การประเมินและการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ [Risk Assessment and Risk Treatment (Threat & Vulner.) of Cybersecurity Act.]

ผู้พิจารณาประเมิน : สภาวิศวกรคณะกรรมการพิจารณาความเสี่ยง
ผู้ปฏิบัติ : นายพิทักษ์พงษ์ เพิ่มเพิ่งศิน (Lead Implementer), สภาวิศวกรคณะกรรมการพิจารณาความเสี่ยง
วันที่ทำการประชุมความเสี่ยงฯพร้อมนำบันทึก : 23 ก.พ. 69
สถานที่ : ห้องประชุมอิ่มสุข โรงพยาบาลเวาสุภัม
ที่อยู่ : 50/1 หมู่ 12 ต.เขาบางศรี อ.ท่าไหม่ จ.จันทบุรี 22120
ระบบบริการสำคัญ : All critical application

มาตรการควบคุมไซเบอร์ขั้นต่ำ	
ผลการประเมินความเสี่ยง (เฉลี่ย) โดยรวมขององค์กร (16 Clusters, 160 Risk Id.)	5.7

	Risk Score
แดง (สูง) = 17 เอกสาร เป็นอย่างน้อย	7.0 - 25
เหลือง (ปานกลาง) = 13 เอกสาร เป็นอย่างน้อย	5.1- 6.9
เขียว (ต่ำ) = 10 เอกสาร เป็นอย่างน้อย	1 - 5.0

ผลการประเมินความเสี่ยง(เฉลี่ย) โดยรวมขององค์กร หลังจัดการความเสี่ยง	5.00
Residual Risk Level	

	Risk Score
เป็นความเสี่ยงขั้นวิกฤติ ต้องมีการดำเนินการโดยทันที	12.50 - 25.00
เป็นความเสี่ยงสูง ต้องมีการดำเนินการบางอย่างเพื่อลดความเสี่ยง	9.50 - 12.49
เป็นความเสี่ยงปานกลาง ต้องมีการติดตามและอาจมีมาตรการป้องกัน	5.01 - 9.49
ต้องมีการติดตามเป็นระยะ แต่ยังไม่ต้องมีการดำเนินการใดๆเพิ่มเติม	1 - 5.0

PART 1 : RISK ASSESSMENT | **Risk Analysis** (A = โอกาสเกิด (Likelihood), B = ความรุนแรง (Impact), C = A*B ระดับความเสี่ยง (Risk Level))

