สำนักบริหารเทคโนโลยีสารสนเทศ
จุฬาลงกรณ์มหาวิทยาลัย

CYBER SECURITY POLICY

นโยบายและแนวปฏิบัติ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

1. นโยบายความมั่นคงปลอดภัยด้านกายภาพ

ครอบคลุมการรักษาความมั่นคงปลอดภัยทางกายภาพของห้องควบคุม ระบบเครือข่ายคอมพิวเตอร์ การควบคุมการเข้า-ออก การกำหนดสิทธิ์ผู้ผ่านเข้า-ออก และความปลอดภัยทางกายภาพของเครือข่ายสื่อสัญญาณภายในมหาวิทยาลัย โดยให้มีการกำหนดมาตรการและแนวทางในการป้องกันอาคารและอุปกรณ์ในห้องควบคุมระบบคอมพิวเตอร์ และมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์ การควบคุมการเข้า-ออก การแบ่งส่วนพื้นที่ และการกำหนดสิทธิ์ผู้ผ่านเข้า-ออก เพื่อให้มั่นใจได้ว่าห้องควบคุมระบบคอมพิวเตอร์มีความปลอดภัยจากอุบัติภัยทางธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม เป็นต้น หรือจากการโจรกรรมทรัพย์สินของเครือข่าย รวมถึง การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิในห้องควบคุมที่สูงเกินขีดจำกัด ห้องควบคุมมีความชื้นสูง หรือการกระทำโดยประมาท เช่น การทำน้ำหกลงเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ เป็นต้น

2. นโยบายการสำรองข้อมูลและกู้คืน

ครอบคลุมทั้งในคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคล เพื่อให้มีชุดข้อมูลสำรองกรณีเกิดความเสียหายกับข้อมูลและสามารถกู้กลับคืนมาได้อย่างมีประสิทธิภาพ โดยให้กำหนดแนวปฏิบัติในการสำรองข้อมูลและกู้คืนระบบอย่างมีขั้นตอนและลดความเสี่ยงที่อาจเกิดขึ้น เพื่อสร้างความมั่นใจในการเก็บรักษาและใช้งานข้อมูล โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้อง และสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

3. นโยบายการบริหารความเปลี่ยนแปลง

ครอบคลุมการบริหารความเปลี่ยนแปลงในระดับการปรับปรุง (Patch/Upgrade) และระดับการเปลี่ยนแปลง (Change) ระบบงานหรือระบบปฏิบัติการ โดยให้มีการกำหนดขั้นตอนและข้อปฏิบัติก่อนดำเนินการเปลี่ยนแปลง เพื่อลดความเสี่ยงในการหยุดให้บริการ และเป็นการเปลี่ยนแปลงโดยมีเหตุอันควร เพื่อให้ผู้ดูแลระบบและผู้ใช้ระบบสารสนเทศสามารถวางแผนปฏิบัติงานล่วงหน้าและลดผลกระทบที่เกิดจากการปรับเปลี่ยนได้

4. นโยบายการบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ

ครอบคลุมการเข้าถึงระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย รวมถึงการใช้งานระบบสารสนเทศต่าง ๆ ของหน่วยงานให้มีความมั่นคงปลอดภัย

5. นโยบายการบริหารจัดการบัญชีผู้ใช้และการใช้งานรหัสผ่าน

ครอบคลุมการบริหารบัญชีรายชื่อผู้ใช้งานระบบ การกำหนดรหัสผ่าน การกำหนดสิทธิ์เฉพาะผู้ที่ได้รับอนุญาต รวมถึงบัญชีของผู้ให้บริการภายนอก (Vendor) ที่มีการปฏิบัติงานโดยมีการเข้าถึงระบบต่าง ๆ ของหน่วยงาน

6. นโยบายการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีของหน่วยงาน

ครอบคลุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีที่เป็นทรัพย์สินของมหาวิทยาลัย ผู้ใช้งานมีหน้าที่รักษาให้สามารถใช้งานได้ และไม่ละเมิดความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศโดยรวมของมหาวิทยาลัย เช่น มีการติดตั้งโปรแกรมป้องกันมัลแวร์ มีการอัปเดตระบบปฏิบัติการ และอัปเดตซอฟต์แวร์อื่น ๆ ที่ติดตั้งอยู่บนเครื่องอย่างสม่ำเสมอ

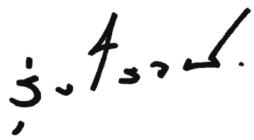
7. นโยบายการทำงานจากระยะไกล และการปฏิบัติงานนอกสถานที่ตั้ง

โดยจัดให้มีแนวทางการทำงานจากระยะไกล และการปฏิบัติงานนอกสถานที่ตั้ง ที่เหมาะสมกับบริบทสภาพแวดล้อมภายใต้สภาวะวิกฤติ เพื่อให้การปฏิบัติงานมีความยืดหยุ่น คล่องตัว รวมทั้งไม่ส่งผลกระทบหรือเกิดผลเสียหายต่อประสิทธิภาพประสิทธิผลในการดำเนินงาน และยังคงมีความมั่นคงปลอดภัยที่เพียงพอสำหรับระบบเทคโนโลยีสารสนเทศ หรือข้อมูลสารสนเทศที่ถูกเข้าถึงจากระยะไกล

8. นโยบายการดำเนินงานต่อเนื่อง Business Continuity Plan (BCP) และรับเหตุการณ์ฉุกเฉิน (Disaster)

โดยจัดให้มีแผนบริหารความต่อเนื่องการดำเนินงาน (BCP) เพื่อให้มั่นใจว่าการให้บริการที่กำหนดไว้ในแผน จะสามารถดำเนินต่อไปได้เมื่อเกิดเหตุการณ์ที่จะต้องประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงาน โดยผู้ที่ได้รับมอบหมายสามารถปฏิบัติตามกระบวนการที่กำหนดไว้ได้อย่างถูกต้อง หรือสามารถกู้คืนระบบกลับมาให้บริการต่อไปได้

ประกาศ ณ วันที่ 7 สิงหาคม 2567



(นายรุ่งโรจน์ กิตติถาวรกุล)
ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ

