นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์

(Clear desk Clear screen Policy)

คณะเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏเชียงราย

---

1. วัตถุประสงค์

เพื่อกำหนดแนวทางในการป้องกันข้อมูลและระบบสารสนเทศของคณะเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏเชียงราย โดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยของทรัพย์สินที่มีความสำคัญภายในองค์กรของคณะเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏเชียงราย ให้เป็นไปตามความรับผิดชอบของผู้ใช้งาน (User responsibilities) ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และนโยบายความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยราชภัฏเชียงราย รวมทั้งกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2553 เพื่อสร้างจิตสำนึกที่ดีและเป็นมาตรฐานเดียวกันในการป้องกันความเสียหายที่อาจเกิดขึ้นจากการเปิดเผยข้อมูลที่สำคัญขององค์กร และการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต หรือเกิดจากการสื่อสารทางอิเล็กทรอนิกส์ที่ไม่ปลอดภัย เพื่อป้องกันการเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ์

2. ขอบเขต

นโยบายนี้ครอบคลุมถึงบุคลากรทุกคนในคณะเทคโนโลยีดิจิทัล รวมถึงผู้ปฏิบัติงานที่ได้รับมอบหมายให้ดำเนินการกับข้อมูลสารสนเทศ ไม่ว่าจะเป็นในรูปแบบกระดาษหรือสื่ออิเล็กทรอนิกส์ ตลอดจนผู้ใช้งานอุปกรณ์สำนักงานและระบบเครือข่ายของหน่วยงาน

3. นโยบาย

ผู้ใช้งานทุกคนจะตระหนักถึงความต้องการทางความปลอดภัยและวิธีการสำหรับการป้องกันข้อมูลเพื่อประโยชน์แก่ผู้ใช้งานไม่อยู่ และมีความรับผิดชอบในการปกป้องข้อมูลที่สำคัญ ดังนี้

แนวปฏิบัติหลัก

1. โต๊ะทำงานต้องไม่มีเอกสารหรือวัสดุที่เป็นข้อมูลสำคัญ โดยเอกสารต้องถูกเก็บในที่ปลอดภัยเมื่อไม่ใช้งาน
2. ไม่ควรทิ้งเอกสารไว้บนเครื่องพิมพ์หรือเครื่องถ่ายเอกสารโดยไม่จัดเก็บทันทีหลังใช้งาน
3. ห้ามให้บุคคลอื่นใช้คอมพิวเตอร์หรือระบบงานแทนโดยไม่ได้รับอนุญาตอย่างเป็นทางการ
4. คอมพิวเตอร์ต้องเข้าสู่ระบบหน้าจอล็อกอัตโนมัติภายในเวลาไม่เกิน 5 นาที หากไม่มีการใช้งาน
5. ห้ามมีการใช้อุปกรณ์จัดเก็บข้อมูลหรืออุปกรณ์ภายนอกใด ๆ ที่ไม่ได้รับอนุญาตต่อกับอุปกรณ์ของหน่วยงาน
6. ห้ามขีดเขียนหรือแปะรหัสผ่าน ข้อมูลลับ หรือรหัสพนักงานบน Post-it หรือใต้คีย์บอร์ด หรือบริเวณที่มองเห็นได้ง่าย
7. เมื่อเลิกงาน/สิ้นสุดการใช้งานโต๊ะ ต้องตรวจสอบและเคลียร์เอกสารทุกแผ่นออกจากพื้นผิวโต๊ะ