No.	หมวดหมู่การเสี่ยง (Risk Cluster)	ระดับความเสี่ยงด้านไซเบอร์และช่องโหว่ ต่างๆ (Risk Identification): ภัยคุกคาม (Threat)	ช่องโหว่ (Vulner.)	มาตรการควบคุมในปัจจุบัน	มีผลกระทบต่อ: C	I	A	B/F	มีผลต่อความรุนแรงต่อด้าน: S	R	I	L	O	A โอกาสเกิด (Likelihood)	B ความรุนแรง (Impact)	C = A*B ระดับความเสี่ยง (Risk Level)	เจ้าของความเสี่ยง (Risk Owner)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk Level) ของแต่ละ Cluster
	กรอบมาตรฐาน																	
1	**การโจมตีด้วยมัลแวร์ (Malware Attacks)**	1. มีการลากวางไฟล์ไฟล์ลำคาญเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งอาจแฝงตัวมัลแวร์	1. ไม่มีระบบหรือมาตรการควบคุมการลากวางไฟล์และติดตั้งซอฟต์แวร์ภายองค์กร	มี Antivirus ที่มีพเลตจัดจุบัน มีการอบรมให้ความรู้ จนท.	-	-	x	x	x	x	x	-	-	2	2	4	CSMR	4.6
		2. มีการติดตั้งเครื่องรับจากการใช้งานภายนอก USB Storage หรือสื่อเก็บข้อมูลภายนอก	2. ไม่มีการติดตั้งหรือบังคับใช้นโยบาย USB Storage	มี Antivirus ที่มีพเลตจัดจุบัน มีการอบรมให้ความรู้ จนท. ออกระเบียบข้อบังคับ	-	-	x	x	x	x	x	-	-	1	3	3	CSMR	
		3. ใช้อีเมลในเว็บแม่มีที่ชวนชื่อและแต่งด้วยมัลแวร์	3. มาตรระบบหรือมาตรการหรือนโยบายการควบคุมการใช้งาน อีเมลที่ใช้โดยเนน	มี Antivirus ที่มีพเลตจัดจุบัน มีการอบรมให้ความรู้ จนท.	-	-	x	x	x	x	x	-	-	2	4	8	CSMR	
		4. การติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ที่ตั้งด้วยมัลแวร์	4. พนักงานขาดความรู้ในการติดตั้งโทรศัพท์หรือเว็บไซต์ที่มีความเสี่ยงของมัลแวร์	มีนโยบายการติดตั้งซอฟต์แวร์ มีการตรวจสอบการติดตั้งซอฟต์แวร์ประจำเดือน ตัวของซัมซุงเดิมไม่ได้เป็นระบบ ฯ	-	-	x	x	x	x	x	x	-	1	4	4	CSMR	
		5. พนักงานเข้าเว็บไซต์ของมัลแวร์ (Malvertising) ด้านวิเคราะห์ ที่ทำไม่ยังเว็บไซต์ที่มีมัลแวร์	5. ไม่มีระบบตรวจเว็บไซต์ ที่มีอกีบมัลแวร์ และพิพเลตเป็นประจำ	มี Antivirus ที่มีพเลตจัดจุบัน มีการอบรมให้ความรู้ จนท. ใช้ SIEM เพื่อตรวจสอบกิจกรรมที่ทำผลผิด	-	-	x	x	x	x	x	-	-	1	4	4	CSMR	
2	**การโจมตีด้วยฟิชชิ่ง (Phishing Attacks)**	1. การหลีกเลี่ยงมาตรฟิชชิ่ง เช่น พนักงานไม่สามารถตรวจสอบเว็บไซต์ที่ถูกต้องได้	1. มาตรการป้องกันมาตรฟิชชิ่ง เช่น พนักงานไม่สามารถตรวจสอบเว็บไซต์ปลอมได้	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	11.2
		2. Spear Phishing ที่ทำลายเป้าหมายเจาะจงบุคคลหรือหน่วยงาน ขอผลเป้าเป็นระบบ	2. ไม่มีระบบตรวจจับอีเมลที่ชวนชื่อ เช่น ไม่มีการวิเคราะห์อีเมลที่ผิดเงื่อนไขที่เป็นปรกติ	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	-	-	2	4	8	CSMR	
		3. มีการรับส่งอีเมลที่มีชื่อชิ่งผ่าน SMS หรือวิธีระยะอื่นเพิ่ม	3. ขาดวิธีการตรวจสอบข้อความที่ถูกส่งไปยังผู้ใช้งานที่ไม่ได้ผ่านการยืนยันตัวตนหรือการเข้ารหัสข้อมูล	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	
		4. เข้าเว็บไซต์ปลอมที่เลียนแบบหน้าเพื่อขโมยข้อมูลส่วนตัวผ่านไลน์	4. ขาดการใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ระบบไม่มีการยืนยันตัวตนเพิ่มเติมสำหรับการเข้าถึงข้อมูลสำคัญ	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	
		5. ถูกกระแสโทรศัพท์หลอก (Call center) หลอกขอข้อมูลส่วนตัว	5. ไม่มีระบบการยืนยันการเรียกรายชื่อผลลัพ เช่น ขาดนโยบายการยืนยันตัวตนของผู้ส่งอีเมลที่มีชื่อชิ่งผ่าน	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	
3	**ภัยคุกคามจากบุคคลภายใน (Insider Threats)**	1. การใช้งานข้อมูลโดยไม่ทราบว่ามีขอบ เช่น พนักงานที่มีสิทธิ์เข้าถึงข้อมูลสำคัญอาจนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต	1. การควบคุมสิทธิ์การเข้าถึงที่ไม่เหมาะสม เช่น พนักงานลาออกไปแล้วสิทธิ์เข้าถึงข้อมูลภายในกับการเข้าถึง	มีการอบรมการหมดหวงสิทธิการเข้าถึงข้อมูลเพราะที่ทำเป็น การยกเลิกสิทธิ์ผู้ใช้งานประจำปี	x	-	-	x	x	x	x	-	-	1	4	4	CSMR	5.6
		2. การทำโดยผลการใช้งานโดยไม่ได้ตั้งใจ เช่น การลบข้อมูลสำคัญที่ควรเก็บรักษาข้อมูลให้บุคคลที่ไม่ควร	2. ขาดระบบตรวจสอบพฤติกรรม เช่น ไม่มีการติดตามกิจกรรมที่ติดปกติจากของพนักงาน	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	x	-	2	4	8	CSMR	
		3. การทำลืมตลาดโดยไม่ได้ตั้งใจ เช่น การลบข้อมูลสำคัญที่ควรเก็บรักษาข้อมูลให้บุคคลที่ไม่ควร	3. มาตรการติดตามเกี่ยวกับการปกป้องข้อมูล เช่น พนักงานไม่เข้าใจถึงความสำคัญของการปกป้องข้อมูล	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	-	-	2	5	10	CSMR	
		4. การใช้ข้อมูลที่ถูกยังคงเหลืออยู่แม้ (Inactive users) เช่น มีบุคซึ่งของพนักงานที่ถูกยังคงเหลืออยู่ที่ถูกการเข้าไปใช้งานการตรวจทำที่ไม่เหมาะสม	4. ไม่มีการจัดการบัญชีผู้ใช้งานที่ออกจากองค์กร เช่น มีบุคซึ่งของพนักงานที่ลาออกยังคงสามารถเข้าถึงระบบได้	สร้างกระบวนการตรวจสอบกิจกรรมของผู้ใช้งาน จาก log file และปิดฯ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR	
		5. มีการปลอมตัวเป็นบุคคลสถานใน เช่น บุคคลภายนอกแอบอ้างเข้าเป็นเจ้าหน้าที่การบริหารของพนักงานภายใน	5. ไม่มีการเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลที่สำคัญไม่ได้รับการป้องกัน ทำให้ง่ายต่อการเข้าถึงและกดีสอดแทรกส่งออก	ตั้งขึ้นเพราะกังเพื่อตรวจสอบและจัดการกิจกรรมภายนอกบุคคลภายใน	x	-	-	x	x	x	x	-	-	1	3	3	CSMR	
