แนวปฏิบัติและระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ (IT Policy & Guidelines)
กองทรัพยากรทุนมนุษย์ สำนักงานมหาวิทยาลัย มหาวิทยาลัยเชียงใหม่

1. วัตถุประสงค์ (Objective)

1. เพื่อกำหนดมาตรฐานและแนวปฏิบัติในการใช้งานระบบคอมพิวเตอร์และข้อมูลขององค์กร
2. เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญและลดความเสี่ยงด้าน Cybersecurity
3. เพื่อสร้างวัฒนธรรมการใช้งานเทคโนโลยีที่มีความรับผิดชอบและมีความปลอดภัย

2. ขอบเขต (Scope)

เอกสารนี้ครอบคลุมถึง

1. ผู้ใช้งานทุกคน (User) : บุคลากรมหาวิทยาลัย, นักศึกษาฝึกงาน, นักศึกษาปฏิบัติงาน และบุคคลภายนอกที่ได้รับสิทธิ์เข้าถึงระบบ
2. ข้อมูลทั้งหมดขององค์กร : รูปแบบดิจิทัลหรือเอกสารกระดาษ
3. อุปกรณ์และระบบสารสนเทศ เช่น คอมพิวเตอร์, Notebook, Server, Mobile Device, ระบบ Cloud, และ Network

3. แนวทางการจัดการบัญชีผู้ใช้งาน (User Account Management)

3.1 การสร้างบัญชี

- ต้องได้รับ **อนุมัติจากหัวหน้างาน/ผู้มีอำนาจ** ก่อนสร้างบัญชีผู้ใช้งาน โดยจะเป็นบุคลากรที่ได้เซ็นสัญญาจ้างอย่างเป็นทางการ เพื่อนำสัญญาจ้างไปขอเปิดใช้งาน CMU Account ที่สำนักบริการเทคโนโลยีสารสนเทศ (ITSC)
- ใช้ข้อมูลจริงของผู้ใช้งาน เช่น ชื่อ-นามสกุล ห้ามใช้ชื่อปลอม

3.2 การกำหนดสิทธิ์ (Access Control)

- ให้สิทธิ์เท่าที่จำเป็น
- ผู้ใช้งานต้องมีบัญชีของตนเอง ห้ามแชร์บัญชีร่วมกัน

3.3 การยกเลิกบัญชี

1. ใช้นโยบายการยกเลิกบัญชีของมหาวิทยาลัย

4. การกำหนดรหัสผ่าน (Password Policy)

รายการ	มาตรฐาน
ความยาวรหัสผ่าน	อย่างน้อย 8-12 ตัวอักษร
องค์ประกอบ	ต้องมีตัวอักษรพิมพ์เล็ก, พิมพ์ใหญ่, ตัวเลข และอักขระพิเศษ
การเปลี่ยนรหัสผ่าน	ทุก 90 วัน หรือทันทีเมื่อสงสัยว่าถูกขโมย
การห้ามใช้	ห้ามใช้รหัสผ่านซ้ำกับระบบอื่นหรือข้อมูลส่วนตัว เช่น วันเกิด, เบอร์โทร
Password ของไฟล์/เอกสาร	ต้องไม่ต่ำกว่า 8 ตัวอักษร และตั้งให้เฉพาะผู้มีสิทธิ์เข้าถึงเท่านั้น

5. การล็อกหน้าจอ (Screen Lock)

1. ต้องตั้งค่าให้คอมพิวเตอร์ ล็อกหน้าจออัตโนมัติภายใน 10 นาที หากไม่มีการใช้งาน
2. เมื่อต้องออกจากโต๊ะทำงาน ให้ กด Lock Screen ทันที (Windows: Win + L, Mac: Ctrl + Command + Q)
3. ห้ามปล่อยคอมพิวเตอร์เปิดไว้โดยไม่มีการป้องกัน

6. การใช้คอมพิวเตอร์และอุปกรณ์ IT

6.1 การใช้งานทั่วไป

- ใช้เพื่องานขององค์กรเท่านั้น ห้ามใช้เพื่อธุรกิจส่วนตัว
- ห้ามติดตั้ง โปรแกรมไม่ได้รับอนุญาต เช่น Crack, เกม หรือซอฟต์แวร์ละเมิดลิขสิทธิ์
- ต้องอัปเดต Antivirus, Patch Security และ OS Update อย่างสม่ำเสมอ
- ห้ามเชื่อมต่อ USB Drive หรืออุปกรณ์ภายนอก โดยไม่ได้รับอนุญาต

6.2 การป้องกันภัยไซเบอร์

- ห้ามคลิกลิงก์หรือเปิดไฟล์แนบจาก อีเมลที่ไม่น่าเชื่อถือ
- ใช้ VPN และ MFA (Multi-Factor Authentication) เมื่อต้องเชื่อมต่อระบบจากภายนอกองค์กร ตามนโยบายของสำนักบริการเทคโนโลยีสารสนเทศ (ITSC) อ้างอิงจาก : https://network.cmu.ac.th/wiki/index.php/CMU_GlobalProtect_VPN
- หากพบพฤติกรรมผิดปกติ เช่น ไฟล์หาย, เครื่องทำงานผิดปกติ ต้องแจ้งฝ่าย IT ภายใน 30 นาที