การควบคุมสิ่งที่เก็บข้อมูลและทรัพย์สินด้านสารสนเทศ

1. อุปกรณ์จัดเก็บข้อมูล เช่น Flash Drive, External Hard Disk, CD-ROM ต้องได้รับอนุญาตจากหัวหน้างานก่อนการใช้งาน
2. ข้อมูลที่จัดเก็บในสื่อบันทึกข้อมูลภายนอกต้องเข้ารหัสและตั้งรหัสผ่าน หากเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่มีความอ่อนไหว
3. การนำสื่อบันทึกออกจากหน่วยต้องขอมีการลงทะเบียน หรือบันทึกการออกไว้โดยผู้รับผิดชอบ
4. ปิดการใช้งาน Active Session เมื่อทำงานเสร็จ หรือหยุดทำงานชั่วคราว เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญ ควรมีการรักษาความปลอดภัยโดยล็อกหน้าจอหรือปิดโปรแกรม เช่น โปรแกรมที่ทำการจัดการข้อมูลหรือระบบที่สำคัญ
5. ห้ามมีการถ่ายโอนข้อมูลโดยการใช้เครื่องคอมพิวเตอร์ที่มิได้รับอนุญาตต่ออินเทอร์เน็ตโดยผิดกฎหมาย

การควบคุมการป้องกันผู้ใช้งานและการเข้ารหัสข้อมูลที่เป็นความลับ

1. ผู้ใช้งานทุกคนต้องเก็บรักษารหัสผ่านที่สำคัญ และห้ามเปิดเผยรหัสผ่านให้ผู้อื่นทราบ
2. การจัดเก็บข้อมูลที่เป็นความลับในสื่อบันทึกข้อมูล เช่น ฮาร์ดดิสก์ เซิร์ฟเวอร์ หรือข้อมูลจากทางอิเล็กทรอนิกส์ต่าง ๆ ต้องเข้ารหัสทั้งในขณะพัก (At Rest) และขณะส่งผ่านระบบ (In Transit)
3. ห้ามใช้บัญชีผู้ใช้งานร่วมกันระหว่าบุคลากร และต้องมีการตรวจสอบสิทธิ์การใช้งานในระบบอย่างน้อยปีละ 1 ครั้ง
4. ผู้ใช้งานอาจมีการเข้ารหัสลับใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับราชการ พ.ศ. ๒๕๔๔

แนวทางการสำรองข้อมูลจากเครื่องคอมพิวเตอร์

เพื่อให้การบริหารจัดการข้อมูลของหน่วยงานมีความมั่นคง ปลอดภัย และสามารถกู้คืนข้อมูลได้อย่างมีประสิทธิภาพในกรณีที่เกิดเหตุขัดข้องหรือสูญหาย จึงกำหนดแนวทางการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้ดังนี้

1. **กำหนดประเภทของข้อมูลที่ต้องสำรอง**
   ให้หน่วยงานพิจารณาและจัดประเภทของข้อมูลที่มีความสำคัญ เช่น ข้อมูลการบริหารจัดการ ข้อมูลทางการเงิน ข้อมูลเอกสารราชการ หรือข้อมูลส่วนบุคคลของเจ้าหน้าที่ เพื่อจัดลำดับความสำคัญในการสำรองข้อมูล
2. **กำหนดรอบระยะเวลาในการสำรองข้อมูล**
   ให้ดำเนินการสำรองข้อมูลเป็นประจำตามรอบระยะเวลาที่เหมาะสม เช่น รายวัน รายสัปดาห์ หรือรายเดือน ทั้งนี้ขึ้นอยู่กับความสำคัญและความถี่ในการเปลี่ยนแปลงของข้อมูล
3. **ใช้สื่อหรือระบบจัดเก็บข้อมูลที่มีความปลอดภัย**
   ให้จัดเก็บข้อมูลสำรองไว้ในสื่อที่มีความปลอดภัยและได้มาตรฐาน เช่น External Hard Disk, Network Attached Storage (NAS), หรือระบบ Cloud Storage ที่ได้รับการรับรองมาตรฐานด้านความปลอดภัยของข้อมูล
4. **จัดเก็บข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัยและแยกจากระบบหลัก**
   เพื่อป้องกันความเสียหายจากเหตุการณ์ไม่คาดคิด เช่น ไฟไหม้ น้ำท่วม หรือไวรัสคอมพิวเตอร์ ให้จัดเก็บข้อมูลสำรองไว้ในสถานที่แยกจากเครื่องคอมพิวเตอร์หลักหรือระบบเครือข่ายภายใน
5. **ตรวจสอบและทดสอบความสมบูรณ์ของข้อมูลสำรองเป็นระยะ**
   ให้มีการตรวจสอบไฟล์ข้อมูลสำรองและทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถใช้งานได้จริงเมื่อเกิดเหตุฉุกเฉิน

