จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University
Pillar of the Kingdom

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(CU IT Security Policy)

ยุทธศาสตร์ที่ 1
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(CU IT Security Policy)

สำนักบริหารเทคโนโลยีสารสนเทศ

เวอร์ชั่นที่ 6.2
วันที่ทบทวน วันที่ 15 กันยายน 2558
เริ่มประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ วันที่ 2 พฤศจิกายน 2558

สารบัญ

หน้า

ยุทธศาสตร์ที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การจัดทำเอกสารชุดนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศจะช่วยให้ผู้ปฏิบัติงานทราบถึงนโยบายและข้อปฏิบัติเพื่อปกป้องระบบและข้อมูลที่มีความสำคัญต่อการดำเนินงาน ลดปัจจัยเสี่ยง รวมทั้ง เป็นการพัฒนาบุคลากรและนิสิตให้สามารถปฏิบัติงานและใช้งานได้สอดคล้องกับหลักการรักษาความปลอดภัย โดยมีเอกสาร จำนวน 10 ฉบับ ประกอบด้วย

1. นโยบายความมั่นคงปลอดภัยด้านกายภาพ ครอบคลุมการรักษาความมั่นคงปลอดภัยทางกายภาพของห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ การควบคุมการเข้าออก การกำหนดสิทธิผู้ผ่านเข้าออกและความปลอดภัยทางกายภาพของเครือข่ายสื่อสัญญาณภายในมหาวิทยาลัย

2. นโยบายการจัดเตรียมระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมมาตรการและแนวปฏิบัติในการดำเนินการติดตั้งอุปกรณ์เครือข่ายและคอมพิวเตอร์ (Hardware) ระบบปฏิบัติการและระบบงานต่างๆ (Software) เพื่อเชื่อมต่อกับระบบสารสนเทศของมหาวิทยาลัย

3. นโยบายการจำแนกและการบริหารข้อมูล ครอบคลุมการกำหนดมาตรฐานในการจัดระดับชั้นความลับของข้อมูลและวิธีการจัดการข้อมูล เพื่อให้มีหลักปฏิบัติที่ใช้ในการจัดการกับข้อมูลอย่างถูกต้องเหมาะสม

4. นโยบายการสำรองข้อมูลและกู้คืน ครอบคลุมทั้งในคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคลเพื่อให้มีชุดข้อมูลสำรองกรณีเกิดความเสียหายกับข้อมูลและสามารถกู้กลับคืนมาได้อย่างมีประสิทธิภาพ

5. นโยบายการบริหารความเปลี่ยนแปลง ครอบคลุมการบริหารความเปลี่ยนแปลงในระดับการปรับปรุง (Patch/Upgrade) และระดับการเปลี่ยนแปลง (Change) ระบบงานหรือระบบปฏิบัติการ เพื่อให้มีข้อปฏิบัติก่อนดำเนินการเปลี่ยนแปลงเพื่อลดความเสี่ยงในการหยุดให้บริการ

6. นโยบายการบริหารระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมการบริหารระบบเครือข่ายทั้งระบบ ข้อกำหนดเกี่ยวกับการจัดการไอพีแอดเดรส การเข้าถึงระบบจากระยะไกล การตรวจสอบระบบ การซ่อมบำรุง และการดำเนินการเมื่อระบบขัดข้อง

7. นโยบายการเข้าถึงข้อมูลและระบบสารสนเทศ ครอบคลุมการบริหารบัญชีรายชื่อผู้ใช้งานระบบ การกำหนดรหัสผ่าน การกำหนดสิทธิเฉพาะผู้ที่ได้รับอนุญาต

8. นโยบายการใช้อุปกรณ์ไอทีส่วนบุคคล ครอบคลุมการใช้งานคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา และสมาร์ทโฟน (Notebook, Tablet, Mobile computing และ IT gadgets) โดยกำหนดแนวทางการใช้งาน ข้อกำหนดที่ผู้ใช้งานต้องดำเนินการ เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส

9. นโยบายการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ ครอบคลุมสิ่งที่ผู้ใช้เครือข่ายคอมพิวเตอร์ต้องปฏิบัติตาม

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

1 นโยบายความมั่นคงปลอดภัยด้านกายภาพ

ให้มีการกำหนดมาตรการและแนวทางในการป้องกันอาคารและอุปกรณ์ในห้องควบคุมระบบคอมพิวเตอร์ และมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์ การควบคุมการเข้า-ออก การแบ่งส่วนพื้นที่และการกำหนดสิทธิผู้ผ่านเข้าออก เพื่อให้มั่นใจได้ว่าห้องควบคุมระบบคอมพิวเตอร์มีความปลอดภัยจากอุบัติภัยทางธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม เป็นต้น หรือ จากการโจรกรรมทรัพย์สินของเครือข่าย 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

ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่

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

ข้อกำหนดการป้องกันทางกายภาพ ประกอบด้วย

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

1. <u>ข้อกำหนดของห้องควบคุมระบบ</u>

   1.1 แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น router, switch และ server ต่างๆ

   1.2 จัดหา rack ในการจัดเก็บอุปกรณ์ต่างๆ ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

   1.3 ไม่วางอุปกรณ์ต่างๆ ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น หรือวางอุปกรณ์ใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น

   1.4 เก็บสายเครือข่าย (Network cable) และสายไฟฟ้าให้เรียบร้อย เพื่อป้องกันการเดินสะดุด

   1.5 ติดประกาศบันทึกการบำรุงรักษา การซ่อมแซมและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

   1.6 ติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV ระบบการเข้า-ออกห้องโดยระบบ RFID เป็นต้น

   1.7 มีระบบและอุปกรณ์ป้องกันอัคคีภัย

   1.8 มีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง เป็นต้น

   1.9 มีระบบป้องกันไฟฟ้าจากฟ้าผ่า

   1.10 มีระบบปรับอากาศแบบควบคุมอุณหภูมิ (10 - 26.7°C) และความชื้นสัมพัทธ์ (20 - 80%)

   1.11 ติดตั้งฉนวนกันไฟไหม้ที่ฝ้าเพดานและผนังกำแพง

2. <u>ข้อกำหนดการเข้าพื้นที่ควบคุม</u>

   2.1 ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้น เจ้าหน้าที่ห้องควบคุมระบบ บุคลากร สบท. ที่ได้รับอนุญาต ผู้บริหารหรือ บุคคลที่ผู้บริหารนำเข้าเยี่ยมชม

   2.2 บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุม ต้องได้รับอนุญาตจากผู้บริหาร และจะต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา

   2.3 ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลให้เกิดความเสียหายต่อทรัพย์สินของ สบท. บุคคลอื่นอาจเข้าในพื้นที่ควบคุมได้หากได้รับอนุญาตจากผู้บริหาร

   2.4 ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าในเขตพื้นที่ควบคุม

3. ข้อกำหนดการเข้าพื้นที่จำกัดการเข้าถึง

3.1 ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ

3.2 ในกรณีมีบุคคลที่มีความจำเป็นต้องเข้าไปปฏิบัติงานในพื้นที่จำกัดการเข้าถึง บุคคลดังกล่าวต้องได้รับอนุญาตจากผู้บริหารและต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย 1 คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

3.3 กรณีมีบุคคลที่ได้รับคำสั่งจากผู้บริหารให้เข้าปฏิบัติหน้าที่ในพื้นที่จำกัดการเข้าถึง จะต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย 1 คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

3.4 ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

3.5 ไม่อนุญาตให้มีการเข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

3.6 ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของ สบท. บุคคลอื่นสามารถเข้าไปในพื้นที่จำกัดการเข้าถึงได้หากได้รับอนุญาตจากผู้บริหาร

