นโยบายและขั้นตอนการปฏิบัติงานในการดูแลรักษาความปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายขององค์กร

องค์กรที่มีระบบคอมพิวเตอร์และเครือข่ายจำเป็นต้องมี **นโยบายด้านความปลอดภัยทาง IT** ที่ชัดเจน เพื่อป้องกันภัยคุกคามทางไซเบอร์และรับรองว่าข้อมูลสำคัญขององค์กรจะปลอดภัย โดยสามารถแบ่งแนวทางออกเป็น **สองกลุ่มหลัก** ได้แก่ **ผู้ดูแลระบบ (Administrators)** และ **ผู้ใช้งานระบบคอมพิวเตอร์ (Users)** ดังนี้:

---

1. นโยบายด้านความปลอดภัยสำหรับผู้ดูแลระบบ (Administrators)

ผู้ดูแลระบบมีหน้าที่รับผิดชอบโดยตรงเกี่ยวกับการจัดการและดูแลระบบคอมพิวเตอร์และเครือข่ายขององค์กร ดังนั้นจึงต้องปฏิบัติตามแนวทางต่อไปนี้:

1.1 การบริหารจัดการบัญชีผู้ใช้และสิทธิ์การเข้าถึง

- กำหนดบัญชีผู้ใช้ให้เหมาะสมกับบทบาทของแต่ละบุคคล (Role-based Access Control - RBAC)
- ใช้หลักการ **Least Privilege** (ให้สิทธิ์เท่าที่จำเป็น) เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- บังคับใช้รหัสผ่านที่มีความซับซ้อนและตั้งค่าการหมดอายุของรหัสผ่านตามนโยบายขององค์กร
- ปิดใช้งานบัญชีที่ไม่ได้ใช้งานและเพิกถอนสิทธิ์ของพนักงานที่ลาออกหรือเปลี่ยนตำแหน่งทันที

1.2 การรักษาความปลอดภัยของระบบและเครือข่าย

- อัปเดตระบบปฏิบัติการ (OS) และซอฟต์แวร์ทั้งหมดเป็นเวอร์ชันล่าสุดอยู่เสมอ
- ติดตั้งและบำรุงรักษา **Firewall** และ **Intrusion Detection/Prevention Systems (IDS/IPS)** เพื่อป้องกันการบุกรุกจากภายนอก
- ใช้งาน **Antivirus** และ **Endpoint Security** และตั้งค่าการอัปเดตอัตโนมัติ
- บังคับใช้นโยบาย **Multi-Factor Authentication (MFA)** สำหรับการเข้าถึงระบบที่สำคัญ

1.3 การสำรองข้อมูลและการกู้คืนระบบ

- ดำเนินการ **สำรองข้อมูล (Backup)** เป็นประจำ และจัดเก็บข้อมูลสำรองในที่ปลอดภัย เช่น Cloud Storage หรือสื่อบันทึกข้อมูลภายนอก
- ทดสอบกระบวนการ **กู้คืนข้อมูล (Disaster Recovery Plan - DRP)** อย่างสม่ำเสมอ เพื่อให้แน่ใจว่าสามารถกู้คืนข้อมูลได้อย่างรวดเร็วเมื่อต้องการ
- ใช้มาตรการป้องกัน **Ransomware** เช่น การบล็อกการรันไฟล์ต้องสงสัยและจำกัดสิทธิ์การเข้าถึงของโปรแกรมที่ไม่จำเป็น

1.4 การตรวจสอบและติดตามการใช้งานระบบ

- บันทึกและติดตามกิจกรรมของผู้ใช้ผ่าน **Log Management System** เช่น SIEM (Security Information and Event Management)
- ตรวจสอบ **Log files** อย่างสม่ำเสมอเพื่อตรวจจับกิจกรรมที่ผิดปกติ
- ตั้งค่าการแจ้งเตือนสำหรับเหตุการณ์ที่เป็นภัยคุกคาม เช่น การล็อกอินล้มเหลวซ้ำๆ หรือการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