ความมั่นคงปลอดภัย
ด้านกายภาพ

นโยบายความมั่นคงปลอดภัยด้านกายภาพ

ให้มีการกำหนดมาตรการและแนวทางในการป้องกันอาคารและอุปกรณ์ในห้องควบคุมระบบคอมพิวเตอร์ และมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์ การควบคุมการเข้า-ออก การแบ่งส่วนพื้นที่และการกำหนดสิทธิ์ผู้ผ่านเข้า-ออก เพื่อให้มั่นใจได้ว่าห้องควบคุมระบบคอมพิวเตอร์มีความปลอดภัยจากอุบัติภัยทางธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม เป็นต้น หรือจากการโจรกรรมทรัพย์สินของเครือข่าย รวมถึง การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิในห้องควบคุมที่สูงเกินขีดจำกัด ห้องควบคุมมีความชื้นสูง หรือการกระทำโดยประมาท เช่น การทำน้ำหกลงเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ เป็นต้น

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. สบท. หมายถึง สำนักบริหารเทคโนโลยีสารสนเทศ
2. ห้องควบคุมระบบ หมายถึง ห้องที่ติดตั้งและจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่าย
3. เจ้าหน้าที่ห้องควบคุมระบบ ได้แก่ ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบฐานข้อมูล
4. ผู้บริหาร ได้แก่ ผู้อำนวยการ สบท. ผู้อำนวยการฝ่ายของ สบท.

การจัดแบ่งพื้นที่ ห้องควบคุมระบบแบ่งเป็น 2 พื้นที่ ได้แก่

- พื้นที่ควบคุม (Control Area) เป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ
- พื้นที่จำกัดการเข้าถึง (Restricted Area) เป็นห้องที่มีระบบคอมพิวเตอร์และเครือข่ายติดตั้งอยู่

ข้อกำหนดการป้องกันทางกายภาพ ประกอบด้วย

1. ข้อกำหนดของห้องควบคุมระบบ
2. ข้อกำหนดการเข้าพื้นที่ควบคุม
3. ข้อกำหนดการเข้าพื้นที่จำกัดการเข้าถึง
4. ข้อกำหนดการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

1. ข้อกำหนดของห้องควบคุมระบบ

- แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้
- จัดหา Rack ในการจัดเก็บอุปกรณ์ต่าง ๆ ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา
- ไม่วางอุปกรณ์ต่าง ๆ ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น หรือไม่วางอุปกรณ์ใกล้ประตู หน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น
- เก็บสายเครือข่าย (Network Cable) และสายไฟฟ้าให้เรียบร้อย เพื่อป้องกันการเดินสะดุด
- ติดประกาศบันทึกการบำรุงรักษา การซ่อมแซม และหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์
- ติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV ระบบควบคุมการเข้า-ออกห้อง เป็นต้น
- มีระบบและอุปกรณ์ป้องกันอัคคีภัย
- มีระบบไฟฟ้าสำรองเพื่อให้สามารถทำงานได้ตลอดเวลา และต้องมีการตรวจสอบระบบไฟฟ้าสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อเป็นการลดความเสียหายที่อาจจะเกิดขึ้น
- มีระบบป้องกันไฟฟ้าจากฟ้าผ่า
- มีระบบปรับอากาศแบบควบคุมอุณหภูมิ (10 - 26.7°C)

2. ข้อกำหนดการเข้าพื้นที่ควบคุม

- ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้น เจ้าหน้าที่ห้องควบคุมระบบ บุคลากร สบท. ที่ได้รับอนุญาต ผู้บริหาร หรือบุคคลที่ผู้บริหารนำเข้าเยี่ยมชม
- บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุม ต้องได้รับอนุญาตจากผู้บริหาร และจะต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา
- ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลให้เกิดความเสียหายต่อทรัพย์สินของ สบท. บุคคลอื่นอาจเข้าในพื้นที่ควบคุมได้หากได้รับอนุญาตจากผู้บริหาร
- ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าในเขตพื้นที่ควบคุม

3. ข้อกำหนดการเข้าพื้นที่จำกัดการเข้าถึง

- ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้น เจ้าหน้าที่ห้องควบคุมระบบ
- ในกรณีมีบุคคลที่มีความจำเป็นต้องเข้าไปปฏิบัติงานในพื้นที่จำกัดการเข้าถึง บุคคลดังกล่าวต้องได้รับอนุญาตจากผู้บริหาร และต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย 1 คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง
- กรณีมีบุคคลที่ได้รับคำสั่งจากผู้บริหารให้เข้าปฏิบัติหน้าที่ในพื้นที่จำกัดการเข้าถึง จะต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย 1 คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง
- ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง
- ไม่อนุญาตให้มีการเข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง
- ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลให้เกิดความเสียหายต่อทรัพย์สินของ สบท. บุคคลอื่นสามารถเข้าไปในพื้นที่จำกัดการเข้าถึงได้ หากได้รับอนุญาตจากผู้บริหาร

4. ข้อกำหนดการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

- ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก 3 เดือน
- กำหนดขั้นตอนและแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟไหม้ หรือมีผู้บุกรุก เป็นต้น
- ทำการซ้อมการปฏิบัติงานรับมือต่อกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ 1 ครั้ง
- ต้องบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย อย่างสม่ำเสมอ หรือตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

การสำรองข้อมูล
และกู้คืน

นโยบายการสำรองข้อมูลและกู้คืน

ครอบคลุมทั้งในคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคล เพื่อให้มีชุดข้อมูลสำรองกรณีเกิดความเสียหายกับข้อมูล และสามารถกู้กลับคืนมาได้อย่างมีประสิทธิภาพ โดยให้กำหนดแนวปฏิบัติในการสำรองข้อมูลและกู้คืนระบบอย่างมีขั้นตอนและลดความเสี่ยงที่อาจเกิดขึ้น เพื่อสรางความมั่นใจในการเก็บรักษาและใช้งานข้อมูล โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถ ดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ดูแลระบบคอมพิวเตอร์ หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลจัดการระบบคอมพิวเตอร์
2. ผู้ดูแลระบบเครือข่าย หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลจัดการระบบเครือข่าย
3. ผู้ใช้ ได้แก่ บุคลากร หรือ นิสิตที่มีชื่ออยู่ในบัญชีรายชื่อที่ออกโดยสำนักบริหารเทคโนโลยีสารสนเทศ และ/หรือ บุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์ และ/หรือ ระบบสารสนเทศของมหาวิทยาลัย
4. การสำรองข้อมูล หมายถึง การทำสำรองข้อมูลทั้งหมด (Full Backup) เพื่อให้สามารถกู้คืนข้อมูลภายหลังได้ครบถ้วนสมบูรณ์ ถูกต้อง