4. ข้อกำหนดการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

4.1 ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก 3 เดือน

4.2 กำหนดขั้นตอนและแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟไหม้ หรือมีผู้บุกรุก เป็นต้น

4.3 ทำการซ้อมการปฏิบัติงานรับมือต่อกรณีเกิดเหตุฉุกเฉินทุก 6 เดือน

4.4 มีตารางกำหนดการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

2 นโยบายการจัดเตรียมระบบเครือข่ายคอมพิวเตอร์

กำหนดให้มีมาตรการและแนวทางในการติดตั้งอุปกรณ์เครือข่ายและเครื่องเซิร์ฟเวอร์ การติดตั้งซอฟต์แวร์ระบบปฏิบัติการ การติดตั้งโปรแกรมประยุกต์สำหรับใช้งานกับอุปกรณ์ รวมถึงการจัดเตรียมระบบเครือข่ายและเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ การทดสอบอุปกรณ์ก่อนทำการติดตั้งในห้องปฏิบัติงานเพื่อให้มีแนวปฏิบัติเป็นมาตรฐานเดียวกันอย่างมีประสิทธิภาพ

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ห้องปฏิบัติงาน หมายถึง ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย
2. อุปกรณ์ หมายถึง อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์เซิร์ฟเวอร์
3. อุปกรณ์ทดสอบ หมายถึง อุปกรณ์ที่มีคุณลักษณะเหมือนกัน หรือใกล้เคียงกับอุปกรณ์ที่ต้องการติดตั้ง อุปกรณ์ต่อพ่วง หรือติดตั้งโปรแกรมประยุกต์เพิ่มเติม โดยที่อุปกรณ์ชุดนี้ต้องไม่ใช่อุปกรณ์ชุดที่ใช้งานอยู่
4. เจ้าหน้าที่ หมายถึง ผู้มีอำนาจในการติดตั้ง และดูแลรักษาอุปกรณ์ภายในห้องปฏิบัติงาน
5. ผู้รับผิดชอบอุปกรณ์ หมายถึง ผู้มีหน้าที่ในการจัดเก็บรายการอุปกรณ์ และเอกสารประกอบอุปกรณ์

ขอบเขต

นโยบายนี้ครอบคลุมถึงอุปกรณ์ทุกชนิดที่เป็นสมบัติของมหาวิทยาลัย และอุปกรณ์ที่ไม่ใช่สมบัติของมหาวิทยาลัย แต่มีการติดตั้งและเปิดใช้งานเชื่อมต่อทั้งอย่างถาวรหรือชั่วคราวกับระบบเครือข่ายของมหาวิทยาลัย และอยู่ในพื้นที่ของมหาวิทยาลัย

1. ข้อกำหนดการเตรียมเอกสารก่อนการติดตั้ง

    1.1 เจ้าหน้าที่ต้องดำเนินการลงทะเบียนอุปกรณ์ทุกชิ้นกับผู้รับผิดชอบอุปกรณ์ โดยระบุ คุณลักษณะที่สำคัญของอุปกรณ์ ระบบปฏิบัติการที่ใช้ พร้อมระบุรุ่น วันที่ติดตั้ง ชื่อผู้ติดตั้ง วัตถุประสงค์การใช้งานของอุปกรณ์รวมถึงรายการโปรแกรมประยุกต์ที่ติดตั้งในอุปกรณ์อย่างชัดเจน

    1.2 เจ้าหน้าที่ต้องทำการรวบรวมเอกสารคุณลักษณะของอุปกรณ์ทั้งที่เป็นสิ่งพิมพ์และโปรแกรมที่ใช้กับอุปกรณ์เพื่อนำส่งไปยังผู้รับผิดชอบอุปกรณ์

    1.3 เจ้าหน้าที่ต้องจัดเตรียมแผนการติดตั้ง ระยะเวลา ผู้รับผิดชอบ และแผนการรับมือในกรณีฉุกเฉิน

    1.4 เจ้าหน้าที่ต้องจัดเตรียมแผนผังทางกายภาพ (Layout) ที่ระบุตำแหน่งของอุปกรณ์ที่จะทำการติดตั้ง

    1.5 เจ้าหน้าที่ต้องจัดเตรียมแผนผังทางตรรกะของเครือข่าย (Network Logical Diagram) ที่ระบุการเชื่อมต่อของอุปกรณ์ที่ต้องการจะติดตั้ง

1.6 เจ้าหน้าที่ต้องเตรียมเอกสารการติดตาม (Monitoring Chart) แบบที่เป็นการจดบันทึกและทำการบันทึกด้วยระบบอิเล็กทรอนิกส์

1.7 เจ้าหน้าที่ต้องเตรียมป้ายชื่ออุปกรณ์ ที่ใช้วัสดุและมีรูปแบบการจัดพิมพ์ตามแบบที่ใช้ในห้องปฏิบัติงานติดตั้งให้เห็นชัดเจนบนตัวอุปกรณ์

1.8 ในกรณีต้องทำการใดๆ กับอุปกรณ์ที่กำลังทำหน้าที่ให้บริการอยู่ โดยเฉพาะกับอุปกรณ์ที่มีผลกระทบสูงต่อผู้ใช้งานและหน่วยงาน ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า รวมถึงทราบผลกระทบที่อาจเกิดขึ้น

1.9 มีหนังสือรับรองเห็นชอบอนุมัติในการติดตั้ง และแผนการติดตั้งจากผู้บริหาร ก่อนดำเนินการเคลื่อนย้ายอุปกรณ์เข้าไปในห้องปฏิบัติงาน รวมทั้งก่อนมีการติดตั้งโปรแกรมใดๆ

2. <u>ข้อกำหนดการทดสอบอุปกรณ์และโปรแกรมก่อนการติดตั้ง</u>

2.1 อุปกรณ์ต้องอยู่ในสภาพทางกายภาพสมบูรณ์พร้อมใช้งาน

2.2 อุปกรณ์ทุกชิ้นต้องผ่านการป้อนไฟเพื่อทดสอบว่าใช้งานได้ และไม่เกิดการลัดวงจร หรือ มีความร้อนมากจนอาจเป็นสาเหตุของไฟฟ้าลัดวงจรหรือไฟไหม้

2.3 ในกรณีที่เป็นการติดตั้งอุปกรณ์ใหม่ เจ้าหน้าที่ต้องทำการติดตั้งระบบปฏิบัติการ โปรแกรมต้านไวรัส พร้อมทั้งโปรแกรมประยุกต์ที่จะใช้งานให้เสร็จสิ้น พร้อมทั้งทดสอบการทำงานให้สมบูรณ์ก่อนนำเข้าติดตั้ง

2.4 ในกรณีที่ต้องการติดตั้งโปรแกรมประยุกต์บนอุปกรณ์ที่กำลังใช้งาน

2.4.1 ต้องจัดเตรียมอุปกรณ์ทดสอบที่ติดตั้งระบบปฏิบัติการ รุ่นของระบบปฏิบัติการ และโปรแกรมประยุกต์ทั้งหมดเหมือนกับอุปกรณ์ที่กำลังใช้งาน

2.4.2 ให้เจ้าหน้าที่ทำการทดลองติดตั้งโปรแกรมประยุกต์ดังกล่าวบนอุปกรณ์ทดสอบ เพื่อศึกษาถึงผลกระทบที่เกิดขึ้น

2.4.3 เจ้าหน้าที่จัดทำรายงานสรุปการทดสอบ

2.4.4 ทำสำเนาข้อมูลของอุปกรณ์ที่กำลังใช้งาน ก่อนการนำโปรแกรมประยุกต์ที่ทดสอบแล้วไปติดตั้ง

