกรุกหรือเหตุการณ์ผิดปกติในการใช้งาน
- ต้องปฏิบัติตามมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนการปฏิบัติงาน (Procedure) อันเกี่ยวเนื่องกับความมั่นคงปลอดภัยด้านสารสนเทศ
- หากพบว่าระบบรักษาความปลอดภัยมีข้อบกพร่อง หรือสงสัยว่ามีผู้ใดกระทำการที่น่าสงสัย ให้แจ้งต่อผู้ดูแลระบบโดยทันที
- ต้องให้ความร่วมมือกับเจ้าหน้าที่ที่ได้รับมอบหมาย ให้ทำการสืบสวนสอบสวนเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัย
- ปกป้องข้อมูลและปฏิบัติตามข้อกำหนดในแนวปฏิบัติมาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง
- รับผิดชอบการดำเนินการใด ๆ ที่เกี่ยวข้องกับการใช้งานข้อมูลสารสนเทศ (Accountability)

4) ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

- การบริหารจัดการโครงการต่าง ๆ ต้องพิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ
- เจ้าของโครงการ ผู้จัดการโครงการ ส่วนงานที่ดูแลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและส่วนงานอื่น ๆ ที่เกี่ยวข้องควรพิจารณาและดำเนินกิจกรรมในแต่ละระยะของกระบวนการบริหารโครงการ

5) แนวปฏิบัติอื่น ๆ ให้ศึกษาและดำเนินการตามเล่ม Information Security Policy, Risk Management Procedure, Communications and Operation Management Policy และ Security Incident Management Guideline

เอกสารเพิ่มเติม

1) SP-ACLP-001_Access Control Management
2) SP-CMOM-003_Communications and Operation Management
3) SP-PHES-002_Physical and Environmental Security
4) PD-RSKM-003_Risk Management Procedure
5) GL-SINC-002_Security Incident Management Guideline
6) PD-SINC-001_Security Incident Management Procedure

10. การบูรณาการและแลกเปลี่ยนข้อมูล (Data Exchange)

10.1 นโยบายการบูรณาการและแลกเปลี่ยนข้อมูล (Data Exchange Policy)

1) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูล เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

2) กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยน ที่จำเป็นให้ครบถ้วน

3) จัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

4) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

5) ต้องบันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อการตรวจสอบย้อนกลับ

6) กำหนดแนวปฏิบัติในการจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยรวมถึงคุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

7) ต้องตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวปฏิบัติกระบวนการแลกเปลี่ยน และมาตรฐานที่กำหนด

10.2 แนวปฏิบัติการบูรณาการและแลกเปลี่ยนข้อมูล (Data Exchange Guideline)

1) กำหนดให้ผู้จัดการโครงการ กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบดังนี้

- การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล
- การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ

2) กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

- ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้หากไม่ครบถ้วนต้องจัดทำเพิ่มเติม ตามความต้องการของหน่วยงานที่ขอใช้
- ตรวจสอบชั้นความลับของข้อมูล ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับ ทางราชการ และความเป็นส่วนบุคคล พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ
- หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งผู้รับผิดชอบข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิคและทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

3) ในกรณีที่มีหน่วยงานที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลส่วนบุคคลในการครอบครองของหน่วยงาน เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ให้หน่วยงานผู้รับผิดชอบข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นโดยไม่แสดงตัวตน (Anonymization)

4) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลเพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

5) ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

6) กำหนดให้ผู้ดูระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่างๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

ข้อกฎหมายและเอกสารอ้างอิง

1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

3) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5) กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

11. การสำรองและกู้คืนข้อมูล (Data Backup & Recovery)

11.1 นโยบายการสำรองและกู้คืนข้อมูล (Data Backup & Recovery Policy)

1) กำหนดรายละเอียดเกี่ยวกับกระบวนการ หรือระบบในการสำรองและกู้คืนข้อมูล (Backup and Recovery Procedures)

2) กำหนดให้ทุกการพัฒนาระบบฐานข้อมูลสารสนเทศ จะต้องจัดให้มีระบบสำรองและกู้คืนข้อมูลที่ได้มาตรฐานสากล

3) มีแนวทางในการสำรองและกู้คืนระบบ เพื่อลดความเสี่ยงจากที่อาจเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ ฮาร์ดดิสก์เสียหายไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยผู้ใช้งานเอง

4) ระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัดและมีนโยบายเกี่ยวกับการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (ดูรายละเอียดเพิ่มเติม Business Continuity Management Policy)

5) เจ้าหน้าที่ในหน่วยงานต้องทราบถึงนโยบายและแนวปฏิบัติ และปฏิบัติตามอย่างเคร่งครัด มีกระบวนการตรวจสอบ

11.2 แนวปฏิบัติการสำรองและกู้คืนข้อมูล (Data Backup & Recovery Guideline)

1) จัดทำรายการเครื่องคอมพิวเตอร์แม่ข่ายและรายการระบบสารสนเทศและฐานข้อมูลต่าง ๆ ที่เกี่ยวข้องเพื่อจัดทำกระบวนการในการสำรองและกู้คืนข้อมูล

2) ติดตั้งโปรแกรมสำรองข้อมูล (Backup Agent) ในเครื่องคอมพิวเตอร์แม่ข่ายที่กำหนด หรือมีการตั้งค่าการสำรองข้อมูลแบบอัตโนมัติ