การจัดให้มีระบบสำรองข้อมูล

1. ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูล
2. การสำรองข้อมูล ผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้ โดยการทำสำรองข้อมูลภายในมหาวิทยาลัย หมายถึงการทำสำรองข้อมูลทั้งหมด ผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้ ตามระยะเวลาที่เหมาะสมและกำหนดไว้ชัดเจน เช่น สำรองข้อมูลอย่างน้อย 1 ครั้งในรอบสัปดาห์ ทุก ๆ สัปดาห์ เป็นต้น
3. การจัดทำบันทึกการสำรองข้อมูล ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น ทุกครั้งที่ทำการสำรองข้อมูล

4. การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการทำสำรองข้อมูล รวมทั้งเสนอวิธีการที่ใช้ในการแก้ไขข้อผิดพลาดด้วย
5. ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ และ/หรือ ผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้ ต้องมีการมอบหมายหน้าที่การสำรองข้อมูลไว้ล่วงหน้าให้กับเจ้าหน้าที่คนอื่น เพื่อให้เจ้าหน้าที่ผู้นั้นสามารถทำหน้าที่สำรองข้อมูลในกรณีที่จำเป็น
6. ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการสำรองข้อมูลอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหา และรายงานต่อผู้บริหาร
7. ผู้ดูแลระบบคอมพิวเตอร์ และ/หรือ ผู้ดูแลระบบเครือข่ายมีหน้าที่กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้ในการเก็บข้อมูล ตัวอย่างรูปแบบการสำรองข้อมูล อาทิ การสำรองข้อมูลทั้งหมด (Full Backup) การสำรองข้อมูลแบบสะสม (Incremental Backup) หรืออาจเลือกใช้การสำรองข้อมูลรูปแบบอื่น ๆ ตามความเหมาะสม แต่ต้องให้มั่นใจว่ามีการสำรองข้อมูลได้ครบถ้วนตามเป้าหมายที่กำหนดไว้ รวมทั้งสามารถกู้กลับคืนได้ด้วย
8. การสำรองข้อมูลภายนอกสำนักงาน (Off-site Backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงาน ทั้งนี้ เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็ว และเพื่อป้องกันระบบจากการถูกโจมตีหรือจากหายนะที่อาจเกิดขึ้น
9. การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองนี้ถูกเปิดเผย
10. นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนการสำรองข้อมูล Backup Procedure โดยเคร่งครัด

การกู้คืนระบบ

1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์ และ/หรือ ระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์ และ/หรือ ผู้ดูแลระบบเครือข่าย มีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไข พร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงาน ต่อผู้บริหารหรือผู้ที่ได้รับมอบหมาย
2. ให้ใช้ชุดข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้เพื่อกู้คืนระบบ หรือใช้ชุดข้อมูลที่สมบูรณ์ที่สุด เพื่อให้ระบบกลับมาใช้งานได้ตามปกติ
3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ ๆ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

การบริหาร
ความเปลี่ยนแปลง

นโยบายการบริหารความเปลี่ยนแปลง

ครอบคลุมการบริหารความเปลี่ยนแปลงในระดับการปรับปรุง (Patch/Upgrade) และระดับการเปลี่ยนแปลง (Change) ระบบงานหรือระบบปฏิบัติการ โดยให้มีการกำหนดขั้นตอนและข้อปฏิบัติก่อนดำเนินการเปลี่ยนแปลง เพื่อลดความเสี่ยงในการหยุดให้บริการ และเป็นการเปลี่ยนแปลงโดยมีเหตุอันควร เพื่อให้ผู้ดูแลระบบและผู้ใช้ระบบสารสนเทศสามารถวางแผนปฏิบัติงานล่วงหน้า และลดผลกระทบที่เกิดจากการปรับเปลี่ยนได้

ความคาดหวังจากการปฏิบัติตามนโยบายนี้ คือ

1. ป้องกันการปรับเปลี่ยนการทำงานของระบบสารสนเทศ โดยผู้ดูแลระบบและผู้ใช้งานไม่ทราบ และมีการเตรียมการรองรับไว้ล่วงหน้า (Announced and Scheduled Changes)
2. สามารถติดตามและลำดับการปรับเปลี่ยนระบบสารสนเทศได้
3. สามารถกู้การทำงานเดิมของระบบสารสนเทศกลับคืนมาได้ ซึ่งต้องมีการเตรียมการก่อนการปรับเปลี่ยน มีการเฝ้าติดตามและการประเมินผล เพื่อให้การปรับเปลี่ยนเป็นไปด้วยดี ทราบล่วงหน้า และเตรียมการลดผลกระทบต่อการปฏิบัติงาน

แนวปฏิบัติตามนโยบาย

ผู้เกี่ยวข้อง

นโยบายฉบับนี้บังคับให้มีผู้มีอำนาจหน้าที่และความรับผิดชอบในการติดตั้ง ควบคุมการทำงานของผู้เกี่ยวข้องทุกคนในการดำเนินการเปลี่ยนแปลงระบบสารสนเทศ โดยกำหนดให้มีผู้ที่มีหน้าที่เฉพาะ ดังต่อไปนี้

1. ผู้ร้องขอปรับเปลี่ยนระบบสารสนเทศ มีภาระหน้าที่ คือ
   - 1.1 ยื่นคำร้องขอปรับเปลี่ยนระบบต่อคณะกรรมการบริหารการเปลี่ยนแปลง
   - 1.2 เป็นผู้รับผิดชอบให้มีการปรับเปลี่ยนระบบตามที่ร้องขอ โดยดำเนินการตามขั้นตอนการปรับเปลี่ยนระบบที่กำหนดโดยคณะกรรมการบริหารการเปลี่ยนแปลง
   - 1.3 ร่วมติดตาม ประเมิน และจัดทำรายงานแจ้งผลกระทบจริงที่เกิดขึ้นจากการปรับเปลี่ยนระบบ ต่อคณะกรรมการบริหารการเปลี่ยนแปลง