1.5 การจัดการภัยคุกคามและตอบสนองต่อเหตุการณ์ความปลอดภัย

- จัดทำแผน **Incident Response Plan (IRP)** เพื่อให้สามารถรับมือกับเหตุการณ์ทางไซเบอร์ได้อย่างมีประสิทธิภาพ
- ฝึกอบรมทีมงานเกี่ยวกับวิธีรับมือกับ **Phishing, Malware, DDoS Attack, Data Breach** เป็นต้น
- มีการทดสอบระบบ **Penetration Testing (Pentest)** เป็นระยะเพื่อประเมินความปลอดภัยของเครือข่าย

---

2. นโยบายด้านความปลอดภัยสำหรับผู้ใช้งานระบบคอมพิวเตอร์ (Users)

ผู้ใช้งานเป็นจุดอ่อนที่มักถูกโจมตีมากที่สุดในระบบ ดังนั้นต้องมีนโยบายที่ชัดเจนในการป้องกันความเสี่ยงที่เกิดจากพฤติกรรมของผู้ใช้งาน

2.1 การใช้รหัสผ่านและข้อมูลส่วนตัว

- ใช้รหัสผ่านที่ **ซับซ้อน** (มีตัวอักษรพิมพ์เล็ก-ใหญ่ ตัวเลข และอักขระพิเศษ)
- ห้ามใช้รหัสผ่านเดิมซ้ำกันระหว่างหลายบัญชี
- ห้ามแชร์รหัสผ่านกับผู้อื่นหรือจดไว้ในที่เปิดเผย
- เปิดใช้งาน **Multi-Factor Authentication (MFA)** ในระบบที่รองรับ

2.2 การใช้งานอีเมลและเว็บไซต์

- หลีกเลี่ยงการเปิด **ไฟล์แนบ (Attachments)** และลิงก์จากอีเมลที่ไม่รู้จัก
- ห้ามกรอกข้อมูลส่วนตัวในเว็บไซต์ที่ไม่น่าเชื่อถือ
- ตรวจสอบ URL ก่อนคลิกลิงก์เสมอ (โดยเฉพาะลิงก์ที่ส่งมาทางอีเมลหรือข้อความ)
- ใช้ **VPN** เมื่อเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะ

2.3 การป้องกันมัลแวร์และภัยคุกคามทางไซเบอร์

- ห้ามติดตั้งซอฟต์แวร์หรือส่วนเสริม (Extensions) ที่ไม่ได้รับอนุญาตจากองค์กร
- หลีกเลี่ยงการใช้ **USB Drive หรือ External Storage** ที่ไม่รู้จักเสียบเข้ากับคอมพิวเตอร์องค์กร
- ห้ามดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ
- เปิดใช้งาน **Antivirus** และอัปเดตซอฟต์แวร์ให้เป็นปัจจุบันเสมอ

2.4 การป้องกันข้อมูลส่วนตัวและข้อมูลขององค์กร

- หลีกเลี่ยงการแชร์ข้อมูลที่เป็นความลับขององค์กรบน Social Media หรือแอปพลิเคชันแชทส่วนตัว
- ไม่ถ่ายภาพหน้าจอที่มีข้อมูลสำคัญขององค์กรโดยไม่ได้รับอนุญาต
- ใช้เครื่องมือเข้ารหัส (Encryption) ในการส่งข้อมูลที่เป็นความลับ

2.5 การรายงานเหตุการณ์ผิดปกติ

- หากพบพฤติกรรมที่น่าสงสัย เช่น อีเมลฟิชชิ่ง หรือกิจกรรมที่ผิดปกติบนบัญชี ให้แจ้งฝ่าย IT ทันที

- ห้ามพยายามแก้ไขปัญหาด้วยตนเองหากไม่มีความรู้ด้านเทคนิคเพียงพอ
- ให้ความร่วมมือกับทีม IT เมื่อมีการตรวจสอบระบบหรือเหตุการณ์ความปลอดภัยเกิดขึ้น