3. <u>ข้อกำหนดการทำงานขณะติดตั้งอุปกรณ์และโปรแกรม</u>

3.1 การเคลื่อนย้ายและการติดตั้งอุปกรณ์ต้องเป็นไปตามนโยบายความมั่นคงทางกายภาพของห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

3.2 เจ้าหน้าที่ต้องทำการบันทึก ชื่อบัญชีผู้ใช้ และรหัสผ่านของระบบ (Root User Name และ Password) ไว้ในที่ปลอดภัยตามนโยบายการรักษาความปลอดภัยและจัดเก็บรหัสลับ

3.3 การตั้งค่าทางเครือข่าย (Network Configuration) หมายเลขไอพี การตั้งค่าเครือข่ายเสมือน และการตั้งค่าอื่นๆ ที่เกี่ยวกับเครือข่าย ต้องเป็นไปตามข้อกำหนดการใช้งานเครือข่าย

4. <u>ข้อกำหนดภายหลังการติดตั้ง</u>

4.1 เจ้าหน้าที่ต้องทำการตรวจสอบติดตามการทำงานของอุปกรณ์ หรือโปรแกรมที่ติดตั้ง และลงบันทึกในเอกสารการติดตาม (Monitoring Chart) ที่ได้เตรียมไว้ ทุกช่วงระยะเวลาที่กำหนด

4.2 เจ้าหน้าที่ต้องจัดเตรียมรายงานการติดตั้ง ข้อเสนอแนะในการดูแลรักษา รวมถึงค่าใช้จ่าย ในการดูแลรักษา เพื่อส่งให้กับหัวหน้าและผู้บริหารรับทราบ

3 นโยบายการจำแนกและการบริหารข้อมูล

กำหนดให้มีมาตรฐานในการจำแนก การจัดระดับชั้นความลับของข้อมูล การติดป้าย และวิธีการจัดเก็บข้อมูล เพื่อให้มีหลักปฏิบัติที่ใช้ในการจัดการข้อมูลอย่างถูกต้องเหมาะสม

แนวปฏิบัติตามนโยบาย

ขอบเขต

ขั้นตอนการปฏิบัติงานจะใช้กับข้อมูลทั้งที่อยู่ในรูปแบบของเอกสารกระดาษและข้อมูลในรูปแบบอิเล็กทรอนิกส์

1. เอกสารกระดาษ หมายถึง ข้อมูลที่พิมพ์ออกมาในรูปกระดาษ เช่น สัญญา รายงานการประชุม เป็นต้น
2. ข้อมูลในรูปแบบอิเล็กทรอนิกส์ หมายถึง ข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่จัดเก็บอยู่ในเครื่องคอมพิวเตอร์ เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์ต่างๆ
3. สื่อบันทึกข้อมูล หมายถึง สื่อที่ใช้ในการเก็บข้อมูลอิเล็กทรอนิกส์ เช่น แผ่นซีดี แถบแม่เหล็ก แฟลชไดร์ฟ เป็นต้น

หน้าที่และความรับผิดชอบ

เจ้าของข้อมูล คือ ผู้สร้างข้อมูล โดยเจ้าของข้อมูลมีหน้าที่ดังต่อไปนี้

- กำหนดระดับชั้นความลับของข้อมูลที่ตนเองเป็นเจ้าของ และระบุชั้นความลับให้กับข้อมูลนั้น
- กำหนดสิทธิการเข้าถึงข้อมูลให้ผู้ใช้
- กำหนดมาตรการในการจัดการข้อมูลให้มีความมั่นคงปลอดภัย

ผู้ดูแลข้อมูล คือ ผู้ที่มีหน้าที่ดูแลและจัดการให้ข้อมูลมีความปลอดภัย ผู้ดูแลข้อมูลมีหน้าที่

- จัดการและบำรุงรักษาให้ข้อมูลอยู่ในระดับชั้นความลับตามที่เจ้าของข้อมูลกำหนดไว้

ผู้ใช้ข้อมูล คือ ผู้ที่ได้รับอนุญาตจากเจ้าของข้อมูลให้เข้าถึงข้อมูลได้ ผู้ใช้ข้อมูลมีหน้าที่

- ปฏิบัติและจัดการกับข้อมูลตามระดับชั้นความลับตามที่เจ้าของข้อมูลกำหนดไว้

หากมีความจำเป็นต้องส่งผ่านข้อมูลไปยังบุคคลหรือหน่วยงานภายนอกมหาวิทยาลัย บุคลากรที่รับผิดชอบในการส่งผ่านข้อมูลจะต้องแจ้งให้กับผู้รับข้อมูลทราบถึงระดับชั้นความลับของข้อมูล และวิธีการในการจัดการกับข้อมูลก่อนนำส่งข้อมูล

การจัดระดับข้อมูล

เนื่องจากหากมีการละเมิดการใช้ข้อมูลอย่างไม่เหมาะสม ข้อมูลบางประเภทอาจถูกนำไปใช้และสร้างความเสียหายให้กับมหาวิทยาลัย บุคลากร หรือนิสิตของมหาวิทยาลัยได้ ดังนั้นทางมหาวิทยาลัยจึงจำเป็นต้องมีมาตรการในการดูแล ป้องกันให้ข้อมูลมีความปลอดภัย จึงต้องมีการจัดระดับชั้นความลับของข้อมูลขึ้น โดยแบ่งออกเป็น 4 ระดับ ได้แก่

- ลับมาก (Secret)
- ลับ (Confidential)
- ใช้เฉพาะภายใน (Internal)
- ใช้ได้ทั่วไป (Public)

ประเภทของข้อมูล

	ลับมาก (Secret)	**ลับ (Confidential)**	**ใช้เฉพาะภายใน (Internal)**	**ใช้ได้ทั่วไป (Public)**
นิยาม	▪ เป็นข้อมูลที่มีความสำคัญมากต่อมหาวิทยาลัย จะอนุญาตให้เฉพาะบุคคลที่มีความจำเป็นอย่างแท้จริงสามารถเข้าถึงข้อมูลได้ ▪ หากมีการเปิดเผยโดยไม่ได้รับอนุญาตอาจจะก่อให้เกิดความเสียหายต่อการดำเนินงานและชื่อเสียงของมหาวิทยาลัย บุคลากร หรือนิสิตอย่างร้ายแรง	▪ เป็นข้อมูลที่มีความสำคัญต่อมหาวิทยาลัย โดยอนุญาตให้เฉพาะผู้ที่มีความจำเป็นในการเข้าถึงข้อมูลสามารถเข้าถึงข้อมูลได้ ▪ หากมีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะก่อให้เกิดความเสียหายในการดำเนินงานของมหาวิทยาลัย และอาจส่งผลกระทบไปถึงนิสิต บุคลากรได้	▪ เป็นข้อมูลที่อนุญาตให้ใช้ได้เฉพาะภายในมหาวิทยาลัย โดยอนุญาตให้บุคคลที่เกี่ยวข้องสามารถเข้าถึงข้อมูลได้ ▪ หากมีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะก่อให้เกิดความเสียหายในวงจำกัด	▪ เป็นข้อมูลที่ต้องการให้มีการเผยแพร่ไปยังภายนอก เช่น ข้อมูลบนเว็บไซต์ และข้อมูลการเผยแพร่งานวิชาการต่างๆ กิจกรรมต่างๆ ของมหาวิทยาลัย เป็นต้น ▪ ไม่มีผลกระทบหากมีการเผยแพร่ไปสู่ภายนอกองค์กร

