ร่างนโยบายที่เกี่ยวข้องต่อการบริหารจัดการธรรมาภิบาลข้อมูล

(DATA GOVERNANCE POLICY AND RELATED)

โครงการจัดจ้างที่ปรึกษาวิเคราะห์และจัดทำแนวทางนโยบายธรรมมาภิบาลข้อมูลภาครัฐเพื่อนำไปสู่การพัฒนาชุดข้อมูลเปิดของกรมประชาสัมพันธ์

MAY 2023

PREPARED BY

THAMMASAT UNIVERSITY
RESEARCH AND CONSULTANCY INSTITUTE
สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

Document Control

Document Owner	Thailand Public Relations Department (PRD)
Document Preparer	Thammasat University Research and Consultancy Institute
Document Name	ร่างนโยบายที่เกี่ยวข้องต่อการบริหารจัดการธรรมาภิบาลข้อมูล (Data Governance Policy and Related)
Version	1.0.0
Status	Final

Document Change Record

Version	Date Last Modified	By	Details of modification
1.0.0	5/15/2023	TU	Final

Document Review

Name	Position

Document Approver

Name	Position	Signature	Date
			Click or tap to enter a date.

สารบัญ

วัตถุประสงค์

1. เพื่อกำหนดนโยบายให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมประชาสัมพันธ์ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศและปฏิบัติอย่างเหมาะสม
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยสารสนเทศของกรมประชาสัมพันธ์ ว่าจะสามารถเข้าถึงได้เฉพาะผู้ที่รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)
3. เพื่อเผยแพร่ให้เจ้าหน้าที่และผู้ใช้งานสารสนเทศของกรมประชาสัมพันธ์ ได้รับทราบและถือปฏิบัติย่างเคร่งครัด

ขอบเขต

ใช้สำหรับการรักษาความปลอดภัยทางเทคโนโลยีที่จะต้องมีการรักษาข้อมูลทั้งที่อยู่ให้เป็นความลับ พร้อมใช้งาน และมีการป้องกันความปลอดภัยอย่างเหมาะสม เพื่อให้พร้อมใช้งานภายในองค์กรมากที่สุด

อ้างอิง

(References outside the company document system, such as the law, regulation, etc.)

- -

คำจำกัดความและความหมาย

“กปส.”	กรมประชาสัมพันธ์

นโยบายธรรมาภิบาลข้อมูล

นโยบายการดำเนินงานด้านธรรมาภิบาลข้อมูล

(Data Governance Policy)

ด้วยกรมประชาสัมพันธ์ (“กปส”) ได้ตระหนักถึงและเล็งเห็นความสำคัญในการบริหารจัดการข้อมูลตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.2562 รวมทั้งคณะกรรมการพัฒนารัฐบาลดิจิทัลได้กำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐใช้เป็นหลักการและแนวทางการดำเนินงานตามพระราชบัญญัติดังกล่าว เพื่อมุ่งเน้นให้เกิดธรรมาภิบาลข้อมูลภาครัฐและการให้บริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ ตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ตลอดจนให้หน่วยงานของรัฐมีการดำเนินการในด้านการบริหารจัดการและบูรณการข้อมูลภาครัฐ โดยให้การทำงานมีความสอดคล้องและเชื่อมโยงข้อมูลเข้าด้วยกันอย่างมั่นคง ปลอดภัย มีธรรมาภิบาล

ดังนั้นเพื่อให้การบริหารจัดการข้อมูลของกรม ฯ เป็นไปด้วยความเรียบร้อยและสอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.2562 จึงได้มีการกำหนดนโยบายในการดำเนินงานด้านธรรมาภิบาลข้อมูลโดยมีสาระสำคัญดังต่อไปนี้

1. กำหนดและจัดให้มีคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) เพื่อให้การบริหารจัดการข้อมูลของ กปส. มีความมั่งคงปลอดภัย (Data Security) มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและสอดคล้องกับกฎหมาย (Data Privacy) และมีคุณภาพ (Data Quality) รวมถึงต้องดำเนินการขับเคลื่อนและผลักดันให้เกิดการบริหารจัดการข้อมูลตามเป้าหมายขององค์กร
2. กำหนดสิทธิ หน้าที่และความรับผิดชอบในการบริหารจัดการข้อมูลของผู้ซึ่งมีหน้าทีเกี่ยวข้องกับการบริหารจัดการข้อมูลของ กปส. ในทุกกระบวนการ
3. กำหนดระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วน ตั้งแต่การจัดทำ การจัดเก็บ การจำแนกหมวดหมู่ การประมวลหรือใช้ข้อมูล การปิดปิดหรือการเปิดเผยข้อมูล การตรวจสอบและการทำลายตามคู่มือบริหารจัดการข้อมูลที่ดี (Data Governance Handbook) ของ กปส.
4. กำหนดและจัดให้มีการวางแผนการดำเนินงาน การปฏิบัติตามแผนการดำเนินงาน การตรวจสอบ การรายงานผลการดำเนินงาน และปรับปรุงแผนการดำเนินงานอย่างต่อเนื่อง เพื่อให้ระบบบริหารและกระบวนการจัดการข้อมูลมีประสิทธิภาพสามารถเชื่องโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างกันทั้งภายในและภายนอกหน่วยงาน และคุ้มครองข้อมูลให้ประสิทธิภาพ
5. กำหนดและจัดให้มีมาตรการควบคุมและพัฒนาข้อมูล ตามคู่มือบริหารจัดการข้อมูลที่ดี (Data Governance Handbook) ของ กปส.เพื่อให้ข้อมูลมีความถูกต้องครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ถูกละเมิดความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยงแลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ
6. กำหนดและจัดให้มีการวัดผลการบริหารจัดการข้อมูล โดยการประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยข้อมูล

7. กำหนดและจัดให้มีการจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับการเข้าถึงข้อมูล ผู้มีสิทธิเข้าถึง และการใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงานและจากหน่วยงานภายนอก สำหรับให้ผู้ที่หน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ
8. กำหนดและจัดให้มีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในครอบครองให้มีความมั่นคงปลอดภัย และมิให้ข้อมูลส่วนบุคคลถูกละเมิด
9. จัดให้มีการจัดทำคำอธิบายชุดข้อมูลดิจิทัลและบัญชีข้อมูลของ กปส. ให้มีความถูกต้อง ครบถ้วน สมบูรณ์และเป็นปัจจุบัน ตามคู่มือบริหารจัดการข้อมูลที่ดี (Data Governance Handbook) ของ กปส.
10. กำหนดและจัดให้มีนโยบาย ขั้นตอนปฏิบัติ มาตรฐาน ข้อกำหนด และระบบงานที่ใช้ในการกำกับดูแลและบริหารจัดการเกี่ยวกับธรรมาภิบาลข้อมูล เพื่อเป็นการวางหลักเกณฑ์แนวทางเกี่ยวกับการบริหารจัดการข้อมูลระดับองค์กรที่ดี รวมทั้งกำหนดให้มีการปรับปรุงเนื้อหาของเอกสารและกระบวนการดังกล่าวอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการบริหารจัดการข้อมูลขององค์กร

นโยบายฯ ฉบับนี้ ประยุกต์ใช้กับทุกหน่วยงานของ กรมประชาสัมพันธ์ ผู้บริหาร บุคลากร และผู้ปฏิบัติงานให้กรมประชาสัมพันธ์ โดยบุคลากรทุกคนทั้งภายในและภายนอกต้องเข้าใจและปฏิบัติตามนโยบาย ฉบับนี้ โดยผู้บริหารในทุกระดับต้องเป็นแบบอย่างที่ดี รวมทั้งสนับสนุน ผลักดัน ให้เกิดการปฏิบัติอย่างจริงจัง

นโยบายการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

นโยบายการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

(Information Technology Security Management Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมประชาสัมพันธ์ (“กปส”) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล และครอบคลุมองค์ประกอบด้านความมั่นคงปลอดภัยสารสนเทศ ที่ประกอบไปด้วย การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) หรือหลัก CIA รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศที่ไม่ถูกต้องและภัยคุกคามต่าง ๆ จึงสมควรกำหนดให้มีการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของกรมประชาสัมพันธ์ โดยมีสาระสำคัญดังต่อไปนี้

1. สร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศให้มีประสิทธิภาพและประสิทธิผล
2. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยอ้างอิงมาตรฐาน ISO/IEC 27001:2022 และพิจารณาปรับปรุงขอบเขต ดังกล่าวอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร
3. จัดให้มีนโยบาย ขั้นตอนปฏิบัติ มาตรฐาน ข้อกำหนด และระบบงานที่ใช้ในการกำกับดูแลและบริหารจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการวางหลักเกณฑ์แนวทางเกี่ยวกับการรักษาความปลอดภัยของสารสนเทศระดับองค์กรที่ดี รวมทั้งกำหนดให้มีการปรับปรุงเนื้อหาของเอกสารและกระบวนการดังกล่าวอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร
4. จัดให้มีการสื่อสาร เผยแพร่ และสร้างความรู้ความเข้าใจถึงการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับในองค์กร
5. ผู้บริหาร บุคลากร ผู้ดูแลระบบและบุคคลภายนอก/หน่วยงานภายนอก ที่ปฏิบัติงานให้กับกรมประชาสัมพันธ์ต้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศของกรมประชาสัมพันธ์ในการดำเนินงานตามมาตรฐานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและต้องมีการลงนามยอมรับและปฏิบัติตามนโยบาย ขั้นตอนปฏิบัติ มาตรฐาน ข้อกำหนด ที่เกี่ยวข้องอย่างเคร่งครัด
6. จัดให้มีการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อป้องกันภัยคุกคามต่าง ๆ ที่อาจจะส่งผลกระทบต่อการดำเนินงาน/ภารกิจของกรมประชาสัมพันธ์
7. จัดให้มีการวิเคราะห์เหตุการณ์ต่าง ๆ ที่ก่อให้เกิดความเสียหายหรือสูญเสียของระบบสารสนเทศ รวมทั้งการรั่วไหลของสารสนเทศ เพื่อพิจารณาหาแนวทางแก้ไขและป้องกัน

นโยบายฯ ฉบับนี้ ประยุกต์ใช้กับทุกหน่วยงานของ กรมประชาสัมพันธ์ ผู้บริหาร บุคลากร และผู้ปฏิบัติงานให้กรมประชาสัมพันธ์ โดยบุคลากรทุกคนทั้งภายในและภายนอกต้องเข้าใจและปฏิบัติตามนโยบาย ฉบับนี้ โดยผู้บริหารในทุกระดับต้องเป็นแบบอย่างที่ดี รวมทั้งสนับสนุน ผลักดัน ให้เกิดการปฏิบัติอย่างจริงจัง

มาตรการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy)

บททั่วไป

- ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และ อุปกรณ์ต่อเชื่อมของ องค์กร จัดหาเพื่อให้บริการที่เกี่ยวข้องกับกิจการของ องค์กร เท่านั้น ไม่อนุญาตให้ใช้ในกิจการที่ไม่เกี่ยวข้อง กับกิจการขององค์กร
- การเข้าใช้งานระบบคอมพิวเตอร์และการต่อเชื่อมทาง อินเทอร์เน็ต ขององค์กร จะต้องปฏิบัติตามนโยบายฯ ฉบับนี้ โดยจะมีการลงทะเบียนก่อนการเข้าใช้งาน
- ในการขออนุญาตเข้าใช้งาน ให้หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานของผู้ที่จะขอใช้บริการเป็นผู้ขอ โดยปฏิบัติตามนโยบายฯ ฉบับนี้
- ผู้เข้าใช้งานจะต้องทำความเข้าใจและลงนามเพื่อยืนยันตามนโยบายการอนุญาตให้ใช้ทรัพย์สินขององค์กร (Acceptable Use Policy) ว่าจะปฏิบัติตามนโยบายที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- นโยบายฯ ฉบับนี้ ถือเป็นส่วนหนึ่งของข้อกำหนดในการปฏิบัติงานของผู้ใช้ทุกคน และจะถือเป็นการผิดวินัยการทำงานเช่นเดียวกันหากไม่ปฏิบัติตาม
- องค์กร ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อทางอินเทอร์เน็ต ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และกฎหมาย ประกอบอื่น ๆ ที่เกี่ยวข้องโดยผู้ใช้สามารถศึกษาตัวกฎหมายได้โดยติดต่อมายัง องค์กร
- องค์กร ไม่สนับสนุน หรือยินยอมให้ผู้ใช้งานขององค์กร กระทำผิดต่อ พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายประกอบอื่น ๆ ที่เกี่ยวข้อง
- หากพบว่าผู้ใช้มีการละเมิดนโยบายฯ ฉบับนี้ จะถูกลงโทษตามกฎระเบียบฯ ขององค์กร รวมไปถึงการส่งตัวเพื่อดำเนินคดีตามกฎหมายหากการละเมิดนั้นผิดต่อกฎหมายของประเทศ
- กำหนดให้มีการทบทวนนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงให้ทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโดยมีนัยยะสำคัญ

มาตรฐานการบริหารจัดการความเสี่ยง (Risk Management Policy)