3) จัดตารางเวลาและกำหนดคนรับผิดชอบในทุกกระบวนงานในการสำรองและกู้คืนข้อมูล

4) มีการตรวจสอบความพร้อมสื่อบันทึกข้อมูล

5) มีการตรวจสอบผลการสำรองข้อมูลสารสนเทศ และบันทึกผลการสำรองข้อมูลสารสนเทศ

6) มีการทดสอบการกู้คืนข้อมูล โดยคัดลอกไฟล์สำรองข้อมูลสารสนเทศเพื่อทดสอบการกู้คืนข้อมูลสารสนเทศ

7) ตรวจสอบผลการกู้คืนข้อมูลสารสนเทศ และบันทึกผลการกู้คืนข้อมูลสารสนเทศ

8) กรณีที่ระบบหรือข้อมูลใดๆที่มีความสำคัญมากๆ จะต้องมีการจัดเก็บการสำรองแยกเน็ตเวิร์กเพื่อป้องกันเหตุการณ์ เช่น ransomware

Backup Data Source Manifest					
Date :		Server Name :		IP :	

Type of OS

	Windows	Version :		Type :	
	Linux	Version :		Type :	
	Unix	Version :		Type :	

List of Files/Folders to be Backup

Backup Agent and Policy

Backup Agent Installed on Server :		☐ Yes		☐ No			
Backup Policy :	MON	TUE	WED	THU	FRI	SAT	SUN
	☐ Full	☐ Full	☐ Full	☐ Full	☐ Full	☐ Full	☐ Full
	☐ Differential	☐ Differential	☐ Differential	☐ Differential	☐ Differential	☐ Differential	☐ Differential
	☐ Incremental	☐ Incremental	☐ Incremental	☐ Incremental	☐ Incremental	☐ Incremental	☐ Incremental

Schedule for Policy :	AM :		PM :	
Retention Period for Backup :	☐ 1 Week	☐ 2 Weeks	☐ 1 Month	☐ 2 Months
Offsite Storage :	☐ Yes		☐ No	

Backup Result

Duration (HH:MM)	Begin :		End :	
Completion :	☐ Yes		☐ No	

Signatures

Backup Administrator Signature :	

ตัวอย่างแบบฟอร์มการบันทึกข้อมูลการกู้คืนข้อมูล

Recovery Data Source Manifest					
Date :		Server Name :		IP :	

Type of OS

	Windows	Version :		Type :	
	Linux	Version :		Type :	
	Unix	Version :		Type :	

List of Files/Folders to be Recovery

Backup Agent and Recovery Method

Backup Agent Installed on Server:	☐ Yes	☐ No	
Recovery Method	☐ Roll Back Data and Configuration Files		
	☐ Recovery with Differential Backup	From Date :	
	☐ Recovery with Incremental Backup	From Date :	
	☐ Recovery with Full Backup	From Date :	
	☐ Recovery with VM Snapshot	From Date :	
	☐ Reinstall OS		

Recovery Result

Duration (HH:MM)	Begin :		End :	
Completion :	☐ Yes		☐ No	

Signatures

Data Owner Signature :	
Recovery Administrator Signature :	

เอกสารเพิ่มเติม

1) PD-002-BCPP_Business Continuity Plan
2) PD-003-RSKM_Risk Management Procedure

12. การประเมินผลธรรมาภิบาลข้อมูล (Data Governance Assessment)

การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐจะทำให้เราได้ทราบถึงสิ่งที่ สขญ. ดำเนินการแล้ว และสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Readiness Assessment) ของ สขญ. ให้อิงตามแนวทางของ สพร. ดังกำหนดเกณฑ์ชี้วัดไว้ใน ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ซึ่งประกอบด้วย ๖ ระดับ ดังนี้

ระดับ ๐ : None หมายถึง ไม่มีธรรมาภิบาลข้อมูลภาครัฐหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ นั่นคือ มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ

ระดับ ๑ : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและธรรมาภิบาลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศทำให้การทำงานร่วมกันระหว่างฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

ระดับ ๒ : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและผู้รับผิดชอบข้อมูล

ระดับ ๓ : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความมั่นคงปลอดภัย

ระดับ ๔ : Advanced หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย

ระดับ ๕ : Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ ๔ วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (non-Conformation) คุณภาพข้อมูลที่ต่ำ และความไม่คุ้มทุนในการบริหารจัดการข้อมูลดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

ระดับ	โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	กระบวนการธรรมาภิบาลข้อมูลภาครัฐ	นโยบายข้อมูลและการตรวจสอบ	การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	การปรับปรุงอย่างต่อเนื่อง
๐ : None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๑ : Initial	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	กระบวนการยังไม่เป็นมาตรฐาน	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๒ : Managed	มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ	มีกระบวนการเป็นมาตรฐานส่วนงาน/บริการ	บังคับใช้ในส่วนงาน/บริการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๓ : Standardized	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๔ : Advanced	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๕ : Optimized	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	มีการปรับปรุงกระบวนการอย่างต่อเนื่อง

รูป ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ที่มา: ธรรมาภิบาลข้อมูลภาครัฐ สพร.

ข้อกฎหมายและเอกสารอ้างอิง

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