2. ผู้ประสานงานการบริหารการปรับเปลี่ยนระบบสารสนเทศ มีภาระหน้าที่ คือ

   2.1 ติดตามการปรับเปลี่ยนระบบสารสนเทศที่ยังไม่เสร็จสมบูรณ์ทั้งหมด
   2.2 จัดการประชุมคณะกรรมการบริหารการเปลี่ยนแปลงระบบสารสนเทศ
   2.3 เวียนปฏิทินการปรับเปลี่ยนระบบสารสนเทศให้กับหน่วยงานที่เกี่ยวข้องทราบ
   2.4 แจ้งหน่วยงานและบุคลากรที่เกี่ยวข้องให้ทราบถึงคาดการณ์ ผลกระทบที่อาจเกิดขึ้นจากการปรับเปลี่ยนระบบ
   2.5 แจ้งสรุปรายการการปรับเปลี่ยนระบบสารสนเทศที่เสร็จสมบูรณ์แล้ว ส่งให้กับคณะกรรมการบริหารการเปลี่ยนแปลง

3. คณะกรรมการบริหารการเปลี่ยนแปลง มีภาระหน้าที่ คือ

   3.1 ทบทวนคำร้องขอปรับเปลี่ยนระบบและให้ความเห็นชอบในการดำเนินการ โดยคำนึงถึงภารกิจของหน่วยงานที่ร้องขอ และภารกิจภาพรวม
   3.2 วิเคราะห์และคาดการณ์ผลกระทบที่จะเกิดขึ้นจากการปรับเปลี่ยนระบบ
   3.3 เสนอทางเลือกและขั้นตอนที่จะลดผลกระทบจากการปรับเปลี่ยนระบบให้มีน้อยที่สุด
   3.4 กำหนดขั้นตอนในการปรับเปลี่ยนระบบอย่างละเอียด
   3.5 จัดทำแผนการปรับกลับคืน อันได้แก่ ขั้นตอนปฏิบัติเพื่อกู้ระบบสารสนเทศ ให้กลับไปมีการทำงานเป็นดังสภาพเดิมก่อนมีการปรับเปลี่ยน เผื่อใช้สำหรับกรณีที่การปรับเปลี่ยนไม่เกิดสัมฤทธิ์ผล
   3.6 กำหนดกระบวนการในการเฝ้าระวังและตรวจสอบความเรียบร้อยของระบบหลังการปรับเปลี่ยน
   3.7 กำหนดปฏิทินในการดำเนินการปรับเปลี่ยนระบบ

4. หัวหน้าหน่วยงาน มีภาระหน้าที่ คือ

   4.1 ทำการอนุมัติการปรับเปลี่ยนระบบ ตามที่เสนอโดยคณะกรรมการบริหารความเปลี่ยนแปลง
   4.2 พิจารณารายงานสรุปการปรับเปลี่ยนระบบสารสนเทศ ของคณะกรรมการบริหารความเปลี่ยนแปลง

คณะกรรมการบริหารความเปลี่ยนแปลง

1. องค์ประกอบคณะกรรมการบริหารความเปลี่ยนแปลง

   คณะกรรมการการบริหารความเปลี่ยนแปลง คือ คณะบุคคลมีหน้าที่พิจารณาและอนุมัติการปรับเปลี่ยนระบบสารสนเทศ มีองค์ประกอบดังนี้

   1) ผู้ประสานงานการบริหารความเปลี่ยนแปลงมาจากหน่วยงานรับผิดชอบโดยตรงที่ดูแลและบำรุงรักษาระบบสารสนเทศ
   2) ผู้ร้องขอปรับเปลี่ยนระบบสารสนเทศ
   3) ตัวแทนจากหน่วยงานที่จะได้รับผลกระทบจากการปรับเปลี่ยนระบบสารสนเทศ

2. การดำเนินการของคณะกรรมการการบริหารความเปลี่ยนแปลง

   จัดให้มีการประชุมกรรมการการบริหารความเปลี่ยนแปลง เป็นอย่างน้อยทุก ๆ 3 เดือน หรือจัดประชุมทุกครั้งก่อนมีการเปลี่ยนแปลงใหญ่ และมีการประกาศ วัน เวลา และสถานที่ชัดเจน

   หัวข้อการประชุมมาตรฐานสำหรับการประชุมกรรมการบริหารความเปลี่ยนแปลง คือ

   1) ทบทวนและรับรองการปรับเปลี่ยนระบบสารสนเทศที่เสร็จสมบูรณ์แล้ว จากการประชุมครั้งก่อน
   2) การยกเรื่องและนำเสนอคำร้องใหม่ในการปรับเปลี่ยนระบบสารสนเทศ

3) กำหนดตารางเวลาปฏิบัติ และจัดทำปฏิทินประกาศตารางเวลาที่จะมีการปรับเปลี่ยนระบบสารสนเทศ ที่ได้รับการอนุมัติแล้วทั้งหมด
4) ดำเนินการแจ้งล่วงหน้าถึงการปรับเปลี่ยนระบบที่จะเกิดขึ้นแก่หน่วยงานและบุคลากร เพื่อให้ทราบถึงวันเวลา และผลกระทบเป็นระยะเวลาล่วงหน้าอย่างน้อย 30 วัน
5) ติดตาม ประเมิน จัดทำรายงานผลการเปลี่ยนแปลงระบบสารสนเทศ และจัดเก็บเข้าในฐานความรู้
6) จัดส่งรายงานผลการเปลี่ยนแปลงให้คณะกรรมการบริหารเทคโนโลยีสารสนเทศ รับทราบอย่างน้อยปีละ 1 ครั้ง