1. การติดป้าย

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
การติดป้าย				
ชื่อที่ใช้ในการระบุ	■ เอกสารลับมาก	■ เอกสารลับ	■ เอกสารภายใน	■ ไม่มีข้อกำหนดเป็นพิเศษ
เอกสารกระดาษ	■ มีการระบุระดับชั้นความลับในทุกๆหน้าของเอกสาร หรืออย่างน้อยที่หน้าแรกของเอกสาร			■ ไม่มีข้อกำหนดเป็นพิเศษ
ข้อมูลในรูปแบบอิเล็กทรอนิกส์	■ มีการระบุระดับชั้นความลับในทุกๆหน้าของไฟล์เอกสาร ยกเว้นในกรณีที่มีข้อจำกัดทางเทคนิค			■ ไม่มีข้อกำหนดเป็นพิเศษ
สื่อบันทึกข้อมูล	■ ไม่จำเป็นต้องติดป้ายบนสื่อบันทึกข้อมูล แต่กำหนดให้มีวิธีการจัดการที่เทียบเท่าตามระดับชั้นความลับของข้อมูลที่บันทึกในสื่อบันทึกข้อมูลดังกล่าว			■ ไม่มีข้อกำหนดเป็นพิเศษ

2. การควบคุมการเข้าถึง

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
การควบคุมการเข้าถึง				
การยืนยันความถูกต้อง	■ รหัสผู้ใช้และรหัสผ่าน	■ รหัสผู้ใช้และรหัสผ่าน	■ รหัสผู้ใช้และรหัสผ่าน	■ ไม่มี
การอนุมัติ	■ ตามสิทธิของผู้ใช้	■ ตามสิทธิของผู้ใช้	■ ตามสิทธิของผู้ใช้	■ ไม่มี

3. การควบคุมการถ่ายโอนข้อมูล

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
การควบคุมการถ่ายโอนข้อมูล				
แฟกซ์	■ ใช้ได้เฉพาะในกรณีที่จำเป็นเท่านั้น ข้อปฏิบัติเช่นเดียวกับข้อมูล “ลับ”	■ ต้องอยู่ ณ เครื่องโทรสารในขณะที่ส่งจนแล้วเสร็จ ■ ตรวจสอบความถูกต้องของหมายเลขปลายทาง ■ ใช้เครื่องโทรสารที่อยู่ในพื้นที่ รับและส่งที่ปลอดภัย ■ มีใบปะหน้าที่ระบุถึงผู้ส่ง ผู้รับ และข้อความการปฏิเสธความรับผิดชอบอันเกิดจากการส่งข้อมูลทางโทรสาร	■ ไม่มีข้อกำหนด	■ ไม่มีข้อกำหนด
เครื่องพิมพ์	■ พิมพ์ที่เครื่องพิมพ์ที่มีความปลอดภัย ■ ตรวจสอบเครื่องพิมพ์ปลายทาง	■ พิมพ์ที่เครื่องพิมพ์ที่มีความปลอดภัย ■ ตรวจสอบเครื่องพิมพ์ปลายทาง	■ ไม่มีข้อกำหนดพิเศษ	■ ไม่มีข้อกำหนดพิเศษ
โทรศัพท์มือถือ	■ ไม่อนุญาต	■ ไม่อนุญาต	■ ไม่มีข้อกำหนดพิเศษ	■ ไม่มีข้อกำหนดพิเศษ

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
การควบคุมการถ่ายโอนข้อมูล				
จดหมายอิเล็กทรอนิกส์ อินทราเน็ต, อินเตอร์เน็ต	■ ไม่อนุญาต เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูลและต้องใช้ในระบบจดหมายอิเล็กทรอนิกส์และอินเตอร์เน็ตของมหาวิทยาลัยที่มีความปลอดภัยเท่านั้น รวมถึงให้ส่งข้อมูลที่มีการ encryption จากผู้ส่ง	■ ไม่อนุญาตเว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล และต้องใช้ในระบบจดหมายอิเล็กทรอนิกส์และอินเตอร์เน็ตของมหาวิทยาลัยที่มีความปลอดภัยเท่านั้น รวมถึง ให้ส่งข้อมูลที่มีการ encryption จากผู้ส่ง	■ ไม่มีข้อกำหนดพิเศษสำหรับการใช้กับจดหมายอิเล็กทรอนิกส์หรืออินทราเน็ต ■ ต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อนที่จะส่งไปยังภายนอก	■ ไม่มีข้อกำหนดพิเศษ
สื่อต่างๆและกระดาษ	■ บรรจุในวัสดุห่อหุ้มที่สามารถป้องกันการแก้ไขข้อมูล ■ ส่งมอบให้ถึงมือผู้รับ หรือบริการ การส่งจดหมายที่ไว้ใจได้	■ บรรจุในซองที่ห่อหุ้มและปิดผนึก	■ บรรจุในซองที่ปิดผนึก	■ ไม่มีข้อกำหนดพิเศษ

4. วิธีการจัดเก็บข้อมูล

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
วิธีการจัดเก็บ				
เอกสารกระดาษหรือสื่อบันทึกข้อมูล	■ เก็บในตู้นิรภัย หรือตู้ที่มีกุญแจปิดล็อก และตู้ดังกล่าวจะต้องตั้งอยู่ในพื้นที่ที่มีการควบคุมด้านความมั่นคงปลอดภัย ■ หากมีความจำเป็นต้องนำเอกสารออกนอกมหาวิทยาลัยจะต้องจัดเก็บใส่ซองพร้อมปิดผนึกเพื่อป้องกันการเปิดซองเอกสารโดยที่ไม่ได้รับอนุญาต และต้องนำเอกสารติดตัวไว้ตลอดเวลา	■ เก็บในตู้ที่มีกุญแจปิดล็อกเมื่อไม่ใช้งาน และตู้ดังกล่าวจะต้องตั้งอยู่ในพื้นที่ที่มีการควบคุมด้านความมั่นคงปลอดภัย ■ หากมีความจำเป็นต้องนำเอกสารออกนอกมหาวิทยาลัยจะต้องจัดเก็บใส่ซองพร้อมปิดผนึกเพื่อป้องกันการเปิดซองเอกสารโดยที่ไม่ได้รับอนุญาต และไม่วางกระเป๋าเอกสารโดยไม่มีผู้ดูแล	■ เก็บในตู้ที่มีกุญแจปิดล็อกเมื่อไม่ใช้งาน ■ เก็บในแฟ้มเมื่อต้องการนำออกไปใช้ภายนอก	■ ไม่มีข้อกำหนดเป็นพิเศษ

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
วิธีการจัดเก็บ				
ข้อมูลในรูปแบบอิเล็กทรอนิกส์	■ จัดเก็บในดิสก์หรือสื่อบันทึกไว้ในตู้ปิดล็อกที่อยู่ในพื้นที่ที่มีการควบคุมด้านความมั่นคงปลอดภัย ■ ห้ามไม่ให้จัดเก็บข้อมูลในพื้นที่เก็บข้อมูลส่วนกลาง เช่น Network Shared Drive	■ จัดเก็บในดิสก์หรือสื่อบันทึกไว้ในตู้ปิดล็อกที่อยู่ในพื้นที่ที่มีการควบคุมด้านความมั่นคงปลอดภัย ■ ควรหลีกเลี่ยงไม่จัดเก็บข้อมูลในพื้นที่เก็บข้อมูลส่วนกลาง เช่น Network Shared Drive ซึ่งหากจำเป็นจะต้องมีการกำหนดสิทธิในการเข้าถึง (Access Control List)	■ จัดเก็บในดิสก์หรือสื่อบันทึกไว้ในตู้ปิดล็อกที่อยู่ในพื้นที่ที่มีการควบคุมด้านความมั่นคงปลอดภัย ■ จัดเก็บข้อมูลในพื้นที่เก็บข้อมูลส่วนกลาง เช่น Network Shared Drive โดยมีการกำหนดสิทธิในการเข้าถึง	■ ไม่มีข้อกำหนดเป็นพิเศษ

