การเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยให้กับข้อมูลส่วนบุคคล

กชิภัท รนิตรนาคุณ

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒

บรรยายโดย กษิภัท ธนิตธนาคุณ

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

หน้า ๑๒
เล่ม ๑๓๗ ตอนพิเศษ ๑๖๔ ง ราชกิจจานุเบกษา ๑๗ กรกฎาคม ๒๕๖๓

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

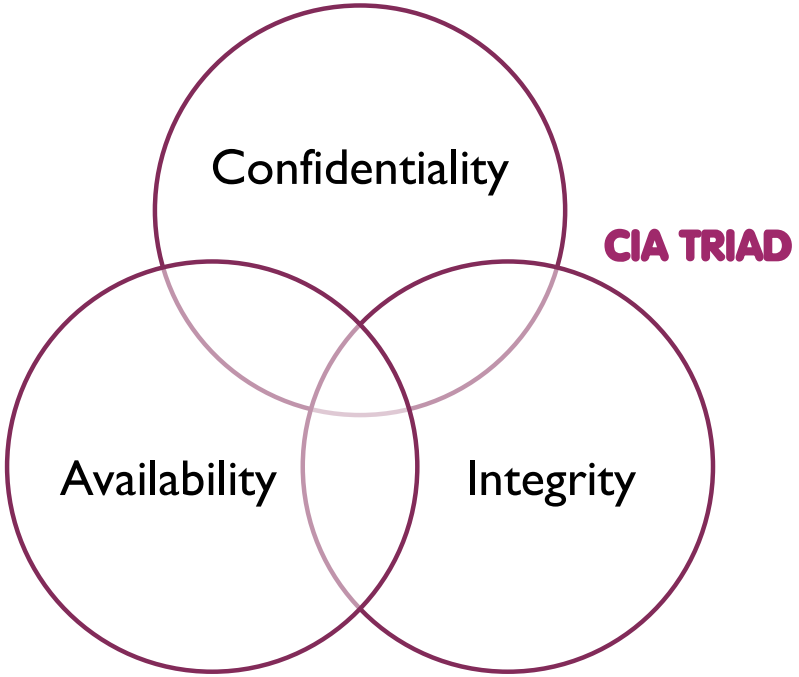
หน้า ๑๐
เล่ม ๑๓๘ ตอนพิเศษ ๑๑๑ ง ราชกิจจานุเบกษา ๒๔ พฤษภาคม ๒๕๖๔

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (ฉบับที่ ๒) พ.ศ. ๒๕๖๔

บรรยายโดย กษิภัท ธนิตธนาคุณ

“ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ



CIA TRIAD

Guideline on Personal Data Classification

Source: Thailand Data Protection Guidelines 3.0

(1) [Data Policy] การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล

(2) [Data Discovery] การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล

(3) [Data Proliferation] การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย

(4) [Data Risk Level] การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆ

(5) [Data Protection] มีมาตรการคุ้มครองข้อมูลส่วนบุคคล

บรรยายโดย กษิภัท ธนิตธนาคุณ

สรุปกระบวนการการสร้างความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

Risk Assessment

ตัวอย่าง เกณฑ์การประเมินความเสี่ยง

เกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria)

1. เกณฑ์การประมาณระดับความเสียหาย (Impact Level)

ระดับค่า	ผลกระทบ	
	ต่อการเงิน	ลูกค้าและชื่อเสียงของสำนักฯ
5=Very High	มากกว่า 10,0000,000 บาท	ลูกค้าได้รับผลกระทบหรือความเสียหายอย่างวงกว้าง จนอาจมีการเผยแพร่ในสื่อต่าง ๆ
4=High	5,000,001-10,000,000 บาท	ลูกค้าได้รับผลกระทบโดยตรง ได้รับความเสียหาย อาจมีการขอยกเลิกการใช้บริการ ร้องเรียน หรือ เรียกร้องความเสียหาย
3=Medium	2,000,001-5,000,000 บาท	ลูกค้าบางรายการอาจได้รับผลกระทบเล็กน้อย อาจไม่พอใจต่อการบริการและมีการเผยแพร่ข่าวในวงจำกัด
2=Low	1,000,001-2,00,000 บาท	ลูกค้าอาจได้รับผลกระทบเล็กน้อยจากการให้บริการที่ล่าช้าหรือหยุดชะงัก
1=Very Low	น้อยกว่า 1,000,000 บาท	ไม่มีผลกระทบต่อลูกค้า แต่อาจทำให้งานภายในหน่วยงานล่าช้าหรือหยุดชะงัก

2. เกณฑ์การประมาณโอกาสเกิดของเหตุการณ์ (Likelihood)