กรณีการปรับเปลี่ยนนอกกำหนดการหรือการปรับเปลี่ยนฉุกเฉิน ซึ่งต้องได้รับอนุมัติเร่งด่วนจากผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศหรือผู้บริหารระดับสูงขึ้นไป ภายหลังการดำเนินการฉุกเฉินให้ผู้ปฏิบัติที่ทำหน้าที่ปรับเปลี่ยนระบบ จะต้องทำเอกสารแสดงรายละเอียดการปรับเปลี่ยนทั้งหมด รวมทั้งผลกระทบที่เกิดขึ้น รายงานต่อคณะกรรมการบริหารความเปลี่ยนแปลง ภายใน 30 วัน เพื่อรับทราบและจัดเก็บเอกสารเข้าในฐานความรู้ต่อไป นับจากวันที่เสร็จสิ้นการดำเนินการปรับเปลี่ยนฉุกเฉิน

การบริหารจัดการการเข้าถึง
และการใช้งานระบบสารสนเทศ

นโยบายการบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ
ครอบคลุมการเข้าถึงระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย รวมถึงการใช้งานระบบสารสนเทศต่าง ๆ ของหน่วยงานให้มีความปลอดภัย

แนวปฏิบัติตามนโยบาย

- ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบเครือข่าย โดยกำหนดให้ผู้ใช้บริการสามารถใช้บริการได้ ตามภารกิจของผู้ใช้บริการ หรือตามบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- มีการจำกัดการใช้งานสารสนเทศ โดยผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ เช่น กำหนดสิทธิ์ในการใช้งาน และกำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ เป็นต้น
- ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายจะต้องกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์ให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้บังคับบัญชาหรือหัวหน้าหน่วยงาน
- ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายจากระยะไกล (Remote Access) โดยกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เช่น SSL VPN เป็นต้น
- การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ต (Port) โดยไม่จำเป็น และต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น
- ผู้ดูแลระบบป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต เช่น การใช้กุญแจล็อกที่ตัวเครื่อง การพิสูจน์ยืนยันตัวตน เป็นต้น
- ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้เป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ
- ผู้ดูแลระบบต้องบันทึกการทำงานของระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้บริการ บันทึกการบุกรุก บันทึกการเข้า-ออกระบบ บันทึกการใช้งาน และข้อมูลจราจรทางคอมพิวเตอร์
- ห้ามผู้ดูแลระบบ ใช้ชื่อผู้ใช้งานที่มีสิทธิ์ระดับสูงในการปฏิบัติงานทั่วไป
- จัดให้มีมาตรการเชิงป้องกันภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ที่เครื่องผู้ใช้งานทุกเครื่อง มีการติดตั้ง Firewall และ IPS (Intrusion Prevention System) เป็นต้น
- ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศของผู้ใช้งานตามรอบระยะเวลาที่กำหนด อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น การโอนย้ายหน่วยงาน การลาออก เป็นต้น

- จัดให้มีการอบรมการใช้งานระบบเทคโนโลยีสารสนเทศให้กับผู้ใช้งานใหม่ และให้ผู้ใช้งานลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเป็นลายลักษณ์อักษร
- ไม่ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น
- ไม่ใช้คอมพิวเตอร์และเครือข่ายโดยก่อผลกระทบต่อประสิทธิภาพโดยรวม เช่น การสร้างภาระให้กับระบบจนกระทั่งส่งผลกระทบต่อผู้ใช้งานอื่น
- ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งาน หรือผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร
- ไม่กระทำการอันละเมิดสิทธิ์ของผู้อื่นหรือระบบ หรือความผิดใด ๆ ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
- หากมีการนำเครื่องคอมพิวเตอร์ส่วนตัวที่ปลอดภัยมาใช้กับระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย ต้องปฏิบัติตามแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีของหน่วยงานอย่างเคร่งครัด

การบริหารจัดการบัญชีผู้ใช้ และการใช้งานรหัสผ่าน

นโยบายการบริหารจัดการบัญชีผู้ใช้และการใช้งานรหัสผ่าน
ครอบคลุมการบริหารบัญชีรายชื่อผู้ใช้งานระบบ การกำหนดรหัสผ่าน การกำหนดสิทธิ์บัญชีของผู้ให้บริการภายนอก (Vendor) ที่มีการปฏิบัติงานโดยมีการเข้าถึงระบบต่าง ๆ ของหน่วยงาน

แนวปฏิบัติตามนโยบาย

- กำหนดให้ผู้ใช้งานแต่ละรายมีชื่อผู้ใช้งาน (User Account) เป็นของตนเอง
- เข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่าน เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง
- ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กรอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชี รายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อที่ติดมากับระบบ (Default User) บัญชีรายชื่อของบุคลากรที่ลาออกแล้ว เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ ได้แก่ การระงับ (Disable) การใช้งาน ลบออกจากระบบ หรือเปลี่ยนรหัสผ่าน เป็นต้น
- กำหนดการส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย และควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านที่ได้รับโดยทันที
- ผู้ใช้งานต้องกำหนดรหัสผ่านที่ปลอดภัยและรักษารหัสให้เป็นความลับอยู่ตลอดเวลา
- รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษรขึ้นไป และไม่ใช้รหัสผ่านที่เคยถูกพบว่ามีการรั่วไหลออกสู่สาธารณะ
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และผู้ใช้งานทุกคนมีหน้าที่ในการป้องกันรหัสผ่านของตนอย่างเคร่งครัด
- ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หรือใช้บัญชีผู้ใช้งานร่วมกัน หากเกิดปัญหาจากการให้ใช้งานบัญชี เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้งานต้องเป็นผู้รับผิดชอบ
- ไม่ลักลอบใช้รหัสผ่านหรือแกะรหัสผ่านของผู้ใช้อื่น หรือการกระทำการอันใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น
- เปลี่ยนรหัสผ่านทุกครั้ง ในทันทีที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้
- เจ้าของบัญชีต้องตรวจสอบว่ามีการกำหนดรหัสผ่านที่รัดกุมตามแนวทางปฏิบัติดังกล่าว สำหรับบัญชีผู้ใช้งานทั้งหมดบนทุกอุปกรณ์เทคโนโลยีสารสนเทศ

- ผู้ใช้งานหรือเจ้าหน้าที่ปฏิบัติงานบางตำแหน่งอาจจะได้รับมอบหมายให้เข้าใช้ระบบงานอื่น ๆ ที่สำนักบริหารเทคโนโลยีสารสนเทศกำหนดให้ใช้ จะต้องปฏิบัติตามกฎการใช้ระบบและเก็บรักษาชื่อและรหัสผ่านไว้ ห้ามมิให้เปิดเผยกับผู้อื่น ยกเว้น กรณีผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติงานได้ อันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แจ้งผู้อำนวยการฝ่ายเพื่อแต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าวเพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ์ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้ว ให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

การใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ไอทีของหน่วยงาน

นโยบายการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีของหน่วยงาน
ครอบคลุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีที่เป็นทรัพย์สินของมหาวิทยาลัย ผู้ใช้งานมีหน้าที่รักษาให้สามารถใช้งานได้ และไม่ละเมิดความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศโดยรวมของมหาวิทยาลัย เช่น มีการติดตั้งโปรแกรมป้องกันมัลแวร์ มีการอัปเดตระบบปฏิบัติการ และอัปเดตซอฟต์แวร์อื่น ๆ ที่ติดตั้งอยู่บนเครื่องอย่างสม่ำเสมอ

แนวปฏิบัติตามนโยบาย

สำหรับเครื่องผู้ใช้งาน

- ไม่ติดตั้งซอฟต์แวร์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานกับเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของมหาวิทยาลัย
- ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย เช่น ไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
- ผู้ใช้งานต้องติดตั้งโปรแกรมตรวจจับมัลแวร์บนเครื่องผู้ใช้งาน สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ
- ห้ามมิให้ผู้ใช้งานทำการปิด หรือยกเลิก หรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ
- ผู้ใช้งานควรทำการปรับปรุงระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และป้องกันการโจมตีจากภัยคุกคาม
- ต้องตั้งค่าการใช้งานโปรแกรมรักษาหน้าจอ (Screen Saver) ทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หรือลงบันทึกออก (Log Out) จากระบบปฏิบัติการทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน หลังจากนั้นเมื่อต้องการใช้งานระบบปฏิบัติการอีก ต้องใส่รหัสผ่านอีกครั้งเพื่อเข้าใช้งาน
- ทำการ Scan ไวรัสคอมพิวเตอร์และมัลแวร์เป็นประจำ
- ผู้ใช้งานมีหน้าที่สำรองข้อมูลตามคำแนะนำของผู้ดูแลระบบ
- แจ้งและติดต่อผู้ดูแลระบบ หรือฝ่ายบริการเทคโนโลยีสารสนเทศทันที เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้นกับเครื่องคอมพิวเตอร์ที่ใช้งาน เช่น มีการติดไวรัสคอมพิวเตอร์ เป็นต้น

- ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต รวมถึงการดาวน์โหลด การปรับปรุง (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- ไม่ใช้คอมพิวเตอร์เพื่อการกระทำที่ผิดกฎหมาย หรือความผิดใด ๆ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

สำหรับเครื่องให้บริการแม่ข่าย

- ดูแลรักษาและปรับปรุงระบบปฏิบัติการให้สามารถใช้งานได้ดีอยู่เสมอ
- อัปเดตระบบปฏิบัติการให้ใช้งาน Patch ล่าสุด รวมทั้งตรวจสอบรายการช่องโหว่ของระบบสารสนเทศ หรือซอฟต์แวร์ที่ให้บริการอย่างสม่ำเสมอ และให้รีบแก้ไขช่องโหว่ทันทีหากพบว่าเป็นความเสี่ยงที่รุนแรง
- ตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้งานบนเครื่อง พร้อมทั้งทบทวนการกำหนดสิทธิ์ตามความจำเป็น และตั้งค่าควบคุมในลักษณะการอนุญาตให้ใช้งานตามรายการสิทธิ์ที่กำหนดไว้เท่านั้น
- ผู้ดูแลระบบต้องตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิด ให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้แก่ สถาบันมาตรวิทยาแห่งชาติ กรมอุทกศาสตร์ กองทัพเรือ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย
- ผู้ดูแลระบบป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต เช่น การใช้กุญแจล็อกที่ตัวเครื่อง การพิสูจน์ยืนยันตัวตน เป็นต้น
- พิจารณาการเปิดใช้งานบริการ (Services/Ports) ที่จำเป็นเท่านั้น และหากบริการใดที่จำเป็นต้องเปิดบริการ มีความเสี่ยงต่อความมั่นคงปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติมด้วย
- ทำการสำรองข้อมูลเป็นประจำ และควรจัดทำอย่างน้อย 2 เวอร์ชัน ไว้ในอุปกรณ์จัดเก็บข้อมูลที่ไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ ยกเว้นเวลาสำรองข้อมูล และในการสำรองข้อมูลแต่ละเวอร์ชันให้มีการจัดเก็บลงในอุปกรณ์ที่แตกต่างกัน
- พิจารณาจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) เพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้อย่างครบถ้วน ถูกต้อง ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- มีการตรวจสอบ Log ของบริการต่าง ๆ ที่เกี่ยวข้อง เพื่อตรวจสอบความผิดปกติของการใช้งานเป็นประจำ
- เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้นกับเครื่องแม่ข่าย ผู้ดูแลระบบที่ได้รับมอบหมายจะต้องรายงานเหตุการณ์ผิดปกติดังกล่าวให้กับผู้อำนวยการฝ่ายรับทราบโดยทันที และหากมีความจำเป็นเพื่อป้องกันความเสียหาย หรือผลกระทบที่อาจเกิดขึ้นต่อผู้อื่น หรือต่อการใช้งานระบบสารสนเทศโดยส่วนรวม ให้ผู้ดูแลระบบระงับการใช้งานดังกล่าว

การทำงานจากระยะไกล
และการปฏิบัติงานนอกสถานที่ตั้ง

นโยบายการทำงานจากระยะไกล และการปฏิบัติงานนอกสถานที่ตั้ง
โดยจัดให้มีแนวทางการทำงานจากระยะไกล และการปฏิบัติงานนอกสถานที่ตั้ง ที่เหมาะสมกับบริบทสภาพแวดล้อมภายใต้สภาวะวิกฤติ เพื่อให้การปฏิบัติงานมีความยืดหยุ่น คล่องตัว รวมทั้งไม่ส่งผลกระทบหรือเกิดผลเสียหายต่อประสิทธิภาพประสิทธิผลในการดำเนินงาน และยังคงมีความมั่นคงปลอดภัยที่เพียงพอสำหรับระบบเทคโนโลยีสารสนเทศ หรือข้อมูลสารสนเทศที่ถูกเข้าถึงจากระยะไกล

