แบบตอบรับการดำเนินการแนวปฏิบัติพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล สำหรับหน่วยงาน

ชื่อหน่วยงาน..... .....

ลำดับ	คำแนะนำ	ดำเนินการเรียบร้อย
1	การควบคุม และตรวจสอบการทำงานของ outsource ต้องมีการกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลหรือระบบงาน รวมถึงมีการตรวจสอบการทำงานของทีม outsource ว่าเป็นไปตามข้อกำหนดหรือไม่ และควรมีมาตรการเอาผิดหรือบทลงโทษ หาก บริษัท outsource ละเมิดหรือทำผิดข้อกำหนดจนเป็นสาเหตุให้ถูกโจมตีทางไซเบอร์ รวมทั้งการละเมิด PDPA ด้วย	☐
2	สำรองข้อมูลที่สำคัญตามกฎ 3-2-1 โดยเก็บข้อมูลสำคัญเอาไว้ 3 ชุด ได้แก่ ข้อมูลหลัก 1 ชุด และข้อมูลสำรอง 2 ชุด เก็บไฟล์เหล่านั้นเอาไว้บนอุปกรณ์ที่แยกขาดจากกัน 2 ประเภท และข้อมูลสำรอง 1 ชุดเก็บไว้แบบ Offline และมีการดำเนินการสำรองข้อมูลเป็นประจำ	☐
3	บัญชีผู้ดูแล ผู้ใช้งาน ควรตั้งรหัสผ่านดังนี้ - ตั้งรหัสผ่านอย่างน้อย 8 ตัว โดยประกอบด้วยตัวอักษรเล็ก (abcd) ตัวอักษรใหญ่ (ABCD) ตัวเลข (1234) และสัญลักษณ์ ($#!?) เพื่อสร้างความหลากหลายให้กับรหัสผ่าน - มีการเก็บหรือจัดการกับรหัสผ่านที่มีความปลอดภัยจากการถูกแฮก - หลีกเลี่ยงการตั้งรหัสผ่านเดียวกันหลาย ๆ ระบบ - ปิดการใช้งาน "hint" หรือคำใบ้ของรหัสผ่าน - เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ - การติดตั้งซอฟต์แวร์ทุกครั้งต้องใช้สิทธิ์ผู้ดูแลเสมอ	☐
4	เปิดการใช้งาน Multi-Factor Authentication (MFA) สำหรับผู้ดูแลระบบในการเข้าสู่ระบบรวมถึงระบบการเข้าถึงจากระยะไกล เพื่อป้องกันการโจมตีด้วย Phishing สำหรับทุกการใช้งาน โดยเฉพาะระบบอีเมล ระบบเครือข่ายภายใน และบัญชีการเข้าใช้งานระบบต่าง ๆ ที่สำคัญ	☐
5	อัปเดตแพตช์ของระบบปฏิบัติการและซอฟต์แวร์ รวมถึงติดตั้งโปรแกรมป้องกันมัลแวร์กับคอมพิวเตอร์ทุกเครื่อง และหมั่นอัปเดตโปรแกรมให้ทันสมัยอยู่เสมอ เช่น ระบบดูแลรักษา ESXi, Firewall และ VPN	☐
6	พิจารณาการใช้แผนความปลอดภัยแบบ Zero Trust บังคับใช้การยืนยันตัวตนและการอนุญาตที่เข้มงวดสำหรับการเข้าถึงทรัพยากรทุกครั้ง โดยให้สิทธิ์เข้าถึงตามหลักการของสิทธิ์น้อยที่สุด (least privilege) และตรวจสอบการเข้าถึง	☐
7	มีแผนการดำเนินการฝึกอบรมเกี่ยวกับการรู้เท่าทันภัยไซเบอร์ (Cyber Security Awareness) อย่างต่อเนื่องแก่พนักงาน	☐
8	ติดตั้ง SW ประเภท Antivirus/Anti Malware บนอุปกรณ์ เช่น โน๊ตบุค PC หรือมือถือ ที่ใช้ในหน่วยงาน เพื่อตรวจสอบและป้องกันอุปกรณ์จากมัลแวร์และแรนซัมแวร์	☐
9	ติดตั้งและกำหนดค่าไฟร์วอลล์และระบบป้องกันการบุกรุก (IPS) เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและตรวจจับการบุกรุกที่อาจเกิดขึ้น เฝ้าระวังและตรวจสอบการจราจรในเครือข่ายอย่างต่อเนื่องเพื่อตรวจจับกิจกรรมที่ผิดปกติ	☐
10	ใช้นโยบายการควบคุมการเข้าถึง (access control policies) เพื่อให้แน่ใจว่าผู้ใช้สามารถเข้าถึงทรัพยากรที่จำเป็นหน้าที่ของตนเท่านั้น ตรวจสอบและปรับปรุงสิทธิ์การเข้าถึงอย่างสม่ำเสมอให้สอดคล้องกับความต้องการของงาน เพื่อลดความเสี่ยงจากการเข้าถึงที่ไม่ได้รับอนุญาต	☐

ลำดับ	คำแนะนำ	ดำเนินการเรียบร้อย
11	ใช้การเข้ารหัสข้อมูล ทั้งในขณะจัดเก็บและระหว่างการส่ง เพื่อป้องกันการเข้าถึงและการดักจับที่ไม่ได้รับอนุญาต ใช้มาตรฐานการเข้ารหัสที่แข็งแกร่งและอัปเดตคีย์การเข้ารหัสอย่างสม่ำเสมอ พัฒนานโยบายความเป็นส่วนตัวของข้อมูลที่ครอบคลุม โดยกำหนดวิธีการเก็บรวบรวม ใช้ จัดเก็บ และปกป้องข้อมูล ให้แน่ใจว่าสอดคล้องกับกฎระเบียบการคุ้มครองข้อมูลที่เกี่ยวข้อง และตรวจสอบแนวปฏิบัติการเข้ารหัสและนโยบายความเป็นส่วนตัวของข้อมูลเป็นประจำ	☐
12	บังคับใช้นโยบายการใช้ USB อย่างปลอดภัย จำกัดหรือห้ามการใช้ USB ที่ไม่ได้รับการอนุญาตการใช้ USB ต้องปฏิบัติตามมาตรฐานการรักษาความปลอดภัยที่ได้รับการกำหนดและจะต้องมีการตรวจสอบและควบคุมเพื่อรักษาความปลอดภัยของระบบและข้อมูลอย่างสม่ำเสมอ	☐
13	มีแผนการตรวจสอบบันทึกการเข้าใช้งาน Audit log ที่เกิดขึ้นในระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น การเข้าถึงข้อมูล การเปลี่ยนแปลงข้อมูล หรือกิจกรรมที่เกี่ยวข้องกับความปลอดภัย อย่างสม่ำเสมอ	☐
14	ในการติดตั้งอุปกรณ์ IT ควรเปลี่ยนรหัสผ่านเริ่มต้น, ปิดการใช้งานบริการที่ไม่จำเป็น, ติดตั้งเครื่องมือป้องกัน, และใช้ความคุ้มครองการเข้าถึงเพื่อรักษาความปลอดภัยในองค์กรได้อย่างมีประสิทธิภาพ	☐
15	ใช้การแบ่งแยกเครือข่าย (network segmentation) โดยใช้ Firewall แยกแยะและกำหนดขอบเขตของเครือข่ายคอมพิวเตอร์ออกเป็นพื้นที่ย่อยที่เล็กกว่าภายในเครือข่ายใหญ่ โดยที่แต่ละพื้นที่นี้จะมีการกำหนดขอบเขตและการเข้าถึงที่เฉพาะเจาะจง ลดความเสี่ยงที่ข้อมูลสำคัญจะถูกขโมยหรือถูกเข้าถึงได้โดยไม่ได้รับอนุญาตและช่วยป้องกันไม่ให้การโจมตีขยายขึ้นไปสู่ส่วนอื่นของเครือข่ายได้	☐
16	ทำการทดสอบการเจาะระบบ (penetration testing) หลังจากที่การทดสอบเจาะระบบพบช่องโหว่แล้ว การแก้ไขช่องโหว่ที่พบจะต้องดำเนินการทันทีเพื่อลดความเสี่ยงและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในอนาคต	☐
17	มีการตรวจสอบและประเมินสิทธิ์การเข้าถึงที่ได้รับอนุญาต (privileged access) และสิทธิ์การเข้าถึงทั่วไปของผู้ใช้ทั้งในระบบและแอปพลิเคชันต่าง ๆ ในองค์กร และการทบทวนและปรับปรุงระบบการกำหนดสิทธิ์ให้เหมาะสม เช่นการกำหนดสิทธิ์ตามหลักการสัมพันธ์งาน (least privilege principle) ฯลฯ	☐
18	มีการทดสอบการโจมตีด้วยอีเมลฟิชชิ่ง สร้างอีเมลล์ฟิชชิ่งที่มีลักษณะเหมือนกับการโจมตีจริง และตรวจสอบว่าระบบป้องกันฟิชชิ่งสามารถตรวจจับและบล็อกการโจมตีนั้นได้หรือไม่ และมีพนักงานหรือผู้บริหารคนไหนที่หลงกดลิงค์ในอีเมล์ เพื่อจะได้สร้างความตระหนักรู้ต่อไป	☐
19	ใช้มาตรการรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์เสมือน (VM) เช่น การใช้ VM isolation ฯลฯ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการแพร่กระจายของ ransomware	☐

ลงชื่อ .....

(.....)

ตำแหน่ง.....

วันที่.....

(หัวหน้าหน่วยงาน หรือผู้รับมอบอำนาจ)