แบบประเมินความเสี่ยงและความพร้อมด้าน Cybersecurity

Cybersecurity Risk & Readiness Assessment Form for Small and Medium Enterprises (SMEs)

ชื่อองค์กร/บริษัท:		**หน่วยงาน/แผนก:**	
ผู้ประเมิน:		**ตำแหน่ง:**	
วันที่ประเมิน:		**รอบการตรวจ:**	☐ ประจำปี ☐ ประจำ 6 เดือน

คำชี้แจงในการให้คะแนนระดับความพร้อม (Readiness Level)

เกณฑ์การประเมินแบ่งเป็น 4 ระดับ (0 - 3 คะแนน) พิจารณาจากสภาพการปฏิบัติงานจริงภายในองค์กร:

- **0 คะแนน = ยังไม่ได้ดำเนินการ (No Implementation):** ไม่มีการดำเนินการใดๆ หรือไม่เคยมีนโยบายนี้ (ความเสี่ยงสูงสุด)
- **1 คะแนน = ดำเนินการบางส่วน (Partial):** มีการทำบ้างแต่ไม่เป็นระบบ ไม่ครอบคลุมทุกเครื่อง/ทุกคน หรือไม่มีนโยบายชัดเจน
- **2 คะแนน = ดำเนินการเกือบครบถ้วน (Mostly Implemented):** มีการปฏิบัติตามมาตรฐาน แต่ยังขาดการทดสอบ/ทบทวนสม่ำเสมอ
- **3 คะแนน = ดำเนินการสมบูรณ์ (Fully Implemented):** ปฏิบัติตามมาตรฐานอย่างครบถ้วน มีการตรวจติดตามและทดสอบสม่ำเสมอ

หมวดที่ 1: การยืนยันตัวตนและการเข้าถึง (Identity & Access Security)

ข้อ	หัวข้อข้อปฏิบัติและการดำเนินการ	รายละเอียดแนวทางปฏิบัติมาตรฐาน	คะแนน (0 - 3)	ข้อสังเกต / ข้อเสนอแนะเพิ่มเติม
1.1	**เปิดใช้งาน MFA (Multi-Factor Authentication)**	เปิดการยืนยันตัวตน 2 ชั้นในทุกระบบสำคัญ เช่น Google Workspace, Microsoft 365, ระบบบัญชี/การเงิน, ERP, Cloud Storage และ VPN	☐	
1.2	**การใช้ Password Manager & นโยบายรหัสผ่าน**	สนับสนุน/บังคับใช้โปรแกรมช่วยจำรหัสผ่าน (Password Manager) กำหนดให้รหัสผ่านมีความซับซ้อน และไม่ใช้รหัสผ่านซ้ำกันในแต่ละระบบ	☐	
1.3	**การจำกัดสิทธิ์เท่าที่จำเป็น (Least Privilege)**	ให้สิทธิ์การเข้าถึงข้อมูลและระบบเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานตามบทบาทหน้าที่เท่านั้น (จำกัด Admin Role)	☐	
1.4	**ยกเลิกสิทธิ์พนักงานที่ออก (Offboarding Process)**	มีกระบวนการเพิกถอน/ลบสิทธิ์การเข้าถึงระบบ อีเมล และอุปกรณ์ขององค์กรทันทีเมื่อพนักงานลาออกหรือเปลี่ยนบทบาท	☐	

หมวดที่ 2: การปกป้องข้อมูลและการสำรองข้อมูล (Data Protection & Backup)

ข้อ	หัวข้อข้อปฏิบัติและการดำเนินการ	รายละเอียดแนวทางปฏิบัติมาตรฐาน	คะแนน (0 - 3)	ข้อสังเกต / ข้อเสนอแนะเพิ่มเติม
2.1	**การสำรองข้อมูลตามกฎ 3-2-1**	มีข้อมูลสำรองอย่างน้อย 3 สำเนา จัดเก็บในสื่อ 2 ประเภทที่แตกต่างกัน และแยกเก็บไว้ภายนอก/Cloud (Offsite/Immutable Backup) 1 แห่ง	☐	
2.2	**การทดสอบกู้คืนข้อมูล (Restore Test)**	มีการทดลองกู้คืนข้อมูล (Restore Test) จากไฟล์สำรองอย่างน้อยปีละ 1-2 ครั้ง เพื่อตรวจสอบความสมบูรณ์และนำมาใช้งานได้จริงเมื่อเกิดเหตุ	☐	

ข้อ	หัวข้อข้อปฏิบัติและการดำเนินการ	รายละเอียดแนวทางปฏิบัติมาตรฐาน	คะแนน (0 - 3)	ข้อสังเกต / ข้อเสนอแนะเพิ่มเติม
2.3	**การเข้ารหัสข้อมูล (Data Encryption)**	เปิดใช้นโยบายเข้ารหัสไดรฟ์บนเครื่องพนักงานทุกคน (เช่น BitLocker บน Windows, FileVault บน Mac) และเข้ารหัสข้อมูลสำคัญขณะจัดส่ง	☐	

หมวดที่ 3: การปกป้องอุปกรณ์และเครือข่าย (Devices & Network Security)

ข้อ	หัวข้อข้อปฏิบัติและการดำเนินการ	รายละเอียดแนวทางปฏิบัติมาตรฐาน	คะแนน (0 - 3)	ข้อสังเกต / ข้อเสนอแนะเพิ่มเติม
3.1	**การอัปเดตระบบอัตโนมัติ (Auto-Update / Patching)**	ตั้งค่าให้อัปเดตระบบปฏิบัติการ (OS), เว็บเบราว์เซอร์ และซอฟต์แวร์ต่างๆ เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอเพื่ออุดช่องโหว่ความปลอดภัย	☐	
3.2	**การติดตั้ง Antivirus / EDR**	ติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ (Antivirus/EDR) บนคอมพิวเตอร์โน้ตบุ๊ก และเซิร์ฟเวอร์ทุกเครื่อง พร้อมตั้งค่าอัปเดตฐานข้อมูลไวรัสอัตโนมัติ	☐	
3.3	**การแยกเครือข่าย Wi-Fi (Network Segmentation)**	แยกการเชื่อมต่อ Wi-Fi สำหรับพนักงานภายในองค์กร ออกจาก Wi-Fi สำหรับผู้มาติดต่อ (Guest Wi-Fi) อย่างชัดเจน ไม่ให้เข้าถึงระบบภายในได้	☐	
3.4	**การบังคับใช้ VPN สำหรับทำงานภายนอก**	บังคับให้พนักงานต้องเชื่อมต่อผ่าน VPN ที่ปลอดภัยทุกครั้งเมื่อต้องเข้าถึงระบบภายในองค์กรจากภายนอก (Work from Anywhere)	☐	

หมวดที่ 4: บุคลากรและการรับมือเหตุการณ์ (People & Incident Response)

ข้อ	หัวข้อข้อปฏิบัติและการดำเนินการ	รายละเอียดแนวทางปฏิบัติมาตรฐาน	คะแนน (0 - 3)	ข้อสังเกต / ข้อเสนอแนะเพิ่มเติม
4.1	**การสร้างความตระหนักรู้ Phishing & Cyber Security**	จัดอบรมความรู้แก่พนักงานอย่างน้อยปีละ 1 ครั้ง ให้รู้จักวิธีสังเกตอีเมล ลิงก์หลอกลวง การหลอกลวงทางวิศวกรรมสังคม (Social Engineering)	☐	
4.2	**การจัดตั้งช่องทางแจ้งเหตุผิดปกติ (Reporting Channel)**	กำหนดช่องทางและผู้รับผิดชอบชัดเจน ให้พนักงานสามารถแจ้งเหตุสงสัย เช่น เผลอกดลิงก์แปลกปลอม โดนไวรัส หรือเครื่องทำงานผิดปกติได้ทันที	☐	
4.3	**การทำแผนรับมือเหตุฉุกเฉิน (Incident Response Plan)**	จัดทำแผนรับมือเมื่อเกิดเหตุภัยคุกคาม Cyber / Ransomware / ข้อมูลรั่วไหล กำหนดบทบาท ผู้ติดต่อฉุกเฉิน และขั้นตอนแจ้งหน่วยงานกฎหมาย (เช่น PDPA/กมม.)	☐	

📊 สรุปผลการประเมินระดับความพร้อมและความเสี่ยง (Scoring & Assessment Result)

การคำนวณคะแนนรวม	คะแนนที่ได้ / คะแนนเต็ม	คิดเป็นร้อยละ (%)
คะแนนรวมทุกหมวด (Total Score)	**..... / 39 คะแนน**	**..... %**

เกณฑ์การแปลผลระดับความพร้อมและความเสี่ยง (Risk & Readiness Matrix):

ช่วงคะแนน (%)	ระดับความพร้อม (Readiness)	ระดับความเสี่ยง (Risk Level)	แนวทางแก้ไขและข้อเสนอแนะ
0% - 49% (0 - 19 คะแนน)	น้อยมาก (Initial)	ความเสี่ยงสูงมาก (Critical)	องค์กรมีความเสี่ยงสูงมากต่อการถูกโจมตี ต้องรีบปรับปรุงข้อปฏิบัติพื้นฐาน (เช่น MFA, Backup, Antivirus) โดยด่วนที่สุด
50% - 69% (20 - 27 คะแนน)	ปานกลาง (Developing)	ความเสี่ยงสูง (High)	มีมาตรการพื้นฐานบางส่วน ขาดการบังคับใช้อย่างเป็นระบบ ควรเร่งทำแผนรับมือและอบรมพนักงานเพิ่มเติม
70% - 89% (28 - 34 คะแนน)	ดี (Defined)	ความเสี่ยงปานกลาง (Medium)	มีความพร้อมค่อนข้างดี ควรปรับปรุงส่วนที่ยังขาด เช่น การทดสอบกู้คืนข้อมูล และการซ้อมแผนรับมือเหตุฉุกเฉิน
90% - 100% (35 - 39 คะแนน)	ดีมาก (Optimized)	ความเสี่ยงต่ำ (Low)	มีความพร้อมสูงและมาตรการครอบคลุม ควรักษาสภาพการทำงาน ทบทวนนโยบาย และทดสอบระบบอย่างน้อยทุก 6 เดือน

(.....)
ผู้ประเมิน / ผู้ดูแลระบบ IT
วันที่: ..... / ..... / .....

(.....)
ผู้รับทราบ / ผู้บริหารองค์กร
วันที่: ..... / ..... / .....