5. วิธีการสำเนาข้อมูล

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
การทำสำเนา				
การทำสำเนาและการพิมพ์งาน	■ ห้ามไม่ให้สำเนา หรือพิมพ์ใหม่ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และผู้บริหารมหาวิทยาลัยขึ้นไป ■ เจ้าของข้อมูลควรเป็นผู้ดำเนินการสำเนาข้อมูลด้วยตนเอง ■ มีบันทึกการแจกจ่ายข้อมูล ■ ให้รอรับเอกสารระหว่างที่เครื่องกำลังพิมพ์งาน ■ ห้ามไม่ให้พิมพ์งานโดยใช้เครื่องพิมพ์สาธารณะ เช่น ในโรงแรม	■ ห้ามไม่ให้สำเนา หรือพิมพ์ใหม่ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และผู้บริหารระดับส่วนงานขึ้นไป ■ มีบันทึกการแจกจ่ายข้อมูล ■ ให้เก็บงานที่สั่งพิมพ์ทันทีหลังจากพิมพ์เสร็จ ■ ควรหลีกเลี่ยงการพิมพ์งานโดยใช้เครื่องพิมพ์สาธารณะ เช่น ในโรงแรม	■ อนุญาตให้ทำสำเนา หรือพิมพ์ใหม่ เฉพาะการเผยแพร่ภายในมหาวิทยาลัย ■ ให้เก็บงานที่สั่งพิมพ์ทันทีที่ทำได้	■ ไม่มีข้อห้ามในการทำสำเนา

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
การทำสำเนา				
การทำสำเนาอิเล็กทรอนิกส์ เช่น external drive หรือ thumb drive	■ ห้ามไม่ให้สำเนา	■ ห้ามไม่ให้สำเนา	■ อนุญาตให้ทำสำเนาใหม่เฉพาะการเผยแพร่ภายในมหาวิทยาลัย	■ ไม่มีข้อห้ามในการทำสำเนา

6. วิธีการลบและทำลายข้อมูล

	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
วิธีการลบข้อมูล				
สื่อบันทึกข้อมูลแบบแถบแม่เหล็ก	▪ ให้ลบไฟล์ทันทีโดยไม่ให้เก็บไว้ใน Recycle bin ▪ มีการใช้ ซอฟต์แวร์ประเภทยูทิลิตี้เพื่อป้องกันการกู้ข้อมูลคืนได้	▪ ให้ลบไฟล์ทันทีโดยไม่ให้เก็บไว้ใน Recycle bin	▪ อนุญาตให้ลบไฟล์โดยใช้วิธีการปกติ	▪ ไม่มีข้อกำหนดเป็นพิเศษ
วิธีการทำลายข้อมูล				
เอกสารกระดาษ	▪ เจ้าของข้อมูล หรือผู้ใช้จะต้องตัดหรือทำลายเอกสารด้วยตนเองโดยตัดหรือทำลายโดยใช้เครื่องทำลายเอกสาร	▪ เจ้าของข้อมูล หรือผู้ใช้จะต้องตัดหรือทำลายเอกสารด้วยตนเองโดยตัดหรือทำลายโดยใช้เครื่องทำลายเอกสาร	▪ ตัดหรือทำลายโดยใช้เครื่องทำลายเอกสาร	▪ ไม่มีข้อกำหนดเป็นพิเศษ
สื่อบันทึกข้อมูลประเภทอื่น	▪ การทำลายสื่อบันทึกข้อมูล			▪ ไม่มีข้อกำหนดเป็นพิเศษ

4 นโยบายการสำรองข้อมูลและกู้คืน

ให้กำหนดแนวปฏิบัติในการสำรองข้อมูลและกู้คืนระบบอย่างมีขั้นตอนและลดความเสี่ยงที่อาจเกิดขึ้น เพื่อสร้างความมั่นใจในการเก็บรักษาและใช้งานข้อมูล โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

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. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูล
2. ผู้ดูแลระบบคอมพิวเตอร์ ต้องกำหนดให้มีกระบวนการสร้างความต่อเนื่องให้กับการดำเนินงาน การบริหารจัดการและการปรับปรุงกระบวนการที่ต้องใช้ในการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ
3. การสำรองข้อมูลผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้ โดยการทำสำรองข้อมูลภายในมหาวิทยาลัย หมายถึง การทำสำรองข้อมูลทั้งหมด ผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้ตามระยะเวลาที่เหมาะสมและกำหนดไว้ชัดเจน เช่น สำรองข้อมูลอย่างน้อย 1 ครั้งในรอบสัปดาห์ ทุกๆ สัปดาห์ เป็นต้น
4. การจัดทำบันทึกการสำรองข้อมูล ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึก รายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่ บันทึก เป็นต้น ทุกครั้งที่ทำการสำรองข้อมูล
5. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการทำสำรองข้อมูล รวมทั้งเสนอวิธีการที่ใช้ในการแก้ไขข้อผิดพลาดด้วย
6. ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้ ต้องมีการมอบหมายหน้าที่การสำรองข้อมูลไว้ล่วงหน้าให้กับเจ้าหน้าที่คนอื่น เพื่อให้เจ้าหน้าที่ผู้นั้นสามารถทำหน้าที่สำรองข้อมูลในกรณีที่จำเป็น

7. ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการสำรองข้อมูลอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บริหาร

8. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายมีหน้าที่กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้ในการเก็บข้อมูล โดยตัวอย่างรูปแบบการสำรองข้อมูล อาทิ การสำรองข้อมูลทั้งหมด (Full backup) การสำรองข้อมูลแบบสะสม (Incremental backup) หรืออาจเลือกใช้การสำรองข้อมูลรูปแบบอื่นๆ ตามความเหมาะสม แต่ต้องให้มั่นใจว่ามีการสำรองข้อมูลได้ครบถ้วนตามเป้าหมายที่กำหนดไว้ รวมทั้งสามารถกู้กลับคืนได้ด้วย

9. การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงาน ทั้งนี้เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็วและเพื่อป้องกันระบบจากการถูกโจมตีหรือจากหายนะที่อาจเกิดขึ้น

10. การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองนี้ถูกเปิดเผย

11. นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนการสำรองข้อมูล Backup Procedure โดยเคร่งครัด

การกู้คืนระบบ

1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่าย มีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้บริหารหรือผู้ที่ได้รับมอบหมาย

2. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest update) ที่ได้สำรองไว้เพื่อกู้คืนระบบ

3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

5 นโยบายการบริหารความเปลี่ยนแปลง

ให้มีการกำหนดขั้นตอนและข้อปฏิบัติก่อนดำเนินการเปลี่ยนแปลงเพื่อลดความเสี่ยงในการหยุดให้บริการซึ่งต้องครอบคลุมความเปลี่ยนแปลงที่เกิดขึ้นกับระบบสารสนเทศทั้งในระดับการปรับปรุง (Patch/Upgrade) และระดับการเปลี่ยนแปลง (Change) ระบบงานหรือระบบปฏิบัติการ โดยเฉพาะเครื่องคอมพิวเตอร์ เครื่องแม่ข่าย ระบบงานและโปรแกรมประยุกต์ให้มีการเปลี่ยนแปลงโดยมีเหตุอันควรและเพื่อให้ผู้ดูแลระบบและผู้ใช้ระบบสารสนเทศสามารถวางแผนปฏิบัติงานล่วงหน้าและลดผลกระทบที่เกิดจากการปรับเปลี่ยนได้