- กำหนดให้มีการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัย และให้มีการทบทวนการประเมินความเสี่ยงเป็นประจำสม่ำเสมอ อย่างน้อย ปีละ 1 ครั้ง หรือ มีการเปลี่ยนแปลงรายการบัญชีทรัพย์สินสารสนเทศ (การเพิ่มการเปลี่ยนแปลงรายละเอียดสำคัญการลด) หรือ มีการเปลี่ยนแปลงที่มีแนวโน้มกระทบต่อมาตรการควบคุมและป้องกันด้านความมั่นคงปลอดภัยต่อสารสนเทศ (ISMS) ให้มีการบริหารจัดการความเสี่ยงที่เพิ่มเข้ามาในระบบ ISMS ได้ทันที ตามระเบียบปฏิบัติงานการประเมินความเสี่ยง (Risk Assessment)
- เสนอรายงานผลการประเมินความเสี่ยง (Risk Assessment Report) และแผนลดความเสี่ยง (Risk Treatment) ต่อผู้บริหารให้รับทราบและอนุมัติการจัดการ

มาตรฐานหน้าที่และความรับผิดชอบของผู้ใช้งาน (User Responsibility)

ผู้ใช้งานมีหน้าที่เกี่ยวข้องกับการบริหารจัดการการใช้งานระบบคอมพิวเตอร์ดังนี้

- การจัดการรหัสผ่าน (Password) ดังนี้
  - ต้องใช้การระบุและพิสูจน์ตัวตนของผู้ใช้งานตาม**นโยบายการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and Authentication)** และรหัสผ่านที่เป็นของตนเองในการแสดงตนเข้าใช้งานหรือปฏิบัติงานในระบบข้อมูลตามสิทธิ์ที่ได้รับเท่านั้น
  - เก็บรักษาบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้เป็นความลับ
  - รหัสผ่านของผู้ใช้งานถือเป็นทรัพย์สินขององค์กร องค์กร ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และผู้ใช้ทุกคนมีหน้าที่ในการป้องกันรหัสผ่านอย่างเคร่งครัด
  - กำหนดให้ใช้แนวทางการตั้งรหัสผ่านที่ปลอดภัย ดังนี้
    - เมื่อได้รับรหัสผ่านในครั้งแรก ต้องเปลี่ยนรหัสผ่านใหม่ทันทีให้เป็นความลับเฉพาะตัว ในกรณีที่รหัสผ่านถูกเปิดเผยแล้ว บุคลากรจะต้องทำการเปลี่ยนรหัสผ่านใหม่ทันที
    - รหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักขระ สำหรับระบบซึ่งมีการใช้งานหลังการประกาศใช้งานนโยบายฯ ฉบับนี้ ซึ่งประกอบด้วย ตัวอักษร ตัวเลข หรือสัญลักษณ์อื่นใดที่ยากต่อการคาดเดา ยกเว้นระบบงานที่มีข้อจำกัดงานด้านอุปกรณ์
    - ไม่กำหนดรหัสผ่านจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือคำศัพท์ที่ปรากฏในพจนานุกรม
    - หลีกเลี่ยงรหัสผ่านที่เดาได้ง่าย เช่น ชื่อบุคคล สถานที่ ฯลฯ
  - หลีกเลี่ยงการเก็บบันทึกรหัสผ่านลงในกระดาษ ไฟล์ข้อมูล ยกเว้นว่ามีขั้นตอนหรือวิธีการเก็บรักษาที่พิสูจน์ได้ว่าปลอดภัยจริง
  - กำหนดให้เปลี่ยนรหัสผ่าน เปลี่ยนรหัสผ่านเป็นประจำ ภายในทุก ๆ 90 วัน
- การป้องกันอุปกรณ์ที่ไม่มีบุคลากรดูแล (Unattended Use Equipment) ดังนี้
  - กำหนดให้มีมาตรการควบคุมดูแลและป้องกันอุปกรณ์ที่ไม่มีบุคลากรดูแล
  - กำหนดให้มีมาตรการควบคุมดูแลและป้องกันอุปกรณ์โดยการตั้งค่า Automatic log off หรือ Screen Saver เพื่อให้ระบบคอมพิวเตอร์ทำการล็อคหน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้มีการใช้งานเกินกว่า 3 นาที หรือ5 นาทียกเว้นระบบคอมพิวเตอร์ที่มีการเฝ้าระวังอยู่ตลอดเวลา
  - หน้าที่และความรับผิดชอบของผู้ใช้งานในการป้องกันการเข้าถึงในทุกระดับโดยไม่ได้รับอนุญาต
  - ห้ามให้บุคคลภายนอกใช้งานเครื่องคอมพิวเตอร์ขององค์กรโดยไม่ได้รับอนุญาต
  - ต้องไม่ใช้เครื่องคอมพิวเตอร์ในทางที่ก่อหรือจะก่อให้เกิดความเสียหายต่อผู้อื่น ต่อองค์กร ผิดกฎหมายหรือศีลธรรมอันดี เช่น
    - การเข้าถึงข้อมูล เครือข่าย หรือระบบงานโดยมิชอบหรือโดยไม่ได้รับอนุญาต
    - การรบกวน หรือก่อความรำคาญต่อเครือข่ายหรือระบบงาน
    - การดักรับหรือดักจับข้อมูลของผู้อื่น
    - การลักลอบถอดรหัสผ่าน
    - การปลอมแปลงหรือเปลี่ยนแปลงข้อมูลโดยมิชอบหรือโดยไม่ได้รับอนุญาต

- การเผยแพร่รูปภาพ ข้อความ หรือเสียงที่ไม่เหมาะสม
- การกระทำสิ่งใดที่ผิดกฎหมายหรือส่อเจตนาไปในทางที่ผิดจากพฤติกรรมการใช้งานปกติ

มาตรฐานโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

- จัดเก็บข้อมูลขององค์กร อย่างปลอดภัยสอดคล้องตามระดับชั้นความลับของข้อมูล ตาม**นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- ไม่เปิดโอกาสให้ผู้ไม่เกี่ยวข้องเข้าถึงข้อมูลขององค์กร ในคอมพิวเตอร์ ทั้งโดยเจตนาหรือไม่เจตนา
- ห้ามติดตั้งหรือถอดถอนโปรแกรมคอมพิวเตอร์ที่ได้ไม่ได้รับอนุญาตเข้าในระบบคอมพิวเตอร์ที่จัดเก็บข้อมูลขององค์กร
- ห้ามติดตั้งและใช้งานโปรแกรมประเภท FTP (File Transfer Protocol) เพื่อการเคลื่อนย้ายข้อมูล โดยไม่ได้รับอนุญาต
- เมื่อมีการใช้งาน Printer Fax และใช้งานอุปกรณ์อื่น ๆ นำออกหรือส่งผ่านข้อมูลสำคัญ ผู้ใช้งานต้องกำกับดูแลจนกระทั่งดำเนินการต่อข้อมูลนั้นเรียบร้อย รวมถึงการฉายภาพ การนำเสนอข้อมูลผ่าน Presentation ในที่สาธารณะ เพื่อให้มั่นใจว่าข้อมูลสำคัญไม่รั่วไหลไปยังผู้ที่ไม่ได้รับอนุญาต
- ก่อนเลิกงาน ต้องแน่ใจว่าได้จัดเก็บเครื่องคอมพิวเตอร์ที่มีข้อมูลสำคัญไว้ในที่เหมาะสม ปลอดภัยและป้องกันผู้ไม่เกี่ยวข้องเข้าถึงได้ ตาม**นโยบายการจัดวางและป้องกันอุปกรณ์ (Equipment Security)**
- หากเกิดการชำรุด เสียหาย หรือสูญหายของเครื่องคอมพิวเตอร์ที่ใช้งาน เมื่อสอบสวนแล้วและพบว่าไม่ได้ใช้ความระมัดระวังและดูแลอย่างเพียงพอ ต้องรับผิดชอบในการชำรุด เสียหาย หรือสูญหายนั้น
- ไม่อนุญาตให้นำเครื่องคอมพิวเตอร์ไปใช้งานเพื่อการอื่นใดที่ไม่เกี่ยวข้องกับงานตามภารกิจหรือหน้าที่ความรับผิดชอบ
- การลบหรือป้องกันข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์ก่อนส่งซ่อม ให้ผู้รับผิดชอบส่งเครื่องคอมพิวเตอร์ให้หน่วยที่รับผิดชอบเพื่อดำเนินการก่อนส่งให้ผู้ให้บริการภายนอกซ่อม
- สำรองข้อมูลในเครื่องคอมพิวเตอร์ที่สำคัญหรือใช้งานอย่างสม่ำเสมอเพื่อป้องกันจากการสูญหายของข้อมูลในกรณีต่าง ๆ เช่น ฮาร์ดดิสก์เสีย ไฟกระชากจนทำให้ฮาร์ดดิสก์พัง หรืออื่น ๆ
- ระมัดระวังและรักษาเครื่องคอมพิวเตอร์
- เมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย และห้ามปล่อยเครื่องคอมพิวเตอร์ทิ้งไว้โดยไม่มีผู้ดูแล
- ห้ามทิ้งเครื่องคอมพิวเตอร์ไว้ในรถยนต์ที่สามารถมองเห็นได้โดยผู้อื่นจากภายนอก

มาตรฐานการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and Authentication)

- ระบบสารสนเทศมีการจำกัดการเข้าถึง (Information Access Restriction) โดยอนุญาตให้เข้าถึงเฉพาะผู้ที่มีสิทธิในการเข้าถึงเท่านั้น
- จัดให้มีการลงทะเบียน (User Registration) เพื่อพิสูจน์ตัวตนของผู้ใช้งานสำหรับระบบงานสารสนเทศ ให้สอดคล้องกับ**ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)**
- ผู้ใช้งานมีบัญชีผู้ใช้งานหรือรหัสประจำตัวของผู้ใช้งานเฉพาะ และไม่ซ้ำกับคนอื่น เมื่อมีการเข้าถึงสารสนเทศในระบบจะต้องมีการพิสูจน์ตัวตนที่ปลอดภัย (Authentication) เพื่อยืนยันว่าเป็นผู้ที่ได้รับสิทธิเข้าถึงข้อมูลสารสนเทศที่แท้จริง ยกเว้นระบบที่มีการจำกัดเรื่องลิขสิทธิ์การใช้งาน
- บัญชีผู้ใช้งานหรือรหัสประจำตัวของผู้ใช้งาน ยังเป็นสิ่งที่ใช้ในการกำหนด หรืออ้างอิงถึงสิทธิ์การเข้าถึงและใช้งานสารสนเทศในระดับต่าง ๆ (Privileged Management) ผู้ใช้งานต้องจัดเก็บให้เหมาะสม หากมีการละเมิดเข้าถึงสารสนเทศหรือละเมิดการใช้งานโดยไม่ได้รับอนุญาต จะถือเป็นหลักฐานในการยืนยันไปยังผู้ถือครองบัญชีผู้ใช้งานหรือรหัสประจำตัวของผู้ใช้งานผู้นั้นได้
- กรณีที่มีความจำเป็นต้องอนุญาตให้บุคคลหลายบุคคลเข้าถึงข้อมูลโดยมีรหัสผู้ใช้งานเหมือนกันได้ ในกรณีเช่นนี้ผู้ใช้งานร่วมกันต้องรับผิดชอบต่อเหตุการณ์ที่เกิดขึ้น ให้สอดคล้องกับ**นโยบายการควบคุมการเข้าถึง (Access Control)**
- หากจะต้องมีการเลิกใช้บัญชีผู้ใช้งานและรหัสผ่าน ให้แจ้งกับหัวหน้าหน่วยงานขององค์กร โดยตรงเพื่อทำเรื่องขอเลิกใช้โดยจะต้องกระทำภายใน 7 วันก่อนที่จะเลิกใช้งานหรือทันทีที่ได้รับทราบ ให้สอดคล้องกับ**ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)**
- จัดให้มีการทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึง (Review of User Access Rights) อย่างน้อยปีละ 1 ครั้ง

มาตรฐานการจัดการและการใช้งานรหัสผ่าน (Password management)

- ผู้ดูแลระบบด้านระบบปฏิบัติการจัดให้มีระบบบริหารจัดการรหัสผ่าน (Password Management System) ที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ โดยระบบดังกล่าวต้องสามารถกำหนดการตั้งรหัสผ่านได้ตามแนวการจัดการรหัสผ่าน (Password) ซึ่งกำหนดไว้ใน **นโยบายหน้าที่และความรับผิดชอบของผู้ใช้งาน (User responsibility)** กรณีที่บางระบบไม่สามารถดำเนินการได้ตามแนวทางดังกล่าวอันเนื่องมาจากข้อจำกัดของระบบ ผู้ดูแลระบบต้องบริหารจัดการความมั่นคงปลอดภัยโดยใช้มาตรการอื่นทดแทน

มาตรฐานหน้าที่และความรับผิดชอบของผู้ใช้ (User responsibility)

รายละเอียดตามระบุในเอกสารไม่เปิดเผยความลับขององค์กร (Non-Disclosure Agreement)

มาตรฐานการใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

- จัดให้มีการทำรายการมาตรฐานซอฟต์แวร์ (Software Baseline) และติดตั้งซอฟต์แวร์ดังกล่าวตามที่กำหนดไว้เท่านั้น องค์กรไม่อนุญาตให้บุคลากรติดตั้งหรือใช้ซอฟต์แวร์ที่อยู่นอกเหนือรายการมาตรฐานซอฟต์แวร์ (Software Baseline) รวมถึงซอฟต์แวร์ประเภท Portable software บนเครื่องคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ ขององค์กร นอกจากได้รับอนุญาตจากผู้มีอำนาจแล้วเท่านั้น
- จัดให้มีการกำหนดมอบหมาย การอนุญาตให้ใช้งาน โดยอนุญาตตามความจำเป็นและพิจารณาถึงหน้าที่และความรับผิดชอบในการดำเนินงานของผู้ใช้งาน
- จัดให้มีการป้องกันการเข้าถึง Software utilities โดยผู้ที่ไม่ได้รับอนุญาต
- สำหรับซอฟต์แวร์ประเภทฟรีแวร์หรือแชร์แวร์ ที่จะทำการติดตั้ง ในระบบ เจ้าหน้าที่ตรวจสอบก่อนที่จะทำการติดตั้งว่าสามารถใช้งานได้ด้วยเงื่อนไขอะไรบ้าง และจะต้องไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น
- สำหรับการติดตั้งซอฟต์แวร์หรือซอฟต์แวร์ยูทิลิตี้ ให้ปฏิบัติตามแนวทางดังนี้ก่อนการติดตั้ง
    - ศึกษาหรือทดสอบก่อนว่าเป็นซอฟต์แวร์ที่น่าเชื่อถือหรือไม่
    - มีการประมวลผลที่ถูกต้องหรือไม่
    - มีผู้ใช้งานอยู่ในจำนวนที่มากพอหรือไม่
    - มีผู้ผลิตซอฟต์แวร์อย่างชัดเจนหรือไม่
    - มีผู้ร่วมอาชีพหรือสายงานเดียวกันด้านสารสนเทศให้การรับรองหรือไม่
    - สามารถรายงานผลหากพบข้อผิดพลาดจากการใช้งานได้หรือไม่
    - มีการใช้งานกันมาเป็นระยะเวลานานพอแล้วหรือไม่
    - และดำเนินการ **นโยบายการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls of Malicious Code and Mobile Code)**

มาตรฐานการติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เทคโนโลยีสารสนเทศขององค์กร

- จัดให้มีการทำรายการการตั้งค่าด้านความปลอดภัย (Security Baseline) สำหรับเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่มีความสำคัญไว้อย่างเป็นลายลักษณ์อักษร และทบทวนปรับปรุงเนื้อหาอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่นัยยะสำคัญ
- เมื่อมีการติดตั้งซอฟต์แวร์สำหรับเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่มีความสำคัญ ผู้รับผิดชอบพิจารณาตั้งค่าให้ตั้งค่าให้สอดคล้องตามรายการการตั้งค่าด้านความปลอดภัย (Security Baseline)

ที่กำหนดไว้ในกรณีที่มีความจำเป็นที่ไม่สามารถกำหนดค่าให้เป็นไปตามรายการการตั้งค่าด้านความปลอดภัย (Security Baseline) ได้ เช่น การกำหนดค่ามีผลกระทบการการทำงานของระบบ เป็นต้น ผู้รับผิดชอบต้องขออนุมัติเพื่อยกเว้นการกำหนดค่าดังกล่าว

- กำหนดให้มีการสุ่มตรวจสอบการตั้งค่าของเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่มีความสำคัญ เพื่อให้มีความสอดคล้องกับรายการการตั้งค่าด้านความปลอดภัย (Security Baseline) ที่กำหนดไว้ อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่นัยยะสำคัญ

มาตรฐานการใช้บริการเครือข่าย (Policy on Use of Network Services)

- กำหนดให้มีการใช้งาน Session time-out /Idle Time-out สำหรับระบบปฏิบัติการ และ/หรือ อุปกรณ์เครือข่าย หากไม่มีการใช้งานเกินกว่า 30 นาที ยกเว้นระบบคอมพิวเตอร์ที่มีการเฝ้าระวังอยู่ตลอดเวลา
- Session ใด ๆ ที่ไม่มีการทำงานในระยะเวลาหนึ่ง (Idle) จะถูกยกเลิกการทำงานของ Session นั้น ๆ
- ระยะเวลา Session Time-out /Idle Time-out ที่กำหนดขึ้น สามารถสะท้อนความเสี่ยงในเรื่องของความปลอดภัยของบริเวณพื้นที่ทำงาน การจัดหมวดหมู่ของข้อมูลสารสนเทศที่มีการจัดการและแอปพลิเคชันที่มีการใช้งาน และความเสี่ยงที่เกี่ยวข้อง

มาตรฐานการใช้บริการเครือข่ายจากระยะไกล (User Authentication for External Connections)

- กำหนดให้มีการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้บริการได้และบริการใดที่ไม่อนุญาตให้ผู้ใช้งานสามารถใช้บริการได้
- จัดให้มีการขออนุญาตเข้าใช้งานบริการเครือข่ายก่อนเข้าใช้งาน เพื่อที่จะกำหนดว่าบุคคลใดสามารถเข้าถึงระบบหรือเครือข่ายใด ให้สอดคล้องตาม**ระเบียบปฏิบัติงานการบริหารจัดการการเชื่อมต่อเครือข่ายและงานบริการเครือข่าย (Network Security Control)**
- กำหนดมาตรการควบคุม กำหนดช่องทางและเงื่อนไขในการเชื่อมต่อเพื่อเข้าใช้งานที่มีความมั่นคงปลอดภัย ก่อนเปิดให้บริการใช้งานระบบจากระยะไกลทั้งแบบ Mobile computing and communication และ Teleworking โดยพิจารณาถึงภัยคุกคาม ช่อง โหว่ และความเสี่ยง
- จัดให้มีมาตรการควบคุมและพิสูจน์ตัวตนก่อนที่อนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กร เข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กร ได้จากอุปกรณ์หรือสถานที่ที่ได้อนุญาตแล้ว
- ในการปฏิบัติงาน ผู้ใช้หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์ของผู้อื่นในการเข้าสู่บริการทั้งแบบ Mobile Computing and Communication และ Teleworking
- ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการใช้งานให้เป็นไปตาม**นโยบายการควบคุมการเข้าถึง (Access Control)**

- มีมาตรการป้องกันโปรแกรมไม่ประสงค์ดีให้กับอุปกรณ์เคลื่อนที่ รวมถึงมีมาตรการจัดการปรับปรุงให้มีประสิทธิภาพในการป้องกันและตรวจจับสิ่งผิดปกติ
- กำหนดมาตรการสำรองข้อมูลของอุปกรณ์สำคัญอย่างสม่ำเสมอ รวมถึงการทดสอบกู้คืนเพื่อให้แน่ใจได้ว่าระบบสำรองข้อมูลมีความพร้อมใช้งาน
- จัดให้มีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) และมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ตาม**ระเบียบปฏิบัติงานการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ**
- การทบทวน ปรับปรุง สิทธิในการเข้าถึงเครือข่ายของผู้ใช้งานตามความจำเป็น**นโยบายการควบคุมการเข้าถึง (Access control)**

มาตรฐานสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

- อุปกรณ์คอมพิวเตอร์แบบพกพาที่องค์กรจัดให้ต้องได้รับการขึ้นทะเบียนขอใช้งานตาม **ระเบียบปฏิบัติงานการใช้งานอุปกรณ์คอมพิวเตอร์พกพา (Mobile Device Security)** สำหรับบุคลากรที่ได้รับอนุมัติ
- อุปกรณ์คอมพิวเตอร์แบบพกพาที่องค์กรจัดให้ต้องได้รับการควบคุมด้านความมั่นคงปลอดภัยตามข้อกำหนดของเอกสาร **Term of use mobile device** อย่างน้อยดังต่อไปนี้
    - ติดตั้ง Application จาก Application Store ที่กำหนดในหัวข้อ “Application Store List”
    - Cloud Based Service ที่อนุญาตให้ใช้กำหนดในหัวข้อ “Cloud-based Service List” โดยต้องได้รับการควบคุมดังนี้
        - ห้ามนำเข้า หรือเผยแพร่ข้อมูลสำคัญขององค์กรที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ เช่น ข้อมูลรหัสผ่าน หรือ ค่าข้อมูลของระบบ (Configuration) เป็นต้น
        - หากมีความจำเป็นต้องใช้งาน Cloud based service เพิ่มเติมบุคลากรต้องแจ้งทีมงาน IT Support เพื่อตรวจสอบ และขออนุมัติก่อนการใช้งานทุกครั้ง
    - ห้ามปรับเปลี่ยน แก้ไขการตั้งค่าระบบของอุปกรณ์คอมพิวเตอร์แบบพกพานอกเหนือจากที่ที่กำหนดในหัวข้อ “Mobile Device Standard Change” หากต้องการปรับเปลี่ยนให้ปฏิบัติตาม นโยบายการบริหารจัดการความเปลี่ยนแปลง (Change Management)
    - ติดตั้ง Application ต้องได้รับการควบคุม ดังต่อไปนี้
        - ห้ามติดตั้ง Application ใดๆ ที่สามารถเข้าถึงระบบบริหารจัดการบริการภายในขององค์กร เช่น VPN, Remote Administrator เป็นต้น
        - ห้ามติดตั้ง Application ใดๆ ที่สุ่มเสี่ยงกับการกระทำผิดกฎหมาย และผิดลิขสิทธิ์

- ห้ามติดตั้ง Application ใดๆ ที่โปรแกรมป้องกันไวรัสในอุปกรณ์คอมพิวเตอร์แบบพกพาตรวจจับว่ามีความเสี่ยงด้านความมั่นคงปลอดภัย

หากมีความจำเป็นต้องติดตั้ง Application ดังกล่าวข้างต้น บุคลากรต้องแจ้งทีมงาน IT Support เพื่อตรวจสอบทดสอบ และขออนุมัติก่อนการติดตั้งทุกครั้ง

- ดำเนินการติดตั้งระบบปฏิบัติการ และปรับปรุงเวอร์ชันล่าสุดเมื่อได้รับการแจ้งจากทีม IT Support
- ห้าม Jailbreak หรือ root อุปกรณ์คอมพิวเตอร์แบบพกพา
- ดำเนินการเข้ารหัสข้อมูลสำคัญในอุปกรณ์คอมพิวเตอร์แบบพกพา โดยปฏิบัติตามนโยบายการเข้ารหัส (Cryptographic) และการจัดการกุญแจ (Key Management) หากมีการติดตั้ง Application เพิ่มเติมให้ดำเนินการขออนุมัติจากคณะทำงาน IT Security และเข้าสู่กระบวนการตรวจสอบ/ทดสอบจากทีม IT Support ก่อนการติดตั้ง นอกจากนี้บุคลากรสามารถเลือกการเข้ารหัสทั้งเครื่องได้ตามความเหมาะสม
- กำหนดให้ตั้งค่า Lock screen ด้วยรหัสที่เดาสุ่มได้ยาก ความยาวอย่างน้อย 8 ตัวอักษร หรือใช้วิธีการยืนยันตัวตนก่อนใช้งานเครื่องที่ดีกว่า เช่น Password หรือ Fingerprint เป็นต้น
- กำหนดให้ตั้งค่า Automatically Lock Screen Timeout เป็น 3 หรือ 5 นาที
- ตั้งค่า Remote Wipe ที่องค์กรกำหนดให้เท่านั้น และในกรณีที่อุปกรณ์คอมพิวเตอร์แบบพกพาสูญหายให้เร่งดำเนินการแจ้งทีม IT Support เพื่อดำเนินการ Remote Wipe อุปกรณ์ดังกล่าว

- อุปกรณ์คอมพิวเตอร์แบบพกพาส่วนตัวต้องเชื่อมต่อกับส่วนเครือข่ายอินเทอร์เน็ตไร้สายเพื่อเชื่อมต่อเข้าสู่เครือข่ายสาธารณะที่องค์กรกำหนดให้เท่านั้น ไม่อนุญาตให้เชื่อมต่อกับเครือข่ายภายในขององค์กร
- บุคลากรต้องปฏิบัติตาม**นโยบายการควบคุมการเข้าถึง (Access Control)** อย่างเคร่งครัด

มาตรฐานสำหรับการใช้งานเครือข่ายไร้สาย (Wireless Access Policy)

- ผู้ดูแลระบบเครือข่ายไร้สายต้องจัดแบ่งเครือข่ายไร้สายตามรูปแบบการใช้งานเครือข่ายตามความต้องการขององค์กร
- สำหรับการให้บริการเครือข่ายไร้สายเพื่อเชื่อมต่อเข้าสู่บริการภายในขององค์กร ผู้ดูแลระบบเครือข่ายไร้สายต้องจัดเตรียมระบบการยืนยันตัวตนผู้ใช้งานก่อนเข้าใช้งานระบบเครือข่ายไร้สาย และต้องปรับปรุงระบบให้มีการเข้ารหัสการเชื่อมต่อในรูปแบบ WPA2-PSK เป็นอย่างน้อย
- สำหรับการให้บริการเครือข่ายไร้สายเพื่อเชื่อมต่อเข้าสู่เครือข่ายสาธารณะ ผู้ดูแลระบบเครือข่ายไร้สายต้องจัดเตรียมระบบการยืนยันตัวตนผู้ใช้งานก่อนเข้าใช้งานระบบเครือข่ายไร้สาย
- กำหนดให้มีการแบ่งแยก และควบคุมเครือข่ายไร้สายกับเครือข่าย LAN ด้วยอุปกรณ์ Firewall เพื่อควบคุมการเข้าถึงที่เหมาะสม
- ห้ามบุคลากรนำ Access Point ส่วนตัวมาเชื่อมต่อเครือข่าย LAN เพื่อกระจายสัญญาณ
- ห้ามบุคลากรปลอม SSID (Rouge SSID) ซ้ำกับ SSID ที่องค์กรกำหนด
- ต้องใช้การเชื่อมต่อที่มีการเข้ารหัสสำหรับการใช้บริการที่มีการรับส่งข้อมูลระดับชั้นลับ เช่น HTTPS หรือ SSH เป็นต้น

มาตรฐานการควบคุมการเข้าถึง (Access Control)

- ต้องมีกระบวนการลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User Registration and De-registration) อย่างเป็นทางการและปฏิบัติตามเพื่อเป็นการให้สิทธิการเข้าถึง
- กำหนดให้มีการแยกหน้าที่และความรับผิดชอบ (Segregation of Duties) ของผู้เกี่ยวข้องในระบบงานต่างๆ เพื่อป้องกันไม่ให้ผู้ใดสามารถเข้าถึงระบบงานทั้งหมด และสามารถเปลี่ยนแปลงแก้ไข หรือดำเนินการใดๆ โดยพลการปราศจากการอนุญาต/รับรู้ โดยบุคคลหรือระบบการตรวจสอบ
- ให้มีการจัดทำ**ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)** อย่างเป็นลายลักษณ์อักษร และปรับปรุงเนื้อหาตามรอบระยะเวลาที่กำหนดไว้
- กำหนดการเข้าถึงระบบสารสนเทศหลักและสนับสนุนประมวลผลด้านกระบวนการทางธุรกิจ ทั้งทางลอจิคัล (Logical Access) และทางกายภาพ (Physical Access) ได้แก่ พื้นที่ปฏิบัติงานขององค์กร ให้ปฏิบัติตามนโยบาย อย่างมีประสิทธิภาพ ตาม **นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security)** เพื่อควบคุมการเข้าถึงหรือวิธีการเข้าถึงสารสนเทศตามสิทธิของผู้ใช้งาน หรือ กลุ่มผู้ใช้งานอย่างชัดเจน
- ให้ใช้เครื่องคอมพิวเตอร์ หรือ Mobile Device หรืออุปกรณ์ประกอบอื่นที่เชื่อมต่อเข้ากับระบบปฏิบัติการระบบงานระบบเครือข่ายขององค์กร โดยต้องปฏิบัติตาม**นโยบายการใช้บริการเครือข่ายจากระยะไกล (User Authentication for External Connections)** และ **นโยบายการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls of Malicious Code and Mobile Code)**
- การเข้าใช้งานระบบงานต่างๆ จะต้องได้รับอนุญาตจากเจ้าของระบบ โดยให้หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน เป็นผู้ขอสิทธิ์ในการใช้ เพื่อให้มีการระบุและพิสูจน์ตัวตนของผู้ใช้งานตาม**นโยบายการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)**
- ควรกำหนดคุณสมบัติหรือวิธีการล็อกอินเข้าใช้ระบบให้มีความปลอดภัย (Secure Log-on) เมื่อมีระบบใหม่ที่ได้รับการอนุมัติให้จัดหาและติดตั้ง พิจารณากำหนดคุณสมบัติ ได้แก่
    - การไม่แสดงชื่อหรือรายละเอียดของระบบจนกว่าจะล็อกอินสำเร็จ
    - การไม่มีหรือไม่แสดงฟังก์ชันให้การช่วยเหลือ (Help menu) ในระหว่างที่ทำการล็อกอิน
    - การบันทึกข้อมูลความสำเร็จหรือการล้มเหลวในการล็อกอินแต่ละครั้งของผู้ใช้งาน (เพื่อใช้ในการตรวจสอบในภายหลัง)
    - การไม่แสดงข้อมูลรหัสผ่านให้เห็นบนจอในขณะที่ผู้ใช้งานใส่ข้อมูลรหัสผ่านของตน
    - การแสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบนี้เป็นทรัพย์สินของ Predictive และอนุญาตให้เฉพาะบุคคลที่มีสิทธิในการเข้าถึงเท่านั้น Predictive มีสิทธิในการตรวจสอบและบันทึกข้อมูลทุกกิจกรรมที่เกิดขึ้นในระบบเพื่อให้เป็นไปตามกฎหมายและวัตถุประสงค์อื่น ๆ การเข้าถึงหรือพยายามเข้าถึง โดยบุคคลที่ไม่มีสิทธิ ถือว่ามีความผิดตามกฎหมาย”หรือ “This system is the property of Predictive and can be accessed only by authorized users. Predictive is entitled to monitor and record any activity or communication on the system

for law enforcement and other purposes. Unauthorized or Intruder must be subject to criminal prosecution.”

- การแสดงผลข้อผิดพลาดเท่าที่จำเป็น รายละเอียดข้อมูลอื่นๆ ของระบบต้องไม่แสดงออกมา

- การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services) ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น
- ผู้ใช้งาน ที่จะเข้าถึงระบบที่สำคัญผ่าน Application หรือ Software ในการบริหารจัดการต่างๆ หรือเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ จากทั้งเครือข่ายสาธารณะ (Public Network) หรือเครือข่ายส่วนตัว (Private Network) ต้องปฏิบัติตามระเบียบปฏิบัติงานการควบคุมการเข้าถึง (Access Control)
- ต้องมีการทบทวน นโยบายการควบคุมการเข้าถึง (Access Control) ตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรฐานการอนุญาตให้ใช้ทรัพย์สินขององค์กร (Acceptable Use Policy)

- บุคลากรสามารถใช้งานทรัพย์สิน (Asset) ขององค์กร เพื่อสนับสนุนการปฏิบัติงานตามหน้าที่และความรับผิดชอบที่เกี่ยวข้องตามภารกิจ โดยมีหน้าที่และความรับผิดชอบตามที่กำหนดใน**นโยบายหน้าที่และความรับผิดชอบของผู้ใช้งาน (User responsibility)**
- จัดให้บุคลากรลงนามในข้อตกลงในการใช้งานทรัพย์สินขององค์กร ใน**เอกสารแบบฟอร์ม Acceptable Use Policy (AUP)** และลงนามรักษาความลับขององค์กร **เอกสารแบบฟอร์มไม่เปิดเผยความลับขององค์กร (Non-Disclosure Agreement)**
- การใช้งานต้องสอดคล้องกับนโยบายขององค์กร รวมถึง กฎระเบียบ และกฎหมายที่เกี่ยวข้อง
- ไม่อนุญาตให้ใช้ทรัพย์สินขององค์กร ในกิจกรรมที่มีแนวโน้มที่จะขัดต่อกฎหมาย ระเบียบ ข้อตกลงกับลูกค้า หรือองค์กรภายนอก
- ไม่อนุญาตให้ใช้ทรัพย์สินขององค์กร ในการทำธุรกิจส่วนตัว
- การใช้งานทรัพย์สินต่าง ๆ ขององค์กร ให้เป็นไปตามลักษณะการใช้งานที่ถูกต้องเหมาะสม ตามชนิด ประเภท และคุณสมบัติที่ผู้ผลิตกำหนด
- การดัดแปลง แก้ไข หรือกระทำการใด ๆ ที่เบี่ยงเบนไปจากสภาพปกติซึ่งเสี่ยงต่อการใช้งานจะต้องได้รับ อนุญาตจากผู้มีอำนาจ
    - หากพบเหตุการณ์การละเมิดนโยบายทางด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศขององค์กร ผู้ใช้งานดำเนินการแจ้งเหตุตาม**นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Management)** และดำเนินการแก้ไขป้องกันที่เหมาะสม

มาตรฐานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)

- กำหนดให้มีการจัดทำ**ระเบียบปฏิบัติงานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- กำหนดให้มีการจัดระดับชั้นความลับของข้อมูล (Information Classification) หมายรวมถึงการสร้างความมั่นคงปลอดภัยให้แก่ข้อมูลซึ่งอยู่ในเอกสารระบบ (Security of System Documentation) เพื่อกำหนดมาตรการควบคุมที่เหมาะสม โดยระบุบุคลากรที่มีหน้าที่ดูแลรับผิดชอบ ผู้มีสิทธิ์หรืออำนาจในการอนุมัติ
- กำหนดให้มีการจัดทำป้าย (Labeling) หรือระบุสารสนเทศแต่ละระดับอย่างชัดเจน โดยติดป้ายหรือระบุคำอธิบายที่มีความสัมพันธ์กับระดับชั้นความลับของข้อมูลสารสนเทศ
- การเก็บรักษา (Storage) จัดเก็บสารสนเทศไว้ในสถานที่ หรือบันทึกข้อมูลลงในเครื่องคอมพิวเตอร์ที่ปลอดภัยป้องกันภัยคุกคามต่อข้อมูลตามระดับชั้นความลับของข้อมูลสารสนเทศ รวมถึงบริหารจัดการหรือการกำหนดการเข้าถึงสารสนเทศอย่างเหมาะสม ตาม**ระเบียบปฏิบัติงานการ การจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- กำหนดแนวทางการจัดการสารสนเทศ (Handling) โดยคำนึงถึงความปลอดภัย และป้องกันภัยคุกคามที่ส่งผลกระทบต่อการเข้าถึง หรือความเสียหายของสารสนเทศ
- การทำลายสารสนเทศ (Disposal) กำหนดผู้อนุมัติให้ทำลายสารสนเทศ และวิธีการทำลายสารสนเทศตามระดับชั้นความลับของข้อมูล ตาม**นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- ไม่อนุญาตให้ดำเนินการสำเนาข้อมูลของลูกค้าจากบนระบบทดสอบ (POC) มายังระบบใช้งานจริง หรือ จากระบบใช้งานจริงมายังบนระบบทดสอบ (POC) ยกเว้นกรณีที่เจ้าของข้อมูลร้องขอและมีการยืนยันอย่างเป็นลายลักษณ์อักษร

มาตรฐานการป้องกันการใช้งานผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)

- ไม่อนุญาตให้มีการเปลี่ยนแปลงแก้ไข Software package (Restrictions on changes to software packages) ที่มาจากผู้ผลิตเนื่องจากมีความเสี่ยงต่อการใช้งาน
- การเปลี่ยนแปลงแก้ไข ต้องคำนึงถึงเงื่อนไขการรับประกันกฎหมายที่เกี่ยวข้อง และประเด็นที่มีผลกระทบอื่น ๆ อย่างรอบคอบ
- หากพบว่ามีการใช้งานที่ละเมิด**นโยบายทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร** จะต้องมีการรายงานตาม**นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Management)** หรือดำเนินการสอบสวนตามกระบวนการขององค์กร (Disciplinary process)

มาตรฐานการควบคุมสื่อบันทึกข้อมูลและการทำลาย (Media Handling and Disposal)

- การจัดการ ควบคุมป้องกันการเข้าถึงสื่อบันทึกข้อมูลและการทำลาย (Media Handling and Disposal) ให้ดำเนินการตามระดับชั้นของข้อมูลที่อยู่ในสื่อบันทึก สอดคล้องตาม**ระเบียบปฏิบัติการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ**

มาตรฐานการอนุมัติการจัดซื้อจัดจ้างทรัพยากรด้านสารสนเทศ (Authorization Process for Information Processing Facilities)

- การอนุมัติการจัดซื้อจัดจ้างทรัพยากรด้านสารสนเทศ (Authorization Process for Information Processing Facilities) ต้องมีการขออนุมัติจากผู้มีอำนาจก่อนการจัดซื้อจัดจ้างก่อนดำเนินการ ตามการจัดซื้อจัดจ้างขององค์กร
- กรณีนำอุปกรณ์หรือระบบเทคโนโลยีสารสนเทศใหม่เข้าสู่การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องมีการประเมินความเสี่ยง ตาม**นโยบายบริหารจัดการความเสี่ยง (Risk Management Policy)**

มาตรฐานการวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity Management and System Acceptance)

- ให้มีการวางแผนเพื่อเฝ้าระวังการใช้งานทรัพยากรสารสนเทศ และแนวโน้มการใช้งานให้เพียงพอและประสิทธิภาพที่เหมาะสมต่อการดำเนินการ ตาม**ระเบียบปฏิบัติงานการวางแผนความต้องการทรัพยากรสารสนเทศ**

มาตรฐานการบริหารจัดการโครงการ (Project Management)

- ผู้รับผิดชอบ ก่อนการจัดตั้งโครงการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบประเมินความเสี่ยงของโครงการที่มีผลกระทบต่อระบบ ISMS ตาม**นโยบายบริหารจัดการความเสี่ยง (Risk Management Policy)** รวมทั้งมีการบริหารจัดการความเสี่ยงที่เกิดขึ้น
- ผู้รับผิดชอบ ควรพิจารณาเลือกแนวตามหลักการวิศวกรรมระบบที่น่าเชื่อถือและมีความมั่นคงปลอดภัย ตาม**เอกสารแนวทาง Principles for Engineering Secure Systems** ในหัวข้อ**นโยบายการรักษาความมั่นคงปลอดภัยในการพัฒนาระบบงาน (Information Systems Acquisition, Development and Maintenance Policy)** มาเป็นแนวทางในการดำเนินการประยุกต์เข้ากับโครงการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ หากการดำเนินการโครงการดังกล่าวจะมีการจ้างผู้ให้บริการภายนอกเข้ามาดำเนินการให้แจ้ง ผู้ดำเนินงานโครงการปฏิบัติตาม **เอกสารแนวทาง Principles for Engineering Secure Systems** ด้วย