7. การจัดการข้อมูลความลับ (Confidential Data)

7.1 ระดับความลับของข้อมูล

ระดับข้อมูล	ตัวอย่าง	แนวทางการจัดการ
Confidential (ลับมาก)	ข้อมูลส่วนตัวบุคลากร, Password	ต้องเข้ารหัสก่อนเก็บ/ส่ง ห้ามแชร์ผ่าน Cloud ส่วนตัว
Internal Use (ใช้ภายใน)	นโยบาย, รายงานประชุม	แชร์ได้เฉพาะผู้เกี่ยวข้องภายในองค์กร
Public (สาธารณะ)	เอกสารประชาสัมพันธ์	เผยแพร่ได้โดยไม่ต้องเข้ารหัส

7.2 การนำข้อมูลความลับมาใช้

- ต้องได้รับอนุญาตจากเจ้าของข้อมูลหรือหัวหน้างานก่อนใช้งาน โดยเป็นการกำหนดในการเข้าใช้งานสิทธิ์ในแต่ละระบบจากการตั้งค่าของผู้มีอำนาจในการตัดสินใจ หรือเป็นเจ้าหน้าที่บุคคลที่ได้รับมอบหมาย
- ใช้เฉพาะข้อมูลที่จำเป็น
- หากเก็บไว้ในคอมพิวเตอร์ ต้องเก็บใน Folder ที่เข้ารหัส เช่น BitLocker, VeraCrypt
- ห้ามเก็บข้อมูลลับใน Cloud ส่วนตัว เช่น Google Drive, Dropbox, Line

8. การส่งข้อมูล (Data Transmission)

1. ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรก่อนทุกครั้ง และต้องเก็บหลักฐานการอนุมัติและการส่งข้อมูล ไว้เพื่อการตรวจสอบ เช่น ใบอนุมัติ อีเมล หรือบันทึกการประชุม
2. ใช้เฉพาะช่องทางที่ มีการเข้ารหัสและมีระบบรักษาความปลอดภัย เช่น Secure Email Gateway, SFTP, หรือ โฟลเดอร์ที่มีการกำหนดสิทธิ์การเข้าถึง (Access Control)
3. ห้ามส่งข้อมูลสำคัญผ่านช่องทางสื่อสารทั่วไป เช่น LINE, Facebook, Gmail ส่วนตัว หรือ Cloud ส่วนตัว ต้องใช้ CMU Mail หรือช่องทางที่กองทรัพยากรทุนมนุษย์กำหนดไว้ เท่านั้น
4. ไฟล์เอกสารที่มีข้อมูลสำคัญหรือข้อมูลส่วนบุคคล ต้องตั้งรหัสผ่านก่อนทุกครั้ง
5. เอกสารทุกฉบับต้องแนบข้อความกำกับความลับอย่างชัดเจน เช่น “เอกสารนี้เป็นความลับของมหาวิทยาลัยเชียงใหม่ ห้ามเผยแพร่ คัดลอก หรือส่งต่อโดยไม่ได้รับอนุญาต หากคุณไม่ใช่ผู้รับ กรุณาลบเอกสารนี้ทันที” และต้องมีลายน้ำ (Watermark) ระบุว่าเป็น Confidential หรือ ข้อมูลลับ บนหน้าเอกสารทุกหน้า
6. ก่อนส่งข้อมูลต้องตรวจสอบและยืนยันตัวตนผู้รับว่าเป็นบุคคลที่มีสิทธิ์เข้าถึงข้อมูล และต้องส่งไปยัง E-mail หรือช่องทางที่เป็นทางการเท่านั้น เช่น E-mail กลางของส่วนงาน

9. การส่งต่อข้อมูล (Forwarding Data)

1. ต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อนทุกครั้ง
2. ตรวจสอบสิทธิ์ของผู้รับว่าเป็นผู้ที่มีสิทธิ์เข้าถึง
3. ส่งเฉพาะข้อมูลที่จำเป็นไม่รวมข้อมูลส่วนเกิน
4. เก็บ Log หรือ Email ยืนยันการส่งต่อเป็นหลักฐาน

10. การทำลายข้อมูล (Secure Data Disposal)

1. ข้อมูลดิจิทัลที่หมดอายุ ต้องลบออกจากเครื่องคอมพิวเตอร์ และ drive shared ต่างๆที่เก็บไว้
2. ทำลายเอกสารตามระเบียบสารบรรณ

ประกาศ ณ วันที่ 15 ตุลาคม 2568

นายวิรุฬห์ ถูกจิตต์
ผู้อำนวยการกองทรัพยากรทุนมนุษย์