4	**การละเมิดข้อมูล (Data Breaches)**	1. มีการเปลี่ยนรูปแบบเพื่อเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลลูกค้า หรือข้อมูลทางการเงิน	1. การขาดการเข้ารหัสข้อมูล (Encryption) เช่น ข้อมูลสำคัญไม่ได้รับการเข้ารหัสทั้งในขณะส่งและจัดเก็บข้อมูล	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	x	-	2	4	8	CSMR	9.4
		2. มีการละเมิดข้อมูลจากการตั้งรหัสผ่านที่ง่ายเกิน	2. ระบบที่ไม่ได้อัปเดต (Outdated Systems) เช่น ระบบปฏิบัติการและซอฟต์แวร์ที่ไม่ได้อัปเดตเป็นเวอร์ชันล่าสุด ไม่ได้ปกป้องดี	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	x	-	2	5	10	CSMR	
		3. มีการรั่วไหลของข้อมูลผ่านพนักงาน (โดยเจตนาหรือไม่เจตนา)	3. การตั้งค่าที่ผิดพลาดที่ไม่ปลอดภัย เช่น ผู้ใช้ตั้งค่าที่ผิดพลาดที่เข้าถึงข้อมูลที่ควรเป็นส่วนตัวของ	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	x	-	2	4	8	CSMR	
		4. มีการส่งข้อมูลสำคัญผ่านของทางที่ไม่ปลอดภัย เช่น มีเมลที่ไม่มีการเข้ารหัส	4. ขาดระบบควรควบคุมการเข้าถึง (Access Control): ไม่มีการควบคุมสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	-	-	3	5	15	CSMR	
		5. มีการโจมตีผ่าน API หรือระบบที่ไม่ได้รับการตรวจสอบความปลอดภัย	5. ขาดการตรวจสอบกิจกรรมโปรแกรม เช่น ไม่มีการตรวจสอบกิจกรรมที่ทำผลผิดในระบบที่สำคัญเพิ่มเติม	มีการอบรมให้ความรู้	x	-	-	x	x	x	x	x	-	2	3	6	CSMR	
5	**การโจมตีแบบ Denial of Service (DoS) และ Distributed Denial of Service (DDoS)**	1. พยายามการส่งคำขอปลอมปลอมจำนวนมากผลเพื่อทำให้ระบบขอผลล้ม	1. ไม่มีการกำหนดขีดจำกัดคำขอหรือกรองคำขอ เช่น ระบบไม่สามารถจำกัดจำนวนคำขอที่ส่งเข้ามาภายในช่วงเวลาที่กำหนดได้	ใช้เครื่อง เช่น DDoS Mitigation ของ Cloudflare	-	-	x	x	x	x	x	x	-	1	5	5	CSMR	7.0
		2. ถูกการโจมตีแบบ DNS Amplification ที่เพิ่มปริมาณคำขอ (เพื่อให้ระบบของเรา (ขอเข้าหมาย) รับภระเกินกำลัง	2. ระบบตรวจจับการโจมตีที่ไม่เพียงพอ เช่น ไม่มีเครื่องมือไม่ในการตรวจจับและออนสของผ่พพลิการบทที่ผิดปกติ	กำหนดจำนวนคำขอที่ระบบสามารถรับได้ต่อวินาทีต่อ IP Address	-	-	x	x	x	x	x	x	-	1	4	4	CSMR	
		3. ถูกการใช้ botnet เพื่อกระจายการโจมตีจากหลายแหล่งไม่ปรับเป้าหมาย	3. ไม่มีการใช้ Load Balancer เช่น ระบบไม่สามารถกระจายโหลดการของการประมวลผลคำขอไปยังเซิร์ฟเวอร์อื่นๆได้	มีการอบรมให้ความรู้	-	-	x	x	x	x	x	x	-	2	4	8	CSMR	
		4. ถูกการโจมตีในระดับแอปพลิเคชัน เช่น การทำให้เว็บเซิร์ฟเวอร์ไม่สามารถรองรับคำขอที่ถูกต้องได้	4. ขาดปกป้องดีพอของ DNS และไม่ได้ตั้งค่าแคชที่ดีพอ เช่น DNS Server ไม่มีการกำหนดค่าเพื่อป้องกันการโจมตีจากที่ DNS Spoofing หรือ Amplification	มีการอบรมให้ความรู้	-	-	x	x	x	x	x	x	-	2	4	8	CSMR	
		5. ถูกการโจมตีไปรโตคอล เช่น SYN Flood, Ping of Death	5. มีการจัดการทรัพยากรระบบไม่เหมาะสม เช่น ระบบเซิร์ฟเวอร์ไม่ระบบตั้งค่าที่ถูกทรัพยากรที่ยอมให้รองรับกิการโจมตี	มีการอบรมให้ความรู้	-	-	x	x	x	x	x	x	-	2	5	10	CSMR	
6	**การโจมตีแบบ Man-in-the-Middle (MitM)**	1. มีการดักฟังการสื่อสาร (Eavesdropping) เช่น แฮ็กเกอร์ดักจับข้อมูลระหว่างผู้ใช้และเซิร์ฟเวอร์ ผ่านทำลายที่ส่งข้อมูลสำคัญ	1. การขาดการใช้ไม่มีการเข้ารหัสลับ เช่น การส่งข้อมูลผ่าน HTTP แทน HTTPS	มีการอบรมให้ความรู้	x	x	-	x	x	x	x	x	-	2	3	6	CSMR	4.2
		2. ถูกการปลอมแปลงเว็บไซต์ (Spoofing) เช่น สร้างเว็บไซต์ที่ดูเหมือนจริงผ่าน Wi-Fi ปลอมเพื่อหลอกให้ผู้ใช้มีข้อมูลส่ง	2. เครือข่าย Wi-Fi สาธารณะ เช่น ไม่มีการตั้งค่าความปลอดภัย เช่าที่ WPA2/WPA3	มีการอบรมให้ความรู้	x	x	-	x	x	x	x	x	-	2	3	6	CSMR	
		3. ถูกการโจมตีผ่าน Wi-Fi ที่ไม่ปลอดภัย เช่น การโจมตีไม่ครึ่งผ่าน Wi-Fi สาธารณะที่ไม่มีการเข้ารหัส	3. การไม่ตรวจสอบใบรับรอง SSL/TLS เช่น ผู้ใช้งานสามารถยอมรับใบรับรองปลอมจากใบรับรองของจริงได้	ติดตั้งระบบ IDS/IPS (Intrusion Detection and Prevention Systems) เพื่อตรวจจับกิจกรรมที่ผิดปกติ	x	x	-	x	x	x	x	-	-	1	2	2	CSMR	
		4. มีการ Hijack เซสชัน (Session Hijacking) เช่น การเข้าควบคุมเซสชันของผู้ใช้งานที่เข้าสู่ระบบแล้ว	4. ขาดมาตรการยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ไม่มีการบังคับให้ยืนยันตัวตนเพิ่มเติมสำหรับการเข้าถึงข้อมูลที่สำคัญ	มีมั่นคงมาร์ซอร์ปและระบบปฏิบัติการเพื่อป้องกันช่องโหว่ใหม่	x	x	-	x	x	x	x	-	-	1	2	2	CSMR	
		5. มีการปลอมใบรับรอง (Certificate Spoofing) เช่น การใช้ใบรับรอง SSL/TLS ปลอมเพื่อหลอกผู้ใช้	5. การตั้งค่าอย่างไม่ถูกต้องที่ไม่ปลอดภัย เช่น ปล่อยให้ เข้าหรือเชื่อมต่อกับเครือข่าย Wi-Fi ในองค์กรและบ้าน	ใช้ WPA3 สำหรับเครือข่าย Wi-Fi ในองค์กรและบ้าน	x	x	-	x	x	x	x	-	-	1	5	5	CSMR	
7	**การโจมตีด้วยแรงบันดาลใจ (Ransomware Attacks)**	1. มีการลากวางไฟล์ไฟล์ลำคาญ ซึ่งอาจแฝงตัวมัลแวร์ที่ทำลายระบบข้อมูลที่ชิชิชิ่ง	1. การขาดการติดตามพนักงาน เช่น พนักงานมีไฟล์ต้องสงสัยที่เป็นอันตรายจากเว็บไซต์	มีไม่มีกรณ Antivirus และ Antimalware และพิพเลตเป็นปัจจุบัน	-	-	x	x	x	x	x	-	-	1	5	5	CSMR	6.0
		2. มีการรับส่งไฟล์ไม่ข้อมูลไวรัสในระบบที่ของหน่วยงานที่ไม่ได้ปลอดภัย	2. ขาดพื้นฐานในการระบบปฏิบัติการที่ไม่ได้อัปเดต เช่น ระบบที่ของซอฟต์แวร์ยังมีช่องโหว่ที่เปิดให้ถูกขยายเข้าถึงได้	ไม่ขอพักวิที่ถูกลิขสิทธิ์ ตั้งค่าการป้องกันอัตโนมัติ	-	-	x	x	x	x	x	-	-	1	5	5	CSMR	
		3. มีการใช้ Remote Desktop Protocol (RDP) ที่ไม่ได้ตั้งค่าความปลอดภัย	3. การตั้งค่าความปลอดภัยของ RDP ที่ไม่เหมาะสม เช่น เปิดใช้งาน RDP โดยไม่มีการควบคุมการเข้าถึงที่เข้มงวด	มีการอบรมให้ความรู้	-	-	x	x	x	x	x	-	-	1	5	5	CSMR	

PART 2 : RISK TREATMENT

No.	ตัวเลือกการตอบสนอง (Risk Treatment)	No.	แผนจัดการความเสี่ยง (Risk Treatment Plan): หัวข้อ	รายละเอียด	ค่าดำเนินการคาดหวังจริง (Expected finish date)
1	Continue Monitoring	1			
2	Continue Monitoring	2			ภายใน 30 ก.ย. 67
3	Mitigate Risk	3	**การให้ความรู้และฝึกอบรมพนักงาน**	จัดอบรมเกี่ยวกับภาวะคลิกเลื่อนการตามข้อโทรศัพท์หรือเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ	ภายใน 30 ก.ย. 67
4	Continue Monitoring	4			ภายใน 30 ก.ย. 67
5	Continue Monitoring	5			ภายใน 30 ก.ย. 67
1	Mitigate Risk	1	**ให้ความรู้และฝึกอบรมพนักงาน**	จัดอบรมพนักงานเกี่ยวกับวิธีการระบุอีเมลและลิงก์ที่ชิชิชิ่ง เช่น การตรวจสอบ URL และหัวข้ออีเมล	ภายใน 30 ก.ย. 67
2	Mitigate Risk	2	**ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA)**	เปิดใช้งาน MFA สำหรับทุกบัญชีโดยเฉพาะบัญชีที่เกี่ยวข้องกับข้อมูลสำคัญ	ภายใน 30 ก.ย. 67
3	Mitigate Risk	3	**ตรวจสอบและควบคุมการเข้าถึงเว็บไซต์**	ใช้ระบบ Web Filtering เพื่อเน้นการเข้าถึงเว็บไซต์ที่ชิชิชิ่ง	ภายใน 30 ก.ย. 67
4	Mitigate Risk	4	**ใช้เครื่องมือ SIEM (Security Information and Event Management)**	ติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามแบบเรียลไทม์	ภายใน 30 ก.ย. 67
5	Mitigate Risk	5	**เน้นมาตรการบางเหตุการณ์ (Incident Reporting)**	จัดทำโดยการสร้างขึ้นพนักงานในการรายงานอีเมลหรือเข้าตรวจที่ทำงานผลิต	ภายใน 30 ก.ย. 67
1	Continue Monitoring	1			ภายใน 30 ก.ย. 67
2	Mitigate Risk	2	**การฝึกอบรมพนักงาน**	ให้ความรู้เกี่ยวกับการป้องกันการทำให้หลงของมุมผลลดหรือการหลงของการทำโดยเฉพาะ	ภายใน 30 ก.ย. 67
3	Mitigate Risk	3	**การเข้ารหัสข้อมูลสำคัญ**	ใช้การเข้ารหัสข้อมูลสำคัญทั้งในขณะรวบรวมการจัดเก็บและการส่งข้อมูล	ภายใน 30 ก.ย. 67
4	Continue Monitoring	4			ภายใน 30 ก.ย. 67
5	Continue Monitoring	5			ภายใน 30 ก.ย. 67
1	Mitigate Risk	1	**การเข้ารหัสข้อมูล (Encryption)**	ใช้การเข้ารหัสข้อมูลทั้งในระหว่างการส่ง (In-Transit) และขณะจัดเก็บ (At Rest)	ภายใน 30 ก.ย. 67
2	Mitigate Risk	2	**กำหนดนโยบายรหัสผ่านที่เข้มงวด**	กำหนดให้ใช้รหัสผ่านที่ซับซ้อนและเปลี่ยนรหัสผ่านเป็นระยะ	ภายใน 30 ก.ย. 67
3	Mitigate Risk	3	**ระบบตรวจสอบและเฝ้าระวังเชิงเน้นภัยคุกคาม**	ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อตรวจสอบและแจ้งเตือนกิจกรรมที่ผิดปกติ	ภายใน 30 ก.ย. 67
4	Mitigate Risk	4	**ใช้ระบบสำรองข้อมูล (Backup)**	กำหนดให้มีการสำรองข้อมูลอัตโนมัติ และเก็บข้อมูลสำรองไว้ในระบบที่แยกออกจากระบบหลัก	ภายใน 30 ก.ย. 67
5	Mitigate Risk	5	**การจัดทำแผนรับมือเหตุการณ์ (Incident Response Plan)**	สร้างกระบวนการตอบสนองเมื่อเกิดเหตุการณ์ Data Breach	ภายใน 30 ก.ย. 67
1	Continue Monitoring	1			ภายใน 30 ก.ย. 67
2	Continue Monitoring	2			ภายใน 30 ก.ย. 67
3	Mitigate Risk	3	**การฝึกซ้อมรับมือเหตุการณ์ตามแบบเรียลไทม์**	ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อเน้นเฝ้าตรวจสอบเหตุการณ์ที่ผิดปกติ	ภายใน 30 ก.ย. 67
4	Mitigate Risk	4	**สร้างแผนงาน Incident Response Plan**	กำหนดขั้นตอนการตอบสนองต่อการโจมตี DoS/DDoS	ภายใน 30 ก.ย. 67
5	Mitigate Risk	5	**การปิดพอดและป้องกันโปรโตคอล**	ปรับแต่ง TCP/IP Stack เพื่อป้องกันการโจมตี เช่น SYN Cookies	ภายใน 30 ก.ย. 67
1	Mitigate Risk	1	**ใช้โปรโตคอล HTTPS และ TLS**	บังคับให้ทุกการสื่อสารระหว่างผู้ใช้และเซิร์ฟเวอร์ใช้ HTTPS	ภายใน 30 ก.ย. 67
2	Mitigate Risk	2	**หลีกเลี่ยงการใช้งาน Wi-Fi สาธารณะที่ไม่มีความปลอดภัย**	ใช้ VPN เพื่อเข้ารหัสข้อมูลขณะใช้งาน Wi-Fi สาธารณะ	ภายใน 30 ก.ย. 67
3	Continue Monitoring	3			ภายใน 30 ก.ย. 67
4	Continue Monitoring	4			ภายใน 30 ก.ย. 67
5	Continue Monitoring	5			ภายใน 30 ก.ย. 67
1	Continue Monitoring	1			ภายใน 30 ก.ย. 67
2	Continue Monitoring	2			ภายใน 30 ก.ย. 67
3	Continue Monitoring	3			ภายใน 30 ก.ย. 67

PART 3 : PROGRESS

No.	สถานะความคืบหน้าดำเนินการ (Progress Status)	ผู้รับผิดชอบในการดำเนินการ
1	100%	
2	80%	
3	100%	
4	50%	
5	100%	
1	77%	
2	100%	
3	88%	
4	33%	
5	22%	
1	100%	
2	33%	
3	100%	
4	100%	
5	66%	
1	23%	
2	100%	
3	100%	
4	2%	
5	100%	
1	67%	
2	100%	
3	65%	
4	43%	
5	100%	
1	100%	
2	100%	
3	34%	
4	100%	
5	55%	
1	100%	
2	100%	
3	55%	

PART 4 : RISK EVALUATION AFTER RESOLVED 100 % — ความเสี่ยงที่คงเหลือ (Risk Residual)

No.	C	I	A	B/F	S	R	I	L	O	A โอกาสเกิด (Likelihood)	B ความรุนแรง (Impact)	C = A*B ระดับความเสี่ยงที่คงเหลือ (Risk Residual Level)	ดำเนินการเพิ่มเติมเพื่อลดความเสี่ยงให้ปลอดภัย (Further actions to be taken to further minimize risk)
1	x	x	x	x	-	-	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
2	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
3	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
4	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
5	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
1	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
2	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
3	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
4	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
5	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
1	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
2	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
3	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
4	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
5	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
1	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
2	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
3	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
4	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
5	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
1	x	x	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
2	x	x	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
3	x	x	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
4	x	x	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
5	x	x	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
1	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
2	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
3	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ

		4. จัดการแผนฉุกเฉินและวิธีรับมือกรณี USB Storage หรืออุปกรณ์พกพาเต็ม	4. การตั้งค่าความปลอดภัยของ ECP ที่ไม่เหมาะสม เช่น มีสิทธิ์มาก ECP โดดไม่มีการควบคุมการเข้าถึงที่เหมาะสม	ออกมาตรการควบคุม เว้นแต่ กำหนดช่องทั้งในการใช้งานอุปกรณ์ส่วนตัว	-	-	x	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	4	**การใช้เทคโนโลยีการจำกัดสิทธิ์ (Access Control)**	ใช้หลักการ Least Privilege เพื่อให้สิทธิ์การเข้าถึงเฉพาะที่จำเป็น	ภายใน 30 ก.ย. 67	100%		-	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		5. จัดการระงานแจ้งเตือนว่าผ่านเครือข่ายที่เชื่อมโยงกับองค์กร	5. ควรอาจขอบเปิดองค์กรเปิดเว้นที่ประสิทธิภาพ เช่น ไม่ใช้ระดับ VPN กับแจ้งเตือนการใช้งานที่ควรตรวจจับและเฝ้าการใช้งานดี	ที่ไม่รองรับ Antivirus และ Antimalware และมีพฤติกรรมปัจจุบัน	-	-	x	x	x	x	x	-	-	1	5	5	CSMR		Continue Monitoring	5			66%		-	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
8	**การโจมตีด้านวิศวกรรมสังคม (Social Engineering)**	1. Phishing - จัดการแจ้งเตือนที่ต้องการให้ผู้ใช้งาน ให้ข้อมูลสำคัญ เช่น รหัสผ่าน หรืออนุมัติสั่งการ	1. ควรหาความตระหนักรู้ของพนักงาน เช่น พนักงานไม่เข้าใจความเสี่ยงจาก Social Engineering	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR	5.4	Mitigate Risk	1	**การฝึกอบรมและสร้างความตระหนัก**	จัดอบรมพนักงานให้เข้าใจรูปแบบการโจมตี Social Engineering เช่น Phishing, Pretexting	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		2. Spear Phishing - จัดการโจมตีที่ใช้การหลอกเป้าหมายเฉพาะบุคคลหรือหน่วยงานเฉพาะ โดยใช้ข้อมูลส่วนตัวของผู้ใช้งาน เพื่อเพิ่มความน่าเชื่อถือ	2. ในวิธีการตรวจสอบตัวตนของผู้ขอข้อมูล เช่น จากระบบการยืนยันตัวตนก่อนให้ข้อมูลสำคัญ	มีการตรวจสอบยืนยันตัวตนของผู้ขอข้อมูลก่อนให้ข้อมูลสำคัญ	x	-	-	x	x	x	x	-	-	1	5	5	CSMR		Continue Monitoring	2			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		3. Pretexting - จัดการสร้างสถานการณ์หลอกลวง เช่น แอบอ้างเป็นพ่าน IT เพื่อขอข้อมูลสำคัญ	3. ในวิธีการตรวจสอบการเข้าถึงพื้นที่ทางกายภาพ เช่น การเข้า ออกพื้นที่สำคัญ ไม่ได้รับการตรวจสอบอย่างเข้มงวด	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	3	**การควบคุมการแผงแยกข้อมูลในโครงข่ายเดียวกัน**	ให้กำหนดเข้าพนักงานในการนำเนินกับการแผงแยกข้อมูลที่มีการจุกการใช้งานดี	ภายใน 30 ก.ย. 67	22%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		4. Baiting - จัดการหลอกล่อ วางเหยื่อ เพื่อให้ผู้ใช้งานเอาไปใช้ เช่น อุปกรณ์ USB Storage ที่มีมัลแวร์ เพื่อให้เข้าพวกหมิ่นไปใช้งาน	4. ควรการป้องกันระบบเสาสแนเทศ เช่น ระบบไม่มีการกรองสื่อมลพิศเว็บไซต์ที่ไม่ดีพอ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	4	**การจำกัดสิทธิ์การเข้าถึง (Access Control)**	ใช้หลักการ Least Privilege เพื่อให้พนักงานเข้าถึงเฉพาะข้อมูลที่จำเป็นต่อการทำงาน	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		5. Tailgating - จัดการเข้าถึงพื้นที่ที่มีการกำหนดการเข้าถึงพื้นที่สำคัญโดยไม่ได้รับอนุญาตเข้าไปในพื้นที่	5. การใช้วิธีระบบยืนยันตัวตนที่ไม่มีการควบคุม เช่น ข้อมูลสำคัญของเอกสารหรือพนักงานถูกละเมิดหรือไม่ระบบยืนยัน	ใช้ระบบ Biometric Authentication เพื่อควบคุมการเข้าถึงพื้นที่สำคัญ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	5			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
9	**ความเสี่ยงด้านความปลอดภัยของคลาวด์ (Cloud Security Risks)**	1. การตั้งค่าคลาวด์ที่ไม่ปลอดภัย (Misconfiguration) เช่น การเปิดเผยข้อมูลสำคัญบนอินเทอร์เน็ตเนื่องจากการตั้งค่าที่ผิดพลาด ซึ่งส่งผลของเปิดเผย	1. ควรการตรวจสอบการตั้งค่าที่ถัดกุม เช่น ไม่มีการตรวจสอบหรือปรับปรุงการตั้งค่าความปลอดภัยในระบบคลาวด์	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	4	4	CSMR	4.0	Continue Monitoring	1			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		2. ถูกการโจมตี API เช่น แฮ็กการโจมตี API ที่ไม่ได้รับการป้องกัน อาทิ API Key หรือ Token ที่ไม่ได้รับการเข้ารหัส	2. การควบคุมการเข้าถึงที่ไม่เพียงพอ เช่น สิทธิ์การเข้าถึงคลาวด์ถูกกำหนดอย่างไม่ชัดเจน เช่น ทุกคนสามารถเข้าถึงได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	4	4	CSMR		Continue Monitoring	2			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		3. จัดการโอนย้ายข้อมูลระหว่างการส่งข้อมูล เช่น การส่งที่เข้ารหัสข้อมูลที่ไม่ได้เข้ารหัสระหว่างการส่งข้อมูล	3. การขาดการเข้ารหัสข้อมูล เช่น ข้อมูลที่จัดเก็บและส่งผ่านคลาวด์ไม่ได้รับการเข้ารหัส	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	4	4	CSMR		Continue Monitoring	3			88%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		4. จัดการผลิตภัณฑ์ซึ่งใช้งานคลาวด์ เช่น ผู้ใช้งานเข้าถึงความลับซึ่งมีการส่งข้อมูลไปยังเซิร์ฟเวอร์ของบริษัทผู้ให้บริการคลาวด์	4. การไม่ปฏิบัติตามกฎระเบียบหรือมาตรฐานความปลอดภัยของการบริการคลาวด์ เช่น ระบบคลาวด์ไม่ได้รับการปรับให้สอดคล้องกับมาตรฐาน เช่น ISO 27001, 27018, 27701	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	1	4	4	CSMR		Continue Monitoring	4			100%		x	-	-	x	x	x	x	x	-	1	5	5	เน้นติดตามเป็นระยะ
		5. ถูกเปิดเผยวิธีคลาวด์ เช่น การอัปโหลดไฟล์ที่ตั้งค่าเปิดเผยทั้งหมดระบบคลาวด์ผ่านการขาดไม่ถ้อยใช้งานอื่นๆ	5. การขาดการตรวจสอบการใช้งานที่ถูกต้องและเพียงพอ เช่น ขาดการตรวจสอบโดยการควบคุมการเข้าถึงข้อมูลที่ให้บริการคลาวด์	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	4	4	CSMR		Continue Monitoring	5			54%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
10	**ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)**	1. จัดการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้จำหน่าย (3rd Party/Suppliers) ที่ไม่ได้มีการควบคุมความปลอดภัยอาจทำให้ข้อมูลของลูกค้ารั่วไหล	1. ควรขาดระบบการตรวจสอบผู้จำหน่าย (3rd Party/Suppliers) เช่น ไม่มีการตรวจสอบความปลอดภัยของผู้จำหน่าย (3rd Party/Suppliers) ก่อนนำมาใช้งาน	ใช้ Vendor Security Assessment Questionnaire เพื่อตรวจสอบมาตรฐานความปลอดภัย	x	-	-	x	x	x	x	-	-	1	3	3	CSMR	6.2	Continue Monitoring	1			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		2. มีการโจมตีผ่านซัพพลายเชน (Supply Chain Attack) เช่น ผู้ใช้งานที่ใช้ของไม่ทราบแฝงพิษผ่านองค์กรเพื่อขอเข้าถึงระบบองค์กร	2. ในวิธีของกองค์ในการปกป้องข้อมูล (Security SLA) เช่น ขาดนิยามกองค์ที่กำหนดบทบาทและความรับผิดชอบด้านความปลอดภัย	ไม่ได้ยึดหลักเพิ่มสิทธิ์ตามระบบผู้จำหน่ายและพนักงานที่จำเป็นเท่านั้น (Principle of Least Privilege)	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	2			65%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		3. พบว่าผู้จำหน่ายภายนอกการมีผู้มีสิทธิ์ตามกฎระเบียบ เช่น ผู้จำหน่ายไม่มีผู้ดีพอมาตรฐานที่ระบุถึงการพลด ด้านความปลอดภัย เช่น ISO 27001, 27018, 27701	3. การเข้าถึงระบบที่ไม่เหมาะสม: ผู้จำหน่ายได้รับสิทธิ์เข้าถึงระบบภายในความจำเป็น	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	3	**การแบ่งปันข้อมูลที่เหมาะสมกับผู้จำหน่าย**	จัดประเภทข้อมูลและระบุเฉพาะข้อมูลที่จำเป็นเท่านั้น	ภายใน 30 ก.ย. 67	23%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		4. การพึ่งพาผู้จำหน่ายที่ไม่มีความเป็นเจ้าในการบริการ เช่น ความผิดพลาดของผู้จำหน่าย อาทิ การหยุดให้บริการ อาจส่งผลกระทบต่อธุรกิจ	4. ขาดการเข้าระวังควบคุมและติดตามข้อมูลผู้จำหน่าย เช่น ไม่มีการติดตามการปฏิบัติตามของผู้จำหน่ายในด้านความปลอดภัย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	4	**การประเมินความเสี่ยงของบริษัทคลาวด์**	ประเมินความเสี่ยงด้านความปลอดภัยของผู้จำหน่ายก่อนเข้าโครงการ	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		5. การแชร์ข้อมูลระหว่างกันกับผู้จำหน่ายที่ไม่ได้การป้องกัน เช่น การส่งข้อมูลสำคัญผ่านช่องทางที่ไม่มีการเข้ารหัส	5. การแชร์ข้อมูลกับผู้จำหน่ายมากเกินไป ผู้จำหน่ายควรมีสิทธิ์เข้าถึงข้อมูลเท่าที่จำเป็นเท่านั้น	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	3	9	CSMR		Mitigate Risk	5	**การจัดทำแผนรับมือเหตุการณ์ร่วมกันผู้จำหน่าย**	สร้าง Incident Response Plan ที่ครอบคลุมผู้จำหน่าย	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
11	**ความเสี่ยงของอุปกรณ์พกพือถือ (Mobile Device Risks) ขององค์กร**	1. จัดการสูญหายหรืออุกรโดย เช่น อุปกรณ์ที่เก็บข้อมูลสำคัญถูกขโมยหรือสูญหายโดยไม่มีการป้องกัน	1. ไม่มีการเข้ารหัสข้อมูล เช่น ข้อมูลในอุปกรณ์ที่เก็บข้อมูลสำคัญถูกขโมยหรือสูญหายโดยไม่มีการป้องกัน	เปิดใช้งานการเข้ารหัสข้อมูลในอุปกรณ์ยืนยันตัวตนผ่าน	x	-	-	x	x	x	x	-	-	1	3	3	CSMR	3.0	Continue Monitoring	1			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		2. มีอแวร์ที่ไม่ปลอดภัยของค์กร เช่น การติดตั้งแอปพลิเคชันที่มีมัลแวร์ซึ่งสามารถเข้าถึงข้อมูลในอุปกรณ์	2. การตั้งค่าความปลอดภัยที่ไม่เหมาะสม เช่น อุปกรณ์ไม่มีการตั้งรหัสผ่านหรือการยืนยันตัวตนผ่าน	ใช้ MDM เพื่อติดตาม ควบคุม และจัดการอุปกรณ์ที่เชื่อมต่อกับเครือข่ายองค์กร	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	2			44%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		3. มีการโจมตีผ่าน พา-ก สายรอยด เช่น การดักจับข้อมูลจากอุปกรณ์ที่เชื่อมต่อเครือข่าย พา-ก ที่ไม่มีการป้องกัน	3. ควรควบคุมไม่ทดสอบมัลแฟลร์ที่ไม่ป้องกัน เช่น การติดตั้งแอปพลิเคชันที่ไม่ได้รับการรับรองจากแหล่งที่ไม่น่าเชื่อถือ	ยังต้องใช้อุปกรณ์ที่ติดตั้งซีเคียวซอฟต์แวร์ป้องกันมัลแพลตฟอร์มความปลอดภัยล่าสุด	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	3			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		4. Phishing ผ่านอุปกรณ์ปรือถือ เช่น การส่งข้อความหรืออีเมล์ ที่หลอกให้ผู้ใช้งานติดตั้งแอปพลิเคชัน	4. ควรขาดการควบคุมการใช้งาน BYOD ในองค์กร เช่น ไม่มีนโยบาย BYOD (Bring Your Own Device) ที่ชัดเจน	สร้างนโยบาย BYOD ที่ครอบคลุมกำหนดการใช้งานอุปกรณ์ส่วนตัวในเครือข่ายองค์กร	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	4			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		5. จัดการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การใช้งานอุปกรณ์ของเพื่อนร่วมงานอุปกรณ์โดยผู้ไม่ได้รับอนุญาต	5. ไม่มีการยืนยันตัวตน เช่น อุปกรณ์ไม่ได้รับการยืนยันตัวตนก่อนการเข้าถึงข้อมูลสำคัญ	ตั้งค่าให้มีการสำรองข้อมูลอัตโนมัติของอุปกรณ์ยังคงไปยังระบบคลาวด์ที่ปลอดภัย	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	5			45%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
12	**ซอฟต์แวร์และระบบที่มีช่องโหว่ (Vulnerable Software and Systems)**	1. พบว่ามีการใช้ช่องโหว่ของซอฟต์แวร์ที่ไม่ได้อัปเดตเพื่อเข้าควบคุมระบบ (Exploitation of Unpatched Software)	1. ซอฟต์แวร์และระบบที่ไม่ได้อัปเดต เช่น การใช้เวอร์ชันที่ล้าสมัยของซอฟต์แวร์และระบบปฏิบัติการ	มีพลบระบบจัดการและติดตั้งแพตช์ความปลอดภัย	x	-	x	x	x	x	x	-	-	1	5	5	CSMR	6.6	Continue Monitoring	1			100%		x	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		2. มีการโจมตีจากช่องโหว่ของระบบปฏิบัติการ เช่น การโจมตีแบบ Zero-Day	2. การตั้งค่าที่ไม่ปลอดภัย (Misconfiguration) เช่น การตั้งค่าซอฟต์แวร์หรือฮาร์ดแวร์ที่มีช่องแอ่นอุดสำคัญ ทำให้เปิดช่องโหว่	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	2	**การตั้งค่าความปลอดภัยของระบบ (Secure Configuration)**	ใช้ Security Hardening Guides เช่น CIS Benchmarks หรือ NIST เพื่อปรับแต่งการตั้งค่าให้ปลอดภัย	ภายใน 30 ก.ย. 67	100%		x	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		3. มีการโจมตีผ่านแอปพลิเคชันเว็บ เช่น SQL Injection, Cross-Site Scripting (XSS)	3. การใช้ซอฟต์แวร์ออปเปิดซึ่งมีช่องโหว่ที่ไม่ได้รับการรับประกันความปลอดภัยหรือไม่มีแพตช์ป้องกันหรือค่าบางอย่างที่ไม่ปลอดภัย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	3	**การตรวจสอบห่วงโซ่ของซอฟต์แวร์ (Software Supply Chain Security)**	เลือกใช้ซอฟต์แวร์จากผู้จัดจำหน่ายที่น่าเชื่อถือและมีประวัติการแก้ไขปมที่ดี	ภายใน 30 ก.ย. 67	55%		x	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		4. จัดการแก้ไขและรีโปสำหรับแอปเก่าซึ่งหรือสามเสริมของซอฟต์แวร์	4. ไม่มีกระบวนการการในการค้นหาและแก้ไขช่องโหว่ในระบบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	4	**การนำเข้าระบบเฝ้าระวังแบบเรียลไทม์**	ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อนำเข้ารวบรวมและวาดข้อมูลต่อ	ภายใน 30 ก.ย. 67	100%		x	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		5. มีการใช้บริการที่ไม่ปรัโตคอลลที่ล้าสมัย เช่น FTP หรือ Telnet	5. ขาดการตรวจสอบพิษพลาดเชนของซอฟต์แวร์ (Software Supply Chain) เช่น ไม่มีการตรวจสอบความน่าเชื่อถือของซอฟต์แวร์จากผู้จัดจำหน่าย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	5	**การทดสอบความปลอดภัย (Penetration Testing)**	ทำการทดสอบช่องโหว่โดยระบบโดยผู้เชี่ยวชาญเพื่อค้นหาความเสี่ยงที่ล้าสมัย	ภายใน 30 ก.ย. 67	23%		x	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
13	**ความเสี่ยงด้านความปลอดภัยของเครือข่าย (Network Security Risks)**	1. ถูกการโจมตีแบบ DDoS (Distributed Denial of Service) เช่น การส่งคำขอจำนวนมากเพื่อทำให้เครือข่ายของค่ากาง	1. การตั้งค่าความปลอดภัยที่ไม่เหมาะสม เช่น การตั้งค่าการเลเอร์หรือไฟร์วอลล์ที่ไม่ปลอดภัย	ไม่ให้ตั้งเลเอร์เพื่อควบคุมการเข้าถึงเครือข่ายและเฝ้าการเข้าถึงที่ไม่ได้รับอนุญาต	-	-	x	x	x	x	x	-	-	1	3	3	CSMR	4.8	Continue Monitoring	1			100%		-	-	x	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		2. ถูกการโจมตีแบบ Man-in-the-Middle (MitM) เช่น การดักฟังข้อมูลระหว่างการสื่อสารข้างเครือข่าย	2. ไม่มีการแยกเครือข่าย (Network Segmentation) เช่น ขาดการแบ่งเครือข่ายอย่างชัดเจนจากเครือข่ายสำคัญ เช่น การเข้าถึงเครือข่ายทั่วไป (VLAN)	ติดตั้งระบบ IDS/IPS เพื่อตรวจจับและป้องกันกิจกรรมที่เป็นอันตรายในเครือข่าย	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	2			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		3. ถูกการโจมตีแบบ Phishing ผ่านเครือข่าย เช่น การส่งอีเมล์ที่ปลอมหรือไฟล์ที่เป็นอันตรายผ่านอีเมล์หรือเครือข่าย	3. ขาดระบบตรวจจับและป้องกันบริเวณคาน เช่น ไม่มีการติดตั้ง IDS/IPS (Intrusion Detection/Prevention Systems)	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR		Mitigate Risk	3	**การควบคุมการเข้าถึง (Access Control)**	ใช้ NAC (Network Access Control) เพื่อตรวจสอบและควบคุมการเข้าถึงเครือข่าย	ภายใน 30 ก.ย. 67	34%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		4. จัดการใช้ช่องโหว่ของโปรโตคอลเครือข่าย เช่น การโจมตีด้วยโปรโตคอล อาทิ DNS Spoofing หรือ ARP Poisoning	4. การใช้โปรโตคอลที่ล้าสมัย เช่น FTP หรือ Telnet ที่ไม่มีการเข้ารหัส	ยังมีเลเวลเคอร์ สวิตช์ และไฟร์วอลล์เป็นประจำเพื่อลดความเสี่ยงจากช่องโหว่	x	-	-	x	x	x	x	-	-	1	5	5	CSMR		Mitigate Risk	4			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ
		5. จัดการเข้าถึงที่ไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรืออุปกรณ์ที่ไม่ได้รับอนุญาตเชื่อมต่อกับเครือข่ายของค่ากาง	5. ไม่มีการควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการตรวจสอบอุปกรณ์ที่ทำเชื่อมต่อกับเครือข่ายของค่ากาง	ใช้บริการ DDoS Mitigation เช่น Cloudflare หรือ AWS Shield เพื่อป้องกันการโจมตี DDoS	x	-	-	x	x	x	x	-	-	1	5	5	CSMR		Mitigate Risk	5			100%		x	-	-	x	x	x	x	-	-	1	5	5	เน้นติดตามเป็นระยะ

14	**ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)**	1. มีการเข้าถึงพื้นที่ที่ละเอียดไม่ได้รับอนุญาต เช่น บุคคลภายนอกที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่สำคัญได้ อาทิ ศูนย์ข้อมูลหรือใช้ทั่วเวชุกรรมหรือสายสำรองข้อมูลต่อเนื่อง	1. การควบคุมความปลอดภัยทางกายภาพ (Access Control) เช่น ใช้มีการกำหนดสิทธิ์เข้าถึงพื้นที่สำคัญ	ใช้ระบบ Biometric Authentication เพื่อควบคุมการเข้าถึงพื้นที่สำคัญ	x	-	x	x	x	x	x	-	-	1	3	3	CSMR	4.2	Continue Monitoring	1		ภายใน 30 ก.ย. 67	100%		x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. มีการใช้เทคโนโลยีเฝ้าระวังต่างๆ เช่น กล้องวงจรปิด (CCTV) เช่น ติดตั้งกล้องวงจรปิดในจุดเสี่ยงต่างๆ เช่น ทางเข้าห้องเซิร์ฟเวอร์ ศูนย์ข้อมูลสำรอง ฯลฯ เพื่อติดตามการเข้าถึงพื้นที่สำคัญ	ออกแบบสถานที่ให้มีการป้องกันน้ำท่วม เช่น การยกพื้นศูนย์ข้อมูลหรือใช้ระบบกันน้ำ	x	-	-	x	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	2		ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการก่อวินาศกรรม (Sabotage) เช่น การทำลายเครื่องมือสื่อสารระบบโดยบุคคลภายในหรือบุคคลภายนอก	3. ใช้ระบบป้องกันการก่อวินาศกรรม เช่น ทางการออกแบบที่ป้องกันทางการป้องกันการก่อวินาศกรรม	จัดทำรายการปฏิบัติเข้าถึงพื้นที่สำคัญและตรวจสอบสิทธิ์เป็นระยะ	-	-	x	x	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	3		ภายใน 30 ก.ย. 67	65%		-	-	x	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. เกิดภัยธรรมชาติ (Natural Disasters) เช่น น้ำท่วม ไฟไหม้ หรือแผ่นดินไหวที่ส่งผลกระทบต่ออุปกรณ์และข้อมูลสำคัญ	3. ใช้มีการป้องกันภัยธรรมชาติ เช่น ทางการออกแบบที่ป้องกันการป้องกันภัยธรรมชาติ อาทิ การป้องกันน้ำท่วม	ดำเนินการป้องกันภัยธรรมชาติ เช่น ทำการเพิ่มเติมเพื่อเพิ่มเติมและ	-	-	x	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	4	**การฝึกอบรมพนักงานด้านความปลอดภัย**	ฝึกอบรมพนักงานให้เข้าใจวิธีป้องกันและรับมือกับภัยคุกคามทางกายภาพ	ภายใน 30 ก.ย. 67	100%		-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. มีการรั่วไหลข้อมูลผ่านการเข้าถึงทางกายภาพ เช่น การเชื่อมต่อกับพอร์ต USB หรือเครื่องบันทึกเสียงในเซิร์ฟเวอร์ เพื่อรั่วไหลข้อมูล	5. การกับเข้าถึงอุปกรณ์สำคัญที่ไม่ได้ปลอดภัย เช่น อุปกรณ์สำคัญถูกทิ้งไว้ในพื้นที่เข้าถึงได้ง่าย	ดำเนินการเพิ่มเติมเพื่อเพิ่มเติมและ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	5	**การตรวจสอบความปลอดภัยทางกายภาพเป็นระยะ**	ตรวจสอบระบบล็อก กล้องวงจรปิด และระบบป้องกันภัยธรรมชาติอย่างสม่ำเสมอ	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
15	**ความเสี่ยงจากการไม่ปฏิบัติตามกฎระเบียบและข้อบังคับ (Regulatory and Compliance Risks)**	1. เพลดไทพทางกฎหมาย เช่น การถูกปรับหรือฟ้องร้องจากการไม่ปฏิบัติตามกฎหมาย เช่น พรบ คอมพิวเตอร์, พรบ ข้อมูลส่วนบุคคล หรือ พรบ ไซบเนอร์	1. การควบคุมความรู้เกี่ยวกับกฎหมายและข้อบังคับที่เกี่ยวข้อง เช่น พนักงานและฝ่ายทรัพยากรไม่ทราบถึงข้อบังคับทางคดและกฎหมายที่ต้องปฏิบัติตาม	ยังไม่มีการควบคุมที่เข้มแข็งและสม่ำเสมอ เพื่อเพิ่ม	x	-	-	x	x	x	x	x	-	-	2	3	6	CSMR	4.2	Mitigate Risk	1	**การติดตามและวิเคราะห์กฎหมายและข้อบังคับ**	แต่งตั้งทีม Compliance หรือให้ที่ปรึกษาเพื่อให้คำแนะนำเกี่ยวกับข้อบังคับทางคดที่เกี่ยวข้อง	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	(Non-Compliance Activity)	2. การเสี่ยงชื่อเสียง เช่น ความน่าเชื่อถือขององค์กรลดลง เนื่องจากการละเมิดกฎระเบียบข้อบังคับทำความไม่ปลอดภัยของข้อมูล	2. ใช้มีระบบติดตามและตรวจสอบการปฏิบัติตามข้อบังคับคดต เช่น ทางคดเรื่องเรื่องหรือการบางการในการประเมินผลทางความสอดคล้อง	ออกนพนักงานเกี่ยวกับข้อบังคับทางคดและความสำคัญของการปฏิบัติตามกฎหมาย	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	2		ภายใน 30 ก.ย. 67	33%		x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการขอคอบรับข้อมูลจากรั่ว เช่น การมีการบนหรือบริการชั่วคราวเนื่องจากการตรวจสอบจากหน่วยงานที่เกี่ยวข้อง	3. ทางคดในทางและการบางการที่ผิดพลาด เช่น ใช้ระบบทางปฏิบัติที่ล้าสมัยไม่พนักงานรวมถึงหน่วยงานที่เกี่ยวข้องกับข้อมูลปฏิบัติตามข้อบังคับได้ง่าย	ดำเนินการ Internal Audit เป็นระยะเพื่อประเมินความสอดคล้องกับข้อกำหนด	x	-	x	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	3		ภายใน 30 ก.ย. 67	100%		x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4.ความเสียหายทางการเงิน เช่น การสูญเสียเงินค่าหรือโอกาสทางธุรกิจเนื่องจากการละเมิดข้อบังคับ	4. การจัดการและสร้างและข้อมูลที่ไม่เพียงพอ เช่น การจัดเก็บและสารที่การตั้งการของ ของข้อมูลไม่ตรงตามข้อบังคับ	สร้าง Incident Response Plan ที่รวมข้อกำหนดด้านการรายงานเหตุการณ์ไว้ที่ตรงตามกฎหมาย	x	-	x	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	4		ภายใน 30 ก.ย. 67	100%		x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. มีความเสี่ยงต่อความปลอดภัยของข้อมูล เช่น การจัดการข้อมูลไม่ตรงตามกฎหมาย อาจทำให้สูญเสียข้อมูล	5. การไม่ทำการประเมินความเสี่ยงด้านข้อกำหนด เช่น ไม่ได้ตรวจสอบว่าการบางการได้มีการตรวจสอบข้อบังคับ	ยังไม่มีการควบคุมที่เข้มแข็งและสม่ำเสมอ เพื่อเพิ่ม	x	-	-	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	5	**การดำเนินการปฏิบัติตามข้อกำหนดอย่างต่อเนื่อง (Compliance Roadmap)**	จัดทำแผนการปฏิบัติตามข้อบังคับในระยะยาว พร้อมตรวจสอบความก้าวหน้า	ภายใน 30 ก.ย. 67	55%		x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
16	**การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)**	1. มีการส่งข้อมูลโดยไม่ได้เข้ารหัส เช่น การส่งข้อมูลสำคัญไปยังผู้ที่ไม่ได้รับสิทธิ์ผ่านช่องทางที่ไม่ปลอดภัย	1. การขาดการควบคุมการเข้าถึงข้อมูล เช่น ใช้มีการกำหนดสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	ยังไม่มีการควบคุมที่เข้มแข็งและสม่ำเสมอ เพื่อเพิ่ม	x	-	-	x	x	x	x	-	-	2	3	6	CSMR	4.2	Mitigate Risk	1	**การเข้ารหัสข้อมูล (Data Encryption)**	เข้ารหัสข้อมูลสำคัญทั้งในขณะจัดเก็บ (At Rest) และระหว่างส่งผ่านเครือข่าย (In Transit)	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. มีการรั่วไหลข้อมูลโดยเจตนา เช่น พนักงานที่ไม่พอใจหรือบุคคลภายนอกรั่วไหลข้อมูลเพื่อผลประโยชน์ส่วนตัว	2. การไม่มีการเข้าถึงข้อมูล เช่น ข้อมูลที่จัดเก็บเกี่ยวกับลับกับ ไม่มีการเข้ารหัส	ยังไม่มีการควบคุมที่เข้มแข็งและสม่ำเสมอ เพื่อเพิ่ม	x	-	-	x	x	x	x	x	-	2	3	6	CSMR		Mitigate Risk	2	**การใช้ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention - DLP)**	ใช้ DLP เพื่อตรวจสอบและบล็อกการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต	ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการละเมิดข้อมูลภายและที่ไม่ปลอดภัย เช่น การรั่วไหลของข้อมูลที่ส่งผ่าน Wi-Fi หรือเครือข่ายที่ไม่มีการเข้ารหัส	3. ทางคดในทางและการบางการจัดการข้อมูล เช่น ไม่มีการกำหนดเครื่องมาใช้ในการจัดการข้อมูลสำคัญและข้อมูลส่วนบุคคล	ตั้งค่าการส่งรองข้อมูลอัตโนมัติไปยังสถานที่ที่ปลอดภัยและอยู่ภายในกรรมหลัก	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	3		ภายใน 30 ก.ย. 67	56%		x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. ถูกการโจมตีแบบ Phishing เช่น ผู้โจมตีปลอมตัวเพื่อเข้าถึงข้อมูลสำคัญผ่านอีเมลหรือข่าวสาร	4. การขาดระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention - DLP) เช่น ไม่มีการใช้ระบบเพื่อตรวจจับและป้องกันการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต	ใช้ MDM เพื่อติดตามและจัดการอุปกรณ์ที่เชื่อมต่อกับข้อมูลสำคัญ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	4		ภายใน 30 ก.ย. 67	100%		x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. มีการติดต้องบริหารจัดการซอฟแวร์ เช่น มีการใช้ข้อมูลเข้าเพื่อเข้าข้อมูลหรือตัดขวางการเข้าถึงข้อมูล	5. อุปกรณ์และข้อมูลที่ทำพิสิทพิสิทที่ไม่ได้ปลอดภัย เช่น อุปกรณ์พกพาที่มีข้อมูลผู้โจมตีสามารถเข้าถึงข้อมูลได้	ใช้ Virtual Private Network (VPN) สำหรับการเข้าถึงข้อมูลผ่านเครือข่ายสาธารณะ	x	-	x	x	x	x	x	-	-	1	3	3	CSMR		Continue Monitoring	5		ภายใน 30 ก.ย. 67	66%		x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