สรุป

นโยบายด้าน IT Security ขององค์กรจำเป็นต้องครอบคลุมทั้งผู้ดูแลระบบและผู้ใช้งาน โดย **ผู้ดูแลระบบ (Administrators)** ต้องรับผิดชอบในการรักษาความปลอดภัยของระบบเครือข่าย อัปเดตซอฟต์แวร์ และติดตามภัยคุกคาม ขณะที่ **ผู้ใช้งาน (Users)** ต้องปฏิบัติตามแนวทางการใช้งานที่ปลอดภัย หลีกเลี่ยงพฤติกรรมที่อาจเป็นช่องโหว่ และแจ้งเหตุการณ์ผิดปกติให้ฝ่าย IT ทราบโดยเร็ว

การทำให้ทุกฝ่ายเข้าใจและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด จะช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และทำให้ระบบขององค์กรมีความมั่นคงปลอดภัยในระยะยาว

สัญญาข้อกำหนดด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ

(Information Technology Security Agreement)

ระหว่าง

[ชื่อองค์กร] ซึ่งต่อไปนี้เรียกว่า "ผู้ว่าจ้าง"

และ

[ชื่อผู้ให้บริการ] ซึ่งต่อไปนี้เรียกว่า "ผู้ให้บริการ"

วันที่ทำสัญญา: [วันที่ทำสัญญา]

ระยะเวลาสัญญา: [ระยะเวลาสัญญา เช่น 1 ปี หรือ ตามข้อตกลง]

---

1. วัตถุประสงค์ของสัญญา

สัญญานี้มีวัตถุประสงค์เพื่อกำหนด **ข้อตกลงด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ (IT Security Requirements)** ระหว่างผู้ว่าจ้างและผู้ให้บริการ เพื่อป้องกันภัยคุกคามทางไซเบอร์และปกป้องข้อมูลขององค์กรจากการรั่วไหล การเข้าถึงโดยไม่ได้รับอนุญาต และการใช้งานโดยมิชอบ

---

2. ขอบเขตของสัญญา

ผู้ให้บริการตกลงให้บริการด้านระบบคอมพิวเตอร์และเครือข่ายของผู้ว่าจ้าง ตามขอบเขตดังต่อไปนี้:

2.1 การจัดการและดูแลรักษาระบบคอมพิวเตอร์และเครือข่าย

2.2 การรักษาความปลอดภัยของข้อมูลและระบบเครือข่าย

2.3 การตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์

2.4 การสำรองข้อมูลและการกู้คืนข้อมูล

2.5 การปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับความปลอดภัยทาง IT

---

3. ข้อกำหนดด้านความปลอดภัยทาง IT

3.1 การรักษาความปลอดภัยของข้อมูล

- ผู้ให้บริการต้องรักษาข้อมูลทั้งหมดของผู้ว่าจ้างเป็น **ข้อมูลลับ** และไม่นำไปเผยแพร่หรือใช้ในทางที่ผิด
- ห้ามมิให้ผู้ให้บริการคัดลอก ถ่ายโอน หรือจัดเก็บข้อมูลของผู้ว่าจ้างโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร
- ผู้ให้บริการต้องเข้ารหัสข้อมูลสำคัญขององค์กรและปฏิบัติตามมาตรฐาน **ISO 27001** หรือ **NIST Cybersecurity Framework**

3.2 การจัดการบัญชีและสิทธิ์การเข้าถึง

- ผู้ให้บริการต้องใช้ หลักการ **Least Privilege Access** ให้สิทธิ์เข้าถึงเฉพาะบุคคลที่จำเป็น
- ต้องมีมาตรการ **Multi-Factor Authentication (MFA)** สำหรับการเข้าถึงระบบสำคัญ
- ผู้ให้บริการต้องจัดทำ **Log การเข้าใช้งานระบบ** และส่งให้ผู้ว่าจ้างตรวจสอบเป็นระยะ

3.3 การอัปเดตและบำรุงรักษาระบบ

- ผู้ให้บริการต้องอัปเดต **ซอฟต์แวร์ แพตช์ความปลอดภัย และเฟิร์มแวร์** ตามระยะเวลาที่เหมาะสม
- ดำเนินการ **Penetration Testing (Pentest)** และแจ้งผลให้ผู้ว่าจ้างทราบทุก [X เดือน]
- ติดตั้ง **Firewall, Intrusion Detection System (IDS), และ Intrusion Prevention System (IPS)**

