WHA GROUP

Policy

นโยบายการจัดการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

(Cybersecurity and Information Security Management Policy)

Document Properties	
Document Number	WHACG-ICT-PLCY-0001
Softcopy Location	CDMS / WHA SharePoint
Owner Division	IT Department
Owner Department	IT Department
Version Number	v6.0.0 (Approved Final)
Release Date	15 Aug 2025
Review/Update Due Date	15 Aug 2028

Document Approval	
Approver	Jareeporn Jarukornsakul (Chairman and Group Chief Executive Officer)
	Pajongwit Pongsivapai (Chief Executive Officer - WHAID)
	Somkiat Masunthasuwun (Chief Executive Officer - WHAUP)
Reviewer	Nunsilp Janvarin (Chief Technology Officer - IT Department)
Owner	Soros Sottitavorn (Infrastructure and Cybersecurity Senior Manager – IT Department)

Document Control

การเปลี่ยนแปลงเอกสาร:

The following table presents the change record of this document.

เวอร์ชั่น	วันที่อนุมัติ	เจ้าของเอกสาร	การเปลี่ยนแปลง
v6.0.0	15 ส.ค. 2568	โสพัส โสตถิถาวร – ผู้จัดการอาวุโสด้านโครงสร้างพื้นฐานและความมั่นคงปลอดภัยทางไซเบอร์	แก้ไขรายละเอียดข้อ 6.16 และเพิ่มหัวข้อ 6.16.3 และ 6.16.4
v5.0.0	01 ส.ค. 2567	โสพัส โสตถิถาวร – ผู้จัดการโครงสร้างพื้นฐานและความมั่นคงปลอดภัยทางไซเบอร์	เปลี่ยนคณะทำงาน เป็นคณะกรรมการ
v4.0.0	01 ก.ค. 2566	โสพัส โสตถิถาวร – ผู้จัดการโครงสร้างพื้นฐานและความมั่นคงปลอดภัยทางไซเบอร์	ปรับเปลี่ยนรูปเล่มและเนื้อหาให้สอดคล้องตามมาตรฐาน ISO/IEC 27001 version 2022
v3.0.0	01 ก.ค. 2564	โสพัส โสตถิถาวร - ผู้จัดการความมั่นคงปลอดภัยสารสนเทศ	ปรับเปลี่ยนรูปเล่มและเนื้อหา
v2.0.0	01 ส.ค. 2563	นายนันท์ศิลป์ เจนวารินทร์ - หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ	เพิ่มเติมเนื้อหาข้อมูลส่วนบุคคล
v1.0.0	20 พ.ย. 2558	อภิชาติ ทองสุขสันต์ - ฝ่ายเทคโนโลยีสารสนเทศ	เวอร์ชั่นแรก

ผู้แต่ง:

The following persons are the authors who drafted this document.

ชื่อ - นามสกุล	ตำแหน่ง
Soros Sottitavorn	ผู้จัดการอาวุโสด้านโครงสร้างพื้นฐานและความมั่นคงปลอดภัยทางไซเบอร์ (Infrastructure and Cybersecurity Senior Manager - IT)

ผู้ตรวจทาน:

In addition to the main reviewers, the following persons have also reviewed this document.

ชื่อ - นามสกุล	ตำแหน่ง
Nunsilp Janvarin	ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ (Chief Technology Officer – IT)

ผู้อนุมัติ:

In addition to the main approvers, the following persons have also approved this document.

ชื่อ - นามสกุล	ตำแหน่ง
Jareeporn Jarukornsakul	Chairman and Group Chief Executive Officer
Pajongwit Pongsivapai	Chief Executive Officer - WHAID
Somkiat Masunthasuwun	Chief Executive Officer - WHAUP

สารบัญ (Table of Contents)

1) บทนำ (Introduction)

ปัจจุบันบริษัทได้มีการใช้งานด้านเทคโนโลยีสารสนเทศอย่างกว้างขวาง ทางบริษัทจึงให้ความสำคัญกับการปกป้องระบบสารสนเทศรวมถึงดำเนินนโยบายในการเตรียมความพร้อมในการรองรับภัยคุกคามทางไซเบอร์ ซึ่งการดำเนินนโยบายนั้นมุ่งเน้นเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (“พ.ร.บ. ไซเบอร์”) นอกจากนี้ทางบริษัทยังให้ความสำคัญในเรื่องการคุ้มครองและเคารพสิทธิในความเป็นส่วนตัวของท่านที่มีอยู่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) และฉบับปรับปรุงแก้ไขตามซึ่งจะมีการปรับปรุงแก้ไขเป็นคราวๆ รวมถึงกฎหมายและกฎระเบียบอื่น ๆ ที่ใช้บังคับในประเทศไทย และมุ่งหมายที่จะคุ้มครองข้อมูลส่วนบุคคลของทุกท่านที่บริษัทได้ทำการเก็บรวบรวม ใช้งาน และเปิดเผยเพื่อการดำเนินกิจการของบริษัท บริษัทมีหน้าที่ตามที่กำหนดไว้ในเรื่องการคุ้มครองข้อมูลส่วนบุคคล ความเป็นส่วนตัว หรือความมั่นคงปลอดภัยของข้อมูล ที่ใช้บังคับและมีผลบังคับอยู่ในประเทศไทย

เพื่ออธิบายถึงจุดประสงค์และขอบเขตของนโยบายด้านความมั่นคงปลอดภัยสารสนเทศในภาพรวม ที่แสดงถึงทิศทางของผู้บริหารขององค์กรด้านความมั่นคงปลอดภัยสารสนเทศที่ต้องการให้บุคคลที่เกี่ยวข้องกับข้อมูลขององค์กรยึดถือและนำมาใช้ในการปฏิบัติงาน โดยมีเป้าหมาย คือการทำให้การปฏิบัติงานของพนักงานที่เกี่ยวข้องกับข้อมูล รวมถึงระบบที่เกี่ยวข้องกับข้อมูลให้มีความมั่นคงปลอดภัยด้านสารสนเทศที่เพียงพอในการรองรับการดำเนินธุรกิจ ณ ปัจจุบัน และในอนาคตขององค์กร

นโยบายการจัดการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศฉบับนี้ จึงครอบคลุมถึงการปกป้องข้อมูลขององค์กรตลอดจนข้อมูลส่วนบุคคล เนื่องด้วยข้อมูล ถือได้ว่าเป็นทรัพย์สินที่มีความสำคัญเป็นอย่างมากในการดำเนินธุรกิจขององค์กร ซึ่งในกรณีที่ข้อมูลสำคัญขององค์กร ไม่มีความมั่นคงปลอดภัย ไม่สามารถรักษาความลับความถูกต้อง และความพร้อมใช้ของข้อมูลได้นั้น จะส่งผลกระทบต่อองค์กร ไม่ว่าจะเป็นด้านการเงิน ด้านความเชื่อถือ หรือด้านชื่อเสียงขององค์กร ข้อมูลที่กล่าวถึงในนโยบายนี้มิได้จำกัดอยู่แต่ในรูปอิเล็กทรอนิกส์เท่านั้น ข้อมูลอาจอยู่ในรูปอื่น ๆ เช่น เอกสาร สิ่งพิมพ์ ฟิล์ม หรือแม้แต่ในรูปของการสนทนา อย่างไรก็ดีการปกป้องข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ จะกล่าวถึงเป็นส่วนใหญ่ เนื่องจากข้อมูลขององค์กรส่วนใหญ่นั้นจะอยู่ในรูปอิเล็กทรอนิกส์ ซึ่งในอนาคตจะมีแนวโน้มเพิ่มขึ้นตามลำดับ

ทั้งนี้เพื่อให้มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท สอดคล้องตามมาตรฐานสากล ISO/IEC 27001 เวอร์ชัน 2022 ดังนั้นบริษัทจึงได้แบ่งกลุ่มของมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ ออกเป็น 4 กลุ่ม ดังนี้

1. มาตรการควบคุมด้านองค์กร (Organizational controls)
2. มาตรการควบคุมด้านบุคลากร (People controls)
3. มาตรการควบคุมทางกายภาพ (Physical controls)
4. มาตรการควบคุมทางเทคโนโลยี (Technological controls)

2) วัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Objectives)

2.1) เพื่อทำให้ระบบเทคโนโลยีสารสนเทศมีเสถียรภาพ มีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ และมีความพร้อมใช้งานที่สอดคล้องกับความต้องการทางธุรกิจขององค์กร

2.2) เพื่อทำให้องค์กรมีการดำเนินการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศในทิศทางเดียวกันอย่างมีระบบ

2.3) เพื่อให้ข้อมูลสารสนเทศมีความถูกต้องและสามารถนำไปใช้งานโดยผู้ที่ได้รับอนุญาต

2.4) เพื่อป้องกันข้อมูลสารสนเทศจากการนำไปใช้ผิดวัตถุประสงค์ หรือถูกทำลาย หรือนำไปเปิดเผยโดยไม่ได้รับอนุญาต

2.5) เพื่อกำหนดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่หน่วยงานและบุคลากรที่เกี่ยวข้อง

3) มาตรการควบคุมด้านองค์กร (Organizational controls)

เนื้อหานโยบาย และการดำเนินการ

3.1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)

3.1.1) การจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ (Policies for Cybersecurity and Information Security)

1) นโยบายการจัดการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศฉบับนี้ ถูกจัดทำเป็นลายลักษณ์อักษรตามจุดประสงค์และขอบเขต และได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการ มีการประกาศใช้และถือปฏิบัติทั่วทั้งองค์กร โดยให้มีผลบังคับใช้กับบุคลากรใน ทุกระดับชั้นขององค์กร ตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและทรัพย์สิน สารสนเทศขององค์กร

2) ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สินสารสนเทศขององค์กร มีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการตาม ระเบียบการใช้งานระบบสารสนเทศขององค์กรอย่างปลอดภัย และให้ความร่วมมือในการดำเนินการตามนโยบายอย่างเคร่งครัด การฝ่าฝืนนโยบายนี้ ถือเป็นความผิดที่ร้ายแรง โดยมีบทลงโทษถึงขั้นสูงสุดตามระเบียบขององค์กร

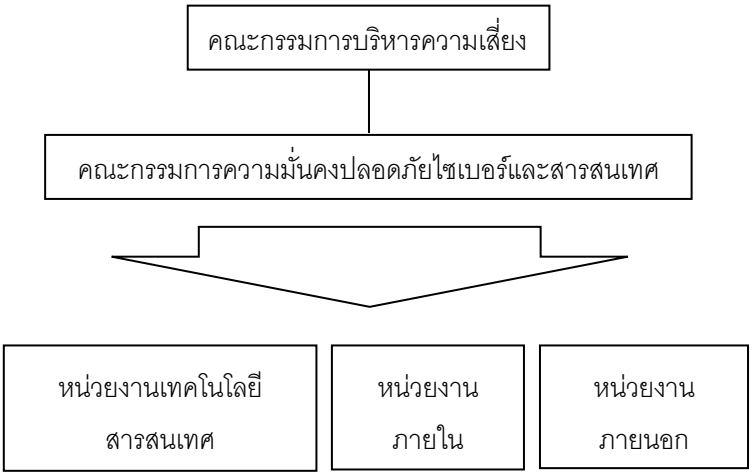
3.1.2) การทบทวนโยบายความมั่นคงปลอดภัยสารสนเทศ (Review of The Policies for Information Security)

คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ อาจทบทวนและปรับปรุงนโยบายฉบับนี้ได้เป็นครั้งคราวไป เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การแก้ไขเพิ่มเติมกฎหมาย รวมถึงกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล การเปลี่ยนแปลงกลยุทธ์หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างเทคโนโลยี เป็นต้น ทั้งนี้ เมื่อมีการปรับปรุงนโยบายฉบับนี้ บริษัทจะแจ้งให้ผู้ใช้งานทราบโดยการแสดงข้อความว่า “ปรับปรุงใหม่” ไว้ที่ลิงค์ของนโยบายความมั่นคงปลอดภัยสารสนเทศ

3.2) การกำหนดบทบาท หน้าที่ และอำนาจหน้าที่ ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

ผู้บริหารให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ โดยอนุมัติให้มีการจัดตั้งคณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศ ดังนี้

1) ลักษณะโครงสร้างของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ แสดงดังภาพด้านล่างนี้



ภาพที่ 1 แสดงโครงสร้างองค์กรของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

2) คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ประกอบจากผู้บริหารของหน่วยงานต่าง ๆ ดังนี้

(1) ผู้ช่วยกรรมการผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ	ประธานคณะกรรมการและผู้อำนวยการความมั่นคงปลอดภัยสารสนเทศ (CISO)
(2) ผู้จัดการความมั่นคงปลอดภัยสารสนเทศ	คณะทำงานและเลขานุการ
(3) ผู้เชี่ยวชาญฝ่ายปฏิบัติการ	คณะทำงาน
(4) ผู้เชี่ยวชาญฝ่ายทรัพยากรบุคคล	คณะทำงาน
(5) ผู้เชี่ยวชาญฝ่ายพัฒนาธุรกิจ	คณะทำงาน
(6) ผู้เชี่ยวชาญฝ่ายการเงิน	คณะทำงาน
(7) เจ้าหน้าที่คุ้มครองข้อมูล	คณะทำงาน

3) คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ มีหน้าที่ดังนี้

(1) ตรวจสอบ และอนุมัติ ปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศ ตามกำหนด หรือตามสถานการณ์

(2) วางแผนประชาสัมพันธ์ และอบรมบุคลากรทุกหน่วยให้เข้าใจถึงความมั่นคงปลอดภัยสารสนเทศ

(3) ตรวจสอบ และให้ความเห็นชอบโครงการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

(4) วางแผน ตรวจสอบ และบริหารจัดการความเสี่ยงต่าง ๆ ที่เกิดจากข้อจำกัดของระบบ

(5) ตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องด้านความมั่นคงปลอดภัย กรณีฉุกฉิน

3.3) การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

คณะกรรมการบริหารความเสี่ยง ได้ทำการกำหนดบทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องตามโครงสร้างของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ดังนี้

1. **หน่วยงานเทคโนโลยีสารสนเทศ**

จัดตั้งขึ้นเพื่อป้องกันความเสียหายขององค์กรอันเกิดจากภัยคุกคามด้านข้อมูล เช่น การสูญหายของข้อมูล หรือการเจาะระบบสารสนเทศ เป็นต้น และทำให้การดำเนินการในส่วนที่เกี่ยวข้องกับข้อมูลมีความมั่นคงปลอดภัยในระดับที่สอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

1.1 **ผู้อำนวยการความมั่นคงปลอดภัยสารสนเทศ** (Chief Information Security Officer : CISO)

(1) เป็นประธานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ และมีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศและเป็นผู้นำในการดำเนินงานทั้งหมดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในองค์กร

(2) กำหนดเป้าหมาย นโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ขององค์กร

(3) เป็นผู้นำเสนอแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ตลอดจนแผนการดำเนินงานทางด้านความมั่นคงปลอดภัยสารสนเทศเพื่อขอดำเนินการอนุมัติจากผู้บริหารระดับสูง และเพื่อให้ผู้บริหารระดับสูงมีความตระหนักในความสำคัญในเรื่องความมั่นคงปลอดภัยสารสนเทศ

(4) วิเคราะห์และบริหารความเสี่ยงที่เกี่ยงข้องกับความมั่นคงปลอดภัยสารสนเทศ รวมถึงเป็นผู้ประเมินทางเลือกในการรับมือกับความเสี่ยงทางด้านความมั่นคงปลอดภัยทางสารสนเทศอย่างเหมาะสม

(5) จัดการพัฒนานโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้องค์กรได้มาซึ่งเสถียรภาพความมั่นคงของระบบ ความถูกต้องและการรักษาความลับของข้อมูล

(6) บริหารจัดการเฝ้าระวังการโจมตีทางสารสนเทศ โดยมีระบบป้องกันผู้บุกรุก มีการใช้ระบบตรวจสอบและแจ้งเตือนผู้บุกรุก หรือระบบจัดการกำจัดไวรัส ตลอดจนวางแผนต่อเนื่องทางธุรกิจหรือแผนฟื้นฟูเมื่อเกิดภัยพิบัติเพื่อกู้ระบบยามฉุกเฉิน

(7) ติดต่อและรักษาความสัมพันธ์กับคู่ค้า, องค์กร หรือบุคคลภายนอกที่มีความเกี่ยวข้องกับเรื่องความมั่นคงปลอดภัยสารสนเทศทั้งภาครัฐและเอกชน

(8) ตรวจสอบและอนุมัตินโยบายความมั่นคงปลอดภัยสารสนเทศ รวมถึงขั้นตอนและแนวทางปฏิบัติขององค์กรเพื่อให้เหมาะสมกับความสำคัญของกระบวนการทางธุรกิจ