คำจำกัดความ

1. ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหน้าที่ให้ดูแลรับผิดชอบระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย
2. ผู้ปฏิบัติงาน ได้แก่ บุคลากรของสำนักบริหารเทคโนโลยีสารสนเทศ และ/หรือ บุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์ และ/หรือ ระบบสารสนเทศของมหาวิทยาลัย

แนวปฏิบัติตามนโยบาย

- ผู้ดูแลระบบต้องพิจารณาและทบทวนมาตรการรักษาความมั่นคงปลอดภัยที่มีอยู่ในปัจจุบัน รวมถึงประเมินความเหมาะสมหรือความเพียงพอของมาตรการดังกล่าว
- ผู้ดูแลระบบต้องจัดเตรียมเครื่องมือที่เหมาะสม อำนวยความสะดวกในการปฏิบัติงาน เช่น ระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับการประชุมทางไกล สำหรับทำงานนอกสถานที่ตั้งให้แก่ผู้ปฏิบัติงาน
- ผู้ดูแลระบบต้องจัดเตรียมช่องทางการเข้าถึงระบบข้อมูล ระบบสื่อสารที่เหมาะสมและปลอดภัยให้แก่ผู้ปฏิบัติงาน
- ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ เฉพาะในส่วนที่จำเป็นแก่การปฏิบัติงาน
- ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของผู้ปฏิบัติงาน ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่นโยบายการบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศได้กำหนดไว้
- ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการ รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

- ในการเข้าใช้งานระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัย จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส
- ผู้ปฏิบัติงานยังคงต้องสามารถปฏิบัติงานตามลักษณะงาน บทบาท หน้าที่ ที่ได้รับมอบหมาย ด้วยการใช้เทคโนโลยีสารสนเทศ และการสื่อสารได้อย่างราบรื่น และไม่ส่งผลกระทบต่อประสิทธิภาพหรือผลลัพธ์ของงาน
- ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นใด เข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน
- ผู้บริหารต้องรับผิดชอบกำกับดูแล สื่อสารเกี่ยวกับรายละเอียดของแนวปฏิบัติดังกล่าวให้ผู้ดูแลระบบ และผู้ปฏิบัติงานได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

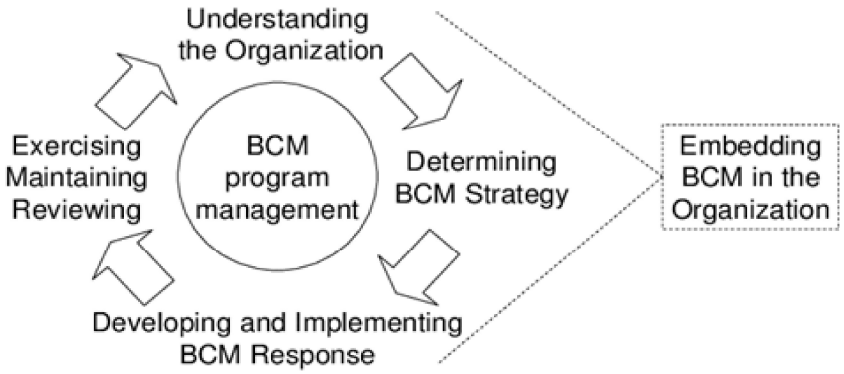
การดำเนินงานต่อเนื่อง
Business Continuity Plan (BCP)
และรับเหตุการณ์ฉุกเฉิน (Disaster)

นโยบายการดำเนินงานต่อเนื่อง Business Continuity Plan (BCP) และรับเหตุการณ์ฉุกเฉิน (Disaster)

โดยจัดให้มีแผนบริหารความต่อเนื่องการดำเนินงาน (BCP) เพื่อให้มั่นใจว่าการให้บริการที่กำหนดไว้ในแผน จะสามารถดำเนินต่อไปได้ เมื่อเกิดเหตุการณ์ที่จะต้องประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงาน โดยผู้ที่ได้รับมอบหมาย สามารถปฏิบัติตามกระบวนการที่กำหนดไว้ได้อย่างถูกต้อง หรือสามารถกู้คืนระบบกลับมาให้บริการต่อไปได้

แนวปฏิบัติตามนโยบาย

- จัดทำแผนการบริหารจัดการความต่อเนื่องทางธุรกิจ และมีการกำหนดโครงสร้างในการบริหารจัดการ
- มีการวิเคราะห์ผลกระทบทางธุรกิจ และทำการประเมินความเสี่ยง
- มีการกำหนดกลยุทธ์ในการรับมือและตอบสนองต่อเหตุการณ์ฉุกเฉิน
- มีการจัดทำแผนและแนวปฏิบัติที่เหมาะสม เพื่อรับมือและตอบสนองต่อเหตุการณ์ฉุกเฉินที่เกิดขึ้น
- มีการซักซ้อมและการทบทวนปรับปรุงแผน



(Reference: BS 25999 Standard)
มาตรฐานการบริหารจัดการความต่อเนื่องทางธุรกิจ

การบริหารจัดการความต่อเนื่องทางธุรกิจ และการกำหนดโครงสร้างในการบริหารจัดการ

- มีกรอบนโยบาย ขอบเขตของแผนบริหารความต่อเนื่องการดำเนินงาน ที่ครอบคลุมและรองรับต่อเหตุการณ์ฉุกเฉิน
- มีโครงสร้างในการบริหารจัดการ การจัดตั้งคณะทำงานหรือทีมงานที่รับผิดชอบในการจัดการตามแผนอย่างเหมาะสม เพื่อให้สามารถบริหารจัดการความต่อเนื่องได้อย่างมีประสิทธิภาพ และกลับสู่สภาวะปกติได้โดยเร็ว โดยอาจกำหนดบทบาทหน้าที่ให้ชัดเจน อาทิ

