บริษัท โนเบิล มายด์ จำกัด (สำนักงานใหญ่)
NOBLE MIND CO.,LTD.
เลขที่ 8 ซอยเอกชัย 76/1 ถนนเอกชัย แขวงคลองบางพราน เขตบางบอน กรุงเทพฯ 10150
8 soi Ekkachai 76/1, Ekkachai Rd., Kwang Khlong Bang Phran, Ket Bangbon Bangkok 10150 Thailand.
โทร./Tel. (66 2)-416-4646 โทรสาร./Fax (66 2)-416-3324 E-Mail : info@noblemind-nm.com

ที่ 12 Rev.00

ประกาศ
เรื่อง นโยบายการด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์ (Objective)

เพื่อกำหนดมาตรฐานและแนวทางปฏิบัติในการปกป้องข้อมูล ระบบคอมพิวเตอร์ เครือข่าย และทรัพย์สินทางเทคโนโลยีสารสนเทศของบริษัท ให้รอดพ้นจากภัยคุกคาม การเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือการนำไปใช้ในทางที่ผิด

2. ขอบเขต (Scope)

นโยบายฉบับนี้มีผลบังคับใช้กับพนักงาน ผู้รับเหมา ลูกจ้างชั่วคราว และบุคคลภายนอกทุกคนที่ใช้งานอุปกรณ์ เครือข่าย หรือเข้าถึงข้อมูลของ [ชื่อบริษัท]

3. ความรับผิดชอบ (Roles & Responsibilities)

- **ฝ่าย IT/ความปลอดภัยไซเบอร์:** มีหน้าที่ดูแล บำรุงรักษา ตรวจสอบ และบังคับใช้นโยบายนี้
- **พนักงานและผู้ใช้งาน:** มีหน้าที่ปฏิบัติตามนโยบายอย่างเคร่งครัด และรายงานความผิดปกติทันทีที่พบ
- **ผู้บริหาร:** สนับสนุนทรัพยากรและเป็นผู้นำในการผลักดันให้เกิดความตระหนักรู้ด้านความปลอดภัย

4. การควบคุมการเข้าถึงข้อมูลและระบบ (Access Control Policy)

- การให้สิทธิ์การเข้าถึงระบบและข้อมูล จะใช้หลักการ **"ให้สิทธิ์เท่าที่จำเป็น" (Principle of Least Privilege)** ตามหน้าที่ความรับผิดชอบ
- ห้ามผู้ใช้งานแบ่งปันบัญชีผู้ใช้ (Username) หรือรหัสผ่าน (Password) ให้แก่บุคคลอื่นโดยเด็ดขาด
- เมื่อมีการพ้นสภาพพนักงานหรือย้ายแผนก ฝ่าย IT ต้องระงับหรือปรับเปลี่ยนสิทธิ์การเข้าถึงทันที

5. นโยบายรหัสผ่าน (Password Policy)

- รหัสผ่านต้องมีความยาวไม่น้อยกว่า [เช่น 8 หรือ 12] ตัวอักษร ประกอบด้วยตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์พิเศษ
- บังคับให้มีการเปลี่ยนรหัสผ่านทุกๆ [เช่น 90] วัน
- ระบบที่สำคัญต้องเปิดใช้งานการยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication: 2FA / MFA)

6. การใช้งานอุปกรณ์และอินเทอร์เน็ตที่เหมาะสม (Acceptable Use Policy)

- อุปกรณ์ที่บริษัทจัดหาให้ (คอมพิวเตอร์ โทรศัพท์มือถือ) ต้องใช้เพื่องานของบริษัทเป็นหลัก
- ห้ามใช้เครือข่ายของบริษัทในการเข้าถึงเว็บพนัน สื่อลามกอนาจาร หรือดาวน์โหลดซอฟต์แวร์เถื่อน
- ห้ามติดตั้งซอฟต์แวร์ใดๆ ที่ไม่ได้รับอนุญาตจากฝ่าย IT ลงบนอุปกรณ์ของบริษัท
- อุปกรณ์เคลื่อนที่และแล็ปท็อปของบริษัท ต้องมีการตั้งรหัสล็อกหน้าจอ (Screen Lock) เสมอ

7. การจัดการข้อมูลและการสำรองข้อมูล (Data Management & Backup)

- ข้อมูลที่เป็นความลับของบริษัทหรือข้อมูลส่วนบุคคล (PDPA) ต้องได้รับการเข้ารหัส (Encryption) หากต้องส่งผ่านอินเทอร์เน็ตหรือบันทึกลงแฟลชไดร์ฟ (USB)
- ฝ่าย IT ต้องจัดให้มีการสำรองข้อมูล (Backup) ระบบที่สำคัญอย่างน้อยสัปดาห์ละ 1 ครั้ง (หรือตามความเหมาะสม) และต้องมีการทดสอบการกู้คืนข้อมูล (Restore Test) เป็นประจำ

8. ความปลอดภัยของระบบและเครือข่าย (Network & System Security)

- คอมพิวเตอร์ทุกเครื่องต้องติดตั้งโปรแกรมป้องกันไวรัส (Antivirus/Endpoint Protection) ที่อัปเดตฐานข้อมูลสม่ำเสมอ
- เครือข่าย Wi-Fi สำหรับพนักงานและสำหรับแขก (Guest) ต้องถูกแยกออกจากกันอย่างชัดเจน
- ต้องมีการติดตั้ง Firewall และอัปเดตระบบปฏิบัติการ (Patch Management) ให้เป็นเวอร์ชันล่าสุดเพื่ออุดช่องโหว่

9. การจัดการเหตุการณ์ละเมิดความปลอดภัย (Incident Management)

- หากผู้ใช้งานพบความผิดปกติ เช่น ติดไวรัส รหัสผ่านถูกแฮ็ก คอมพิวเตอร์หรือโทรศัพท์ของบริษัทสูญหาย ต้องแจ้งฝ่าย IT ทันทีที่ช่องทาง [ระบุเบอร์โทร/อีเมล]
- ห้ามผู้ใช้งานพยายามแก้ไขปัญหาที่เกิดจากการโจมตีทางไซเบอร์ (เช่น Ransomware) ด้วยตนเองโดยเด็ดขาด ให้ตัดการเชื่อมต่ออินเทอร์เน็ตและแจ้งฝ่าย IT ทันที

10. บทลงโทษ (Enforcement)

พนักงานที่ละเมิดนโยบายฉบับนี้ อาจถูกพิจารณาลงโทษทางวินัยตามข้อบังคับของบริษัท ซึ่งอาจรวมถึงการตักเตือน พักงาน หรือเลิกจ้าง และอาจถูกดำเนินคดีตามกฎหมายหากเกิดความเสียหายร้ายแรง

ประกาศ ณ วันที่ 6 กุมภาพันธ์ 2569

บริษัท โนเบิล มายด์ จำกัด N.M. NOBLE MIND CO.,LTD.

(นายวิสิทธิ์ ชำนาญรัตนกุล)
กรรมการผู้จัดการ

หมายเหตุ : หากมีการพบเห็นหรือทราบข้อมูลการกระทำผิดที่ละเมิดข้อปฏิบัติของนโยบายนี้ สามารถแจ้งข้อมูล โดยใช้ช่องทางการแจ้งข้อร้องเรียน ซึ่งทางบริษัทฯ ได้กำหนดไว้ และอ้างอิงตามนโยบายการแจ้งเบาะแสการกระทำผิด (Whistle Blower Policy)