(9) จัดตั้งทีมงานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้สามารถปฏิบัติงานในยามที่เกิดภาวะฉุกเฉินขึ้นในองค์กร

1.2 **ผู้จัดการความมั่นคงปลอดภัยสารสนเทศ** (Information Security Manager)

(1) รายงานโดยตรงกับ CISO ในการดำเนินงานทั้งหมดที่เกี่ยวข้องกับสารสนเทศ รวมถึง รายงานความคืบหน้าในการรักษาความมั่นคงปลอดภัยสารสนเทศให้ CISO ทราบเป็นประจำ

(2) ออกแบบนโยบายความมั่นคงปลอดภัยสารสนเทศ รวมถึงขั้นตอนและแนวทางปฏิบัติขององค์กรเพื่อให้เหมาะสมกับความสำคัญของกระบวนการทางธุรกิจ

(3) ทบทวนนโยบาย และขั้นตอนทั้งหมดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

(4) เป็นที่ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศให้กับ CISO เพื่อช่วยในการวิเคราะห์และบริหารความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม รวมถึงให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศแก่แผนกอื่น ๆ

(5) ตรวจสอบให้แน่ใจว่ากระบวนการและการควบคุมตามที่ระบุไว้ในนโยบายนี้มีการนำไปใช้อย่างยั่งยืน

(6) บริหารจัดการเฝ้าระวังการโจมตีทางสารสนเทศ โดยมีระบบป้องกันผู้บุกรุก มีการใช้ระบบตรวจสอบและแจ้งเตือนผู้บุกรุกหรือระบบจัดการกำจัดไวรัส ตลอดจนวางแผนต่อเนื่องทางธุรกิจหรือแผนฟื้นฟูเมื่อเกิดภัยพิบัติ เพื่อกู้ระบบยามฉุกเฉิน

(7) ตรวจสอบและมีการติดตามการสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ

(8) เตรียมพร้อมรับสถานการณ์และเรียนรู้สิ่งใหม่เกี่ยวกับสารสนเทศอย่างสม่ำเสมอ

(9) ควบคุมและบริหารทีมงานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้สามารถปฏิบัติงานในยามที่เกิดภาวะฉุกเฉินขึ้นในองค์กร เช่น การระบาดของไวรัสคอมพิวเตอร์

1.3 **ผู้ดูแลระบบโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ** (IT Infrastructure Team)

(1) ดูแลงานระบบโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศให้ดำเนินงานได้อย่างราบรื่น

(2) ป้องกัน ตรวจสอบ และเฝ้าระวังระบบโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยสารสนเทศ

(3) ปฏิบัติงานในยามที่เกิดภาวะฉุกเฉินขึ้นในองค์กร เช่น การกู้คืนระบบยามฉุกเฉิน การแก้ไขปัญหาการระบาดของไวรัสคอมพิวเตอร์ เป็นต้น

(4) เป็นที่ปรึกษาและคอยช่วยเหลือในระหว่างการพัฒนาระบบต่าง ๆ และในการจัดกิจกรรมการให้ความรู้ การฝึกอบรม รวมถึงการสร้างความตระหนักในด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้

1.4 **ผู้ดูแลการพัฒนาแอปพลิเคชันทางด้านธุรกิจ** (IT Business Application Development Team)

(1) ดูแลงานระบบแอปพลิเคชันทางด้านธุรกิจให้ดำเนินงานได้อย่างราบรื่น

(2) ป้องกัน ตรวจสอบ และเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชันทางด้านธุรกิจเพื่อให้มีความมั่นคงปลอดภัยสารสนเทศ

(3) ปฏิบัติงานในยามที่เกิดภาวะฉุกเฉินขึ้นในองค์กร เช่น ช่วยเหลือในการกู้คืนระบบแอปพลิเคชันทางด้านธุรกิจยามฉุกเฉิน เป็นต้น

(4) เป็นที่ปรึกษาและคอยช่วยเหลือในระหว่างการพัฒนาระบบแอปพลิเคชันทางด้านธุรกิจและในการจัดกิจกรรมการให้ความรู้ การฝึกอบรม รวมถึงการสร้างความตระหนักในด้านความมั่นคงปลอดภัยสารสนเทศด้านแอปพลิเคชันทางด้านธุรกิจแก่ผู้ใช้

2. **หน่วยงานภายใน** คือพนักงานทุกคนขององค์กร ที่มีส่วนเกี่ยวข้องกับสารสนเทศไม่ว่าทางใดทางหนึ่ง สามารถแบ่งได้ดังนี้

2.1 **หน่วยงานฝ่ายทรัพยากรบุคคล** (Human Resources) มีหน้าที่รับผิดชอบ ดังนี้

(1) ให้คำแนะนำปรึกษาทางด้านนโยบายที่เกี่ยวข้องกับการจ้างงาน การประเมินผลงาน ปัญหาด้านทรัพยากรบุคคลที่เกี่ยวข้อง รวมถึงการให้คำแนะนำเกี่ยวกับข้อมูลส่วนบุคคล

(2) ให้การสนับสนุนด้านการบริหารจัดการเพื่อเก็บบันทึกข้อมูลที่จำเป็นเพื่อให้เป็นไปตามกฎหมายข้อบังคับและนโยบายภายในที่เกี่ยวข้องกับทรัพยากรบุคคล ซึ่งอาจมีความจำในการควบคุมการเข้าถึงระบบและการตรวจสอบการเข้าใช้งานระบบสารสนเทศ ให้กับหน่วยงานเทคโนโลยีสารสนเทศ

2.2 **หน่วยงานฝ่ายกฎหมาย** (Legal) เป็นหน่วยงานที่ดำเนินกิจกรรมทางด้านกฎหมายให้แก่องค์กร รวมถึงให้คำแนะนำทางด้านกฎหมายโดยผู้เชี่ยวชาญให้แก่ฝ่ายบริหารและพนักงาน มีหน้าที่รับผิดชอบดังนี้

(1) ดำเนินกิจกรรมทางธุรกิจในลักษณะที่สอดคล้องกับกฎหมาย / ข้อบังคับในปัจจุบัน

(2) ตรวจสอบการก่ออาชญากรรมต่อองค์กรและป้องกันการดำเนินการทางกฎหมาย

(3) ปกป้องทรัพย์สิน สินทรัพย์และพนักงานขององค์กรจากความเสี่ยงทางกฎหมายในด้านต่าง ๆ

2.3 **หัวหน้าฝ่าย/หัวหน้าแผนก** มีหน้าที่ดังนี้

(1) ให้คำแนะนำและย้ำถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศต่อพนักงานภายใต้การดูแลและความจำเป็นในการปกป้องข้อมูลที่เหมาะสมสำหรับการดำเนินธุรกิจ

(2) ดำเนินการตัดสินใจทางธุรกิจให้สอดคล้องกับนโยบายการจัดการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

2.4 **เจ้าของข้อมูล/สารสนเทศ** มีหน้าที่ดังนี้

(1) เป็นเจ้าของและควบคุมข้อมูล/สารสนเทศของตนอย่างเต็มที่ตามกฎหมาย รวมถึงข้อกำหนดในการปฏิบัติงานอื่น ๆ ที่เกี่ยวข้อง

(2) กำหนด จัดการ ควบคุม การสร้าง การประมวลผล การเผยแพร่ และการกำจัดข้อมูล/สารสนเทศ

2.5 **เจ้าหน้าที่คุ้มครองข้อมูล** (Data Protection Officer : DPO) เป็นผู้ควบคุมหรือผู้ประมวลผลที่ต้องแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนด มีหน้าที่รับผิดชอบดังนี้

(1) ให้คำแนะนำ และความรู้ในการปฏิบัติตามข้อกำหนดสำคัญต่าง ๆ เกี่ยวกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act : PDPA) แก่ผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล และบุคคลอื่น ๆ ที่เกี่ยวข้อง

(2) ตรวจสอบการดำเนินงานขององค์กรในการเข้าถึงและดูแลข้อมูลส่วนบุคคลต่าง ๆ ให้เป็นไปอย่างถูกต้องตามข้อกำหนด พรบ.คุ้มครองข้อมูลส่วนบุคคล และตามนโยบายคุ้มครองข้อมูลขององค์กร

(3) ประเมินผลและระบุถึงจุดประสงค์ของการนำข้อมูลส่วนบุคคลไปใช้หรือเผยแพร่ และชี้แจงถึงสิทธิ์ของเจ้าของข้อมูล รวมถึงมาตรการที่องค์กรนำมาใช้ในการปกป้องข้อมูลส่วนบุคคล

(4) ประสานงานกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีเกิดปัญหาเกี่ยวกับการใช้ พรบ.คุ้มครองข้อมูลส่วนบุคคล ในองค์กร

(5) รักษาความลับของข้อมูลส่วนบุคคลจากการปฏิบัติหน้าที่

2.6 **พนักงานองค์กร** คือพนักงานทุกคนขององค์กร ที่มีส่วนเกี่ยวข้องกับสารสนเทศไม่ว่าทางใดทางหนึ่ง มีหน้าที่รับผิดชอบ ดังนี้

(1) ปฏิบัติตามนโยบายการจัดการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศอย่างเคร่งครัด

(2) รักษาความลับของข้อมูลสารสนเทศขององค์กร และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง

(3) รักษาความลับของข้อมูลส่วนบุคคล และ ความยินยอมให้ใช้งานของ เจ้าของข้อมูลส่วนบุคคล

(4) รายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ และปัญหาทางด้านความมั่นคงปลอดภัยเมื่อเกิดเหตุการณ์

(5) ใช้งานข้อมูล และทรัพย์สินทางข้อมูลขององค์กรอย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบหรือได้รับอนุญาตเท่านั้น

3. **หน่วยงานภายนอก** คือบุคคลภายนอกที่เข้ามาปฏิบัติงานในองค์กรหรือทำงานให้กับองค์กร ซึ่งมีส่วนเกี่ยวข้องในการใช้ข้อมูลหรือทรัพย์สินสารสนเทศอื่นขององค์กร เช่น ผู้ให้บริการ/ผู้จำหน่าย ระบบคู่สัญญาหรือผู้ที่ได้รับอนุญาตโดยมีหน้าที่ความรับผิดชอบเช่นเดียวกับพนักงานขององค์กร

3.4) หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

กำหนดให้ ผู้บริหารทุกระดับ หัวหน้าฝ่ายและหัวหน้างานของทุกหน่วยงาน ต้องควบคุมดูแลให้บุคลากร บุคลากรชั่วคราว และคู่สัญญา (บุคคล) ปฏิบัติตามนโยบายฯ มาตรฐาน และขั้นตอนฯ ขององค์กร รวมทั้งมีความตระหนักเรื่องหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

3.5) การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำทะเบียนหน่วยงานกำกับดูแลภายนอก ซึ่งรวมถึงหน่วยงานภายนอกที่กำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศ และต้องทบทวนเพื่อปรับปรุงทะเบียนนี้อย่างน้อยปีละ 1 ครั้ง

3.6) การติดต่อกับกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน (Contact with special interest groups)

1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องติดต่อประสานงานกับกลุ่มเฉพาะ ที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อนำประสบการณ์ความรู้มาปรับปรุงพัฒนาความมั่นคงปลอดภัยสารสนเทศขององค์กร
2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องติดต่อประสานงานกับหน่วยงานภายนอกเพื่อรับการเตือนภัยการบุกรุกและแจ้งเหตุ รวมถึงการแลกเปลี่ยนข้อมูลเหตุการณ์การบุกรุกและแนวทางการป้องกัน
3) ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งภายใน และภายนอก
4) ทุกหน่วยงาน ต้องมอบหมายตัวแทนแต่ละหน่วยงาน อย่างน้อยหน่วยงานละ 1 คน เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

3.7) ข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย (Threat intelligence)

ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศต้องมีการเก็บรวบรวมและวิเคราะห์เพื่อจัดทำหรือผลิตข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

3.8) ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

ความมั่นคงปลอดภัยไซเบอร์และสารสนเทศต้องมีการบูรณาการเข้าไปกับการบริหารจัดการโครงการ โดยมีผู้จัดการโครงการ (Project Manager) เป็นผู้ดูแลรับผิดชอบทั้งหมด

3.9) การบริหารจัดการทรัพย์สิน (Asset Management)

ทรัพย์สิน หมายถึง ทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ข้อมูลซอฟต์แวร์ หรือแม้แต่อุปกรณ์ ที่เกี่ยวข้องในการประมวลผล นอกจากนี้องค์กรควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน อย่างไรก็ดีเจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว เพื่อให้มีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

3.9.1) **การจัดการบัญชีทรัพย์สิน** (Inventory of Assets)

หน่วยงานเทคโนโลยีสารสนเทศ จะต้องดำเนินการจัดทำบัญชีทะเบียนทรัพย์สินลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม ที่เกี่ยวข้องกับข้อมูลขององค์กร และข้อมูลส่วนบุคคล โดยระบุรายละเอียดต่าง ๆ ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ลงบันทึกตามแบบฟอร์มการขอใช้ทรัพย์สิน ของพนักงานที่ได้มีการอนุมัติ หน่วยงานเทคโนโลยีสารสนเทศจะทำการตรวจสอบทรัพย์สินร่วมกับผู้ถือครองทรัพย์สินในทุกหน่วยงานขององค์กร เพื่อปรับปรุงบัญชีทรัพย์สินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

3.9.2) **ผู้ถือครองทรัพย์สิน** (Ownership of Assets)

ในการจัดทำทะเบียนทรัพย์สิน แต่ละหน่วยงานจะต้องกำหนดเจ้าของทรัพย์สินที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น ๆ เจ้าของทรัพย์สินต้องสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สิน ตลอดจนการแจ้งถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินทราบ

3.10) การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable Use of Assets)

กฎเกณฑ์การใช้ อย่างเหมาะสมสำหรับการใช้งานสารสนเทศ ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการระบุจัดทำเป็นลายลักษณ์อักษร ผู้ใช้งาน พนักงาน หรือหน่วยงานภายนอกต้องยินยอมทำตามข้อกำหนดในการใช้งานข้อมูลและทรัพย์สินสารสนเทศ

3.11) การคืนทรัพย์สิน (Return of Assets)

พนักงาน และลูกจ้างของหน่วยงานภายนอกทั้งหมด ต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง โดยทรัพย์สินที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจะต้องมีการตรวจสภาพทรัพย์สินจากฝ่ายเทคโนโลยีสารสนเทศก่อน โดยลงบันทึกในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ลงบันทึกโดยใช้แบบฟอร์มการคืนทรัพย์สิน หากผลการตรวจสอบพบว่ามีความชำรุดเสียหาย หรือมีข้อมูลบางอย่างขาดหายไป ผู้ถือครองทรัพย์ต้องรับผิดชอบตามข้อกำหนดที่ได้ตกลงไว้

3.12) นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

การกำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้น และได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้นโยบายยังได้กำหนดถึงบทบาทของเจ้าของข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้องกับการจัดลำดับชั้นของข้อมูล เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

ข้อมูลสารสนเทศต้องมีการจัดชั้นความลับ โดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหว หากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศได้จัดทำเอกสารแสดงชั้นความลับสารสนเทศ เพื่อให้หน่วยงานต่าง ๆ มาลงทะเบียนเอกสารต่าง ๆ ตามลำดับชั้นที่กำหนดไว้ ดังนี้

1. **ชั้นที่ 1 ข้อมูลเปิดเผยได้** (Public)
ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย

2. **ชั้นที่ 2 ข้อมูลใช้ภายในองค์กรเท่านั้น** (Internal)
เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้พนักงานทุกคนภายในองค์กรทราบได้ หรือหากต้องการเปิดเผยต่อบุคคลภายนอกองค์กรสามารถกระทำได้ก็ต่อเมื่อเป็นบุคคลที่มีรายชื่ออยู่ในทะเบียนผู้รับสิทธิ์รับข้อมูล

3. **ชั้นที่ 3 ข้อมูลเฉพาะกลุ่ม** (Restricted)
เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิ์ความจำเป็นที่ควรทราบเพื่อให้เพียงพอต่อการปฏิบัติงาน ไม่ว่าจะเป็นการจำกัดสิทธิ์ให้พนักงานภายในองค์กรของกลุ่มธุรกิจ (HUB), ฝ่าย, แผนก, กลุ่มผู้ที่เกี่ยวข้อง หรือหากต้องการเปิดเผยต่อบุคคลภายนอกองค์กรก็สามารถกระทำได้ ก็ต่อเมื่อเป็นบุคคลที่มีรายชื่ออยู่ในทะเบียนผู้รับสิทธิ์การได้รับข้อมูล