1. คณะกรรมการบริหารความต่อเนื่อง มีหน้าที่ในการประเมินลักษณะ ขอบเขต และแนวโน้มของอุบัติการณ์ที่เกิดขึ้น เพื่อกำหนดทิศทางในการดำเนินการบริหารความต่อเนื่อง และให้การสนับสนุนการดำเนินงาน ตลอดจนสรรหาทรัพยากรตามที่ได้กำหนดไว้ในแผนดำเนินธุรกิจอย่างต่อเนื่องฯ
2. ผู้ประสานงานคณะกรรมการบริหารความต่อเนื่อง มีหน้าที่ในการติดต่อคณะกรรมการบริหารความต่อเนื่อง และผู้ที่เกี่ยวข้อง หากมีการประกาศใช้งานแผนดำเนินธุรกิจอย่างต่อเนื่องฯ รวมถึง สนับสนุนการปฏิบัติงานของทีมกู้คืนระบบและตรวจสอบผลการกู้คืนระบบ
3. ทีมบริหารจัดการการกู้คืนระบบ มีหน้าที่ในการดำเนินการกู้คืนและฟื้นฟูระบบที่สำคัญตามที่กำหนดไว้ในแผนการดำเนินงาน
4. ฝ่ายสนับสนุนและแจ้งข่าวสาร มีหน้าที่ในการติดต่อและประสานงานแก่หน่วยงานที่เกี่ยวข้อง รวมทั้ง การจัดเตรียมทรัพยากรที่สำคัญ เช่น อาคาร/สถานที่ปฏิบัติงานสำรอง อุปกรณ์ต่าง ๆ ที่จำเป็นสำหรับการดำเนินงาน เป็นต้น

การวิเคราะห์ผลกระทบทางธุรกิจ และทำการประเมินความเสี่ยง

- มีการวิเคราะห์ความเสี่ยงและผลกระทบต่อกระบวนการทำงานหรือการให้บริการ (Business Impact Analysis) ที่สำคัญ เพื่อกำหนดวิธีการดำเนินการในเหตุการณ์ฉุกเฉินตามระดับของผลกระทบ
- ระบุสถานการณ์/เหตุการณ์ ที่ทำให้เกิดความเสี่ยงเพื่อจัดทำแผนรับมือ โดยแผนรับมืออาจแตกต่างกันไปในแต่ละสถานการณ์ อาทิ

1. แผ่นดินไหว
2. อัคคีภัย
3. วาตภัย
4. อุทกภัย
5. เหตุการณ์ก่อการร้าย
6. เหตุการณ์ประท้วงหรือชุมนุมทางการเมือง
7. อุปกรณ์เครือข่ายชำรุดหรือได้รับความเสียหาย
8. โรคระบาด
9. การโจมตีทางไซเบอร์

การกำหนดกลยุทธ์ในการรับมือและตอบสนองต่อเหตุการณ์ฉุกเฉิน

- กลยุทธ์ความต่อเนื่อง เป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต กำหนดกลยุทธ์ในการตอบสนองต่อเหตุการณ์วิกฤติ เช่น การกู้คืนการดำเนินงาน การจัดการทรัพยากรที่เหมาะสมและส่งผลกระทบกับหน่วยงานน้อยที่สุด

การจัดทำแผนและแนวปฏิบัติที่เหมาะสม เพื่อรับมือและตอบสนองต่อเหตุการณ์ฉุกเฉินที่เกิดขึ้น

- ให้มีการกำหนดขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ความเสี่ยง ครอบคลุมการวางแผนรองรับเหตุการณ์ฉุกเฉิน การวางแผนการกู้คืนระบบสำหรับระบบหรือบริการที่สำคัญ ให้สามารถดำเนินการได้ภายในระยะเวลาที่กำหนด

1. การเตรียมการก่อนเกิดเหตุการณ์ฉุกเฉิน
2. การรับมือกับเหตุการณ์ฉุกเฉิน
3. การจัดเตรียมสถานที่
4. สถานการณ์และขั้นตอนการกู้คืนระบบ

การซักซ้อมและการทบทวนปรับปรุงแผน

- เมื่อได้แผนบริหารความต่อเนื่องการดำเนินงาน (BCP) มาแล้ว จะต้องมีการทดสอบและประเมินแผน อาจทำการทดสอบโดยใช้สถานการณ์จำลองตามความเสี่ยงที่ได้วิเคราะห์ และดำเนินการตามแผนนั้น ทั้งนี้ เพื่อทดสอบประสิทธิภาพของแผนในการแก้ไขสถานการณ์และสามารถรองรับให้ธุรกิจดำเนินไปได้อย่างต่อเนื่อง เป็นการซักซ้อมวิธีปฏิบัติทดสอบและปรับปรุงแผนให้เหมาะสม เพื่อให้สามารถใช้การได้จริงตามแผนงานที่กำหนดไว้

อ้างอิง

การบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ

- ประกาศสำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ https://dol.thaihealth.or.th/File/media/23e6a66d-9421-49bd-bbb1-b0e06509ad8a.pdf
- วิธีปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย

การบริหารจัดการบัญชีผู้ใช้และการใช้งานรหัสผ่าน

- NIST SP 800-63B https://pages.nist.gov/800-63-3/sp800-63b.html, CyLab Carnegie Mellon University https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab11008.pdf
- ประกาศสำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ https://dol.thaihealth.or.th/File/media/23e6a66d-9421-49bd-bbb1-b0e06509ad8a.pdf

การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีของหน่วยงาน

- โปรแกรม Anti-Malware https://www.it.chula.ac.th/service/antivirus/
- ประกาศ กระทรวงไอซีที เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ https://bit.ly/36AziYF
- วิธีปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย

การทำงานจากระยะไกล และการปฏิบัติงานนอกสถานที่ตั้ง

- แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้า
- แนวทางสำหรับการปฏิบัติงานนอกสถานที่ตั้ง (Work from Home) กรณีโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) กรมควบคุมโรค กระทรวงสาธารณสุข

การดำเนินงานต่อเนื่อง Business Continuity Plan (BCP) และรับเหตุการณ์ฉุกเฉิน (Disaster)

- บทความเดือนมีนาคม Business Continuity Plan เรียบเรียงโดย สำนักประสานด้านการต่างประเทศ สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
- การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) งานบริหารความเสี่ยง สำนักงานอธิการบดี มหาวิทยาลัยมหิดล