ความคาดหวังจากการปฏิบัติตามนโยบายนี้ คือ

1. ป้องกันการปรับเปลี่ยนการทำงานของระบบสารสนเทศ โดยผู้ดูแลระบบและผู้ใช้งานไม่ทราบ และมีการเตรียมการรองรับไว้ล่วงหน้า (Announced and scheduled changes)
2. สามารถติดตามและลำดับการปรับเปลี่ยนระบบสารสนเทศ
3. สามารถกู้การทำงานเดิมของระบบสารสนเทศกลับคืนมา

ซึ่งต้องมีการเตรียมการก่อนการปรับเปลี่ยน มีการเฝ้าติดตามและการประเมินผล เพื่อให้การปรับเปลี่ยนเป็นไปด้วยดี ทราบล่วงหน้าและเตรียมการลดผลกระทบต่อการปฏิบัติงาน

แนวปฏิบัติตามนโยบาย

ผู้เกี่ยวข้อง

นโยบายฉบับนี้บังคับให้มีผู้มีอำนาจหน้าที่ และความรับผิดชอบในการติดตั้ง ควบคุมการทำงานของผู้เกี่ยวข้องทุกคนในการดำเนินการเปลี่ยนแปลงระบบสารสนเทศ โดยกำหนดให้มีผู้ที่มีหน้าที่เฉพาะ ดังต่อไปนี้

1. ผู้ร้องขอปรับเปลี่ยนระบบสารสนเทศ มีภาระหน้าที่ คือ

    1.1 ยื่นคำร้องขอปรับเปลี่ยนระบบต่อคณะกรรมการบริหารการเปลี่ยนแปลง
    1.2 เป็นผู้รับผิดชอบให้มีการปรับเปลี่ยนระบบตามที่ร้องขอ โดยดำเนินการตามขั้นตอนการปรับเปลี่ยนระบบที่กำหนดโดยคณะกรรมการบริหารการเปลี่ยนแปลง
    1.3 ร่วมติดตาม ประเมิน และจัดทำรายงานแจ้งผลกระทบจริง ที่เกิดขึ้นจากการปรับเปลี่ยนระบบต่อคณะกรรมการบริหารการเปลี่ยนแปลง

2. ผู้ประสานงานการบริหารการปรับเปลี่ยนระบบสารสนเทศ มีภาระหน้าที่ คือ

    2.1 ติดตามการปรับเปลี่ยนระบบสารสนเทศที่ยังไม่เสร็จสมบูรณ์ทั้งหมด
    2.2 จัดการประชุมคณะกรรมการบริหารการเปลี่ยนแปลงระบบสารสนเทศ
    2.3 เวียนปฏิทินการปรับเปลี่ยนระบบสารสนเทศให้กับหน่วยงานที่เกี่ยวข้องทราบ
    2.4 แจ้งหน่วยงานและบุคลากรที่เกี่ยวข้องให้ทราบถึงคาดการณ์ ผลกระทบที่อาจเกิดขึ้นจากการปรับเปลี่ยนระบบ

2.5 แจ้งสรุปรายการการปรับเปลี่ยนระบบสารสนเทศที่เสร็จสมบูรณ์แล้ว ส่งให้กับคณะกรรมการบริหารการเปลี่ยนแปลง

3 <u>คณะกรรมการบริหารการเปลี่ยนแปลง</u> 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 <u>ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ (สบท.)</u> มีภาระหน้าที่ คือ

4.1 ทำการอนุมัติการปรับเปลี่ยนระบบ ตามที่เสนอโดยคณะกรรมการบริหารความเปลี่ยนแปลง
4.2 พิจารณารายงานสรุป การปรับเปลี่ยนระบบสารสนเทศของคณะกรรมการบริหารความเปลี่ยนแปลง

<u>คณะกรรมการบริหารความเปลี่ยนแปลง</u>

1. องค์ประกอบคณะกรรมการบริหารความเปลี่ยนแปลง

คณะกรรมการการบริหารความเปลี่ยนแปลง คือ คณะบุคคลมีหน้าที่พิจารณาและอนุมัติการปรับเปลี่ยนระบบสารสนเทศ มีองค์ประกอบดังนี้

1) ผู้ประสานงานการบริหารความเปลี่ยนแปลงมาจากหน่วยงานรับผิดชอบโดยตรงที่ดูแลและบำรุงรักษาระบบสารสนเทศ
2) ผู้ร้องขอปรับเปลี่ยนระบบสารสนเทศ
3) ตัวแทนจากหน่วยงานที่จะได้รับผลกระทบจากการปรับเปลี่ยนระบบสารสนเทศ

2. การดำเนินการของคณะกรรมการการบริหารความเปลี่ยนแปลง

จัดให้มีการประชุมกรรมการ การบริหารความเปลี่ยนแปลง เป็นอย่างน้อยทุกๆ 3 เดือน หรือ จัดประชุมทุกครั้ง ก่อนมีการเปลี่ยนแปลงใหญ่และมีการประกาศ วัน เวลา และสถานที่ชัดเจน

หัวข้อการประชุมมาตรฐานสำหรับการประชุมกรรมการบริหารความเปลี่ยนแปลง คือ

1) ทบทวนและรับรองการปรับเปลี่ยนระบบสารสนเทศที่เสร็จสมบูรณ์แล้ว นับจากการประชุมครั้งก่อน
2) การยกเรื่องและนำเสนอคำร้องใหม่ในการปรับเปลี่ยนระบบสารสนเทศ

3) กำหนดตารางเวลาปฏิบัติและจัดทำปฏิทินประกาศตารางเวลาที่จะมีการปรับเปลี่ยนระบบสารสนเทศที่ได้รับการอนุมัติแล้วทั้งหมด
4) ดำเนินการแจ้งล่วงหน้าถึงการปรับเปลี่ยนระบบที่จะเกิดขึ้นแก่หน่วยงานและบุคลากรเพื่อให้ทราบถึงวัน เวลา และผลกระทบเป็นระยะเวลาล่วงหน้าอย่างน้อย 30 วันและย้ำเตือนทุกสัปดาห์ จนถึงวันเริ่มดำเนินการผ่านสื่อต่างๆ
5) ติดตาม ประเมิน จัดทำรายงานผลการเปลี่ยนแปลงระบบสารสนเทศ และจัดเก็บเข้าในฐานความรู้
6) จัดส่งรายงานผลการเปลี่ยนแปลงให้คณะกรรมการบริหารเทคโนโลยีสารสนเทศ รับทราบอย่างน้อยปีละ 1 ครั้ง

กรณีการปรับเปลี่ยนนอกกำหนดการหรือการปรับเปลี่ยนฉุกเฉินซึ่งต้องได้รับอนุมัติเร่งด่วนจากผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศหรือผู้บริหารระดับสูงขึ้นไป ภายหลังการดำเนินการฉุกเฉินให้ผู้ปฏิบัติที่ทำหน้าที่ปรับเปลี่ยนระบบ จะต้องทำเอกสาร แสดงรายละเอียดการปรับเปลี่ยนทั้งหมด รวมทั้งผลกระทบที่เกิดขึ้นรายงานต่อคณะกรรมการบริหารความเปลี่ยนแปลง ภายใน 30 วันเพื่อรับทราบและจัดเก็บเอกสารเข้าในฐานความรู้ต่อไป นับจากวันที่เสร็จสิ้นการดำเนินการปรับเปลี่ยนฉุกเฉิน