4. **ชั้นที่ 4 ข้อมูลลับ** (Confidential)
เป็นข้อมูลที่มีผลทางธุรกิจของบริษัท เป็นข้อมูลซึ่งใช้งานโดยผู้ใช้บางกลุ่มขององค์กรเท่านั้น (ส่วนใหญ่เป็นผู้บริหาร) ไม่สามารถเปิดเผยให้พนักงานทุกคนหรือบุคคลภายนอกองค์กรทราบ ข้อมูลประเภทนี้จำเป็นต้องถูกเข้ารหัสและการเข้าถึงต้องเป็นบุคคลที่มีรายชื่ออยู่ในทะเบียนผู้รับสิทธิ์การได้รับข้อมูลเท่านั้น หากต้องการเปิดเผยต่อบุคคลภายนอกองค์กรสามารถกระทำได้ก็ต่อเมื่อเป็นบุคคลที่มีรายชื่ออยู่ในทะเบียนผู้รับสิทธิ์การได้รับข้อมูลและต้องได้รับการอนุมัติเพื่อนำไปใช้จากผู้บริหารเท่านั้น

5. **ชั้นที่ 5 ข้อมูลส่วนบุคคล** (Personal)
เป็นข้อมูลที่สามารถระบุถึงตัวตนของเจ้าของข้อมูล (Personal Identifiable Information) หรือเชื่อมโยงไปยังบุคคลนั้นได้ทั้งทางตรงและทางอ้อม ให้ใช้ภายในองค์กร ก็ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้นแล้ว ไม่สามารถเปิดเผยต่อบุคคลภายนอกก่อนได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น ๆ แล้ว

3.13) การบ่งชี้ข้อมูล (Labeling of information)

องค์กรต้องกำหนดวิธีการบ่งชี้ข้อมูลตามความเหมาะสม ที่สอดคล้องกับชั้นความลับของข้อมูล

3.14) การถ่ายโอนข้อมูล (Information transfer)

องค์กรกำหนดให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กร และ/หรือ ถ่ายโอนกับหน่วยงานนอกองค์กร

3.14.1) **นโยบายและขั้นตอนการปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ** (Information transfer policies and procedures)

หน่วยงานที่ต้องการแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานภายนอก หรือคู่ค้า ต้องปฏิบัติตามมาตรฐานฯ ให้สอดคล้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

3.14.2) **ข้อตกลงสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ** (Agreements on information transfer)

1) หน่วยงานที่ต้องการแลกเปลี่ยนข้อมูลสารสนเทศและ/หรือโปรแกรมซอฟต์แวร์ ตั้งแต่ระดับข้อมูลลับ (Confidential) ขึ้นไป ต้องตรวจสอบสิทธิ์ในการแลกเปลี่ยนข้อมูลสารสนเทศและ/หรือโปรแกรมซอฟต์แวร์กับบุคคลหรือหน่วยงานภายนอก โดยประสานงานร่วมกับหน่วยงานกฎหมาย เพื่อตรวจสอบข้อจำกัดด้านกฎหมาย ระเบียบข้อบังคับขององค์กร และต้องได้รับการพิจารณาอนุมัติจากเจ้าของข้อมูล ก่อนการแลกเปลี่ยนข้อมูลสารสนเทศและ/หรือโปรแกรมซอฟต์แวร์กับบุคคลหรือหน่วยงานภายนอก

2) หน่วยงานกฎหมาย ต้องจัดทำ/ปรับปรุงข้อตกลงหรือสัญญาการรักษาความลับ (Confidential Agreement) ให้เป็นไปตามมาตรฐานฯ ที่กำหนด

3.14.3) **การส่งข้อความทางอิเล็กทรอนิกส์** (Electronic Messaging)

สารสนเทศที่เกี่ยวข้องกับการส่งข้อความอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม โดย

1) หน่วยงานที่ดูแลระบบ ต้องพัฒนาระบบที่มีการส่งข้อมูลสารสนเทศทางอิเล็กทรอนิกส์ ให้ส่งข้อมูลสารสนเทศอย่างมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึง การเปลี่ยนแปลง และการแก้ไขข้อความอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

2) หน่วยงานที่ดูแลระบบ ต้องบริหารจัดการและควบคุมระบบงานจดหมายอิเล็กทรอนิกส์ให้สอดคล้องกับมาตรฐานฯ และกฎหมายที่เกี่ยวข้อง

3) ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้งานจดหมายอิเล็กทรอนิกส์ตามมาตรฐานฯ ที่กำหนด

3.15) การควบคุมการเข้าถึง (Access Control)

เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสมจำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็นและความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความมั่นคงปลอดภัย หน่วยงานด้านเทคโนโลยีสารสนเทศ ต้องจัดทำรายการการเข้าถึงลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ลงบันทึกโดยใช้แบบฟอร์ม ที่สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และต้องนำรายการดังกล่าว มาทบทวนตามความต้องการทางธุรกิจ และความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต และเพื่อป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิเข้าใช้งานในระดับระบบปฏิบัติการ (Operating System)

3.16) การบริหารจัดการอัตลักษณ์ (ที่ใช้ในการพิสูจน์ตัวตนเข้าระบบ) (Identity management)

วัฏจักรทั้งวงจรชีวิตของข้อมูลอัตลักษณ์ ที่เป็นส่วนหนึ่งของการพิสูจน์ตัวตนในการเข้าถึงระบบ ต้องได้รับการบริหารจัดการตลอดวงจรชีวิตของข้อมูลดังกล่าว

3.17) ข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน (Authentication information)

การจัดสรรและการบริหารจัดการข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน ต้องได้รับการควบคุมผ่านกระบวนการบริหารจัดการ ซึ่งรวมถึงการให้คำแนะนำแก่บุคลากรเกี่ยวกับการจัดการอย่างเหมาะสมสำหรับข้อมูลการพิสูจน์ตัวตนดังกล่าว

ทั้งนี้เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตและเพื่อมุ่งเน้นให้ผู้ใช้งานระบบมีความตระหนักถึงความมั่นคงปลอดภัยในการใช้งานระบบข้อมูล โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่าน และต้องทราบถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานคอมพิวเตอร์

3.17.1) **การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ** (Use of Secret Authentication Information)

ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูล การพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังต่อไปนี้

1) รหัสผ่านสำหรับการเข้าสู่ระบบถือเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสผ่านของตน ให้บุคคลอื่น

2) ผู้ใช้ต้องกำหนดและใช้รหัสผ่านที่มีประกอบด้วย ตัวเลข สัญลักษณ์ และตัวอักษร รวมกันอย่างน้อย 8 ตัวอักษร (สำหรับผู้ดูแลระบบและสำหรับระบบสารสนเทศ ต้องกำหนดรหัสผ่านแบบความมั่นคงปลอดภัยสูงและมีความยาวอย่างน้อย 14 ตัวอักษร)

3) ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ ทุก ๆ 90 วัน ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตามและผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำกับของเดิมอย่างน้อย 12 ครั้ง (ยกเว้นรหัสผ่านสำหรับ รหัสผู้ใช้ที่ใช้สำหรับระบบสารสนเทศ)

4) ผู้ใช้ต้องตรวจสอบว่าสิทธิที่ตนได้รับในการเข้าใช้ระบบเหมาะสมกับหน้าที่ที่ตนรับผิดชอบหรือไม่ ถ้าพบว่าสิทธิที่ได้รับไม่เหมาะสมต้องแจ้งผู้บังคับบัญชาให้รับทราบ เพื่อพิจารณาและปรับเปลี่ยนให้เหมาะสม

3.18) นโยบายบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต โดยลงบันทึกในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ลงบันทึกโดยอาศัยแบบฟอร์ม การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน การควบคุมสิทธิในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบเริ่มตั้งแต่การขอจดทะเบียนไปจนถึงการยกเลิกสิทธิในกรณีที่ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้อีกต่อไป รวมไปถึงการควบคุมสิทธิของผู้ใช้ ซึ่งมีสิทธิพิเศษที่สามารถแก้ไขสิทธิต่าง ๆ ของระบบได้

3.18.1) **การลงทะเบียนและการถอดถอนผู้ใช้งาน** (Account Registration and Deregistration)

กระบวนการลงทะเบียน และถอดถอนสิทธิ์ผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตาม เพื่อเป็นการให้สิทธิการเข้าถึง

1) พนักงานทุกคนที่มีสิทธิเข้าใช้งานระบบข้อมูลต้องมีรหัสผู้ใช้เฉพาะบุคคลในการเข้าสู่ระบบ

2) รหัสผู้ใช้เป็นรหัสเฉพาะบุคคล โดยไม่มีการใช้รหัสผู้ใช้ร่วมกัน (Shared User Account) ในกรณีที่พนักงานลาออกรหัสผู้ใช้รายนั้นต้องไม่ถูกนำกลับมาใช้ใหม่

3) รหัสผู้ใช้ที่ใช้สำหรับตรวจสอบหรือดูแลระบบตลอดเวลาที่จำเป็นต้องมีรหัสผู้ใช้ร่วมกัน (Shared User Account) ต้องกำหนดสิทธิต่ำที่สุด เช่น สามารถดูข้อมูลได้อย่างเดียว (Read Only)

4) รหัสผู้ใช้ที่ใช้สำหรับระบบสารสนเทศซึ่งจำเป็นต้องเปิดใช้งานตลอดเวลาและการเปลี่ยนรหัสผ่านมีผลกระทบต่อการใช้งานระบบสารสนเทศ (System/Service Account) ต้องกำหนดสิทธิ์ต่ำที่สุดตามที่มีความจำเป็นต้องใช้ และทุกครั้งที่มีการใช้รหัสผ่านในการเข้าระบบต้องทำการลงบันทึกการเข้าใช้งานทุกครั้ง

3.18.2) **การเปลี่ยนแปลงสิทธิผู้ใช้งาน** (Access Right Change)

1) ในการร้องขอเพื่อเข้าใช้งานระบบใด ๆ ผู้บังคับบัญชาในหน่วยงานต้องทำการพิจารณา เพื่อให้ความเห็นชอบ

2) หน่วยงานเจ้าของข้อมูล และหน่วยงานด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการร่วมกันในการถอดถอนสิทธิของผู้ใช้ซึ่งไม่มีความต้องการใช้ระบบอีกต่อไปโดยทันที

3.18.3) **การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน** (Review of User Access Rights)

คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานทั่วไปทุก 6 เดือน และสิทธิของผู้ดูแลระบบอย่างน้อยปีละ 1 ครั้ง โดยทางฝ่ายเทคโนโลยีสารสนเทศทำรายการข้อมูลผู้ใช้งานและสิทธิ์การเข้าใช้งานของระบบต่าง ๆ เพื่อให้ทางเจ้าของระบบงานนั้นตรวจสอบและลงนาม หากพบความผิดปกติและต้องการแก้ไขให้แจ้งทางฝ่ายเทคโนโลยีสารสนเทศเพื่อดำเนินการแก้ไขให้ถูกต้อง

3.19) นโยบายเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship Policy)

องค์กรต้องมีการกำหนดกระบวนการและขั้นตอนปฏิบัติ เพื่อบริหารจัดการความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์ และ/หรือ บริการของผู้ให้บริการภายนอก เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงให้บริการของผู้ให้บริการภายนอก และเพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอก ให้เป็นไปตามข้อตกลงที่ได้จัดทำไว้

3.19.1) **ความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ด้านความสัมพันธ์กับผู้ให้บริการภายนอก** (Cybersecurity and Information Security Policy for Supplier Relationships)

ความต้องการด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินขององค์กรโดยผู้ให้บริการภายนอก ต้องมีการกำหนดและตกลงกับผู้รับบริการและจัดทำเป็นลายลักษณ์อักษร

3.20) การระบุข้อกำหนดการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอก (Addressing information security within supplier agreements)

หน่วยงานที่มีการจ้างบุคคลหรือหน่วยงานภายนอกที่มีการเข้าถึง การประมวลผล การสื่อสาร การบริหารจัดการ ข้อมูลสารสนเทศและ/หรือระบบสารสนเทศ ต้องจัดให้บุคคลหรือหน่วยงานภายนอกที่เป็นผู้ให้บริการภายนอก ลงนามใน ข้อตกลงการรักษาความลับหรือสัญญาการไม่เปิดเผยความลับ ที่สอดคล้องกับนโยบายฯ ซึ่งรวมถึงระบุความรับผิดชอบของผู้ให้บริการภายนอก หากเกิดความเสียหายขึ้น

3.21) การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่การให้บริการและผลิตภัณฑ์ด้าน ICT (Managing information security in the information and communication technology (ICT) supply chain)

หน่วยงานที่มีการจ้างบุคคลหรือหน่วยงานภายนอกที่มีการเข้าถึง การประมวลผล การสื่อสาร การบริหารจัดการ ข้อมูลสารสนเทศและ/หรือระบบสารสนเทศ ต้องจัดทำข้อตกลงกับผู้ให้บริการภายนอก เพื่อระบุถึงความรับผิดชอบของผู้ให้บริการภายนอกในทุกกรณี เมื่อผู้ให้บริการภายนอกทำการจ้างช่วงงานต่อไปยังผู้ให้บริการรายอื่น ๆ (Supply chain)

3.22) การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services)

องค์กรต้องมีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ กรณีที่บริษัทมีการจ้างหน่วยงานภายนอกที่เกี่ยวกับการดำเนินการจัดเก็บเอกสารที่เป็นข้อมูลส่วนบุคคลของพนักงาน เช่น บริษัทรับฝากเอกสารต่าง ๆ ที่ทางบริษัทได้ใช้บริการ บริษัทจะกำหนดให้หน่วยงานที่ถูกว่าจ้างในการดำเนินการดังกล่าวให้จัดเก็บข้อมูลเป็นความลับเพื่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของพนักงานและมิให้มีการนำเอกสารดังกล่าวไปใช้นอกเหนือจากการดำเนินงานของทางบริษัทเท่านั้น โดยที่

1) ต้องมีการตรวจสอบการให้บริการจากหน่วยงานภายนอก ผู้ทำหน้าที่ตรวจสอบจำเป็นต้องมีความรู้ ความเข้าใจในเรื่องความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคล ตลอดจนเงื่อนไขและข้อตกลงต่าง ๆ

2) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการเพื่อรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมายในกรณีที่จำเป็น เช่น สัญญาการเก็บรักษาความลับ (Non-Disclosure Agreement) เป็นต้น

3) มีการตรวจประเมินผู้ให้บริการจากภายนอกทุกปี โดยจัดทำในรายงานการตรวจประเมินผู้ให้บริการภายนอก ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม

3.23) ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการ Cloud (Information security for use of cloud services)

กระบวนการสำหรับการจัดหา การใช้บริการ การบริหารจัดการ และการสิ้นสุดการใช้บริการ Cloud ต้องมีการกำหนดโดยให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

3.24) การวางแผนและการเตรียมการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ และจุดอ่อนความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคลให้ได้รับทราบ เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ และข้อมูลส่วนบุคคล

3.24.1) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

องค์กรต้องมีการกำหนดหน้าที่ความรับผิดขอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการ เพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผลและตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ โดยลงบันทึกในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้จัดทำเอกสารสำหรับการรับแจ้งปัญหาใน ฟอร์มการรับแจ้งปัญหา หรือ แจ้งเหตุเกี่ยวกับการละเมิดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Internal Privacy Policy)

3.24.2) การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

ประเด็นปัญหาต่าง ๆ ที่ได้รับแจ้ง และที่ได้ดำเนินการแก้ไขเสร็จแล้ว จะถูกนำข้อมูลดังกล่าวมาประมวลผล เพื่อสรุปออกมาเป็นรายงานตามรอบระยะเวลาที่กำหนด เพื่อแสดงให้เห็นว่าในช่วงเวลาที่ผ่านมานั้น มีปัญหาเรื่องอะไรมากที่สุด สาเหตุของปัญหาดังกล่าวเกิดจากอะไร และจะมีวิธีการป้องกันไม่ให้ปัญหานั้นเกิดขึ้นมาได้อย่างไร โดยหน่วยงานเทคโนโลยีสารสนเทศ

จะทำรายงานสรุปดังกล่าว เพื่อนำเสนอคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ เป็นประจำทุก 6 เดือน เพื่อร่วมพิจารณาปัญหาและวางแนวทางป้องกันปัญหาที่เกิดขึ้นในอนาคต

3.24.3) **การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล** (Breach Management)