ระดับค่า	ความหมาย	ความหมาย
5=Extremely	เกิดขึ้นอย่างน้อย 1 ครั้ง ต่อสัปดาห์	Weekly
4=Likely	เกิดขึ้นอย่างน้อย 1 ครั้ง ต่อเดือน	Monthly
3=Possible	เกิดขึ้นอย่างน้อย 1 ครั้ง ต่อไตรมาส	Quarterly
2=Unlikely	เกิดขึ้นอย่างน้อย 1 ครั้ง ภายใน 6 เดือน	Half-Yearly
1=Rarely	ในรอบ 1 ปี อาจจะเกิด 1 ครั้ง	Yearly

เกณฑ์การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยง (RISK LEVEL)		โอกาสที่จะเกิด (LIKELIHOOD)				
		1	2	3	4	5
ผลกระทบ (IMPACT)	5 : VH	M5	H10	E15	E20	E25
	4 : H	M4	M8	H12	E16	E20
	3 : M	L3	M6	H9	H12	E15
	2 : L	L2	M4	M6	M8	H10
	1 : VL	L1	L2	L3	M4	M5

บรรยายโดย กษิภัท ธนิตธนาคุณ

ตัวอย่าง การประเมินความเสี่ยง

ลำดับ	สินทรัพย์ (Asset)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	ผลกระทบต่อธุรกิจ (Impact)	โอกาสเกิดเหตุการณ์ (Probability)	ระดับความเสี่ยง (Risk Level)	การตัดสินใจดำเนินการ (Risk Control)	เลือกมาตรการควบคุม (Control Selection)	แผนการลดความเสี่ยง (Risk Treatment Action Plan)	ระดับความเสียหายหลังทำการลดความเสี่ยง (Exposure)	โอกาสเกิดเหตุการณ์หลังทำการลดความเสี่ยง (Probability)	ระดับความเสี่ยงที่หลงเหลือ (Residual Risk)
1	ข้อมูลนักศึกษา(SIF)	T038 การขโมยสื่อบันทึกข้อมูลหรือเอกสาร (Theft of Media or Documents)	V040 ไม่มีการควบคุมการเข้าถึงสิทธิ์	5=Very High	5=Extremely	25	ควบคุมความเสี่ยง	1. กำหนดนโยบายการควบคุมการเข้าถึง (Access Control Policy) 2. กำหนดมาตรฐานการกำหนดรหัสผ่าน 3. จัดทำ User Authorization Matrix 4. สอบทานบัญชีผู้ใช้งานและสิทธิ์ทุกไตรมาส 5. เปิด Security Log และสอบทานเป็นประจำ	RPT#1	5=Extremely	1=Rarely	5
2	ข้อมูลนักศึกษา(SIF)	T038 การขโมยสื่อบันทึกข้อมูลหรือเอกสาร (Theft of Media or Documents)	V042 ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	4=High	3=Possible	12	ควบคุมความเสี่ยง	1. จัดทำกระบวนการ Security Patch Management	RPT#2	4=Likely	1=Rarely	4
3												
4												
5												

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

บรรยายโดย กษิภัท ธนิตธนาคุณ

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

อ้างอิง : ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 และ (ฉบับที่ 2) พ.ศ. 2564

ต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศนี้ ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ รวมถึง**สร้างเสริมความตระหนักรู้ด้าน**ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

(๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

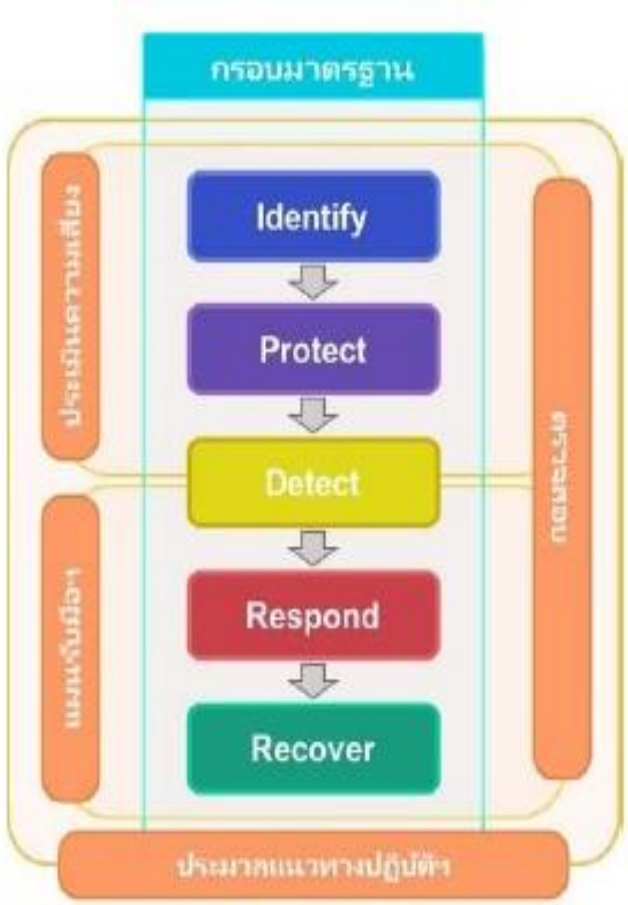
(๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๖ ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้