6 นโยบายการบริหารระบบเครือข่ายคอมพิวเตอร์

ให้มีการกำหนดมาตรการและแนวทางในการบริหารระบบเครือข่าย ทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์ ข้อกำหนดเกี่ยวกับการจัดการไอพีแอดเดรส (IP address) การตรวจสอบระบบเครือข่าย การเข้าถึงระบบจากระยะไกล การซ่อมบำรุง และการดำเนินการเมื่อระบบขัดข้อง

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหน้าที่ให้ดูแลรับผิดชอบระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย
2. ผู้ตรวจสอบระบบคอมพิวเตอร์และเครือข่าย หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายประจำวัน
3. การหยุดระบบ หมายถึง การปิดระบบและ/หรือการหยุดการให้บริการระบบคอมพิวเตอร์และ/หรือเครือข่าย ทั้งด้านซอฟต์แวร์และ/หรือฮาร์ดแวร์ ซึ่งส่งผลให้การใช้บริการระบบคอมพิวเตอร์ขัดข้องไม่ว่าจะเป็นการชั่วคราว ครั้งคราว หรือตลอดเวลาใน และมีช่วงเวลาการซ่อมบำรุงนานกว่า 1 ชั่วโมง

ขอบเขต

นโยบายนี้ครอบคลุมถึงอุปกรณ์เครือข่ายทุกชนิด ทั้งฮาร์ดแวร์และซอฟต์แวร์ การเข้าถึงเครือข่าย และระบบสนับสนุนเครือข่ายที่เป็นสมบัติของมหาวิทยาลัย และอุปกรณ์ที่ทางมหาวิทยาลัยอนุญาตให้เชื่อมต่อกับเครือข่ายของมหาวิทยาลัย

1. การจัดการไอพีแอดเดรส (IP address)

   การจัดสรรไอพีแอดเดรส

   1.1 สบท. มีหน้าที่จัดสรรไอพีแอดเดรสสำหรับหน่วยงานต่างๆ ของมหาวิทยาลัย
   1.2 คณะและสำนักงานต่างๆ ในมหาวิทยาลัยสามารถยื่นเรื่องขออนุมัติต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ เพื่อขอใช้ไอพีแอดเดรส
   1.3 ผู้ดูแลระบบมีหน้าที่ประเมินปริมาณความต้องการใช้งานไอพีแอดเดรสและสามารถเสนอแนวทางการลดหรือเพิ่มจำนวนไอพีแอดเดรสสำหรับคณะและสำนักงานต่างๆ ในมหาวิทยาลัยได้ตามผลการพิจารณาคำขออนุมัติ ซึ่งต้องระบุเหตุผลความจำเป็นในการเพิ่มลดและต้องแจ้งให้คณะและสำนักงานนั้นๆ ทราบเป็นระยะเวลาไม่น้อยกว่า 5 วันก่อนเริ่มใช้งานจริง มหาวิทยาลัยขอสงวนสิทธิในการขอคืนหมายเลขไอพี หากพบว่าไม่มีการใช้งานในระยะเวลาพอสมควร

2. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

   2.1 ผู้ดูแลระบบต้องประเมินการใช้งานไอพีแอดเดรสของคณะ ส่วนงาน และหน่วยงานที่ได้รับการจัดสรรไป ว่าได้ใช้งานอย่างมีประสิทธิภาพหรือไม่ หลังจากการใช้งานจริง 1 เดือน และมหาวิทยาลัยขอสงวนสิทธิในการขอคืนหมายเลขไอพี หากพบว่าไม่มีการใช้งานในระยะเวลาพอสมควร

2.2 ผู้ดูแลระบบมีหน้าที่บันทึกข้อมูลการจัดสรรไอพีแอดเดรสในเอกสารข้อมูลการจัดสรรไอพีแอดเดรสทันที

3. <u>การตรวจสอบระบบคอมพิวเตอร์และเครือข่าย</u>

3.1 ข้อปฏิบัติการตรวจสอบประจำวัน

3.1.1 ผู้ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายมีหน้าที่ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายเป็นประจำทุกวันทันทีที่มาปฏิบัติงานตามเวลาราชการ โดยกำหนดให้ตรวจสอบให้เสร็จสิ้นก่อนเวลา 12.00 น.

3.1.2 ผู้ตรวจสอบระบบคอมพิวเตอร์และระบบเครือข่ายบันทึกผลการตรวจสอบแล้วรายงานต่อผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทุกวัน

3.1.3 ให้ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานมอบหมาย เจ้าหน้าที่สำรองอีก1คนไว้ตรวจสอบระบบประจำวัน ในกรณีที่ผู้ตรวจสอบระบบคอมพิวเตอร์และระบบเครือข่ายไม่สามารถปฏิบัติงานได้

3.1.4 ในกรณีที่ตรวจสอบแล้วพบปัญหา ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาในรายงานการตรวจสอบประจำวัน

3.1.5 ในกรณีที่ตรวจสอบพบปัญหาที่อาจสร้างความเสียหายอย่างรุนแรงทั้งในเวลาราชการและนอกเวลาราชการ ให้ผู้ตรวจสอบระบบคอมพิวเตอร์และระบบเครือข่ายแจ้งผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเพื่อดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกในรายงานการตรวจสอบประจำวัน และให้ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานรายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ

3.2 การตรวจสอบระบบคอมพิวเตอร์

3.2.1 ตรวจสอบความคงอยู่และการให้บริการของระบบคอมพิวเตอร์ว่ายังสามารถให้บริการได้ตามปกติหรือไม่ โดยทดลองขอเข้าใช้บริการเสมือนเป็นผู้ขอใช้บริการตามปกติ โดยตรวจสอบระบบคอมพิวเตอร์แม่ข่ายหลักที่ให้บริการ

3.2.2 ตรวจสอบการทำงานของระบบคอมพิวเตอร์ทั้งหมดโดย พิจารณาจากหลักเกณฑ์ต่อไปนี้

- การทำงานของโปรเซสเซอร์
- ภาระงานหน่วยประมวลผลกลาง
- ปริมาณการใช้เนื้อที่ดิสก์ในพาร์ติชัน (partition) ต่างๆ
- ปริมาณการใช้หน่วยความจำหลัก
- แฟ้มบันทึกการทำงาน

3.2.3 ตรวจสอบเซิร์ฟเวอร์และระบบปฏิบัติการในเซิร์ฟเวอร์อื่นๆ ที่มีความสำคัญ

3.3 การตรวจสอบระบบเครือข่าย

3.3.1 ตรวจสอบการเชื่อมโยงเซิร์ฟเวอร์กับเส้นทางเชื่อมโยงการสื่อสารของเครือข่ายว่ายังสามารถใช้งานได้ตามปกติหรือไม่

3.3.2 ตรวจสอบการทำงานของอุปกรณ์เครือข่ายหลักและระบบสนับสนุนการให้บริการ

3.3.3 ตรวจสอบการให้บริการพิสูจน์ตัวตนจริง (Authentication)

3.3.4 ตรวจสอบการให้บริการของแอกเซสพอยส์ในเครือข่ายไร้สาย ChulaWiFi Chula-guest และ Eduroam

3.3.5 ตรวจสอบสถิติและ/หรือข้อมูลที่เกี่ยวข้องทางสถิติของการใช้ช่องสัญญาณ เป็นต้น

4. <u>การเข้าใช้ระบบคอมพิวเตอร์จากระยะไกล</u>

ข้อปฏิบัติในการขอเข้าใช้ระบบคอมพิวเตอร์จากระยะไกล

4.1 ผู้ดูแลระบบมีหน้าที่จัดเตรียมระบบที่มีความมั่นคงปลอดภัยเพื่อรองรับการเชื่อมต่อระยะไกล