เนื่องจากการรักษาความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคลของท่านเป็นสิ่งที่ทางบริษัทให้ความสำคัญอย่างสูงสุด หากเกิดเหตุละเมิดบริษัทจะแจ้งเหตุการณ์ซึ่งอาจทำให้ข้อมูลส่วนบุคคลของท่านได้รับผลกระทบ ดังรายละเอียด

- [ระบุวันที่สถานที่ที่เหตุการณ์เกิดขึ้น]
- [รายละเอียดบริษัท – รายละเอียดประเภทข้อมูลที่อาจได้รับผลกระทบ]
- [มาตรการที่บริษัทได้ทำแล้วและกำลังจะทำเพื่อลดผลกระทบ]
- [รายละเอียดอื่น ๆ ถ้ามี]

นอกจากนี้ บริษัทจะทำการแจ้งเหตุดังกล่าวไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามหน้าที่ของบริษัทในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3.25) การประเมินและตัดสินใจสำหรับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)

1) Incident Response Team (IRT) ต้องกำหนดประเภทของเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ (Information security incident category)

2) Incident Response Team (IRT) ต้องกำหนดระดับความรุนแรงของเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ (Severity level)

3) Incident Response Team (IRT) ต้องประเมินสถานการณ์เบื้องต้น โดยวิเคราะห์ขอบเขต ระดับของความรุนแรง ผลกระทบ และความเสียหายที่เกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

3.26) การรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

1) หน่วยงานที่รับผิดชอบในการแก้ไขเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ (Incident Response Team) ต้องเข้าควบคุมเหตุอย่างรวดเร็วที่สุด เพื่อให้เหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ ส่งผลกระทบต่อองค์กรน้อยที่สุด

2) Incident Response Team (IRT) รับผิดชอบในการแก้ไขเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ โดยต้องค้นหาสาเหตุ และดำเนินการแก้ไขเพื่อกำจัดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ อย่างรวดเร็วที่สุด

3.27) การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

Incident Response Team (IRT) ต้องนำเสนอข้อมูลทางสถิติ ภาพรวม แนวโน้ม สาเหตุหลัก (Root cause) ของการเกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ แนวทางการกำกับดูแลและ/หรือข้อมูลอื่นที่จำเป็นที่เกี่ยวกับเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ ต่อฝ่ายเทคโนโลยีสารสนเทศ เพื่อรับทราบสถานการณ์ของเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ และสนับสนุนการวางแผนดำเนินการแก้ไขและ/หรือวางแนวทางกำกับดูแลและ/หรือวางแนวทางตรวจสอบ เพื่อป้องกันไม่ให้เกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศแบบเดิมซ้ำอีก

3.28) การเก็บรวบรวมหลักฐาน (Collection of evidence)

Incident Response Team (IRT) ต้องจัดเก็บรวบรวมหลักฐานเบื้องต้น สำหรับเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในสถานะที่มีความน่าเชื่อถือ เพียงพอต่อการสืบค้นหาสาเหตุของการเกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ และสามารถใช้เป็นหลักฐานพยานในชั้นศาลได้

3.29) ความมั่นคงปลอดภัยสารสนเทศในช่วงที่เกิดการหยุดชะงัก (Information security during disruption)

เพื่อป้องกันและรับมือกับการหยุดชะงักของการดำเนินธุรกิจ อันเนื่องมาจากภัยคุกคามต่อการทำงานของระบบ ไม่ว่าจะด้วยอุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหายต่อองค์กรไม่มากก็น้อย ดังนั้นจึงควรจัดทำแผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (BCP) ตามเอกสาร (P-ISP-1301) เพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักขององค์กรต่อไปได้

3.29.1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

(Planning Cybersecurity and Information Security Continuity)

องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสภาพการณ์ความเสีย หายที่เกิดขึ้น เช่น ในช่วงที่เกิดภัยพิบัติ ผู้บริหารหรือหน่วยงานที่เกี่ยวข้องต้องมีการจัดการกระบวนการต่าง ๆ เพื่อพัฒนาและคงไว้ซึ่งความต่อเนื่องทางธุรกิจ การจัดการกระบวนการต่าง ๆ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจดังกล่าว ต้องคำนึงถึงสิ่งต่าง ๆ ดังต่อไปนี้

1) การวิเคราะห์และการประเมินความเสี่ยงที่กระทบต่อการดำเนินธุรกิจขององค์กร

2) การจัดทำเอกสารกลยุทธ์ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ ต้องสอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

3) การฝึกอบรมพนักงาน เพื่อให้ตระหนักถึงความมั่นคงปลอดภัย และเข้าใจในแผนฯ พร้อมทั้งสามารถปฏิบัติตามแผนฯ ได้

4) การกำหนดหน้าที่ความรับผิดชอบในการประสานงาน การพัฒนา การตรวจทาน และการปรับปรุงแผนฯ

3.30) ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)

3.30.1) การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

(Implementing Cybersecurity and Information Security Continuity)

องค์กรต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุง กระบวนการ ขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

1) มีการสื่อสารไปยังพนักงานทุกคนทราบถึงแผนการดำเนินการเมื่อเกิดเหตุฉุกเฉิน

2) แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่าง ๆ ต้องมีการทดลอง ซักซ้อม ตามระยะเวลาที่กำหนด

3) เจ้าของแผนงานและแนวทางปฏิบัติซึ่งเจ้าของแผนฯ ต้องรับผิดชอบในการบำรุงรักษา และทดสอบ พัฒนาหลักเกณฑ์ความต้องการและเงื่อนไขสำหรับการนำแผนฯ ไปใช้

3.30.2) การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

(Verify, Review and Evaluate Cybersecurity and Information Security Continuity)

องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมไว้ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้อง และได้รับผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น พื้นฐานของการจัดการเพื่อให้เกิดความต่อเนื่องในการดำเนินธุรกิจคือ เข้าใจถึงกระบวนการ และเหตุการณ์ที่สามารถก่อให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจ ดังนั้นหน่วยงานเจ้าของกระบวนการรวมถึงหน่วยงานเจ้าของระบบงานธุรกิจที่สนับสนุนกระบวนการธุรกิจนั้น ต้องเข้าร่วมในการ

ดำเนินการ ระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ตลอดจนการประเมินความเสี่ยง เพื่อให้ได้มาซึ่งข้อมูลที่ มีความถูกต้อง และครบถ้วนในการดำเนินการจัดทำแผนบริหารจัดการความต่อเนื่องทางธุรกิจในการดำเนินธุรกิจลำดับต่อไป

3.31) นโยบายความสอดคล้องด้านกฎหมายและสัญญาจ้าง
(Compliance With Legal and Contractual Requirements Policy)

เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ รวมทั้งการคุ้มครองข้อมูลส่วนบุคคล และที่เป็นความต้องการด้านความมั่นคงปลอดภัย

3.31.1) การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง
(Identification of Applicable Legislation and Contractual Requirements)

ความต้องการทั้งหมดที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง รวมทั้งวิธีการขององค์กร เพื่อให้สอดคล้องกับความต้องการดังกล่าว ต้องมีการระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัย

3.32) การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights)

สำหรับแต่ละระบบและสำหรับหน่วยงาน องค์กรกำหนดให้เอกสารสัญญาต่าง ๆ ที่มีผลเกี่ยวข้องกับกฎหมายลิขสิทธิ์ซอฟต์แวร์และสิทธิ์ในทรัพย์สินทางปัญญา (Intellectual Property Rights) ถูกจัดเก็บไว้ที่หน่วยงานสารสนเทศ โดยจะบันทึกลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้จะจัดเก็บอยู่ในแบบฟอร์ม รายการสัญญา เพื่อควบคุมจำนวนผู้ใช้งานไม่ให้เกินจำนวนลิขสิทธิ์ที่ได้รับอนุญาต และผู้ใช้งาน ต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น

3.33) การป้องกันข้อมูลบันทึก (Protection of records)

ผู้ที่มีข้อมูลบันทึก ที่เกี่ยวข้องกับกฎหมาย และข้อกำหนดทางธุรกิจ ต้องมีการจัดการ จัดเก็บ และการทำลายข้อมูลบันทึก รวมถึงการป้องกันข้อมูลบันทึกจากการสูญหาย ถูกทำลาย การปลอมแปลง และนำข้อมูลบันทึกไปใช้ผิดวัตถุประสงค์

3.34) การป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

ข้อมูลส่วนบุคคลของผู้ใช้งานและพนักงานทั้งในรูปแบบเอกสารและข้อมูลอิเล็กทรอนิกส์ ถือเป็นข้อมูลความลับ การเปิดเผย ต้องได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคลก่อนเท่านั้น

3.35) การสอบทานการรักษาความมั่นคงปลอดภัยสารสนเทศโดยหน่วยงานอิสระ
(Independent review of information security)

หน่วยงานอิสระ ต้องสอบทานการปฏิบัติตามนโยบายฯ อย่างน้อยปีละ 1 ครั้ง เพื่อสนับสนุนให้เกิดการพัฒนาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และรายงานผลการสอบทานต่อฝ่ายเทคโนโลยีสารสนเทศ

3.36) การปฏิบัติตามนโยบาย กฎเกณฑ์ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ
(Compliance with policies, rules and standards for information security)

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศอย่างสอดคล้องกับนโยบาย และขั้นตอนปฏิบัติขององค์กร

3.36.1) **ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย**

(Compliance with Security Policies and Standards)

หัวหน้าฝ่ายต่าง ๆ มีหน้าที่ต้องดำเนินการทบทวนความสอดคล้องของขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบายมาตรฐานและความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ กำหนดให้หน่วยงานความมั่นคงปลอดภัยสารสนเทศนำเสนอระบบโครงสร้างสารสนเทศระบบความมั่นคงปลอดภัยหลัก เทคโนโลยีใหม่ ๆ รวมถึงข้อมูลเชิงเทคนิค กับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ปีละ 1 ครั้ง เพื่อใช้เป็นข้อมูลในการพิจารณาความสอดคล้องกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ได้จัดทำรายการต่าง ๆ ที่จะต้องปฏิบัติไว้ในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้จะลงบันทึกไว้ในแบบฟอร์ม การทบทวนความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ เพื่อใช้เป็นตัวกลางในการตรวจสอบการทบทวนขั้นตอนต่าง ๆ ว่าได้ปฏิบัติตามครบถ้วนหรือไม่

3.36.2) **ความสอดคล้องกับกฎหมายการปกป้องข้อมูลส่วนบุคคล และ มาตรฐาน**

(Compliance with Personal Data Protection Act and Standards)

หัวหน้าฝ่ายต่าง ๆ มีหน้าที่ต้องดำเนินการทบทวนความสอดคล้องของขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบายมาตรฐานและข้อกำหนดทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง โดยคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศกำหนดให้หน่วยงานความมั่นคงปลอดภัยสารสนเทศนำเสนอระบบโครงสร้างสารสนเทศระบบความมั่นคงปลอดภัยหลัก เทคโนโลยีใหม่ ๆ รวมถึงข้อมูลเชิงเทคนิค กับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ปีละ 1 ครั้ง เพื่อใช้เป็นข้อมูลในการพิจารณาความสอดคล้องกับนโยบาย และมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ขององค์กร โดยคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศได้จัดทำรายการต่าง ๆ ที่จะต้องปฏิบัติลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้จะลงบันทึกไว้ในแบบฟอร์ม การทบทวนความมั่นคงปลอดภัยไซเบอร์สารสนเทศ เพื่อใช้เป็นตัวกลางในการตรวจสอบการทบทวนขั้นตอนต่าง ๆ ว่าได้ปฏิบัติตามครบถ้วนหรือไม่

3.37) เอกสารประกอบการปฏิบัติงาน (Documented operating procedures)

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย เพื่อทำให้เกิดการปฏิบัติงานด้านระบบประมวลผลที่มีความมั่นคงปลอดภัยและถูกต้อง ควรกำหนดหน้าที่ความรับผิดชอบ และกระบวนการด้านการจัดการและปฏิบัติงานของระบบประมวลผลที่ชัดเจน ซึ่งหน้าที่ความรับผิดชอบที่กำหนดนี้ ควรพิจารณาถึงการแบ่งแยกหน้าที่ที่เหมาะสม นอกจากกระบวนการทำงานปกติแล้ว ควรมีการกำหนดขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์กระทบความมั่นคงปลอดภัยขึ้นในระบบประมวลผล เพื่อรองรับกับเหตุการณ์ดังกล่าว

หน่วยงานที่ดูแลระบบ และหน่วยงานด้านการประมวลผลระบบสารสนเทศและเครือข่าย ต้องจัดทำ/ปรับปรุงเอกสารการปฏิบัติงาน (Operating procedure documents) ให้ถูกต้องครบถ้วนและเป็นปัจจุบันอยู่เสมอ

3.38) นโยบายการจัดการเอกสาร (Document Management Policy)

เพื่อให้พนักงานสามารถจัดการเอกสารของบริษัทซึ่งถือเป็นข้อมูลที่มีความสำคัญ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม

3.38.1) ขั้นตอนการจัดการเอกสาร และการแบ่งแยกอำนาจหน้าที่ในการจัดการเอกสาร

ในการจัดการเอกสารนั้นมีทั้งสิ้น 3 ขั้นตอน โดยเริ่มจากเจ้าของเอกสาร (Document Owner) จัดทำเอกสารฉบับร่างเสร็จสิ้นส่งไปยัง ผู้ตรวจทานเอกสาร (Document Reviewer) เมื่อแก้ไขตรวจทานเสร็จแล้ว จึงนำเสนอผู้อนุมัติเอกสาร (Document Approver) ดำเนินการอนุมัติเอกสารนั้น ๆ จากนั้นจึงสามารถนำเอกสารที่ได้รับการอนุมัติแล้วไปใช้สื่อสารหรือเผยแพร่ ทั้งภายในและภายนอกได้

การแบ่งแยกอำนาจหน้าที่ (Document Accountability List)

(1) เจ้าของเอกสาร จะต้องไม่เป็น ผู้ตรวจทานเอกสาร หรือ ผู้อนุมัติเอกสาร

(2) ผู้ตรวจทานเอกสาร จะต้องไม่เป็น เจ้าของเอกสาร แต่เป็น ผู้อนุมัติเอกสารได้

(3) ผู้อนุมัติเอกสาร จะต้องไม่เป็น เจ้าของเอกสาร แต่เป็น ผู้ตรวจทานเอกสารได้

สิทธิในการดำเนินการกับเอกสาร

- เจ้าของเอกสาร เป็นผู้ที่มีสิทธิในการกำหนดหรือปรับเปลี่ยนชั้นความลับ (Information Classification Level : ICL) ของเอกสาร
- เจ้าของเอกสารเท่านั้น ที่จะมีสิทธินำเอกสาร หรือ อนุญาตให้นำเอกสารที่ได้รับการอนุมัติแล้วนำไปสื่อสารหรือเผยแพร่ทั้งภายในและภายนอกบริษัท ตามข้อกำหนดของเอกสารในแต่ละชั้นความลับ

3.38.2) การจัดชั้นความลับของเอกสาร

(1) การจัดชั้นความลับจะต้องถูกกำหนด และฝังลงในเนื้อเอกสารในบริเวณที่เห็นได้อย่างชัดเจน เช่น หัวเอกสาร ท้ายเอกสาร ทั้งเอกสารที่อยู่ในรูปแบบกระดาษ หรือรูปแบบอิเล็กทรอนิกส์ไฟล์

(2) เอกสารที่ถูกนำออกจากระบบคอมพิวเตอร์จะต้องถูกกำหนดชั้นความลับอย่างถูกต้อง

(3) เอกสารในรูปแบบกระดาษจะต้องถูกกำหนดชั้นความลับ และจัดเก็บในสถานที่ที่ปลอดภัยและป้องกันการเข้าถึง

(4) เอกสารซึ่งที่ไม่มีการกำหนดชั้นความลับไว้ ทุกเอกสารจะถูกกำหนดชั้นความลับแบบ “ใช้ภายในองค์กรเท่านั้น (Internal)” โดยอัตโนมัติ

3.38.3) การจัดการเอกสารที่ได้รับการอนุมัติแล้ว

เอกสารควบคุม หรือเอกสารที่มีการจัดชั้นความลับ (Information Classification Level : ICL) ในระดับ ความลับ (Confidential) หรือ ข้อมูลส่วนบุคคล (Personal) และได้รับการอนุมัติแล้ว จะต้องปฏิบัติ ดังนี้

- ได้รับการตรวจทาน ปรับปรุง (เมื่อจำเป็น) ควบคุมการเปลี่ยนแปลง ควบคุมเวอร์ชันเอกสาร อนุมัติ และทำเป็นเอกสารในรูปแบบอิเล็กทรอนิกส์ไฟล์เพื่อจัดเก็บไว้ในระบบ WHA Document Management System (WHA-DMS) ก่อนที่จะถูกนำไปใช้สื่อสารหรือเผยแพร่
- ได้รับการกำหนดชั้นความลับ (ICL) อย่างชัดเจนและปกป้องดูแลตามข้อกำหนดของแต่ละชั้นความลับ
- เอกสารในรูปแบบอิเล็กทรอนิกส์จะต้องถูกจัดเก็บใน WHA-DMS เท่านั้น เพื่อให้เกิดความพร้อมในการเข้าถึงของผู้มีสิทธิเข้าถึง โดยสิทธิการเข้าถึงเอกสารจะต้องถูกกำหนดอย่างถูกต้องและเหมาะสม
- มิให้ทำสำเนาเอกสาร หรือเผยแพร่ ก่อนได้รับการอนุญาตจาก เจ้าของเอกสาร (Document Owner)
- เอกสารเวอร์ชันก่อนการปรับปรุง จะต้องถูกกำหนดสถานะเป็นยกเลิกการใช้งาน และต้องไม่สามารถนำไปใช้งานได้

3.38.4) **ประเภทเอกสารควบคุม**

เอกสารควบคุมของบริษัท มีดังต่อนี้

(1) นโยบายของบริษัท (organization policy)

(2) ข้อกำหนดการปฏิบัติงานของบริษัท (organization procedure)

(3) สัญญา (contract / agreement)

(4) บันทึกข้อตกลง (letter of engagement)

(5) โฉนดที่ดิน (land deed)

(6) ใบอนุญาต (permit)

(7) หนังสือรับรอง (certificate / license)

(8) แบบ (drawing)

(9) ขั้นตอนการทำงาน (work instruction)

(10) ฟอร์ม (form template)

หมายเหตุ

แผนกต่าง ๆ สามารถกำหนดเอกสารควบคุมของแผนกนอกเหนือไปจากรายการประเภทเอกสารควบคุมข้างต้นได้ โดยให้ใช้นโยบายการบริหารจัดการเอกสารควบคุมเดียวกันในการบริหารจัดการ

3.38.5) **การจัดการเอกสารฉบับร่าง**

เอกสารฉบับร่างทั้งหมด จะต้องปฏิบัติ ดังนี้

- ไม่ต้องจัดเก็บใน WHA-DMS
- ไม่มีผลบังคับใช้ และไม่นำถูกนำไปปฏิบัติ
- ได้รับการกำหนดชั้นความลับอย่างชัดเจนและปกป้องดูแลตามข้อกำหนดของแต่ละชั้นความลับ

3.39) การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ (Cybersecurity and Information Security Risk Management)

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศนั้น ไม่ได้เป็นความรับผิดชอบอยู่เพียงหน่วยงานเทคโนโลยีสารสนเทศเท่านั้น แต่เป็นเรื่องที่บุคลากรทุกระดับและทุกฝ่ายในองค์กร จำเป็นต้องให้ความตระหนักและมีแนวทางการบริหารความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศครอบคลุมทั้งทางด้านนโยบายและการปฏิบัติ เพื่อให้องค์กรสามารถป้องกัน ตรวจสอบ และรับมือความเสี่ยงซึ่งอาจเกิดขึ้นได้ คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ได้ออกแบบการประเมินความเสี่ยงและกระบวนการลดความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศต่าง ๆ ดังนี้

3.39.1) **การประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ** (Cybersecurity and Information Security Risk Assessment)

- บริษัทควรมีการออกแบบและดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศดังนี้
  - กำหนดเกณฑ์การยอมรับความเสี่ยง และเกณฑ์สำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

- ตรวจสอบให้มั่นใจว่าการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศให้ผลลัพธ์ที่ถูกต้อง
- ระบุความเสี่ยง:
  - ใช้กระบวนการประเมินความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องและความพร้อมใช้งานสำหรับข้อมูลและระบบสารสนเทศ
  - ระบุเจ้าของความเสี่ยง
- วิเคราะห์ความเสี่ยง:
  - ประเมินผลที่อาจเกิดขึ้นซึ่งจะเกิดขึ้นหากความเสี่ยงที่ระบุไว้ข้างต้นเกิดขึ้นจริง
  - ประเมินความเป็นไปได้ที่จะเกิดขึ้นจริงของความเสี่ยงที่ระบุไว้ข้างต้น และ
  - กำหนดระดับความเสี่ยง
- ประเมินความเสี่ยง:
  - เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดไว้ข้างต้น และ
  - จัดลำดับความสำคัญของความเสี่ยงที่วิเคราะห์ไว้สำหรับการรักษาความเสี่ยง

- บริษัทควรดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศตามช่วงเวลาที่วางแผนไว้ หรือเมื่อมีการเสนอหรือเกิดการเปลี่ยนแปลงที่สำคัญโดยคำนึงถึงเกณฑ์ความเสี่ยงที่กำหนดไว้ข้างต้นที่กำหนดไว้
- การประเมินความเสี่ยงจะต้องคำนึงถึงช่องโหว่ แหล่งที่มาของภัยคุกคามและการควบคุม ความมั่นคงปลอดภัยที่วางแผนไว้หรือในสถานที่เพื่อกำหนดระดับผลลัพธ์ของความเสี่ยงที่เหลือที่เกิดขึ้นกับการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคลตามการดำเนินงาน

3.39.2) **การลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ** (Cybersecurity and Information Security Risk Treatment)

- บริษัทควรมีการออกแบบและดำเนินการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศดังนี้
  - กำหนดความมั่นคงปลอดภัยไซเบอร์และสารสนเทศที่เหมาะสม โดยคำนึงจากผลการประเมินความเสี่ยง เช่น
    - สร้างระบบหรือกระบวนการควบคุมที่เหมาะสมเพื่อลดความเสี่ยง
    - ลดความเสี่ยงด้วยการหลีกเลี่ยง ป้องกัน หรือไม่อนุญาตให้มีการดำเนินการรวมถึงสถานการณ์ที่อาจก่อให้เกิดความเสี่ยงขึ้นได้
    - โอนหรือกระจายความเสี่ยงไปยังผู้อื่น เช่น ประกัน หรือ คู่ค้าทางธุรกิจ (ในสัญญา)
    - มีกระบวนการในการยอมรับความเสี่ยง หากมีความเสี่ยงที่บริษัทยอมรับได้อย่างชัดเจน
  - กำหนดแผนการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ และดำเนินการตามที่ได้กำหนดไว้

แผนการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ควรได้รับการอนุมัติอย่างเป็นทางการจากคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

4) มาตรการด้านบุคลากร (People controls)

เพื่อเป็นแนวทางการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการทรัพยากรบุคคลตั้งแต่ การรับเข้าทำงานจนถึงการเลิกจ้าง เพราะกระบวนการด้านทรัพยากรบุคคลจึงมีความจำเป็นในการช่วยทำให้สารสนเทศขององค์กรมีความมั่นคงปลอดภัย

เพื่อลดความเสี่ยงของสารสนเทศที่เกิดจากบุคลากร ทั้งที่เกิดจากการละเมิดความมั่นคงปลอดภัยสารสนเทศโดยเจตนาและไม่ได้เจตนา หรือจากการละเลยต่อการปฏิบัติหน้าที่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

เพื่อเพิ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการบุคลากรที่กำลังจะเลิกจ้าง โดยระบุหน้าที่ความรับผิดชอบและบทบาทของผู้เกี่ยวข้องกับกระบวนการ นอกจากนี้ยังเป็นการควบคุมความมั่นคงปลอดภัยสารสนเทศให้ดียิ่งขึ้น และเพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

<u>เนื้อหานโยบาย และการดำเนินการ</u>

4.1) การคัดเลือก (Screening)

การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการโดยมี ความสอดคล้องกับกฎหมาย และระเบียบข้อบังคับโดยหน่วยงานทรัพยากรบุคคลต้องตรวจสอบประวัติของบุคคลก่อนที่จะทำการว่าจ้าง เช่น หลักฐานการศึกษา บุคคลอ้างอิงประวัติการทำงานจากหน่วยงานต้นสังกัดเดิม และเอกสารที่ทางราชการออกให้ เป็นต้น โดยเฉพาะตำแหน่งงานที่เกี่ยวข้องกับข้อมูลสำคัญขององค์กร จะต้องมีการตรวจสอบเป็นพิเศษ

4.2) ข้อตกลง และเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

ข้อตกลง และเงื่อนไขในสัญญาจ้างกับพนักงาน มีการระบุถึงหน้าที่ความรับผิดชอบ (Job Description) ที่ชัดเจน และระบุถึงความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ การฝ่าฝืนหรือละเลยต่อหน้าที่และนโยบายถือว่ามีความผิด ต้องพิจารณาตามบทลงโทษขององค์กร ซึ่งขึ้นอยู่กับความรุนแรงของผลกระทบที่เกิดขึ้นกับองค์กร

4.3) การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ (Cybersecurity and Information Security Awareness, Education and Training)

ฝ่ายทรัพยากรบุคคลจัดให้พนักงานทุกคน ต้องเข้ารับฟังการอบรมจากหน่วยงานด้านเทคโนโลยีสารสนเทศหรือจากหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยไซเบอร์และสารสนเทศเพิ่ม และมีการประเมินผล อย่างน้อยปีละ 1 ครั้ง เพื่อรับทราบถึงนโยบายความมั่นคงปลอดภัยเพิ่มเติมขององค์กร เหตุการณ์ละเมิดความมั่นคงปลอดภัย และกรณีศึกษาใหม่ ๆ ในขณะที่หน่วยงานด้านเทคโนโลยีสารสนเทศจะต้องได้รับการฝึกอบรมจากหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง

4.4) กระบวนการทางวินัย (Disciplinary Process)

กระบวนการทางวินัยต้องกำหนดอย่างเป็นทางการ พนักงานทุกคนต้องรับทราบกระบวนการทางวินัยผ่านทางระบบสารสนเทศของบริษัทที่มีความน่าเชื่อถือ หรือในกรณีที่ไม่สามารถดำเนินการผ่านระบบสารสนเทศได้ พนักงานสามารถรับทราบผ่านระบบสารสนเทศ หรือ ลงลายมือชื่อรับทราบ ระเบียบว่าด้วยการใช้ ระบบสารสนเทศขององค์กรอย่างปลอดภัย ที่หน่วยงานทรัพยากรบุคคล ซึ่งกระบวนการทางวินัยที่กำหนดขึ้นนี้ เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยหน่วยงานทรัพยากรบุคคล และหน่วยงานด้านกฎหมายต้องกำหนดบทลงโทษสำหรับพนักงาน ซึ่งละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง

4.5) ความรับผิดชอบภายหลังการสิ้นสุด หรือการเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)

หน่วยงานทรัพยากรบุคคลและหน่วยงานต่าง ๆ ร่วมกันกำหนดขั้นตอนการปฏิบัติ ของพนักงานที่ออกจากองค์กร เมื่อสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อมีการเปลี่ยนการจ้างงาน ดังนี้

1) หน่วยงานที่เกี่ยวข้อง มีหน้าที่แจ้งไปยังหน่วยงานทรัพยากรบุคคล ถึงเรื่องการลาออก หรือการปรับเปลี่ยนตำแหน่งของพนักงาน

2) หน่วยงานทรัพยากรบุคคล ปฏิบัติตามนโยบายการบริหารจัดการการเข้าถึงของผู้ใช้ ข้อที่ 3.18 ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม โดยต้องแจ้งหน่วยงานด้านเทคโนโลยีสารสนเทศทราบทันที ที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานขององค์กรเพื่อทำการถอดถอนสิทธิ์การเข้าใช้ระบบงานต่าง ๆ และการเข้า-ออกพื้นที่ขององค์กร

3) หน่วยงานด้านเทคโนโลยีสารสนเทศปฏิบัติตามหัวข้อ การคืนทรัพย์สิน ข้อที่ 3.11 ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม โดยทำการตรวจสอบทรัพย์สินของพนักงาน และรายงานผลการตรวจสอบกลับมายังหน่วยงานทรัพยากรบุคคล

4) หน่วยงานด้านเทคโนโลยีสารสนเทศ ทำการสำรองข้อมูลที่จำเป็นของพนักงานดังกล่าวเป็นระยะเวลา 1 ปี และแจ้งให้หัวหน้าหน่วยงานที่เกี่ยวข้องทราบถึงวิธีเข้าถึงข้อมูลดังกล่าว

4.6) ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or nondisclosure agreements)

องค์กรต้องจัดทำและทบทวนเพื่อปรับปรุงข้อตกลงการรักษาความลับหรือสัญญาการไม่เปิดเผยความลับให้สอดคล้องกับนโยบายฯ ขององค์กร สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

4.7) การปฏิบัติงานจากระยะไกล (Remote working)

เป็นมาตรการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกล ต้องมีการนำมาใช้เพื่อป้องกันข้อมูลที่มีการเข้าถึง การประมวลผล หรือการจัดเก็บจากสถานที่ดังกล่าว

1) มีการระบุอย่างชัดเจนว่า ใครสามารถที่จะ Remote เข้ามาทำงานได้

2) กรณีที่ต้องให้ หน่วยงานภายนอก Remote เข้ามาต้องมี การบันทึก และมีการเฝ้าดู การทำงานตลอดเวลา และมีการเปลี่ยนแปลง Password ในการเข้าใช้ของหน่วยงานภายนอกทุกครั้ง หรือมีการกำหนด Expired User/Password หรือตามความจำเป็นของงาน

3) มีการกำหนด Session Timeout กรณีที่ผู้ Remote เข้ามาปล่อยหน้าจอทิ้งไว้

4) จัดทำบันทึกการเชื่อมต่อระยะไกลในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถดำเนินการได้ให้บันทึกในรายการเชื่อมต่อระยะไกล ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม

4.8) การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

ในกรณีที่พนักงานพบจุดอ่อนหรือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ พนักงานมีหน้าที่แจ้งให้หน่วยงานที่รับแจ้งเหตุการณ์ผิดปกติ รับทราบ เพื่อให้เกิดการแก้ไขป้องกันก่อนเหตุการณ์ผิดปกติจะเกิดขึ้น

5) มาตรการทางกายภาพ (Physical controls)

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงานที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในองค์กร และกำหนดมาตรการป้องกันที่เหมะสมตามระดับของความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศขององค์กรขั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับการอนุญาต ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามและการรบกวนไม่ว่าโดยตั้งใจหรือจากภัยธรรมชาติ

เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินการขององค์กร อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายถือว่าเป็นอุปกรณ์ที่สำคัญต่อสารสนเทศ และการดำเนินธุรกิจ ดังนั้น อุปกรณ์เหล่านี้ควรมีการป้องกันอันตรายจากสภาพแวดล้อม รวมถึงการจำกัดการนำอุปกรณ์ดังกล่าวไปใช้นอกสถานที่

<u>เนื้อหานโยบาย และการดำเนินการ</u>

5.1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

หน่วยงานได้จัดหาที่ตั้งห้อง Server ที่มีสภาพแวดล้อมภายนอกปลอดภัยจากภัยคุกคามภายนอก คือ อยู่ในสถานที่ ๆ เข้าถึงได้โดยยากจากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้ พื้นที่โดยรอบโปร่ง และสามารถมองเห็นได้ชัดหากมีการเข้าถึงห้อง Server

5.2) การควบคุมการเข้าออกทางกายภาพ (Physical entry)

หน่วยงานที่ดูแลพื้นที่ ต้องควบคุมการเข้า-ออกทางกายภาพของพื้นที่ที่กำหนดให้เป็นพื้นที่ควบคุมพิเศษ เช่น ห้อง Server โดยอนุญาตให้บุคคลผ่านเข้า-ออกพื้นที่ควบคุมพิเศษได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

ต้องมีการจัดเตรียมอุปกรณ์รักษาความมั่นคงปลอดภัยในการเข้าถึงห้อง Server ดังนี้

1) มีการติดตั้งกล้องวงจรปิด และบันทึกภาพภายในห้องตลอดเวลา โดยสามารถดูข้อมูลย้อนหลังได้ 60 วัน

2) ห้องระบบคอมพิวเตอร์และศูนย์คอมพิวเตอร์ (ห้อง Server หรือ Data Center) เป็นห้องที่มีกุญแจล็อค หรือมีระบบแตะบัตร (Key Card) หรือมีระบบที่สามารถตรวจสอบการระบุตัวตน ซึ่งจำกัดสิทธิการเข้าถึงเฉพาะผู้ที่ได้รับการอนุญาตเท่านั้น

5.3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing Office, Room and Facilities)

องค์กรต้องมีการออกแบบและการปฏิบัติใช้งาน การรักษาความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และห้องอุปกรณ์ต่าง ๆ เพื่อให้เกิดการป้องกันพื้นที่เหล่านี้จากภัยคุกคามต่าง ๆ อย่างเป็นรูปธรรม เช่น การกำหนดสิทธิ์คนเข้า-ออกให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น การติดตั้งระบบปรับอากาศ ระบบไฟส่องสว่าง ระบบดับเพลิง เป็นต้น

5.4) การเฝ้าระวังด้านความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)

ศูนย์คอมพิวเตอร์ พื้นที่ในสำนักงาน ห้องทำงาน และห้องอุปกรณ์ต่าง ๆ ควรได้รับการตรวจสอบโดยระบบเฝ้าระวัง ซึ่งอาจรวมถึงการใช้เจ้าหน้าที่รักษาความมั่นคงปลอดภัย ระบบสัญญาณเตือนภัยเมื่อมีผู้บุกรุก และการติดตั้งกล้อง CCTV เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

5.5) การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environmental Threats)

การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ ดังนี้

1) ศูนย์คอมพิวเตอร์ ต้องมีระบบป้องกันอัคคีภัย ระบบปรับอากาศและความชื้น ระบบกระแสไฟฟ้า

2) เครื่องปรับอากาศ ต้องมี 2 ชุดทำงานสลับกัน โดยตั้งความเย็นอยู่ที่ 20-23 องศาเซลเซียส และมีความชื้นอยู่ที่ 40-50%

3) ไม่ควรจัดเก็บอุปกรณ์ที่เป็นเชื้อเพลิง หรือวัตถุอันตรายไว้ในศูนย์คอมพิวเตอร์

4) ต้องติดตั้งอุปกรณ์ตรวจจับน้ำรั่วซึม (Water Leak Detector) สำหรับพื้นที่ที่มีความเสี่ยงในศูนย์คอมพิวเตอร์

5) ต้องติดตั้งอุปกรณ์ป้องกันภัยที่เกิดจากสัตว์จำพวก นก หนู แมลง หรือสัตว์เลื้อยคลาน สำหรับพื้นที่ที่มีความเสี่ยงในเรื่องนี้

5.6) การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

1) หน่วยงานที่ดูแลพื้นที่ ควรจัดทำคู่มือ และ/หรือ แสดงให้เห็นถึงมาตรการควบคุมการปฏิบัติงานในพื้นที่ที่ต้องควบคุมความมั่นคงปลอดภัย รวมทั้งต้องประชาสัมพันธ์มาตรการควบคุมการปฏิบัติงานในพื้นที่ที่ต้องควบคุมความมั่นคงปลอดภัย ให้ผู้ที่เกี่ยวข้อง สามารถปฏิบัติงานได้อย่างถูกต้อง

2) ผู้ที่ปฏิบัติงานในพื้นที่ที่ต้องควบคุมความมั่นคงปลอดภัย ต้องติดบัตรอนุญาต และ/หรือ บัตรพนักงานให้เห็นอย่างชัดเจนตลอดเวลาเมื่ออยู่ในพื้นที่

3) ผู้ที่ปฏิบัติงานในพื้นที่ที่ต้องควบคุมความมั่นคงปลอดภัย ต้องบันทึกข้อมูลการเข้า-ออกทุกครั้งที่ผ่านเข้า-ออกพื้นที่

4) ผู้ที่ปฏิบัติงานในพื้นที่ที่ต้องควบคุมความมั่นคงปลอดภัย ต้องไม่นำผู้ที่ไม่เกี่ยวข้องกับการปฏิบัติงานเข้ามาในพื้นที่

5) ผู้ที่ปฏิบัติงานในพื้นที่ที่ต้องควบคุมความมั่นคงปลอดภัย ต้องไม่นำอุปกรณ์คอมพิวเตอร์ และ/หรือ อุปกรณ์เครือข่ายที่ไม่ใช่ทรัพย์สินขององค์กรมาเชื่อมต่อกับระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต

5.7) โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen)

1) ผู้ใช้งานต้องไม่วางเอกสารสำคัญทิ้งไว้บนโต๊ะทำงาน โดยปราศจากการดูแลอย่างใกล้ชิด

2) ผู้ใช้งานต้องเก็บเอกสารสำคัญไว้อย่างมั่นคงปลอดภัย ทุกครั้งเมื่อไม่ได้ใช้งาน เพื่อป้องกันการสูญหาย หรือการใช้งานจากผู้ที่ไม่ได้รับอนุญาต เช่น เก็บเอกสารสำคัญไว้ในตู้เอกสารที่สามารถล็อคกุญแจได้ทุกครั้ง เมื่อไม่ได้ใช้งานแล้ว เป็นต้น

3) ผู้ใช้งาน ต้องออกจากระบบ และล็อคจอภาพคอมพิวเตอร์ด้วยรหัสผ่านทุกครั้ง เมื่อไม่ได้ใช้งานแล้ว เพื่อป้องกันการใช้งานจากผู้ที่ไม่ได้รับอนุญาต

5.8) การจัดวางและป้องกันอุปกรณ์ (Equipment siting and protection)

1) หน่วยงานที่ดูแลพื้นที่ ต้องควบคุมดูแล ให้อุปกรณ์สารสนเทศที่สำคัญ ถูกติดตั้งอยู่ในสถานที่ที่สามารถป้องกันการเข้าถึงอุปกรณ์สารสนเทศจากผู้ที่ไม่ได้รับอนุญาต

2) หน่วยงานที่ดูแลพื้นที่ ต้องควบคุมดูแล ให้อุปกรณ์สารสนเทศที่สำคัญ ถูกติดตั้งอยู่ในสถานที่ที่สามารถป้องกันความเสียหายจากภัยธรรมชาติ การถูกขโมย ไฟฟ้าดับ ไฟไหม้ และภัยจากมนุษย์

5.9) ความมั่นคงปลอดภัยของทรัพย์สินที่มีการใช้งานนอกองค์กร (Security of assets off-premises)

ผู้ถือครองทรัพย์สิน ต้องมีมาตรการป้องกันอุปกรณ์ต่าง ๆ ก่อนที่จะนำอุปกรณ์ออกไปใช้งานภายนอกองค์กร โดยอุปกรณ์เหล่านั้นต้องได้รับการอนุมัติก่อนนำไปติดตั้ง และ/หรือ ใช้งานภายนอกองค์กร

5.10) นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling Policy)

เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล (Hard Copy และ Electronics) เพื่อป้องกันความเสียหายต่อการดำเนินธุรกิจ อันเนื่องมาจากความเสียหายของสื่อบันทึกข้อมูลต่าง ๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม

5.10.1) การบริหารจัดการสื่อบันทึกข้อมูล (Management of Media)

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธี หรือ ขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์การกำหนดไว้

1) สื่อบันทึกข้อมูลต้องตั้งชื่อตามที่กำหนด และต้องมีทะเบียนควบคุมการใช้งาน
2) การเบิกและจ่ายสื่อบันทึกข้อมูลจะต้องผ่านการอนุมัติจากผู้มีอำนาจของหน่วยงานผู้ใช้
3) สื่อบันทึกข้อมูลต้องมีการตรวจนับอย่างน้อยปีละ 1 ครั้ง

5.10.2) การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

5.11) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้องได้รับการป้องกันการล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ

1) อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สำคัญต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน (UPS) เพื่อให้ระบบทำงานต่อเนื่องหรือสิ้นสุดการทำงานอย่างเหมาะสม เมื่อระบบไฟฟ้าขัดข้อง

2) ต้องทำการตรวจสอบอุปกรณ์สำรองไฟฟ้าฉุกเฉินตามขั้นตอนของผู้ผลิตอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าวสามารถรองรับการทำงานได้เมื่อเกิดปัญหาไฟฟ้าขัดข้อง

5.12) ความมั่นคงปลอดภัยของสายสัญญาณ (Cabling security)

องค์กรต้องควบคุมให้การเดินสายไฟฟ้าและสายสัญญาณเป็นไปตามมาตรฐานฯ ที่กำหนด สายไฟฟ้าและสายสัญญาณ ควรเดินแยกออกจากกันอย่างเป็นระเบียบ ไม่เดินสายปะปนกัน เพื่อป้องกันการรบกวนสัญญาณ

5.13) การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

ผู้ถือครองทรัพย์สิน ต้องบำรุงรักษาอุปกรณ์ เพื่อให้มีความพร้อมใช้งาน ตามรอบระยะเวลาที่กำหนด

5.14) ความมั่นคงปลอดภัยสำหรับการจำหน่ายออกหรือการทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

เพื่อให้มั่นใจว่าข้อมูลสารสนเทศและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทำลายอย่างถาวรก่อนนำอุปกรณ์นั้นกลับมาใช้งานใหม่ หรือก่อนการทิ้ง/บริจาคอุปกรณ์ อุปกรณ์และสื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ

1)ข้อมูลลำดับชั้นลับหรือ ข้อมูลส่วนบุคคล ที่อยู่ในรูปเอกสารที่ต้องการทำลาย ต้องทำลายโดยการเข้าเครื่องย่อยกระดาษ เผาทำลาย หรือ ด้วยวิธีการอื่นที่จะไม่สามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้

2)การทำลายอุปกรณ์และสื่อบันทึกข้อมูลที่บันทึกข้อมูลลำดับชั้นลับ หรือ ข้อมูลส่วนบุคคล ต้องได้รับการอนุมัติจากผู้มีอำนาจและต้องมีการบันทึกการทำลายทุกครั้ง เพื่อเป็นหลักฐานในการตรวจสอบในภายหน้า

6) มาตรการทางเทคโนโลยี (Technological controls)

เนื้อหานโยบาย และการดำเนินการ

6.1) อุปกรณ์ปลายทางของผู้ใช้งาน (User end point devices)

ข้อมูลที่มีการจัดเก็บไว้ มีการประมวลผล หรือมีการเข้าถึงโดยอุปกรณ์ปลายทางของผู้ใช้งาน ต้องได้รับการป้องกัน (อุปกรณ์ปลายทางของผู้ใช้งานนี้ โดยทั่วไปหมายรวมถึง เครื่องคอมพิวเตอร์ โน้ตบุ๊ค โทรศัพท์มือถือ แท็บเล็ต และอุปกรณ์ที่สามารถประมวลผลข้อมูลอื่น ๆ โดยอุปกรณ์เหล่านี้สามารถติดต่อสื่อสารถ่ายโอนข้อมูลกันผ่านทางเครือข่ายได้)

6.1.1) อุปกรณ์พกพา (Mobile Device)

องค์กรได้กำหนดมาตรการควบคุมการนำอุปกรณ์พกพา (Mobile Device) มาใช้งานเกี่ยวกับข้อมูลขององค์กรให้เป็นไปอย่างปลอดภัย โดยผู้ใช้อุปกรณ์พกพานั้นมีหน้าที่ที่ต้องปฏิบัติ ดังต่อไปนี้

1) ผู้ใช้สามารถลงทะเบียนการใช้งานอุปกรณ์พกพาโดยการใช้รหัสผู้ใช้และรหัสผ่านเพื่อลงทะเบียนเข้าใช้งาน โดยหน่วยงานเทคโนโลยีสารสนเทศ (IT) ต้องมีการกำหนดสิทธิ์และรูปแบบในการเข้าถึงข้อมูลเพื่อให้มีความมั่นคงปลอดภัยทางไซเบอร์และข้อมูลส่วนบุคคล

2) ต้องให้หน่วยงานเทคโนโลยีสารสนเทศติดตั้งโปรแกรมตามความจำเป็น เพื่อเข้าถึงข้อมูล หรือระบบงานที่ได้รับความเห็นชอบจากผู้บังคับบัญชาตามสังกัดของผู้ใช้นั้น โดยคำถึงนึงความมั่นคงปลอดภัยทางไซเบอร์และข้อมูลส่วนบุคคลเป็นสำคัญ

3) เจ้าหน้าที่หน่วยงานสารสนเทศจะต้องมีระบบการตรวจสอบอุปกรณ์พกพาที่มีการลงทะเบียนเข้าใช้งาน และมีระบบป้องกันการบุกรุกโจมตีจากบุคคลภายนอก

6.2) สิทธิการเข้าถึงในระดับพิเศษ (Privileged access rights)

ผู้ดูแลบัญชีรหัสผู้ใช้งานที่มีสิทธิพิเศษ อย่างเช่น administrator หรือ root ต้องมีการควบคุมการใช้งานบัญชีรหัสผู้ใช้งานที่มีสิทธิพิเศษของระบบปฏิบัติการ ให้มีการร้องขอและอนุมัติ ก่อนการใช้งาน และมีการตรวจสอบบันทึกเหตุการณ์การใช้งาน (Log) หลังจากใช้งานเรียบร้อยแล้ว เพื่อให้มั่นใจว่า การใช้งานบัญชีรหัสผู้ใช้งานที่มีสิทธิพิเศษนั้น เป็นไปตามกิจกรรมที่ได้รับการอนุมัติเท่านั้น

6.3) การจัดการเข้าถึงสารสนเทศ (Information Access Restriction)

การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ผู้ดูแลระบบต้องจัดการให้ระบบแสดงข้อความเตือนถึง “**การอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าใช้งาน**” ก่อนที่จะทำการเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ขององค์กร และระบบต้องเปิดโอกาสให้ผู้ใช้สามารถยกเลิกการเชื่อมต่อเข้าสู่ระบบในกรณีที่ทราบว่าระบบนั้น ๆ ไม่ได้เกี่ยวข้องกับตนเอง

1) ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้ (User Account) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้ แต่ละคนได้

2) รหัสผู้ใช้ที่ใช้สำหรับตรวจสอบหรือดูแลระบบตลอดเวลาที่จำเป็นต้องมีรหัสผู้ใช้ร่วมกัน (Shared User Account) ต้องกำหนดสิทธิต่ำที่สุด เช่น สามารถดูข้อมูลได้อย่างเดียว (Read Only) และต้องระบุผู้ใช้งานเฉพาะกลุ่ม

3) รหัสผู้ใช้ที่ใช้สำหรับระบบสารสนเทศซึ่งจำเป็นต้องเปิดใช้งานตลอดเวลาและการเปลี่ยนรหัสผ่านมีผลกระทบต่อการใช้งานระบบสารสนเทศ (System/Service Account) เจ้าของระบบต้องทำการตั้งรหัสผ่านซึ่งมีความมั่นคงปลอดภัยสูง (Strong

Password) หลังจากติดตั้งระบบสารสนเทศเรียบร้อยแล้วต้องทำการเก็บบันทึกรหัสผ่านส่งให้ทางผู้ดูแลระบบ และในการใช้รหัสผ่านในการเข้าระบบต้องมีการตรวจสอบและลงบันทึกการเข้าใช้งานทุกครั้ง

4) ผู้ใช้ควรออกจากระบบเครือข่าย (Log-off) ทันที เมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก

5) ผู้ใช้ถูกติดตั้งโปรแกรมถนอมหน้าจอ (Screen Saver) ที่มีรหัสผ่านบนเครื่องคอมพิวเตอร์ โดยโปรแกรมเหล่านี้จะเริ่มทำงานหลังจากไม่มีการใช้งานใด ๆ บนเครื่องคอมพิวเตอร์นั้น ๆ ตามเวลาที่กำหนดไว้

6) หากไม่มีการใช้งานเป็นเวลานาน ผู้ใช้ต้องปิดเครื่องคอมพิวเตอร์ หรือเครื่องปลายทางให้เรียบร้อย

6.4) การจำกัดการเข้าถึงซอร์สโค้ด (Access to source code)

1) หน่วยงานที่ดูแลระบบ ต้องกำหนดสิทธิ์ในการเข้าถึงโปรแกรมต้นฉบับ (Source code) โดยให้เข้าถึงได้เท่าที่จำเป็นสำหรับผู้ที่มีหน้าที่ในการปฏิบัติงานเท่านั้น รวมถึงปรับปรุงรายชื่อผู้ใช้งานและสิทธิ์การใช้งาน ให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

2) หน่วยงานที่ดูแลระบบการจัดเก็บโปรแกรมต้นฉบับ ต้องจัดให้มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ที่แสดงการเข้าถึงโปรแกรมต้นฉบับให้เพียงพอในการตรวจสอบ การเข้าถึง การเปลี่ยนแปลง และการแก้ไขโปรแกรมต้นฉบับ

6.5) การพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย (Secure authentication)

องค์กรต้องมีการใช้เทคโนโลยีและขั้นตอนปฏิบัติสำหรับการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย เพื่อจำกัดการเข้าถึงข้อมูล ให้สอดคล้องตามนโยบายที่เกี่ยวข้องกับการควบคุมการเข้าถึง

ในกรณีที่มีการใช้งานระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง (Critical Information Systems) องค์กรควรพิจารณายกระดับของการพิสูจน์ตัวตนให้มีความมั่นคงปลอดภัยที่สูงขึ้น ด้วยการพิสูจน์ตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication) ซึ่งเป็นกระบวนการเข้าสู่ระบบเทคโนโลยีสารสนเทศแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้งานต้องป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน

6.6) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

การใช้ทรัพยากรของระบบต้องมีการติดต่อ ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ หน่วยงานเทคโนโลยีสารสนเทศ จึงได้จัดทำแผนแม่แบบเทคโนโลยีสารสนเทศ (IT Master Plan) ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม เพื่อทำให้เกิดความมั่นใจว่าสารสนเทศขององค์กร และข้อมูลส่วนบุคคล มีความมั่นคงปลอดภัย และสามารถเข้าถึงและใช้งานได้ตามสิทธิ์โดยง่าย มีการจัดเตรียมซอฟต์แวร์คอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่คอยสนับสนุนการทำงานของหน่วยงานต่าง ๆ ตามแผนกลยุทธ์ภาพรวมองค์กร

6.7) นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware Policy)

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ และข้อมูลส่วนบุคคล ได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี เพื่อควบคุม และป้องกัน ซอฟต์แวร์ และข้อมูลจากโปรแกรมที่ไม่ประสงค์ดีและซอฟต์แวร์อันตราย

6.7.1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against Malware)

มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักให้แก่ผู้ใช้งานที่เหมาะสม

1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกัน Virus Version ล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่อง Server โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา

2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้โปรแกรมค้นหา Virus ทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย

3) ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ดาวน์โหลดมาจากอินเทอร์เน็ตมีการตรวจหา Virus ก่อนนำไปใช้งาน

4) ห้ามพนักงานดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนา Virus หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

5) ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้น ต้องตรวจสอบ Virus คอมพิวเตอร์ก่อนใช้งานทุกครั้ง

6.8) นโยบายการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management Policy)

เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

6.8.1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิค จุดอ่อนต่อช่องโหว่ขององค์กร มีการเก็บรวบรวม การประเมินและเตรียมมาตรการที่เหมาะสม ต้องถูกนำมาใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง โดยช่องโหว่ทั้งหมดจะถูกจัดเก็บไว้ที่เอกสารช่องโหว่ทางเทคนิคลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม และช่องโหว่ทั้งหมดจะถูกนำมาทวนสอบกับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศอย่างน้อยปีละ 1 ครั้ง

6.9) การบริหารจัดการการตั้งค่าระบบ (Configuration Management)

เพื่อให้แน่ใจว่าฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่าย ทำงานอย่างถูกต้องด้วยการตั้งค่าความมั่นคงปลอดภัยที่จำเป็น และการกำหนดค่าจะไม่ถูกแก้ไขโดยการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตหรือไม่ถูกต้อง องค์กรควรกำหนดกระบวนการและเครื่องมือเพื่อบังคับใช้ในการกำหนดการตั้งค่าความมั่นคงปลอดภัยไว้

6.10) การลบข้อมูล (Information deletion)

องค์กรกำหนดให้ข้อมูลที่มีการจัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือบนสื่อบันทึกข้อมูลอื่น ๆ ต้องถูกลบทำลายด้วยวิธีการที่มีความมั่นคงปลอดภัย (Secure delete) เมื่อข้อมูลนั้นไม่มีความจำเป็นในการใช้งานอีกต่อไป

6.11) การปิดบังข้อมูล (Data masking)

เพื่อลดการเปิดเผยของข้อมูลอ่อนไหวซึ่งรวมถึงข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมาย ข้อบังคับ กฎระเบียบ และข้อตกลงในสัญญาที่เกี่ยวข้อง

องค์กรต้องมีการนำเทคนิคการปิดบังข้อมูลมาใช้งาน เพื่อไม่ให้ข้อมูลที่จัดเก็บไว้ในระบบสารสนเทศถูกมองเห็น หรือถูกนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาต โดยปฏิบัติใช้ให้เป็นไปตามความต้องการทางธุรกิจ สอดคล้องตามนโยบายการควบคุมการเข้าถึงระบบสารสนเทศขององค์กร และกฎหมายที่เกี่ยวข้อง

6.12) การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)

องค์กรต้องมีการนำมาตรการการป้องกันการรั่วไหลของข้อมูล มาประยุกต์ใช้กับระบบ เครือข่าย และอุปกรณ์ต่าง ๆ ที่มีการประมวลผล จัดเก็บ หรือรับ-ส่งข้อมูลสำคัญ

6.13) นโยบายการสำรองข้อมูล (Backup Policy)

เพื่อป้องกันการสูญหายของข้อมูล เพื่อให้อุปกรณ์ประมวลผลสารสนเทศถูกต้องสมบูรณ์และพร้อมใช้งานเสมอ

6.13.1) **การสำรองข้อมูล** (Information Backup)

ข้อมูลสำหรับสารสนเทศ และข้อมูลส่วนบุคคล ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการดำเนินการสำรองไว้ และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอ ตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้

1) มีการจัดเตรียมแผนการสำรองข้อมูล และทดสอบกู้คืนระบบ/ข้อมูลใน แผนสำรองข้อมูล และแผนทดสอบการกู้คืนลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม และมีการปรับปรุงทบทวนแผนการสำรองข้อมูลทุกปี

2) จัดทำคู่มือที่ใช้ในการสำรองข้อมูล รวมถึงกู้คืนระบบและข้อมูลกับระบบสำคัญต่าง ๆ ทั้งหมด โดยจัดทำอยู่ใน คู่มือการสำรองและกู้คืนข้อมูล ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม

3) หน่วยงานเทคโนโลยีสารสนเทศ ทำตรวจสอบการสำรองข้อมูลในระบบทุกวันที่มีการสำรองข้อมูล ว่ามีสถานะเป็นอย่างไร พร้อมทั้งทันกับสถานการณ์สำรองข้อมูลลงในรายการสถานการณ์สำรองข้อมูล ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม ในกรณีที่ใช้บริการจากหน่วยงานภายนอกซึ่งหน่วยงานเทคโนโลยีสารสนเทศไม่สามารถตรวจสอบการสำรองข้อมูลในระบบได้ หน่วยงานจากภายนอกต้องส่งข้อมูลรายการสถานการณ์สำรองข้อมูลให้หน่วยงานเทคโนโลยีสารสนเทศทราบทุกวันที่มีการสำรองข้อมูล และหน่วยงานจากภายนอกต้องทำสรุปสถานการณ์สำรองข้อมูลจัดส่งให้กับทางหน่วยงานเทคโนโลยีสารสนเทศอย่างน้อยเดือนละ 1 ครั้ง

4) หน่วยงานเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการดำเนินการทดสอบกู้ข้อมูลสำรองในทุกระบบที่มีความสำคัญ โดยระบบที่สำคัญต้องมีการทดสอบตามแผนการกู้คืน พร้อมทั้งสรุปเป็นรายงานเพื่อแจ้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศตามรอบระยะเวลาที่กำหนด

5) คอมพิวเตอร์ส่วนบุคคล ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลไฟล์ที่สำคัญ

6.14) นโยบายการเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies Policy)

เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

6.14.1) **สภาพพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ** (Availability of Information Processing Facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

6.15) นโยบายการบันทึกข้อมูลล็อก และการเฝ้าระวัง (Logging and Monitoring Policy)

เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

6.15.1) **การบันทึกข้อมูลล็อก แสดงเหตุการณ์** (Event Logging)

ข้อมูล Log แสดงเหตุการณ์ ซึ่งบันทึกกิจกรรมของผู้ใช้งาน ครอบคลุมถึงการเข้าถึงข้อมูลการทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บ และทบทวนอย่างสม่ำเสมอ อุปกรณ์บันทึกข้อมูล Log จะได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไข และการเข้าถึงโดยไม่ได้รับอนุญาต

6.16) การเฝ้าระวัง การตอบสนอง และการปรับปรุงการทำงานของระบบและอุปกรณ์ (Monitoring, Responding, and Improving Information Security System)

องค์กรต้องมีการเฝ้าระวังการทำงานของเครือข่าย ระบบ และแอปพลิเคชัน เพื่อตรวจหาพฤติกรรมที่ผิดปกติ และดำเนินการประเมินความเป็นไปได้ของภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น

6.16.1) การติดตามการทำงานของเครื่องแม่ข่าย (Server Monitor)

องค์กรต้องมีการจัดทำรายงานสถานการณ์ทำงานของเครื่องแม่ข่ายต่าง ๆ รวมถึงอุปกรณ์รอบข้างที่จำเป็น เป็นประจำทุกวัน โดยผู้ปฏิบัติจะทำการบันทึกสถานการณ์การทำงานต่าง ๆ ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถบันทึกลงในระบบสารสนเทศได้ให้บันทึกลงในรายการสถานการณ์ทำงานของคอมพิวเตอร์ แม่ข่าย และมีการจัดทำรายงานสรุปสถานการณ์ทำงานของเครื่อง Server ให้กับทางผู้บริหารให้ทราบเป็นประจำทุก 6 เดือน

6.16.2) การตรวจสอบรายการการใช้งานเครือข่าย (Network Monitoring)

หน่วยงานสารสนเทศต้องตรวจสอบการใช้งานเครือข่ายขององค์กร และจัดทำรายงานสรุปการใช้งานเครือข่าย ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม เพื่อนำเสนอต่อคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศตามรอบระยะเวลาที่กำหนด

6.16.3) การตอบสนองต่อภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องตอบสนองและจัดการกับภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบจากกิจกรรมการเฝ้าระวังอย่างทันท่วงที โดยทีมงานด้านความปลอดภัยสารสนเทศ หรือ Incident Response Team (IRT) ต้องเป็นผู้รับผิดชอบในการดำเนินการแก้ไขอย่างมีประสิทธิภาพเพื่อขจัดภัยคุกคามหรือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศดังกล่าว

6.16.4) การปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องปรับปรุงและอัปเดตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อให้สามารถรับมือกับภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้นได้ โดยต้องทำให้มั่นใจได้ว่าระบบฯ มีความแข็งแกร่ง มีความทันสมัย และสามารถลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ได้อย่างมีประสิทธิภาพ

6.17) การตั้งนาฬิกาให้ถูกต้องตรงกัน (Clock Synchronization)

หน่วยงานที่ดูแลระบบ ต้องควบคุมดูแลการตั้งเวลาของระบบสารสนเทศให้ตรงกันตามมาตรฐานฯ ที่กำหนด และสอดคล้องตามข้อกำหนดทางด้านกฎหมายหรือระเบียบปฏิบัติที่เกี่ยวข้อง

6.18) การใช้โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิในระดับพิเศษ (Use of privileged utility programs)

1) หน่วยงานที่ดูแลระบบ ควรจำกัดผู้ใช้งาน และจำกัดสิทธิ์การใช้โปรแกรมอรรถประโยชน์ (System utilities) บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้สามารถใช้งานได้ตามความจำเป็นเท่านั้น

2) หน่วยงานที่ดูแลเครื่องคอมพิวเตอร์ผู้ใช้งาน ควรจำกัดผู้ใช้งาน และจำกัดสิทธิการใช้ โปรแกรมอรรถประโยชน์ บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน (Client) ให้สามารถใช้งานได้ตามความจำเป็นเท่านั้น

6.19) นโยบายการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software Policy)

เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

6.19.1) การติดตั้งซอฟต์แวร์ระบบให้บริการ (Installation of Software on Operational Systems)

ซอฟต์แวร์คอมพิวเตอร์ทุกเครื่อง จะถูกติดตั้งโดย หน่วยงานเทคโนโลยีสารสนเทศเท่านั้น โดยมีการตรวจสอบตามข้อกำหนดเรื่อง การบริหารจัดการทรัพย์สิน (Asset Management)

6.20) นโยบายบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management Policy)

เพื่อให้มีการป้องกันสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ เพื่อทำให้ระบบเครือข่ายมีความมั่นคงปลอดภัย และสามารถใช้เป็นสื่อในการรับส่งข้อมูลต่าง ๆ ได้อย่างมีประสิทธิภาพ

6.20.1) มาตรการเครือข่าย (Network Controls)

เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่าง ๆ หัวหน้าหน่วยงานควบคุมระบบเครือข่าย ต้องรับผิดชอบในการจัดให้มีการควบคุมการปฏิบัติการด้านเครือข่าย ดังต่อไปนี้

1) กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร (Network Configuration) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สายที่ใช้ในการสื่อสารของเครือข่ายทั้งหมดอย่างชัดเจน โดยจัดทำและปรับปรุงแผนภาพเครือข่าย ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม ให้ทันสมัยอยู่เสมอ

2) จัดให้มีการควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่จัดไว้

3) มีมาตรการในการควบคุมดูแลสภาพและประเมินประสิทธิภาพการใช้งานของคู่สาย สายสื่อสารและอุปกรณ์ในเครือข่ายสื่อสาร เพื่อให้พร้อมใช้งานตลอดเวลา

4) บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

5) ประเมินประสิทธิภาพของระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และวางแผนในการปรับปรุงระบบเครือข่ายให้สามารถรองรับปริมาณงานที่จะขยายตัวในอนาคต

6.21) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าบริการเหล่านี้จะมีการให้บริการโดยองค์กรเอง หรือจ้างการให้ บริการก็ตาม ผู้ให้บริการทางเครือข่าย ต้องได้รับการตรวจสอบ และวิเคราะห์ในเรื่องระดับการให้บริการ รูปแบบความมั่นคงปลอดภัยของเครือข่าย การจัดการความต้องการขององค์กร

6.22) การแบ่งแยกเครือข่าย (Segregation in networks)

หน่วยงานที่ดูแลระบบเครือข่าย ต้องแบ่งแยกเครือข่าย ตามกลุ่มที่กำหนด เช่น กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน กลุ่มผู้บริหาร กลุ่มผู้ดูแลระบบ เป็นต้น

6.23) การคัดกรองเว็บ (Web filtering)

องค์กรกำหนดให้การเข้าถึงเว็บไซต์ภายนอกต้องได้รับการบริหารจัดการ เพื่อลดโอกาสการเข้าถึงเนื้อหาที่เป็นอันตราย เช่น โปรแกรมไม่ประสงค์ดี ซอฟต์แวร์ที่เป็นอันตรายต่าง ๆ ที่อาจสร้างความเสียหายให้แก่ข้อมูลและเครื่องคอมพิวเตอร์ขององค์กรได้ในลักษณะใดลักษณะหนึ่ง

6.24) นโยบายมาตรการเข้ารหัสข้อมูล (Cryptographic Controls Policy)

เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และป้องกันความลับการปลอมแปลง หรือความถูกต้องของสารสนเทศเพื่อรักษาความมั่นคงปลอดภัยของข้อมูล ข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่มีความอ่อนไหว ทั้งในด้านความลับและความถูกต้องของข้อมูลจำเป็นต้องพิจารณาถึงการนำซอฟต์แวร์และเทคนิคต่าง ๆ มาให้ในการเข้ารหัสข้อมูลที่มีความเสี่ยงสูงและต้องการปกป้องสูง

6.24.1) **การใช้มาตรการเข้ารหัสข้อมูล** (Use of Cryptographic Controls)

นโยบายการใช้มาตรการเข้ารหัสข้อมูล เพื่อป้องกันสารสนเทศต้องมีการจัดทำและปฏิบัติตาม

1) รหัสผ่านต่าง ๆ ที่เก็บอยู่ในระบบฐานข้อมูล จะถูกเข้ารหัสไว้ เจ้าของรหัส รวมถึงซอฟต์แวร์เจ้าของข้อมูลเท่านั้นที่ทราบรหัสผ่านดังกล่าว

2) รหัสผ่านต่าง ๆ ที่เก็บอยู่ในระบบฐานข้อมูลส่วนบุคคล จะถูกเข้ารหัสไว้ เจ้าของรหัสรวมถึงซอฟต์แวร์เจ้าของข้อมูลเท่านั้นที่ทราบรหัสผ่านดังกล่าว

3) ในการรับส่ง Email ได้ทำการเปิดใช้งานการเข้ารหัส (Encryption) โดยทำการเข้ารหัสตามความจำเป็น

6.25) วัฏจักรการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development life cycle)

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบ และดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ โดยที่

1) ต้องมีการผนวกการรักษาความมั่นคงปลอดภัยเข้าเป็นส่วนหนึ่งของวงจรการพัฒนาระบบสารสนเทศ (Security embedded into SDLC) โดยกำหนดกิจกรรมด้านการวิเคราะห์ วางแผน และ/หรือสร้างมาตรการรักษาความมั่นคงปลอดภัยในแต่ละระยะ (Phase) ของวงจรการพัฒนาระบบสารสนเทศ