ข้อ ๗ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามประกาศนี้ และให้มีอำนาจตีความและวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

อ้างอิง : ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 และ (ฉบับที่ 2) พ.ศ. 2564

บรรยายโดย กษิภัท ธนิตธนาคุณ



รูปที่ ๒ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Source: Thailand Data Protection Guidelines 3.0

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม)

1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

1.1) การจัดการทรัพย์สิน (Asset Management)

1.2) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

1.3) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

1.4) การจัดการผู้ให้บริการภายนอก (Third Party Management)

2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

2.1) การควบคุมการเข้าถึง (Access Control)

2.2) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

2.3) การเชื่อมต่อระยะไกล (Remote Connection)

2.4) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

2.5) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

2.6) การแบ่งปันข้อมูล (Information Sharing)

Source: Thailand Data Protection Guidelines 3.0

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม)

3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

3.1) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

4.1) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

4.2) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

4.3) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

5.1) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

Source: Thailand Data Protection Guidelines 3.0

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

Identify

1.1) การจัดการทรัพย์สิน (Asset Management)

- ต้องมีทะเบียนทรัพย์สิน (Inventory)
- ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ
- การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

1.2) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

ทะเบียนความเสี่ยงอย่างน้อยควรประกอบด้วย

(ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

(ข) คำอธิบายของความเสี่ยง (Description of the Risk)

(ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

(ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

(จ) การจัดการความเสี่ยง (Risk Treatment)

(ฉ) เจ้าของความเสี่ยง (Risk Owner)

(ช) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ

(ซ) ความเสี่ยงที่เหลือ (Residual Risk)

<<< รายละเอียดอ้างอิงเอกสารก่อนหน้า >>>

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

Identify

1.3) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

- ต้องมีการทำ VA/Pentest ระบบที่สำคัญอย่างสม่ำเสมอ เช่น Internet Facing เป็นต้น
- พิจารณาทำเมื่อมีการเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

1.4) การจัดการผู้ให้บริการภายนอก (Third Party Management)

Source: ประกาศ ธปท. ที่ สนส.21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

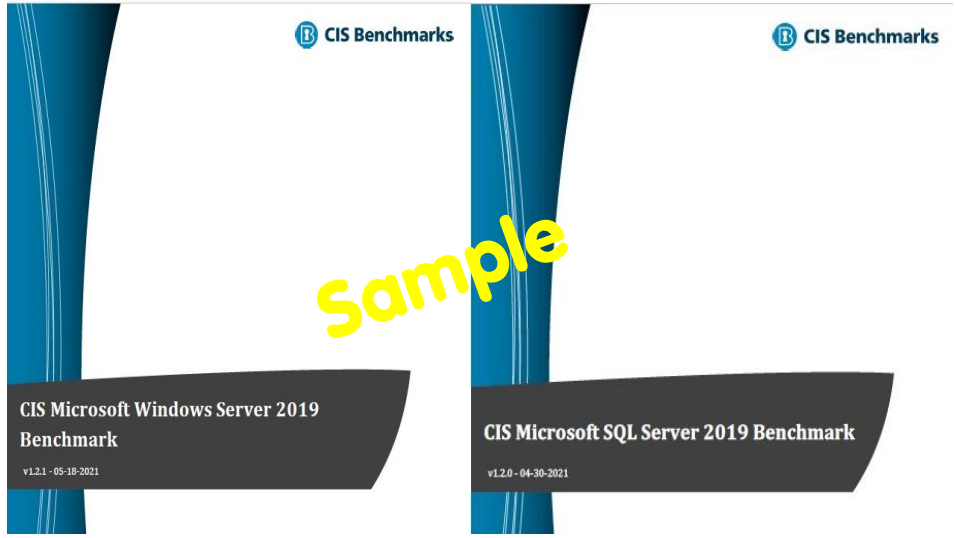
Protect

2.1) การควบคุมการเข้าถึง (Access Control)

- ต้องให้สิทธิ์เท่าที่จำเป็น และมีการทำ User Access Management (Add/Modify/Delete/Review)
- ต้องเปิดและสอบทาน Security Access Log
- ต้องควบคุมเรื่อง Interface เช่น Port และ USB