3.4 การสำรองข้อมูลและการกู้คืนระบบ

- ผู้ให้บริการต้องดำเนินการ **สำรองข้อมูล (Backup)** อย่างสม่ำเสมอ และตรวจสอบความถูกต้องของข้อมูลสำรอง
- ต้องมีแผน **Disaster Recovery Plan (DRP)** เพื่อให้สามารถกู้คืนระบบได้อย่างรวดเร็ว
- จัดเก็บข้อมูลสำรองแยกออกจากระบบหลัก และใช้มาตรการเข้ารหัสข้อมูลสำรอง

3.5 การตรวจสอบและติดตามภัยคุกคาม

- ผู้ให้บริการต้องมี ระบบตรวจจับภัยคุกคามทางไซเบอร์ **(Threat Detection System)**

- ต้องรายงาน **เหตุการณ์ความปลอดภัยทางไซเบอร์ (Cybersecurity Incident)** ให้ผู้ว่าจ้างทราบภายใน [X ชั่วโมง]
- ต้องจัดทำ **Security Audit Report** ให้ผู้ว่าจ้างทุก [X เดือน]

3.6 การปฏิบัติตามกฎหมายและมาตรฐาน

- ผู้ให้บริการต้องปฏิบัติตามกฎหมายที่เกี่ยวข้อง เช่น **PDPA, GDPR, และ Cybersecurity Act**
- ปฏิบัติตามมาตรฐานความปลอดภัยสากล เช่น **ISO/IEC 27001, NIST, CIS Controls**

---

4. เงื่อนไขและบทลงโทษกรณีละเมิดข้อตกลง

4.1 หากผู้ให้บริการ **ละเมิดข้อตกลงด้านความปลอดภัย** เช่น การปล่อยให้ข้อมูลรั่วไหล การละเลยการอัปเดตซอฟต์แวร์ หรือการไม่แจ้งเหตุการณ์ความปลอดภัยภายในเวลาที่กำหนด ผู้ว่าจ้างมีสิทธิ์เรียกร้องค่าเสียหายตามกฎหมาย

4.2 หากมีการละเมิดข้อมูล (Data Breach) ผู้ให้บริการต้อง **รับผิดชอบค่าใช้จ่ายทั้งหมดในการกู้คืนระบบและค่าเสียหายที่เกิดขึ้น**

4.3 ผู้ว่าจ้างมีสิทธิ์ **ยกเลิกสัญญาโดยไม่ต้องแจ้งล่วงหน้า** หากพบว่าผู้ให้บริการจงใจละเมิดข้อกำหนดด้านความปลอดภัย

---

5. การยกเลิกสัญญา

5.1 สัญญานี้สามารถยกเลิกได้โดยฝ่ายใดฝ่ายหนึ่ง โดยแจ้งเป็นลายลักษณ์อักษรล่วงหน้า [X วัน]

5.2 หากผู้ให้บริการละเมิดเงื่อนไขที่สำคัญของสัญญา ผู้ว่าจ้างสามารถยกเลิกสัญญาได้ทันที

---

6. ข้อกำหนดอื่นๆ

6.1 สัญญานี้อยู่ภายใต้กฎหมายของ **[ประเทศหรือเขตอำนาจศาลที่เกี่ยวข้อง]**

6.2 หากมีข้อพิพาทเกิดขึ้น ทั้งสองฝ่ายต้องพยายามเจรจาเพื่อหาข้อยุติก่อน หากไม่สามารถตกลงกันได้ ให้ดำเนินการตามกฎหมาย

6.3 ข้อตกลงใดๆ ที่เพิ่มเติมจากสัญญานี้ต้องได้รับการยืนยันเป็นลายลักษณ์อักษรจากทั้งสองฝ่าย

ลงนามสัญญา

ฝ่ายผู้ว่าจ้าง

ชื่อ: _____

ตำแหน่ง: _____

วันที่: _____

ฝ่ายผู้ให้บริการ

ชื่อ: _____

ตำแหน่ง: _____

วันที่: _____