หมายเหตุ : โครงการ/บริการ หมายความถึง ระบบงาน/งานเครือข่าย ซึ่งจะเป็นเครื่องมือที่จะช่วยให้หน่วยงานสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ หรือบริการที่ต้องการพัฒนาขึ้นใหม่ โดยผ่านขบวนการศึกษาความเป็นไปได้ (Project Feasibility Study) เรียบร้อยแล้ว

มาตรฐานการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls of Malicious Code and Mobile Code)

- จัดให้มีการกำหนดมาตรการสำหรับตรวจจับและป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี และมาตรการควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ ให้เป็นไปตามรายการของซอฟต์แวร์ประเภทแอปพลิเคชัน (Software Application) ที่องค์กร กำหนดขึ้น
- จัดให้มีการติดตั้งโปรแกรมป้องกันไวรัส และซอฟต์แวร์ไม่ประสงค์ดี สำหรับเครื่องคอมพิวเตอร์ที่เกี่ยวข้องตามรายการของ Software Baseline ที่องค์กร กำหนดขึ้น และดำเนินการตาม **ระเบียบปฏิบัติงานการควบคุมซอฟต์แวร์ที่ไม่ประสงค์ดี (Control of Malicious Code and Mobile Code)**

มาตรฐานการบริหารจัดการความเปลี่ยนแปลง (Change Management)

- จัดให้มีการขออนุมัติใช้งาน ติดตั้ง ปรับปรุง หรือแก้ไข งานบริการประมวลผลสารสนเทศ โดยให้หน่วยงานที่รับผิดชอบในการดำเนินการเปลี่ยนแปลงทำการประเมินผลกระทบที่จะเกิดขึ้นรวมทั้งผล กระทบด้านความปลอดภัยจากการเปลี่ยนแปลง รวมทั้งจัดทำแผนถอยหลังกลับ (Roll Back Plan) ก่อนที่จะมีการขออนุมัติจากผู้ที่มีอำนาจหรือระดับผู้บริหารที่รับผิดชอบในเรื่องดังกล่าว
- กำหนดให้มีการจัดทำ**ระเบียบปฏิบัติงานการบริหารจัดการเปลี่ยนแปลง (Change Management)**

มาตรฐานการสำรองข้อมูล (Backup Management)

- จัดให้มีการสำรองให้ครบถ้วนพร้อมใช้งานได้อย่างต่อเนื่องตาม**ระเบียบปฏิบัติงานการสำรองข้อมูล** รวมถึงมีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่และทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ เพื่อให้ข้อมูลที่สำรองมีความพร้อมใช้เมื่อต้องการนำมาใช้งาน

มาตรฐานการจัดการความมั่นคงปลอดภัยสำหรับเครือข่าย (Network Security Management)

- การบริหารจัดการสิทธิการเข้าใช้งานระบบเครือข่ายขององค์กรต้องปฏิบัติตาม **ระเบียบปฏิบัติงานการบริหารจัดการการเชื่อมต่อเครือข่ายและงานบริการเครือข่าย (Network Security Control)** และการทบทวนสิทธิการเข้าถึงตาม **ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน(User Access Management)**
- มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการ สำหรับบริการเครือข่าย รวมถึงการกำหนดระดับการให้บริการเครือข่ายภายในขององค์กร หรือบริการที่ได้รับจากผู้ให้บริการภายนอก ตาม**นโยบายการควบคุมผู้ให้บริการจากภายนอก (Supplier Management)**
- จัดให้มีการแยกสภาพแวดล้อมสำหรับระบบสำคัญ (Sensitive system isolation) โดยทำการแยกออกจากระบบอื่น (Segregation in Networks)
- การเชื่อมต่อเครือข่ายจากระยะไกล (Teleworking) ผู้ใช้งานจากระยะไกล (Remote User) หรือจากการเชื่อมต่อผ่านอุปกรณ์ Mobile Device ที่ทำการเชื่อมต่อเครือข่ายจะมีการระบุตัวตนหรือยืนยันตัวตน (Authentication) ผ่านกลไกของ VPN (Virtual Private Network)เพื่อเข้าถึงเครือข่ายขององค์กร
- ต้องมีการบันทึกกิจกรรมและการเฝ้าระวังเหตุการณ์ผิดปกติต่าง ๆ ของการใช้งานระบบเครือข่าย ตาม**นโยบายการจัดเก็บ เฝ้าระวัง ตรวจสอบการวิเคราะห์และจัดการกับข้อมูลล็อก (Log Monitoring and Management) การเทียบเวลาระบบคอมพิวเตอร์ (Clock Synchronization)**
- ต้องมีการทบทวน Firewall Policy 3 เดือนครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลง

มาตรฐานการบริหารจัดการแลกเปลี่ยนข้อมูล (Information Exchange Management)

- ก่อนการแลกเปลี่ยนสารสนเทศระหว่างองค์กร ต้องมีการประเมินความเสี่ยงที่เกี่ยวข้องในการดำเนินการแลกเปลี่ยนสารสนเทศนั้น
- เมื่อมีการแลกเปลี่ยนสารสนเทศระหว่างองค์กร ต้องผ่านการอนุมัติผู้บริหารระดับสูง หรือผู้บริหารตามระดับชั้น (ระดับการอนุมัติขึ้นอยู่กับระดับความสำคัญของข้อมูลที่ต้องการแลกเปลี่ยน) อย่างเป็นลายลักษณ์อักษร และลงนามในข้อตกลงระหว่างกันในการที่จะไม่เปิดเผยความลับขององค์กร (Non-Disclosure Agreement) ระหว่างองค์กรสำหรับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)
- มีการกำหนดช่องทางการแลกเปลี่ยนสารสนเทศหรือสื่อบันทึกข้อมูลสารสนเทศระหว่างองค์กร กับหน่วยงานภายนอกด้วยวิธีการที่มีความมั่นคงปลอดภัยและสอดคล้องกับการจัดการระดับชั้นข้อมูล
- กำหนดให้มีการจัดทำ**เอกสารไม่เปิดเผยความลับขององค์กร (Non-Disclosure Agreement)** เพื่อใช้ในการลงนามสำหรับข้อตกลงการไม่เปิดเผยความลับขององค์กร

มาตรฐานการควบคุมการสื่อสาร Electronic Messaging (Control of electronic messaging)

- ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ การสนทนา หรือการติดต่อสื่อสาร ใด ๆ ให้ถือเสมือนเป็นการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรืออีเมล์ขององค์กร
- ต้องใช้งานอีเมล์แอดเดรสขององค์กร (@Predictive.co.th) เพื่อการติดต่อหรือใช้เพื่อการปฏิบัติงานตามความรับผิดชอบของตนเองที่ได้รับมอบหมายเท่านั้น ห้ามมิให้ใช้อีเมล์ขององค์กร เพื่อหาผลประโยชน์ส่วนตน
- ห้ามใช้อีเมล์แอดเดรสอื่น ๆ เพื่อติดต่อธุรกิจหรืองานขององค์กร โดยไม่ได้รับอนุญาต
- ใช้ความระมัดระวังและตรวจสอบอีเมล์แอดเดรสของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งข้อมูลสำคัญผิดตัวผู้รับและทำให้ข้อมูลเกิดการรั่วไหล
- ควรระบุชื่อของผู้ส่ง ตำแหน่ง และข้อมูลติดต่อกลับไว้ในอีเมล์ทุกฉบับที่ส่งไปเพื่อเป็นข้อมูลในการติดต่อกลับ
- จำกัดการส่งหรือส่งต่อข้อมูลทางอีเมล์ไปยังผู้รับหรือกลุ่มผู้รับอีเมล์เท่าที่มีความจำเป็นต้องรับทราบข้อมูลในอีเมล์นั้นเท่านั้น
- ใช้คำที่สุภาพในการส่งอีเมล์ ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อองค์กร หรือบุคคลอื่น ๆ
- ควรสำรองข้อมูลอีเมล์ตามความจำเป็นอย่างสม่ำเสมอ
- ห้ามเข้าถึงข้อมูลอีเมล์ของผู้อื่นโดยไม่ได้รับอนุญาต
- ห้ามรับหรือส่งอีเมล์แทนผู้อื่นโดยไม่ได้รับอนุญาต
- ห้ามลงทะเบียนด้วยอีเมล์แอดเดรสขององค์กรไว้ตามที่อยู่เว็บไซต์ต่างๆ ที่ไม่มีความเกี่ยวข้องกับภารกิจงานของตนเอง
- ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) หรือที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter) หรือที่มีลักษณะเป็นการละเมิดต่อกฎหมาย ทรัพย์สินทางปัญญา หรือสิทธิของบุคคลอื่น หรือที่มีโปรแกรมไม่ประสงค์ดีไปให้กับผู้อื่นโดยเจตนาห้ามปลอมแปลงหรือสวมรอยใช้อีเมล์ของผู้อื่น

มาตรฐานสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly Available Information)

- ตรวจสอบความถูกต้องและความเหมาะสมของซอฟต์แวร์, ข้อมูล, และข้อมูลสารสนเทศอื่น ๆ ที่จะเผยแพร่ออกสู่สาธารณะหรือก่อนนำเผยแพร่ผ่านเว็บต่าง ๆ
- จัดให้มีมาตรการควบคุมดูแลความมั่นคงปลอดภัยของบริการข้อมูลสาธารณะที่ให้บริการ ตาม**ระเบียบปฏิบัติงานการบริหารจัดการเว็บไซต์**
- การเผยแพร่ข้อมูลต้องผ่านการทบทวน ตรวจสอบ และอนุมัติ โดยหัวหน้าหน่วยงานต้นสังกัดขึ้นไปก่อนดำเนินการ หากเอกสารมีชั้นความลับ “ระดับเปิดเผยได้ (Public)” สามารถเผยแพร่ออกสู่สาธารณะได้ทันที
- หลังจากนำข้อมูลขึ้นเผยแพร่แล้ว ให้เฝ้าระวังหน้าเว็บไซต์ดังกล่าวอย่างสม่ำเสมอ เพื่อดูว่ามีการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตเกิดขึ้นหรือไม่

มาตรฐานการติดต่อกับหน่วยงานอื่นและกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with Authorities and Special Interested Groups)

- จัดให้มีรายชื่อและข้อมูลที่เพียงพอสำหรับติดต่อกับหน่วยงานภายนอกที่เกี่ยวข้องกับการดำเนินธุรกิจขององค์กร ใน**เอกสารรายชื่อหน่วยงานอื่นและกลุ่มที่มีความสนใจเป็นพิเศษ** การรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงหน่วยงานที่เกี่ยวข้องกับกฎหมาย กฎระเบียบ และมีการทบทวน และปรับปรุงรายชื่อดังกล่าว อย่างน้อยปีละ 1 ครั้ง
- กำหนดลักษณะของเหตุการณ์ที่เข้าข่ายต้องแจ้งไปยังหน่วยงานภายนอก

มาตรฐานการควบคุมช่องโหว่ทางเทคนิค (Control of Technical Vulnerabilities)

- มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว
- มีการดำเนินการตรวจสอบช่องโหว่ทางเทคนิค เพื่อค้นหาช่องโหว่ใหม่ ๆ ที่เกิดขึ้น อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และดำเนินการตาม **ระเบียบปฏิบัติงานการควบคุมช่องโหว่ทางเทคนิค (Control of Technical Vulnerabilities)**
- ในการดำเนินการตามมาตรการปิดช่องโหว่ จะต้องแน่ใจว่ามาตรการดังกล่าวมีความน่าเชื่อถือเพียงพอ ผ่านกระบวนการจัดการเปลี่ยนแปลง สอดคล้องตาม**นโยบายการบริหารจัดการความเปลี่ยนแปลง (Change management)**
- มีการปรับปรุง Patch อย่างสม่ำเสมอ ทั้งแบบ Manual และ Automatic update เพื่อป้องกันช่องโหว่ของระบบ
- เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินขององค์กร ผู้ใช้งานมีหน้าที่รักษาให้สามารถใช้งานได้ ทั้งนี้รวมไปถึงการ อัพเดท ระบบปฏิบัติการและ โปรแกรมป้องกัน ไวรัส หรือชุดคำสั่งไม่พึงประสงค์
- การดำเนินการใด ๆ ที่มีผลกระทบต่อการทำงานหรือให้บริการให้ดำเนินการตามนโยบายการบริหารจัดการความเปลี่ยนแปลง (Change management) และ**นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information security incident management)** ให้มีการตรวจสอบช่องโหว่ทางเทคนิคหลังจากการดำเนินการดังกล่าวเสร็จสิ้นทุกครั้ง

มาตรฐานการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Management)

- ผู้ใช้งาน และรวมถึงผู้ที่เข้าถึงพื้นที่หรือระบบงาน (ยกตัวอย่างเช่น ผู้ใช้บริการ, ผู้ให้บริการภายนอก, บุคลากรองค์กร) จะต้องมีความระมัดระวังและมีความรับผิดชอบจากการทำงาน โดยมีหน้าที่ในการรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัยของสารสนเทศทันทีทันใดที่พบเห็นเหตุการณ์
- จัดให้มีระเบียบปฏิบัติงานในการรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Management) ซึ่งครอบคลุมถึงการตอบสนองและการยกระดับของปัญหาอย่างเหมาะสม
- จัดให้มีการเก็บหลักฐาน (Collection of Evidence) และเรียนรู้เหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศที่เกิดขึ้น (Learning from Security Incidents) เพื่อเตรียมการป้องกันที่จำเป็นในอนาคตต่อไป

มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ (Business continuity management)

- กำหนดให้มีการบริหารความต่อเนื่องทางธุรกิจ เมื่อเกิดภัยพิบัติหรือการล้มเหลวของระบบสารสนเทศก่อให้เกิดผลกระทบรุนแรงต่อการให้บริการซึ่งครอบคลุมถึงประเด็นด้านความมั่นคงปลอดภัยของสารสนเทศที่เกี่ยวข้อง
- กำหนดให้มีการระบุกระบวนการที่มีความสำคัญ (Critical Business Process)
- ระบุเหตุการณ์ที่อาจเป็นเหตุให้กระบวนการธุรกิจหยุดชะงักหรือติดขัด (Business Process Interruptions) พร้อมทั้งประเมินโอกาสเกิดและผลกระทบ
- ทำการประเมินความเสี่ยง (Business Continuity Risk Assessment)
- เมื่อประเมินความเสี่ยงและพบว่าระบบสารสนเทศหรือระบบโครงสร้างพื้นฐานที่มีความสำคัญ ผู้บริหารต้องพิจารณาในการเลือกมาตรการในจัดทำระบบสำรองที่สามารถใช้งานได้ทันที (Redundancy) เพื่อให้ระบบมีความต่อเนื่องทางธุรกิจได้
- จัดทำแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ภัยพิบัติ หรือระบบสารสนเทศล้มเหลว ซึ่งก่อให้เกิดผลกระทบรุนแรง แผนดังกล่าวสามารถทำให้บริการสามารถดำเนินการต่อไปได้
- แผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) อย่างน้อยต้องกำหนดรายละเอียดที่สำคัญดังนี้
    - เงื่อนไขในการเรียกใช้แผน BCP (Activating)
    - ขั้นตอนการปฏิบัติเมื่อเกิดเหตุฉุกเฉิน (Emergency Procedure)
    - กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการสนับสนุนปฏิบัติการตามแผน BCP

- กำหนดให้มีการทดสอบแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และปรับปรุงให้ทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง
- กำหนดให้มีการทดสอบแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และปรับปรุงให้ทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง หรือ ทดสอบแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เมื่อองค์กรมีการเปลี่ยนแปลงที่สำคัญที่มีผลกระทบกับ กระบวนการทดสอบ ขั้นตอนการทดสอบ หรือสภาพแวดล้อมการปฏิบัติงานเปลี่ยนแปลง (ตัวอย่างเช่น Infrastructure, Technology, Re-organization, เปลี่ยนสถานที่ตั้งของศูนย์คอมพิวเตอร์หรือสถานที่ตั้งทำงาน เป็นต้น)
- กำหนดผู้เข้าร่วมทดสอบ แผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ที่เกี่ยวข้องทั้งภายในและภายนอก (ตัวอย่างเช่น ลูกค้า, ผู้ให้บริการภายนอก, ผู้ค้าร่วม เป็นต้น) โดยพิจารณาจากเหตุการณ์ที่ซักซ้อมของแต่ละครั้งเมื่อเกิดเหตุภัยพิบัติเพื่อเชิญเข้าร่วมทดสอบแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

- เอกสารแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และเอกสารที่เกี่ยวข้องทั้งหมดจะถูกจัดเก็บไว้เป็น Electronic File จัดเก็บไว้บน Google Drive และ บน Intranet

มาตรฐานการปฏิบัติตามกฎหมาย (Legal compliance) การป้องกันข้อมูลสำคัญขององค์กร (Protection of Organization Records) การควบคุมป้องกันข้อมูลส่วนบุคคล (Data Protection and Privacy of Personal Information)

- จัดให้มีการระบุกฎหมาย หรือข้อกำหนดต่าง ๆ ด้านเทคโนโลยีสารสนเทศ และด้านอื่น ๆ ที่เกี่ยวข้องกับธุรกิจขององค์กร และมีผู้ดูแลในเรื่องการติดตาม และปรับปรุงรายการดังกล่าว อย่างน้อยปีละ 1 ครั้ง
- จัดให้มีการสร้างความตระหนักสำหรับนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เพื่อให้บุคลากรมีความตระหนักในการใช้งานและการป้องกันสารสนเทศขององค์กร ข้อมูลส่วนบุคคล ในการปฏิบัติตาม นโยบาย ข้อปฏิบัติ กฎ ระเบียบ ข้อบังคับ ขององค์กร และไม่ละเมิดลิขสิทธิ์ ทรัพย์สินทางปัญญาของผู้อื่น
- การจัดเก็บข้อมูลส่วนบุคคลไว้ในเครื่องคอมพิวเตอร์ Mobile Device หรือบนระบบต่าง ๆ ต้องมีการควบคุมการเข้าถึงให้เป็นไปตาม นโยบายหน้าที่และความรับผิดชอบของผู้ใช้งาน (User Responsibility) และปฏิบัติตามระเบียบปฏิบัติการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ

มาตรฐานการเข้ารหัส (Cryptographic) และการจัดการกุญแจ (Key Management)

- กำหนดระดับชั้นความลับของข้อมูลและพิจารณาใช้งานการเข้ารหัสตามระดับชั้นความลับของข้อมูล พร้อมทั้งพิจารณาจากความเสี่ยงที่สามารถเกิดขึ้นกับข้อมูลนั้นได้ กรณีข้อมูลมีชั้นความลับ ต้องกำหนดมาตรการในการบริหารจัดการการเข้ารหัสข้อมูล โดยปฏิบัติตามระเบียบปฏิบัติงานการควบคุมการเข้ารหัส (Cryptographic Control)
- การเข้ารหัสจะต้องใช้เทคนิคที่เป็นมาตรฐานสากล หรือตามที่กฎหมายกำหนด โดยพิจารณาถึงความแข็งแกร่ง (Strength) ของอัลกอริทึมที่ใช้รวมถึงความเหมาะสมในการนำมาใช้งาน
- กำหนดมาตรการในการบริหารจัดการการเข้ารหัสของข้อมูลและบริหารจัดการกุญแจเข้ารหัส (Key Management) ตามระเบียบปฏิบัติงานการควบคุมการเข้ารหัส (Cryptographic Control) ทั้งที่ข้อมูลอยู่ระหว่างการพัฒนาและการนำมาใช้งาน เพื่อสร้างความมั่นคงปลอดภัยของข้อมูลตามระดับชั้นความลับของข้อมูล

มาตรฐานการรักษาความมั่นคงปลอดภัยระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) พื้นที่ปลอดภัย (Secure Areas)

- มีการจัดการดูแลประตูทางเข้า-ออก บุคคลภายนอกที่มาติดต่อกับองค์กร ต้องรอเจ้าหน้าที่ขององค์กร มารับที่บริเวณต้อนรับก่อน แล้วจึงจะพาไปตามบริเวณต่าง ๆ ตามที่กำหนดไว้
- การผ่านประตูต่าง ๆ จะต้องใช้ระบบสแกนต่าง ๆ โดยระบบจะต้องบันทึกเวลาและ Identity
- ในบริเวณที่เป็นเขตหวงห้าม จะต้องจัดให้มีการจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออก และอาจจะมีเจ้าหน้าที่รักษาความปลอดภัยคอยดูแลหรือติดตั้งระบบรักษาความปลอดภัย และต้องติดป้ายบอกว่า บริเวณใดเป็นเขตหวงห้ามให้เห็นได้อย่างชัดเจน พร้อมจัดทำข้อความเตือน เช่น ห้ามนำอาหาร เครื่องดื่ม อุปกรณ์ถ่ายภาพ เข้าภายในพื้นที่ เป็นต้น และในบริเวณดังกล่าวมีระบบป้องกัน เช่น ระบบประตูล็อคอัตโนมัติ และหน้าต่างที่ถูกปิด และ ล็อคไว้ตลอดเวลา เป็นต้น
- จัดให้มีการกำหนดว่า พื้นที่ หรือ บริเวณใดในเขตสำนักงานเป็นบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas) อ้างอิงเอกสารสนับสนุน ขอบเขตและพื้นที่ปลอดภัย (ISMS Scope and Secure Areas)
- มีการจัดแบ่งและบริหารพื้นที่ที่เป็น สำนักงาน ห้องทำงาน และ สิ่งอำนวยความสะดวก (Facilities) ตามมาตรฐานความปลอดภัยในสำนักงาน ให้กำจัดบริเวณที่สาธารณะภายในสำนักงาน
- ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์ (Loading Area) โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กร โดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก
- เจ้าหน้าที่หรือบุคลากรที่ทำงานใน เขตหวงห้าม ต้องได้รับทราบข้อมูลในข้อปฏิบัติ หรือ ข้อควรระมัดระวัง ในเรื่องเฉพาะที่จำเป็นต้องรู้เท่านั้น

- ในบริเวณพื้นที่ว่าง หรือ ไม่ค่อยได้ใช้งาน หรือบริเวณประตู หน้าต่าง ในเขตหวงห้าม ต้องปิดล็อคไว้ตลอดเวลาและมีการตรวจตราเป็นระยะ
- อุปกรณ์สนับสนุนประมวลผลสารสนเทศขององค์กร ถ้าเป็นไปได้ควรมีการจัดสรรแยกออกมาจากการใช้งานร่วมกับบุคคลภายนอก
- มีการแจ้งเตือน ห้ามถ่ายภาพ หรือบันทึกเสียง เข้าไปในพื้นที่เขตหวงห้าม
- มีการตรวจสอบและเฝ้าระวังการผ่านเข้า-ออกในบริเวณพื้นที่ที่สำคัญอย่างสม่ำเสมอ
- มีการควบคุมดูแล สิ่งของ หรือ อุปกรณ์ที่นำเข้ามา หรือ นำออก ในเขตสำนักงาน และต้องมีการจดบันทึกที่เป็นลายลักษณ์อักษร
- มีระบบป้องกันอัคคีภัยที่เหมาะสม เช่น ในบริเวณใด ควรเลือกใช้ สารดับเพลิงประเภทใด มีการติดตั้งอุปกรณ์ดับเพลิงไว้ในที่เหมาะสม ไม่กีดขวางทาง หรือ อยู่ในที่ไม่สะดวกต่อการนำมาใช้ในกรณีฉุกเฉิน
- จัดให้มีระเบียบปฏิบัติในการตรวจสอบบริเวณที่ต้องรักษาความปลอดภัย เช่น สิ่งของ, บริเวณ, อุปกรณ์ หรือ สินค้าที่เป็นวัตถุอันตราย เป็นต้น และมีการแยกพื้นที่สำหรับวางสิ่งของที่นำเข้ามา และ นำออกไปเป็น บริเวณต่างหาก
- จัดให้มีระบบไฟฟ้าสำรอง (Uninterrupted Power Supply) ในกรณีที่ระบบไฟฟ้าหลักเกิดขัดข้อง แบบที่เป็น Online Backup หรือแบบที่เป็น Offline Backup

มาตรฐานการจัดวางและป้องกันอุปกรณ์ (Equipment Security)

- อุปกรณ์ควรต้องมีการจัดวางในพื้นที่ทำงานที่ป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาตให้มากที่สุด
- ระบบบริการสารสนเทศที่จัดการเกี่ยวกับข้อมูลระดับชั้นลับ ควรจะต้องมีการจัดวางในมุมที่ไม่มีความเสี่ยงในการที่บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงหรือมองเห็นได้ในระหว่างที่มีการใช้งาน
- อุปกรณ์ใด ๆ ที่มีความจำเป็นที่ต้องมีการเก็บรักษาเป็นพิเศษ ควรที่จะต้องแยกป้องกันต่างหาก
- มีมาตรการควบคุมเพื่อลดความเสี่ยงจากช่องโหว่ทางกายภาพ
- มีการควบคุมอุณหภูมิและความชื้นในพื้นที่จัดวางอุปกรณ์ และมีการเฝ้าดูเป็นระยะ
- มีการจัดเรื่องของแสงสว่างให้เพียงพอในจุดต่าง ๆ
- การควบคุมการเข้า-ออก พื้นที่เพื่อเข้าถึงอุปกรณ์
- มีการควบคุมป้องกันอุปกรณ์ที่มีข้อมูลสารสนเทศในระดับชั้นลับ เพื่อป้องกันข้อมูลรั่วไหว

มาตรฐานการเดินสายไฟ สายสื่อสาร และสายเคเบิ้ล (Cabling Security)

- การเดินสายไฟฟ้าและสายสื่อสาร ที่อยู่ภายในพื้นที่ ควรเดินสายให้มีความปลอดภัย หรือมีการป้องกันในรูปแบบที่เหมาะสม
- การติดตั้งสายไฟฟ้าแยกจาก สายสัญญาณ Telecommunication เพื่อป้องกันการรบกวน
- มีการทำเครื่องหมายหรือป้ายบอกสายแต่ละสาย และ ระบุประเภทอย่างชัดเจน

มาตรฐานการบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

- จัดให้มีตารางการบำรุงรักษาอุปกรณ์ตามที่ผู้จำหน่ายแนะนำ หรือตามคู่มือการใช้งานของอุปกรณ์
- ผู้ที่ทำการบำรุงรักษาอุปกรณ์ ต้องเป็นผู้ที่มีคุณสมบัติตามที่ระบุไว้โดยผู้ผลิต หรือ ตามคู่มือที่แนะนำ
- มีการเก็บบันทึกการบำรุงรักษาอุปกรณ์ต่าง ๆ
- มีการจัดทำและจัดเก็บค่าการติดตั้งของอุปกรณ์ (Configuration) อยู่ในตำแหน่งและสภาพที่มีความพร้อมใช้เสมอ

มาตรฐานการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment Off-premises)

- การนำอุปกรณ์ประมวลผลสารสนเทศไปใช้งานนอกสำนักงานจะต้องมีการขออนุญาตจากองค์กร ก่อนนำอุปกรณ์ดังกล่าวออกไปใช้งานภายนอกสำนักงาน
- ผู้ใช้งานที่นำอุปกรณ์ไปใช้งานนอกสำนักงาน มีความตระหนัก พึงระวัง รักษา หวงแหน รักษาข้อมูล เครื่องคอมพิวเตอร์ หรืออุปกรณ์ซึ่งเป็นทรัพย์สินขององค์กร เสมือนเช่นทรัพย์สินของตนเอง และพิจารณาความเสี่ยงของการปฏิบัติงานภายนอกสำนักงาน

มาตรฐานการกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

- ก่อนการนำอุปกรณ์กลับมาใช้ใหม่ หรือทำลาย ให้ทำลายข้อมูลทั้งหมดที่อยู่ในสื่อบันทึกดังกล่าวก่อน
- การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง ให้ดำเนินการทำลาย (Disposal) ตามระดับชั้นของข้อมูลที่อยู่ในสื่อบันทึก สอดคล้องตาม **นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**

มาตรฐานการนำเครื่องมืออุปกรณ์ออกนอกองค์กร (Removal of Property)

- ห้ามนำเครื่องคอมพิวเตอร์ อุปกรณ์ เครื่องมือ ขององค์กร ออกภายนอกก่อนได้รับอนุญาต
- กำหนดให้มีการขออนุญาตนำทรัพย์สินขององค์กร ออกสู่ภายนอกและช่วงเวลาส่งคืนอย่างชัดเจน
- กำหนดให้มีการเก็บบันทึกการขออนุญาตเพื่อใช้เป็นหลักฐานในการตรวจสอบและยืนยันการดำเนินการ

มาตรฐานการรักษาความมั่นคงปลอดภัยในการพัฒนาระบบงาน (Information Systems Acquisition, Development and Maintenance Policy)

กรณีหากองค์กรต้องมีการพัฒนาระบบหรือระบบงานให้มีความมั่นคงปลอดภัย องค์กรจะต้องดำเนินการดังต่อไปนี้

- กำหนดให้มีการระบุความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศในการพัฒนาระบบงาน ให้ครอบคลุมถึงการพัฒนาระบบใหม่ และการปรับปรุงระบบเดิม
- กำหนดให้มีการพิจารณาความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศในช่วงเริ่มต้นของโครงการพัฒนาระบบ ให้ครอบคลุมถึงการพัฒนาระบบใหม่ และการปรับปรุงระบบเดิม
- ให้ปฏิบัติตามหลักการวิศวกรรมระบบที่น่าเชื่อถือและมีความมั่นคงปลอดภัย ตาม**เอกสารแนวทาง Principles for Engineering Secure Systems** โดยผู้พัฒนาต้องระบุหลักการที่นำมาพัฒนาหรือปรับปรุง หรือการประยุกต์กับการพัฒนา
- กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลป้อนเข้า (Input Validation)
- หากต้องมีการใช้ข้อมูลขององค์กรในการทดสอบ จะต้องบริหารจัดการตาม **นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)** และปฏิบัติตาม **นโยบายการบริหารจัดการแลกเปลี่ยนข้อมูล (Information Exchange Management)**
- กำหนดขั้นตอนการปฏิบัติเมื่อเกิดข้อผิดพลาดของการป้อนข้อมูลเข้า (Responding to Validation Errors)
- มีมาตรการควบคุมให้แน่ใจว่าระบบงานมีการตรวจสอบและป้องกันกรณีเกิดข้อผิดพลาดที่เกิดจากการประมวลผล รวมถึงการดำเนินการกรณีเกิดข้อผิดพลาดระหว่างการประมวลผล
- มาตรการในการตรวจสอบหากข้อมูลถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต (Message Integrity)
- ตรวจสอบการแสดงผลให้แน่ใจว่ามีความถูกต้องสมบูรณ์ (Output Data Validation)
- ต้องแน่ใจว่าข้อมูลที่จะเข้ารหัสไม่ปนเปื้อนซอฟต์แวร์ไม่ประสงค์ดี (Malicious) เพื่อป้องกันผล กระทบต่อมาตรการป้องกันไวรัสหากซอฟต์แวร์ป้องกันไวรัสไม่สามารถตรวจสอบข้อมูลที่ถูกเข้ารหัสไว้ได้
- จัดให้มีการแยกสภาพแวดล้อมสำหรับการพัฒนาระบบ การทดสอบระบบ และระบบที่ใช้งานจริง (Separation of Development, Test and Operational Facilities) ไม่ให้อยู่สภาพแวดล้อมเดียวกัน เพื่อหลีกเลี่ยงการเข้าถึง Operational System โดยไม่ได้รับอนุญาต
- กำหนดให้มีการแบ่งแยกหน้าที่และความรับผิดชอบ (Segregation of Duties) ระหว่างบุคคลหรือหน่วยงาน โดยจัดให้มีการสอบยันความถูกต้องระหว่างกันไม่ให้บุคคลคนเดียวปฏิบัติงานตั้งแต่ต้นจนจบเพื่อป้องกันความเสี่ยงต่อ

ข้อผิดพลาดและการทุจริตหรือการกระทำที่ไม่เหมาะสม เช่น แยกหน้าที่การพัฒนาระบบหรือจัดทำระบบทดสอบออกจากหน้าที่ของผู้มีอำนาจอนุมัติหรือดำเนินการนำระบบออกสู่การให้บริการ เป็นต้น

- กำหนดขั้นตอนการปฏิบัติสำหรับการเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบและทดสอบกระบวนการของระบบสารสนเทศนั้นก่อนตรวจรับระบบงาน ตาม**นโยบายการบริหารจัดการความเปลี่ยนแปลง (Change management)**
- ต้องมีการทบทวนและทดสอบเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบสำคัญ เพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร
- ไม่อนุญาตการดำเนินการเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูป และจำกัดการเปลี่ยนแปลงเท่าที่จำเป็นและต้องมีการควบคุมอย่างรัดกุม
- หากองค์กรต้องมีการจัดจ้างผู้ให้บริการภายนอกเป็นผู้ดำเนินการพัฒนาระบบใหม่ให้มีกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอก ตาม**นโยบายการควบคุมผู้ให้บริการจากภายนอก (Supplier Management)** พร้อมทั้งแจ้งให้ผู้ให้บริการภายนอกทราบถึง**นโยบายการรักษาความมั่นคงปลอดภัยในการพัฒนาระบบงาน (Information Systems Acquisition, Development and Maintenance Policy)** ก่อนการพัฒนา
- ต้องมีการดำเนินการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบในระหว่างที่ระบบอยู่ในช่วงการพัฒนา
- จัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่หรือปรับปรุงเพิ่มเติมตาม**ระเบียบปฏิบัติงานการตรวจรับระบบงาน (System Acceptance)** รวมถึงการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบตามที่กำหนดไว้ในช่วงการพัฒนา

มาตรฐานการจัดเก็บ เฝ้าระวัง ตรวจสอบการวิเคราะห์และจัดการกับข้อมูลล็อก (Log Monitoring and Management) การเทียบเวลาระบบคอมพิวเตอร์ (Clock Synchronization)

- จัดให้มีระเบียบปฏิบัติที่เกี่ยวข้องในการจัดเก็บ เฝ้าระวัง ตรวจสอบการวิเคราะห์และจัดการกับข้อมูลล็อก (Log Monitoring and Management) การเทียบเวลาระบบคอมพิวเตอร์ (Clock Synchronization) เพื่อดำเนินการให้เป็นไปตามนโยบายอย่างเคร่งครัด
- ผู้ปฏิบัติงานด้านเทคนิค (System Admin) ต้องดำเนินการ
    - กำหนดให้มีทำการบันทึกกิจกรรมการใช้งานของผู้ใช้และผู้ปฏิบัติงานด้านเทคนิค (System Admin, Network Admin) การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ (รวมถึงเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ) ที่เกี่ยวกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามรอบระยะเวลา และจัดเก็บไว้ในสถานที่ที่ปลอดภัย เพียงพอต่อการใช้งาน และจำกัดการเข้าถึงทางลอจิคัล (Logical access) และทางกายภาพ (Physical access) อย่างมีประสิทธิภาพตามระเบียบปฏิบัติงานการจัดการข้อมูลจราจรทางคอมพิวเตอร์

- อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์สื่อสารที่สามารถตั้งเวลาได้ ต้องตั้งค่าเวลาตามมาตรฐานสากล ซึ่งต้องตรวจสอบการเทียบเวลาดังกล่าว 3 เดือนครั้ง และปฏิบัติตามขั้นตอนในการเทียบเวลาระบบคอมพิวเตอร์ให้เป็นไปตาม **วิธีปฏิบัติงานในการเทียบเวลาระบบคอมพิวเตอร์** กรณีที่มีการร้องขอการตั้งเวลาจากผู้ใช้บริการหรือลูกค้าที่นอกเหนือการตั้งเวลาตาม Standard ที่องค์กรกำหนดไว้ ให้ผู้ที่เกี่ยวข้องนำเสนอข้อมูลให้คณะทำงาน IT Security พิจารณาและอนุมัติแนวทางในการดำเนินการตั้งเวลาดังกล่าวตามความเหมาะสม
- จัดให้มีมาตรการป้องกันและทบทวนความถูกต้องของข้อมูลล็อกที่บันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ ให้สอดคล้องตาม **ระเบียบปฏิบัติการเฝ้าระวัง ตรวจสอบการวิเคราะห์และการจัดการกับข้อมูลล็อก (Monitoring and Log Management)**
- ควรนำบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ มาดำเนินการวิเคราะห์ และดำเนินการแก้ไขตามความเหมาะสม รวมทั้งการรายงานเหตุการณ์ข้อผิดพลาดให้ผู้บริหารสารสนเทศรับทราบ 3 เดือนครั้ง (หากเป็นกรณีเหตุการณ์ข้อผิดพลาดต่างๆ ที่มีผลกระทบสูงให้ผู้ปฏิบัติงานด้านเทคนิค (System Administrator และ System Operator) ทบทวนและวิเคราะห์นั้นทันที
- กรณีกล้องวงจรปิด ต้องจัดเก็บและบันทึกภาพตาม **ระเบียบปฏิบัติการเฝ้าระวัง ตรวจสอบการวิเคราะห์และการจัดการกับข้อมูลล็อก (Monitoring and Log Management)** โดยต้องตรวจสอบและวิเคราะห์ความปลอดภัยอย่างสม่ำเสมอ และต้องสามารถตรวจดูว่าระบบบันทึกภาพสามารถเรียกมาดูได้ตามปกติย้อนหลังได้ตามระยะเวลาที่จัดเก็บ และจัดทำแผนการตรวจสอบและบันทึกผลที่เป็นลายลักษณ์อักษร
- จัดให้มีการจัดระดับชั้นของข้อมูลล็อกตาม **นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**

มาตรฐานความปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

- กำหนดให้บุคลากรทุกท่านมีหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ รวมถึงบุคลากรผู้ที่องค์กร ทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กร จะว่าจ้างมาปฏิบัติงานให้องค์กร ให้รับรู้รับทราบใน**เอกสารแบบฟอร์ม Acceptable Use Policy (AUP)** ปฏิบัติตาม**นโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร** อย่างเคร่งครัด
- การสรรหาและคัดเลือก จะต้องมีการตรวจสอบคุณสมบัติของผู้รับจ้าง เพื่อทำให้แน่ใจว่า ผู้รับจ้างมีความรู้ความสามารถ มีพฤติกรรมที่เหมาะสม และไม่เคยกระทำความผิดร้ายแรง โดยเฉพาะในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ
- เมื่อมีการตกลงจ้างงาน ให้มีการทำสัญญาจ้างและกำหนดเงื่อนไขการจ้างงานให้ชัดเจน โดยระบุหน้าที่ความรับผิดชอบตามข้อกำหนดความมั่นคงปลอดภัยสารสนเทศ

- ผู้รับจ้างต้องลงนามยอมรับเงื่อนไข การรักษาความลับขององค์กร และเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ถึงแม้จะพ้นสภาพการเป็นผู้รับจ้างไปแล้วก็ตามใน**เอกสารแบบฟอร์มไม่เปิดเผยความลับขององค์กร (Non-Disclosure Agreement)**
- ผู้รับจ้างจะต้องมีหน้าที่ ความรับผิดชอบ และปฏิบัติตามระเบียบทางด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร
- จัดให้มีการดำเนินการฝึกอบรมให้ความรู้ในเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อให้รับทราบ และเข้าใจวิธีการปฏิบัติอย่างถูกต้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
- เมื่อมีการจ้างงาน เปลี่ยนแปลงการจ้าง เปลี่ยนแปลงหน้าที่ความรับผิดชอบ หรือสิ้นสุดการจ้างให้หน่วยงานทรัพยากรบุคคลมีหน้าที่ในการแจ้งให้ทุกหน่วยงานรับทราบ เพื่อให้หน่วยงานที่เกี่ยวข้องดำเนินการกำหนดสิทธิ เปลี่ยนแปลงสิทธิ หรือยกเลิกสิทธิในการเข้าถึงสารสนเทศ ทั้งทางลอจิคัล (Logical access) และทางกายภาพ (Physical access) อย่างมีประสิทธิภาพ ตามนโยบายการควบคุมการเข้าถึง (Access Control) ภายใน 7 วัน หลังจากที่ฝ่ายทรัพยากรบุคคลดำเนินการแจ้ง และหน่วยงานที่เกี่ยวข้องต้องดำเนินการตรวจสอบ ติดตาม และรับคืนทรัพย์สิน เครื่องมือและอุปกรณ์ในการทำงานขององค์กร ให้สอดคล้องกับนโยบายการระบุและพิสูจน์ตัวตัวของผู้ใช้งาน (User Identification and Authentication) และแจ้งกลับผลการดำเนินการกลับให้เจ้าหน้าที่ทรัพยากรบุคคลรับทราบ สำหรับทรัพย์สินอุปกรณ์อื่น ๆ ให้ปฏิบัติตาม**ระเบียบปฏิบัติการสรรหาและการว่าจ้าง** ขององค์กร

มาตรฐานการควบคุมผู้ให้บริการจากภายนอก (Supplier Management)

- จัดให้มีการคัดกรองผู้ให้บริการภายนอกก่อนการจัดจ้างเพื่อให้ เข้าถึง ดำเนินการ ติดตั้ง สื่อสาร เชื่อมต่อ หรือให้บริการโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศต่อข้อมูลสารสนเทศขององค์กร เช่น การตรวจสอบคุณสมบัติทางการเงินขององค์กรผู้ให้บริการภายนอกซึ่งแสดงถึงความน่าเชื่อถือขององค์กร เป็นต้น
- กรณีจัดจ้างผู้ให้บริการภายนอกที่ เข้าถึง ดำเนินการ ติดตั้ง สื่อสาร เชื่อมต่อ หรือให้บริการโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศต่อข้อมูลสารสนเทศขององค์กร องค์กรต้องควบคุมและบริหารจัดการผู้ให้บริการภายนอกตาม **ระเบียบปฏิบัติงานการบริหารจัดการผู้ให้บริการภายนอก (Supplier management)** จะต้องปฏิบัติตามข้อกำหนด ดังนี้
    1. พิจารณาเพิ่มข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศในระหว่างการดำเนินการโครงการ
    2. ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้องในด้านความมั่นคงปลอดภัยสารสนเทศ และลงนามในสัญญารักษาความลับ (NDA) และ AUP
    3. กรณีผู้ให้บริการภายนอกมีการจ้างช่วง ดำเนินการดังต่อไปนี้
        3.1 ดำเนินการแจ้งรายชื่อผู้รับการจ้างช่วงต่อหัวหน้าโครงการเพื่อขออนุญาตให้เข้าดำเนินการ
        3.2 กรณีมีการเปลี่ยนแปลงต่อการดำเนินการโครงการ เช่น รายละเอียดโครงการ ผู้รับจ้างช่วงในระหว่างดำเนินโครงการ เป็นต้น ผู้ให้บริการภายนอกต้องแจ้งและดำเนินการตามขั้นตอนปฏิบัติการบริหารจัดการการเปลี่ยนแปลง ได้ความยินยอมจากสำนักเทคโนโลยีสารสนเทศก่อน

- จัดให้มีการประเมินความเสี่ยงผู้ให้บริการภายนอกในด้านการเข้าถึงระบบสารสนเทศ ในกรณีที่เป็นผู้ให้บริการภายนอกรายใหม่หรือรายเดิมที่เข้าถึงระบบใหม่ **ตามระเบียบปฏิบัติงานการบริหารจัดการผู้ให้บริการภายนอก (Supplier Management)** และต้องประเมินความเสี่ยงของผู้ให้บริการภายนอกตามกระบวนการประเมินความเสี่ยงตามรอบระยะเวลาให้สอดคล้องตาม**ระเบียบปฏิบัติงานการประเมินความเสี่ยง (Risk Assessment)**
- ต้องมีการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก
- ต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกในเรื่องความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการโครงสร้างพื้นฐานของระบบสำหรับสารสนเทศขององค์กรโดยผู้ให้บริการภายนอก โดยจัดให้มีการทำ Service Level Agreement ที่ครอบคลุมถึงข้อตกลงด้านความปลอดภัยในการให้บริการโดยหน่วยงานภายนอก ได้แก่ คุณลักษณะและรายละเอียดของการให้บริการ, มาตรการจัดการด้านความมั่นคงปลอดภัยในการให้บริการ โดยข้อตกลงนี้เป็นที่ยอมรับของทั้งสองฝ่าย และกำหนดให้มีการทบทวน Service Level Agreement ดังกล่าวอย่างน้อยปีละ 1 ครั้ง
- ในการใช้บริการผู้ให้บริการภายนอก องค์กร ต้องจัดให้มีการควบคุมด้านความปลอดภัย ในการถ่ายโอนข้อมูล เครื่องมือ อุปกรณ์ระหว่างองค์กร กับ ผู้ให้บริการภายนอกให้เกิดความมั่นคงปลอดภัย
- กำหนดให้มีผู้รับผิดชอบอย่างเป็นทางการในการติดต่อประสานงาน และควบคุมผู้ให้บริการภายนอก
- มีการทบทวนรายงานผลของผู้ให้บริการภายนอก (รวมถึงมีการประชุมร่วมกันตามเงื่อนไขที่ระบุใน Agreement)
- แลกเปลี่ยนข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident) ระหว่างองค์กร กับ ผู้ให้บริการภายนอกเพื่อเสริมองค์ความรู้และเตรียมการป้องกัน โดยดำเนินการตามขอบเขตของ Agreement อย่างเคร่งครัด
- ติดตามผล และสนับสนุนการแก้ไขปัญหาและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) ร่วมกับผู้ให้บริการภายนอกตามขอบเขตที่ตกลงกันไว้
- การเปลี่ยนแปลงผู้ให้บริการภายนอกต้องพิจารณาอย่างผลการปฏิบัติงาน ความเหมาะสมในการเปลี่ยนแปลงตามความจำเป็น
- มีการพิจารณาอย่างรอบคอบถึงความจำเป็นในการเปลี่ยนแปลงแก้ไขสัญญา หรือข้อตกลงร่วมกัน หากต้องดำเนินการเปลี่ยนแปลงใด ๆ ต้องได้รับอนุมัติจากผู้มีอำนาจก่อนเปลี่ยนแปลง รวมถึงการพิจารณาความเสี่ยงที่อาจกระทบต่อธุรกิจขององค์กรระหว่างการเปลี่ยนแปลง

มาตรฐานการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

- ต้องกำหนดการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูล หรือสารสนเทศที่มีอยู่ในระบบ
- ต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน

การควบคุมการเข้าออก (Physical Entry Control)

- บุคลากรองค์กร จะได้รับสิทธิเข้า-ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงาน
- หากมีบุคคลอื่น ที่ไม่ใช่บุคลากรขององค์กร ขอเข้าพื้นที่ โดยไม่ได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานที่เกี่ยวข้องต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลดังกล่าวจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรยืนยันตัวตนอื่น ๆ โดยหน่วยงานที่เกี่ยวข้องจะต้องจดบันทึกบุคคลดังกล่าวและการขอเข้าไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่อนุญาตเข้าพื้นที่)
- บุคลากรองค์กร จะต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้ามาภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการ ป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต
- หน่วยงานที่เกี่ยวข้อง ควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สำนักงาน

การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

- สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด
- ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการท าลายอย่างเหมาะสมวิธีการทำลายข้อมูล สื่อบันทึก วัสดุ
- เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (Protecting against External and Environmental Threats)

- หน่วยงานต้องมีการป้องกันจากการท าลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น ซึ่งเป็นภัยคุกคามจาก ภายนอกต้องมีการเตรียมการป้องกันเหตุที่อาจเกิดขึ้น

มาตรฐานคุ้มครองสิทธิและทรัพย์สินทางปัญญา (IP and Copyright Compliance)

- ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด
- ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย
- ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศขององค์กร โดยเด็ดขาด

มาตรฐานการกำกับดูแล และการใช้บริการ Cloud Computing

- กำหนดกลยุทธ์ที่ชัดเจนในการใช้งานระบบ Cloud Computing เช่น เหตุผลและความจำเป็นทางธุรกิจ ประโยชน์และต้นทุน การดำเนินการตามกฎหมายและข้อบังคับทั้งภายในและภายนอกประเทศ ความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ การจัดการด้านทรัพยากรบุคคลและองค์ความรู้ เป็นต้น
- จัดให้มีการสื่อสารนโยบายการใช้งาน Cloud Computing ไปยังบุคลากรและเจ้าหน้าที่ที่เกี่ยวข้อง เช่น บุคลากรและผู้บริหารหน่วยงาน (Business unit) ผู้ดูแลระบบ (Administrator) ผู้พัฒนาระบบและผู้พัฒนาระบบการเชื่อมโยง (Developer & Integrator) ผู้ใช้งาน รวมถึงบุคลากรและเจ้าหน้าที่ที่เกี่ยวข้อง ให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ Cloud Computing ได้แก่
    - มาตรฐานและขั้นตอนการปฏิบัติงานในการใช้บริการ Cloud Computing
    - ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจากการใช้งาน Cloud Computing และแนวทางการจัดการความเสี่ยง
    - ความเสี่ยงด้านระบบงาน และเครือข่ายจากการใช้งาน Cloud Computing
    - ข้อกำหนดทางกฎหมายที่เกี่ยวข้อง
- จัดเตรียมและพัฒนาองค์ความรู้ด้านการบริหารจัดการ Cloud Computing ให้แก่ผู้ดูแลระบบ (Administrator) และบุคลากรที่เกี่ยวข้องอย่างเพียงพอ เช่น การประเมินความเสี่ยงและการบริหารจัดการความเสี่ยงจากการใช้งานระบบ Cloud Computing กรอบการกำกับดูแลด้านความมั่นคงปลอดภัยระบบ Cloud Computing (Cloud Security Framework) กรอบการกำกับดูแลข้อมูล (Data Governance) เพื่อการรักษาความปลอดภัยและการบริหารจัดการข้อมูลที่จัดเก็บอยู่บนระบบ Cloud Computing เครื่องมือและกรรมวิธีการในการรักษาความปลอดภัยของข้อมูล เช่น การเข้ารหัสโทเคนข้อมูล (Data Tokenization) การลบการเชื่อมโยงถึงบุคคลได้หรือการลบอัตลักษณ์บุคคลออกไปจากฐานข้อมูล (Data anonymization หรือ de-identification) เป็นต้น
- ทบทวนนโยบายการใช้Cloud Computing อย่างน้อยปีละ 1 ครั้ง

- สอบทานและปรับปรุงแนวทางการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมความเสี่ยงจากการใช้บริการ Cloud Computing ทั้งในเรื่องของการระบุความเสี่ยง การประเมินความเสี่ยง การควบคุมความเสี่ยงให้อยู่ในระดับที่ ยอมรับได้ และการกำหนดผู้รับผิดชอบต่อความเสี่ยง โดยพิจารณาถึงความเสี่ยงด้านต่าง ๆ ดังต่อไปนี้
    - ความเสี่ยงด้านกลยุทธ์ เช่น ความเสี่ยงจากการพึ่งพิงผู้ให้บริการภายนอกและความสามารถในการเปลี่ยนแปลง ผู้ให้บริการ (vendor locked-in)
    - ความเสี่ยงด้านปฏิบัติการ เช่น ระบบประมวลผลผิดพลาดจากระบบให้บริการหรือบุคลากรผู้ให้บริการ การใช้งาน เทคโนโลยีร่วมกัน (Share technology risk) การละเมิดข้อกำหนดและข้อตกลงการใช้งาน Cloud Computing หรือความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลหรือการจำกัดการเข้าถึงของข้อมูลจากผู้ให้บริการ
    - ความเสี่ยงด้านกฎหมาย เช่น การไม่ปฏิบัติตามกฎหมาย หลักเกณฑ์และข้อกำหนดของทางการทั้งภายในประเทศ และต่างประเทศ
    - ความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น การเรียกใช้โปรแกรม (APIs) หรือช่องทางบริหารจัดการที่ไม่ปลอดภัย
    - ความเสี่ยงด้านข้อมูลส่วนบุคคล (data privacy) และการรักษาความปลอดภัยของข้อมูล (data security)
    - ความเสี่ยงจากการใช้ผู้ให้บริการภายนอกที่มีการใช้ผู้ให้บริการภายนอกอื่นรับช่วงจัดการงาน (sub-contract)
- รายงานผลการประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงจากการใช้บริการ Cloud Computing ให้แก่คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการที่ได้รับมอบหมาย