สรุปนโยบาย

นโยบาย Clear-desk-Clear-screen ต้องถูกนำมาใช้อย่างเหมาะสมกับประเภทของข้อมูล ข้อกำหนดของกฎหมายและสัญญาและความเสี่ยงต่าง ๆ ที่เกี่ยวข้อง รวมทั้งความตระหนักของคณะเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏเชียงราย โดยมีแนวทางต่อไปนี้ควรได้รับการพิจารณา

1. ข้อมูลทางการดำเนินงานที่เกี่ยวข้องกับสื่อสำคัญ เช่น บันทึกประชุมหรือบันทึกข้อมูลอิเล็กทรอนิกส์ ต้องถูกจัดเก็บอย่างปลอดภัย (เช่น ในตู้นิรภัย ตู้ หรือชั้นที่มีการล็อก) ซึ่งไม่อนุญาตให้บุคคลอื่นเข้าถึงได้โดยเฉพาะอย่างยิ่งในเวลาที่ไม่มีผู้ปฏิบัติงาน เช่น เวลาพัก หรือเลิกงาน เป็นต้น
2. อุปกรณ์คอมพิวเตอร์ที่ไม่ได้ใช้งาน ต้องดำเนินการ log-off หรือ lock หน้าจอด้วยรหัสผ่าน token หรือวิธีการพิสูจน์ตัวตนอื่น ๆ ที่เหมาะสม
3. ต้องมีการปิดไม่ให้มีการใช้งานเครื่องสแกนเอกสาร แฟกซ์ เครื่องสแกนเนอร์ หรือกล้องดิจิตอล โดยไม่ได้รับอนุญาต

4. สื่อที่มีข้อมูลสำคัญ ที่มีการเก็บรักษาภายใน ต้องมีการนำออกจากเครื่องพิมพ์ทันทีหลังการใช้งาน
5. นโยบาย Clear-desk-Clear-screen ต้องถูกนำมาใช้อย่างเหมาะสมเพื่อป้องกันการสูญหายของข้อมูล เอกสาร และความเสียหายที่อาจเกิดขึ้นต่อข้อมูลสำคัญ และความมั่นคงปลอดภัยของหน่วยงานที่ครอบคลุมถึงการปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูล
6. จัดเก็บข้อมูลสำรองไว้ในสื่อที่มีความปลอดภัยและได้มาตรฐานเช่น External Hard Disk, Network Attached Storage (NAS), หรือระบบ Cloud Storage
7. พิจารณาการใช้เครื่องพิมพ์ที่มีการตั้ง PIN เพื่อให้ผู้ใช้งานเอกสารที่เกี่ยวข้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับงานพิมพ์ เมื่ออยู่หน้าเครื่องพิมพ์เท่านั้น

การควบคุมเอกสาร

การอนุมัติการใช้เอกสาร

เอกสารนี้ผ่านการทบทวนและอนุมัติโดย :

จัดเตรียมเอกสารโดย	ทบทวนเอกสารโดย	อนุมัติเอกสารโดย
 (นายชิณรัฐ คำมาสุข) นักวิชาการคอมพิวเตอร์	 (ผศ.อนุสรณ์ ใจแก้ว) รองคณบดีด้านการจัดการศึกษา	 (ผศ.ดร.ภูมิพงษ์ ดวงตั้ง) คณบดีคณะเทคโนโลยีดิจิทัล

ประวัติการปรับปรุงเอกสาร

ตารางบันทึกประวัติการปรับปรุงเอกสาร :

ฉบับที่	วันที่	รายละเอียดการปรับปรุงเอกสาร	อนุมัติโดย
1.0		เริ่มต้นการใช้งานเอกสาร	ผศ.ดร.ภูมิพงษ์ ดวงตั้ง