2.2) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

- ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมด
- ต้องมี Change Management Process
- ต้องมีการตรวจสอบการตั้งค่าอย่างสม่ำเสมอ เช่น ปีละ 1 ครั้ง



มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

Protect

2.3) การเชื่อมต่อระยะไกล (Remote Connection)

- ต้องใช้เมื่อจำเป็นเท่านั้น
- ต้องเข้ารหัสการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh เป็นต้น

2.4) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

- ต้องมีการควบคุมทั้ง Removable Storage และ Mobile Device
- ก่อนนำ Removable Storage มาเชื่อมต่อต้องสแกนไวรัส
- ต้องมีการเข้ารหัสข้อมูลที่สำคัญ

2.5) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

- ต้องสร้างความตระหนักรู้ให้กับ บุคลากรทุกระดับทั้งเก่าและใหม่ อย่างสม่ำเสมอ เช่น ปีละ 1 ครั้ง
- ต้องสร้างความตระหนักรู้ให้กับ Vendor/Outsource อย่างสม่ำเสมอ เช่น ปีละ 1 ครั้ง

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

Protect

2.6) การแบ่งปันข้อมูล (Information Sharing)

- ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

Detect

3.1) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

- ต้องสร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัย เช่น SOC/NOC เป็นต้น
  - Security Operations Center (SOC)
  - Network Operations Center (NOC)
- ต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อยปีละ 1 ครั้ง

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

Respond

4.1) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

4.2) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

4.3) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

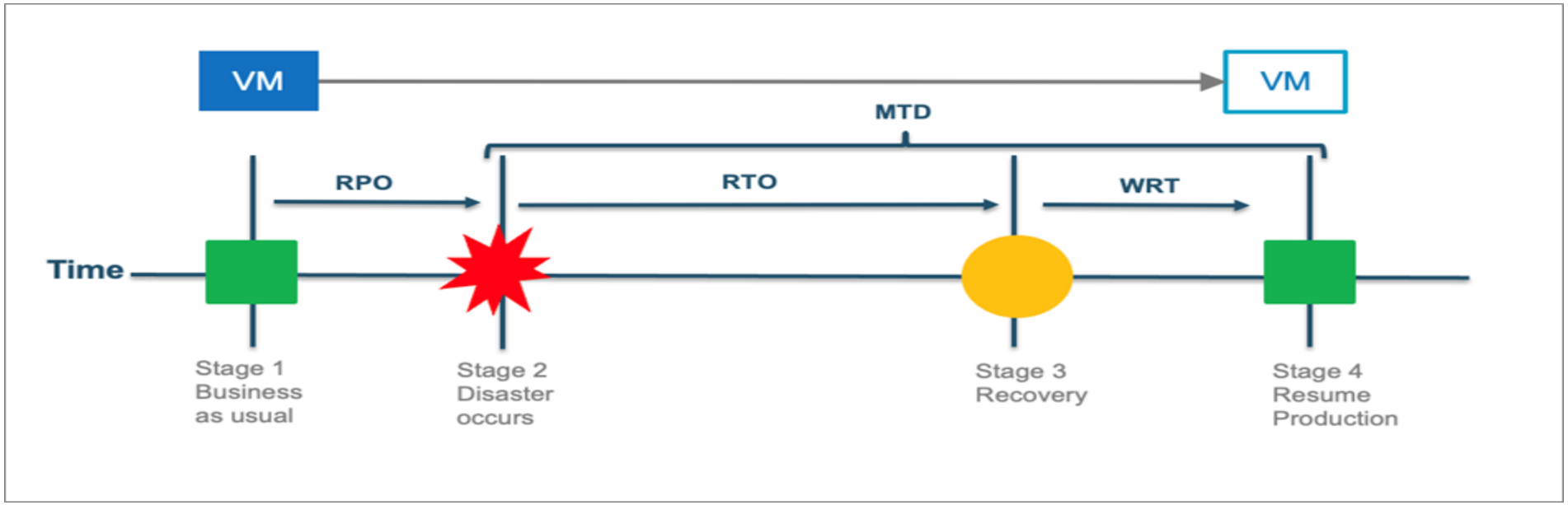
- **ต้องต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง**

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (เพิ่มเติม) – รายละเอียด

Recover

5.1) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

- ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)
- ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้ง



Maximum Tolerable Period of Disruption (MTPD/MTD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)

Source: https://aws.amazon.com/blogs/apn/addressing-multiple-disaster-recovery-slas-with-vmware-cloud-on-aws/

แหล่งข้อมูลอ้างอิง

- พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (ฉบับที่ 2) พ.ศ. 2564
- Thailand Data Protection Guidelines 3.0
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
- ประกาศ ธปท. ที่ สนส.21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน