SME CYBERSECURITY TOOL

แบบประเมินความปลอดภัยคู่ค้า (Vendor Assessment)

เช็กลิสต์ประเมินความเสี่ยงด้านไซเบอร์สำหรับ Vendor / Supplier / Outsource

รหัสเอกสาร: **SEC-CHK-001**
เวอร์ชัน: 1.0 (2026)

ชื่อบริษัท/คู่ค้า (Vendor): .....

วันที่ประเมิน: _____ / _____ / _____

ประเภทบริการ: [ ] IT/Software [ ] บัญชี/HR [ ] การตลาด [ ] สินค้า

ผู้ประเมิน (SME): .....

🟢 หมวดที่ 1: การบริหารจัดการสิทธิ์และการเข้าถึง (Access Control)

- ☐ **1.1 หลักการสิทธิ์ต่ำสุด (Least Privilege)**
  ขอสิทธิ์การเข้าถึงระบบเฉพาะเท่าที่จำเป็นต่อการทำงาน ไม่ขอสิทธิ์ Admin สูงสุดโดยไม่จำเป็น
- ☐ **1.2 การยืนยันตัวตนสองชั้น (MFA / 2FA)**
  เปิดใช้งาน MFA (OTP / Authenticator App) กับทุกบัญชีที่จะเข้าถึงระบบหรือเพจของบริษัท
- ☐ **1.3 บัญชีผู้ใช้แยกรายบุคคล (No Shared Account)**
  พนักงานคู่ค้าใช้รหัสผ่านแยกเฉพาะตัวบุคคล ไม่ใช้รหัสผ่านส่วนกลางร่วมกัน
- ☐ **1.4 การยกเลิกสิทธิ์ทันทีเมื่อเปลี่ยนพนักงาน (Offboarding Process)**
  มีระบบแจ้งตัดสิทธิ์พนักงานออกทันทีเมื่อพนักงานคนนั้นลาออกหรือย้ายออกจากโครงการ

🟡 หมวดที่ 2: ความปลอดภัยของอุปกรณ์และระบบ (Device & Software Security)

- ☐ **2.1 อัปเดตระบบและแพตช์ความปลอดภัย (Patch Management)**
  เครื่องคอมพิวเตอร์ที่ใช้ทำงานมีการอัปเดต OS (Windows/Mac) และระบบความปลอดภัยเสมอ
- ☐ **2.2 ติดตั้งโปรแกรมป้องกันมัลแวร์ (Antivirus / EDR)**
  เครื่องที่ปฏิบัติงานมีการติดตั้ง Antivirus ที่เปิดใช้งานจริงและอัปเดตฐานข้อมูลสม่ำเสมอ
- ☐ **2.3 ไม่ใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์ (No Pirated Software)**
  ไม่มีการติดตั้งโปรแกรมเถื่อน/ตัวเคร็ก ซึ่งเป็นแหล่งแพร่ระบาดหลักของมัลแวร์ขโมยคุกกี้
- ☐ **2.4 ช่องทางเชื่อมต่อปลอดภัย (Secure VPN/Encryption)**
  การเชื่อมต่อเข้าถึงระบบบริษัทจากระยะไกลทำผ่านช่องทางเข้ารหัส เช่น VPN หรือ HTTPS

🔴 หมวดที่ 3 & 4: การคุ้มครองข้อมูล การเงิน และข้อตกลง (Data, BEC & SLA)

- ☐ **3.1 การคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)**
  รักษาความลับข้อมูลลูกค้า/พนักงาน ไม่นำไปใช้ผิดวัตถุประสงค์ตามกฎหมาย PDPA
- ☐ **3.2 กระบวนการยืนยันการโอนเงิน (Voice Verification for BEC)**
  มีขั้นตอนโทรยืนยันทางเสียงกับผู้มีอำนาจ หากมีการแจ้งเปลี่ยนเลขบัญชีรับเงินทางอีเมล/แชต
- ☐ **3.3 การจัดเก็บและส่งมอบข้อมูลปลอดภัย (Secure File Transfer)**
  ส่งไฟล์สำคัญผ่านระบบล็อกรหัสผ่าน ไม่ส่งผ่านช่องทางสาธารณะที่ไม่ได้เข้ารหัส
- ☐ **4.1 แจ้งเตือนเมื่อเกิดเหตุภัยไซเบอร์ (Incident Notification)**
  ตกลงที่จะแจ้งให้บริษัททราบภายใน 24 ชั่วโมง หากระบบของคู่ค้าโดนแฮกหรือข้อมูลรั่วไหล
- ☐ **4.2 ข้อตกลงความรับผิดชอบในสัญญา (SLA & Liability Clause)**
  มีการระบุขอบเขตความรับผิดชอบกรณีเกิดความเสียหายจากความย่อหย่อนของคู่ค้า

📊 สรุปผลการประเมิน (Scoring Summary) — รวมคะแนนช่อง "ใช่": _____ / 13 คะแนน

คะแนนรวม	ระดับความเสี่ยง	แนวทางดำเนินการสำหรับ SME
11 – 13 ข้อ	🟢 **เสี่ยงต่ำ (Pass)**	ผ่านการประเมิน สามารถเริ่มงานและให้สิทธิ์เข้าถึงตามปกติได้
8 – 10 ข้อ	🟡 **เสี่ยงปานกลาง**	ให้คู่ค้าปรับปรุงข้อที่ขาด **ก่อน** ให้สิทธิ์เข้าถึงระบบสำคัญ
น้อยกว่า 8 ข้อ	🔴 **เสี่ยงสูง (High Risk)**	**ไม่อนุญาตให้เชื่อมต่อระบบ** หรือต้องจำกัดสิทธิ์เข้มงวดเป็นพิเศษ

🌐 **มาตรฐานอ้างอิงของแบบประเมินนี้ (Reference Frameworks):**
แบบประเมินนี้สรุปย่อมาจากกรอบมาตรฐานสากล: **ISO/IEC 27001:2022 (Control A.5.19–A.5.22 Supplier Relationships)**, **NIST SP 800-161 (Cybersecurity Supply Chain Risk Management)**, และ **แนวทางการคุ้มครองข้อมูลส่วนบุคคล (PDPA Thailand)** เพื่อให้เหมาะกับการปฏิบัติจริงของ SME ไทย