2) ต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่ต้องการพัฒนา ได้แก่

2.1) การตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input data validation)

หน่วยงานเจ้าของระบบ ต้องพัฒนาระบบสารสนเทศให้มีการตรวจสอบความถูกต้องของข้อมูลนำเข้าตามมาตรฐานฯ ที่กำหนด เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องครบถ้วนก่อนนำเข้าสู่ระบบสารสนเทศ

2.2) การตรวจสอบความถูกต้องของการประมวลผล (Control of internal processing)

หน่วยงานเจ้าของระบบต้องพัฒนาระบบสารสนเทศให้มีการควบคุมการประมวลผล ตามมาตรฐานฯ ที่กำหนด เพื่อป้องกันการแก้ไข และ/หรือเปลี่ยนแปลงข้อมูลสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต

2.3) การตรวจสอบความถูกต้องของข้อความ (Message integrity)

หน่วยงานเจ้าของระบบ ต้องพัฒนาระบบสารสนเทศให้มีการตรวจสอบความถูกต้องของข้อความที่รับส่งในระบบสารสนเทศ หรือระหว่างระบบสารสนเทศ เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง รวมทั้งควบคุม เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความ/ข้อมูลสารสนเทศ โดยผู้ที่ไม่ได้รับอนุญาต

2.4) การตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ (Output data validation)

หน่วยงานเจ้าของระบบ ต้องพัฒนาระบบสารสนเทศให้มีการควบคุม และตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ ให้เป็นไปตามมาตรฐานฯ ที่กำหนด เพื่อให้มั่นใจว่าผลลัพธ์ของการประมวลผล มีความถูกต้อง รวมทั้งควรจัดเก็บบันทึกเหตุการณ์ที่มาของข้อมูลผลลัพธ์ (Result logging) อย่างเพียงพอต่อการตรวจสอบในกรณีเกิดเหตุการณ์ที่ส่งผลต่อความมั่นคงปลอดภัยสารสนเทศ

3) สำหรับระบบสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ (เช่น อินเทอร์เน็ต) หน่วยงานเจ้าของระบบควรทำการประเมินความเสี่ยง และวางแผนแก้ไขความเสี่ยง

4) ควรใช้หลักการออกแบบระบบสารสนเทศโดยคำนึงถึงความมั่นคงปลอดภัย (Secure Software Development Principles)

5) การพัฒนาซอฟต์แวร์ต้องใช้วิธีการที่มีความมั่นคงปลอดภัย

6) ในระหว่างการออกแบบและการพัฒนาระบบสารสนเทศ ต้องมีการกำหนดจุดตรวจสอบด้านความมั่นคงปลอดภัย (Security Checkpoint) เพื่อตรวจสอบให้มั่นใจว่ามาตรการการรักษาความมั่นคงปลอดภัย (Controls) จะถูกพัฒนาขึ้นเพื่อตอบสนองต่อความต้องการด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น ดำเนินการทบทวน Source Code (Security Code Review) ก่อนเข้าสู่กระบวนการทดสอบซอฟต์แวร์

7) ปัญหาที่พบในขั้นตอนการพัฒนาซึ่งอาจส่งผลต่อความมั่นคงปลอดภัย ต้องถูกแจ้งไปยังผู้จัดการโครงการ หรือหัวหน้างาน และต้องได้รับการแก้ไขและจดบันทึกไว้ทุกกรณี

8) หน่วยงานเจ้าของระบบและผู้พัฒนาระบบสารสนเทศควรได้รับการฝึกอบรมความรู้ด้านการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย และ/ หรือความรู้เกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ เป็นประจำทุกปี

6.26) ความต้องการด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application security requirements)

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศ และความเป็นข้อมูลส่วนบุคคล เป็นองค์ประกอบสำคัญหนึ่งของระบบ ตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย เพื่อให้มั่นใจได้ว่าการพัฒนาระบบงาน ได้คำนึงถึงความมั่นคงปลอดภัยและการควบคุมที่เพียงพอ องค์กรต้องมีการกำหนดให้มีการพิจารณาถึงความต้องการด้านความมั่นคงปลอดภัยของระบบงาน และความเป็นข้อมูลส่วนบุคคล ก่อนที่จะมีการพัฒนาระบบงาน รวมถึงการกำหนดให้มีควบคุมภายในของระบบงาน

6.26.1) การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ต้องมีการรวมเข้ากับความต้องการสำหรับระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้ว

1) เจ้าของระบบงานธุรกิจ ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องบันทึกลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้จัดทำเป็นเอกสาร ฟอร์มร้องขอพัฒนาโปรแกรม ลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน

2) ความต้องการที่เกิดขึ้นจะต้องได้รับการอนุมัติจากผู้บังคับบัญชาของผู้ร้องขอก่อนส่งมายังหน่วยงานเทคโนโลยีสารสนเทศ เพื่อพิจารณาความเป็นไปได้ ในการพัฒนาหรือไม่

6.27) สถาปัตยกรรมของระบบที่มีความมั่นคงปลอดภัยและหลักการวิศวกรรมระบบ (Secure system architecture and engineering principles)

องค์กรต้องกำหนดหลักการวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure System Engineering Principles) ขึ้นเพื่อให้ระบบสารสนเทศมีความน่าเชื่อถือ มีระดับของการรักษาความมั่นคงปลอดภัยที่เหมาะสม และสามารถตอบสนองต่อความต้องการทางธุรกิจขององค์กรได้

หลักการดังกล่าวต้องได้รับการนำไปใช้งานร่วมกับวงจรการพัฒนาระบบสารสนเทศขององค์กร (SDLC) และประกอบด้วยประเด็นพื้นฐานที่ต้องได้รับการพิจารณาในระหว่างการออกแบบ สร้าง และ/หรือพัฒนาระบบสารสนเทศ ดังต่อไปนี้

1) **การออกแบบระบบสารสนเทศให้มีความมั่นคงปลอดภัย** (Security by design)

มาตรการรักษาความมั่นคงปลอดภัย ต้องได้รับการพิจารณาและกำหนดตั้งแต่ช่วงแรกของการระบุความต้องการในการพัฒนาระบบสารสนเทศ (Requirements Development Phase) และถือเป็นส่วนหนึ่งของการออกแบบระบบสารสนเทศในภาพรวม ในกรณีที่มีการปรับเปลี่ยนความต้องการของระบบสารสนเทศ ต้องมีการพิจารณาปรับเปลี่ยนหรือเพิ่มเติมมาตรการรักษาความมั่นคงปลอดภัยให้มีความสอดคล้องกับความต้องการที่เปลี่ยนแปลงไปเสมอ

2) **การสร้างสมดุลระหว่างความเสี่ยงและมาตรการรักษาความมั่นคงปลอดภัย** (Balance risk and control)

มาตรการรักษาความมั่นคงปลอดภัยที่เลือกใช้ต้องมีประสิทธิผลที่เหมาะสมกับความเสี่ยง ค่าใช้จ่าย วัตถุประสงค์ทางธุรกิจ และประสิทธิผลของการใช้งานระบบสารสนเทศ เพื่อป้องกันปัญหาการเลือกใช้งานมาตรการรักษาความมั่นคงปลอดภัยที่ไม่มั่นคงปลอดภัย เช่น เข้มงวดน้อยเกินไป หรือเข้มงวดมากเกินความจำเป็น จนทำให้เกิดค่าใช้จ่ายที่สูงเกินกว่าประโยชน์ที่จะได้รับ

3) **ความเหมาะสมในการใช้งานและการบริหารจัดการ** (Usability and manageability)

มาตรการรักษาความมั่นคงปลอดภัยต้องได้รับการออกแบบให้ใช้งานง่ายและไม่เป็นภาระต่อผู้ใช้งานมากเกินไป การบริหารจัดการมาตรการรักษาความมั่นคงปลอดภัย (เช่น การแก้ไขค่าการปรับแต่ง) ต้องไม่ซับซ้อนเกินความจำเป็นจนอาจก่อให้เกิดข้อผิดพลาด (Human error) ได้โดยง่าย

4) **การใช้มาตรการรักษาความมั่นคงปลอดภัยหลายชั้น** (Defense-in-depth)

ควรมีการวางมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศไว้หลายชั้น (Multi-layered) โดยครอบคลุมมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical) และทางตรรกะ (Logical) ทั้งในระดับระบบปฏิบัติการ ฐานข้อมูล แอปพลิเคชัน และระบบเครือข่าย เพื่อให้สามารถทำงานสอดประสานและทดแทนกันได้ ในเวลาที่มาตรการใดมาตรการหนึ่งทำงานผิดพลาดหรือถูกข้ามผ่านได้

5) **การลดความซับซ้อน** (Simplicity)

ระบบสารสนเทศต้องได้รับการออกแบบให้มีความซับซ้อนน้อยที่สุด เพื่อลดองค์ประกอบที่ไม่จำเป็น ลดข้อผิดพลาดที่อาจเกิดขึ้น และลดโอกาสในการถูกโจมตีโดยผู้ที่ไม่ประสงค์ดี

6) **การสร้างความสามารถในการต้านทานภัยคุกคามและการฟื้นคืนสภาพ** (Resilience and Recoverability)

ระบบต้องได้รับการออกแบบให้มีความสามารถในการต้านทานภัยคุกคาม เช่น เมื่อมาตรการรักษาความมั่นคงปลอดภัยทำงานผิดพลาดหรือถูกข้ามผ่าน ระบบต้องจำกัดหรือปฏิเสธการเข้าใช้งาน ไม่ใช่ยอมให้เข้าใช้งานได้) และมีความสามารถในการฟื้นคืนสภาพ (Recoverability) (โดยอัตโนมัติ หรือโดยการสร้างกระบวนการกู้คืน) ภายในระยะเวลาที่เหมาะสมกับความต้องการทางธุรกิจ

7) **การปกป้องข้อมูล** (Confidentiality and integrity)

ต้องมีการสร้างมาตรการรักษาความมั่นคงปลอดภัยเพื่อปกป้องความลับและความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูลสารสนเทศ ทั้งในระหว่างการประมวลผล การรับ-ส่ง และการจัดเก็บข้อมูลสารสนเทศ

8) **การบังคับใช้นโยบาย** (Enforced policy)

มาตรการรักษาความมั่นคงปลอดภัยต้องได้รับการออกแบบเพื่อบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนขั้นตอนปฏิบัติงาน มาตรฐาน หรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องขององค์กร

9) **การออกแบบระบบสารสนเทศเพื่อรับมือต่อผู้ที่ไม่ประสงค์ดี หรือ การใช้งานในสภาพแวดล้อมที่ไม่พึงประสงค์** (Design for malicious actor/environment)

ต้องมีการออกแบบมาตรการรักษาความมั่นคงปลอดภัยเชิงป้องกัน ตรวจจับ และกู้คืน โดยพิจารณาในมุมมองของผู้ที่ไม่ประสงค์ดีที่ไม่ได้อยู่ภายใต้กรอบของนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร หรือพยายามข้ามผ่านมาตรการรักษาความมั่นคงปลอดภัยที่มีอยู่ และต้องสร้างมาตรการรักษาความมั่นคงปลอดภัยในกรณีที่จำเป็นต้องใช้งานระบบสารสนเทศในสภาพแวดล้อมที่ไม่พึงประสงค์ เช่น การใช้งานระบบในระหว่างเกิดเหตุฉุกเฉิน หรือ เกิดภัยพิบัติ

10) **การออกแบบระบบสารสนเทศเพื่อรองรับการใช้งานแบบโมบาย** (Mobility)

ต้องมีการออกแบบหรือปรับแต่งมาตรการรักษาความมั่นคงปลอดภัยให้เหมาะสม สำหรับระบบสารสนเทศที่ให้บริการหรือทำงานร่วมกับอุปกรณ์โมบาย โดยคำนึงถึงความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง เช่น การควบคุมความมั่นคงปลอดภัยทางกายภาพ การใช้งานอุปกรณ์โมบายที่เป็นทรัพย์สินส่วนบุคคล การใช้งานเครือข่าย การใช้งานโมบายแอปพลิเคชัน การแลกเปลี่ยนข้อมูลสารสนเทศ การใช้งานฟังก์ชันด้านการระบุตำแหน่งที่อยู่

6.28) การเขียนโปรแกรมให้มีความมั่นคงปลอดภัย (Secure Coding)

องค์กรต้องนำหลักการการเขียนโปรแกรมให้มีความมั่นคงปลอดภัย มาปฏิบัติกับการพัฒนาซอฟต์แวร์

6.29) การทดสอบด้านความมั่นคงปลอดภัยในการพัฒนาและรับรองระบบ (Security testing in development and acceptance)

แผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการจัดทำสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชันใหม่

1) กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูล ผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์

2) ผู้ร้องขอจะต้องเป็นผู้ทดสอบ และตรวจรับระบบในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ลงบันทึกในฟอร์มร้องขอพัฒนาโปรแกรม

6.30) การพัฒนาระบบโดยหน่วยงานภายนอก (Outsourced development)

หน่วยงานที่จ้างหน่วยงานภายนอก ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยของซอฟต์แวร์ และควบคุมให้หน่วยงานภายนอกพัฒนาซอฟต์แวร์ ให้เป็นไปตามมาตรฐานฯ ที่กำหนด

6.31) การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกัน เพื่อลดความเสี่ยงของการเข้าถึง หรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

1) ในการพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ ในการพัฒนา (Development System) และระบบที่ใช้งานจริง (Production System)

2) ต้องไม่นำข้อมูลส่วนบุคคลมาใช้ทดสอบระบบงาน ก่อนได้รับความยินยอมจากเจ้าของข้อมูล

3) ต้องไม่นำข้อมูลลับหรือข้อมูลที่มีความอ่อนไหวมาใช้ทดสอบระบบงาน หากมีความจำเป็น ต้องทำการปิดบังข้อมูล (masking data) ก่อนที่จะนำมาใช้ทดสอบระบบงาน

4) ต้องไม่มีการติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาโปรแกรมอื่น ๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง

6.32) การบริหารจัดการการเปลี่ยนแปลง (Change management)

การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบ มีการควบคุมโดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ โดยหน่วยงานเทคโนโลยีสารสนเทศ จะทำการลงบันทึกการเปลี่ยนแปลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้จะทำการปรับปรุงเอกสารการควบคุมเวอร์ชันของระบบลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม

6.33) ข้อมูลสำหรับการทดสอบ (Test information)

เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

6.33.1) **การป้องกันข้อมูลสำหรับการทดสอบระบบสารสนเทศ** (Protection of test data)

1) หน่วยงานที่ทดสอบระบบ และหน่วยงานที่พัฒนาระบบ ต้องได้รับอนุมัติจากเจ้าของข้อมูล ก่อนนำข้อมูลในระบบสารสนเทศที่ให้บริการจริงมาใช้ในการทดสอบระบบสารสนเทศ

2) หน่วยงานที่ทดสอบระบบ และหน่วยงานที่พัฒนาระบบ ต้องแปลงข้อมูลความลับ จากระบบสารสนเทศที่ให้บริการจริงก่อนนำมาใช้ทดสอบ และทำลายข้อมูลสารสนเทศที่ใช้ทดสอบ หลังสิ้นสุดการทดสอบ เพื่อป้องกันข้อมูลความลับจากระบบที่ให้บริการจริงรั่วไหลระหว่างทดสอบระบบสารสนเทศ

3) หน่วยงานที่ดูแลระบบ ควรควบคุมการเข้าถึงเครื่องทดสอบให้มีความมั่นคงปลอดภัยเทียบเท่ากับระบบสารสนเทศที่ให้บริการจริง

6.34) การป้องกันระบบสารสนเทศในช่วงที่มีการทดสอบระบบโดยผู้ตรวจประเมิน (Protection of information systems during audit testing)

เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินระบบให้บริการ

6.34.1) **มาตรการตรวจประเมินระบบ** (Information Systems Audit Controls)

ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการต้องมีการวางแผนและตกลงร่วมกันอย่างระมัดระวัง เพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ หน่วยงานเทคโนโลยีสารสนเทศ จะทำการกำหนดแผนการประเมินระบบสำคัญต่าง ๆ ไว้ในรายการตรวจประเมินระบบลงในระบบสารสนเทศ หรือในกรณีที่ไม่สามารถลงบันทึกในระบบสารสนเทศได้ให้ดำเนินการตามแบบฟอร์ม และนำผลการตรวจประเมินเสนอคณะกรรมการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ตามรอบระยะเวลาที่กำหนด

- END OF DOCUMENT -