4.2 ผู้ขอใช้งานต้องยื่นเรื่องขอใช้งานผ่านหน่วยงาน เพื่อขออนุมัติต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศและคำขออนุมัติจะต้องลงนามรับรองโดยคณบดีหรือผู้อำนวยการส่วนงานหรือผู้อำนวยการสำนักบริหารหรือเทียบเท่า

4.3 ผู้ดูแลระบบต้องเป็นผู้ติดตามผลการพิจารณาคำขออนุมัติ และแจ้งให้ผู้ใช้งานนั้นๆ ทราบผลเป็นระยะเวลาไม่เกิน 1 สัปดาห์

4.4 ถ้าผลการพิจารณาเป็นการอนุมัติ ผู้ดูแลระบบต้องเตรียมเอกสาร ขั้นตอนการติดตั้งซอฟต์แวร์ ข้อมูลชื่อผู้ใช้ และรหัสผ่านที่จำเป็นแก่ผู้ใช้งานพร้อมกับการแจ้งผล

4.5 ผู้ขอใช้งานต้องปฏิบัติตามข้อปฏิบัติต่างๆ ที่เกี่ยวข้องกับการใช้งานเครือข่ายอย่างเคร่งครัด

5. <u>ความปลอดภัยการใช้งาน</u>

5.1 ผู้ดูแลระบบมีหน้าที่เตรียมระบบความปลอดภัย ในการรองรับการเชื่อมต่อระยะไกล เช่น การเข้ารหัสการติดตั้งและใช้งานระบบ VPN เป็นต้น

5.2 ผู้ดูแลระบบมีหน้าที่เตรียมเอกสารในการใช้งานและติดตั้งระบบความปลอดภัยให้พร้อมใช้งานได้ตลอดเวลา

5.3 ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนตามประเภทของงานที่ได้รับอนุมัติให้ใช้ระบบจากระยะไกล

6. <u>การซ่อมบำรุง</u>

ข้อปฏิบัติการซ่อมบำรุงรักษาระบบ

6.1 ผู้ดูแลระบบมีหน้าที่ซ่อมบำรุงรักษา แก้ไขข้อบกพร่องและจัดทำตารางเวลาแผนบำรุงรักษา เพื่อให้ระบบสามารถให้บริการได้ตามปกติ

6.2 ในกรณีที่ต้องหยุดระบบเพื่อซ่อมบำรุง ผู้ดูแลระบบต้องจัดทำแผนและขั้นตอนการซ่อมบำรุงรักษาระบบ เสนอขออนุมัติจากผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศก่อนดำเนินการล่วงหน้าไม่น้อยกว่า 10 วันทำการ

6.3 ผู้ดูแลระบบต้องวางแผนงานและดำเนินการเพื่อประชาสัมพันธ์ ให้ผู้ใช้งานทราบเป็นเวลาไม่น้อยกว่า 5 วันทำการ นับจากวันประกาศถึงวันที่ต้องหยุดระบบ ยกเว้น ในกรณีฉุกเฉินที่ต้องดำเนินการทันทีเพื่อแก้ปัญหาความมั่นคงปลอดภัย โดยให้มีการประกาศข้อความผ่านทางระบบงานนั้นๆ ก่อนการหยุดระบบ และ/หรือระหว่างการหยุดระบบ

6.4 ผู้ดูแลระบบต้องจัดทำรายงานสรุปการดำเนินงานและเสนอต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศภายใน 1 วันหลังจากเสร็จสิ้นการหยุดระบบ

7. <u>ข้อปฏิบัติเมื่อระบบคอมพิวเตอร์หรือเครือข่ายขัดข้อง</u>

การแก้ไขปัญหา

7.1 ให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายวิเคราะห์ผลกระทบเบื้องต้นในกรณีที่ระบบคอมพิวเตอร์และ/หรือเครือข่ายขัดข้อง และรายงานต่อผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
7.2 ให้เริ่มดำเนินการแก้ไขระบบคอมพิวเตอร์และเครือข่ายที่ขัดข้องหลังจากการวิเคราะห์ผลกระทบทันทีภายใน 1 ชั่วโมง ในกรณีที่มีผลกระทบระดับสูง อนุญาตให้ดำเนินการในเวลาทำการและให้ดำเนินการโดยไม่เว้นวันหยุดราชการ
7.3 ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือเครือข่ายกำหนดแนวทางการแก้ปัญหา ขั้นตอน และเวลาการปฏิบัติที่ชัดเจน โดยสรุปลักษณะปัญหา ผลกระทบที่อาจจะเกิดขึ้น หากมีความจำเป็นต้องได้รับความร่วมมือจากผู้มีส่วนเกี่ยวข้อง ให้เรียกประชุมพร้อมกันในคราวเดียว
7.4 ให้เจ้าหน้าที่ปฏิบัติงานแก้ปัญหาตามแนวทางที่กำหนดในข้อก่อนหน้าและรายงานผลการปฏิบัติงานต่อผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
7.5 หากมีผลกระทบที่จำเป็นต้องแจ้งข่าวสารให้กับผู้ใช้งานทราบ จะต้องตรวจสอบให้แน่ชัดและแจ้งให้ผู้ใช้งานทราบทันที

8. <u>ข้อปฏิบัติเมื่อระบบจ่ายไฟฟ้าขัดข้อง</u>

การแก้ไขปัญหา

8.1 ให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายวิเคราะห์ผลกระทบ ในกรณีที่ระบบคอมพิวเตอร์และ/หรือเครือข่ายขัดข้องเป็นระยะเวลานานเกินกว่าระบบสำรองไฟฟ้าจะจ่ายไฟฟ้าได้ โดยพิจารณาและรายงานต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ
8.2 ให้ผู้ดูแลระบบเครือข่ายดำเนินการตรวจสอบระบบไฟฟ้าและติดต่อผู้เกี่ยวข้องกับปัญหาด้านไฟฟ้าโดยนำข้อมูลมาวิเคราะห์ว่ามีระบบใดบ้างได้รับผลกระทบ กำหนดแนวทางการแก้ปัญหาด้านเครือข่ายและระบบ คอมพิวเตอร์ ขั้นตอนและตารางเวลาการปฏิบัติ โดยสรุปลักษณะปัญหาและผลกระทบที่อาจจะเกิดขึ้น
8.3 หากมีผลกระทบที่จำเป็นต้องแจ้งข่าวสารให้กับผู้ใช้งานทราบ จะต้องตรวจสอบให้อย่างแน่ชัดและแจ้งให้ผู้ใช้งานทราบทันที
8.4 ให้เจ้าหน้าที่ปฏิบัติงานดำเนินการแก้ปัญหาตามแนวทางที่กำหนดและรายงานผลการปฏิบัติงานต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ

9. <u>การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550</u>

9.1 ให้ สบท. เป็นผู้จัดทำระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของมหาวิทยาลัย

9.2 ส่วนงาน/หน่วยงานอาจจะขอยกเว้นไม่ใช้งานระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ที่จัดทำโดย สบท. โดยส่วนงาน/หน่วยงานนั้นๆ จะต้องเป็นผู้จัดเก็บข้อมูลจราจรคอมพิวเตอร์

9.3 ให้สบท. และส่วนงาน/หน่วยงานตามข้อ 9.2 แต่งตั้งผู้ที่สามารถเข้าถึงข้อมูลจราจรคอมพิวเตอร์ได้

9.4 ให้สบท. และส่วนงาน/หน่วยงานตามข้อ 9.2 แต่งตั้งผู้ประสานงานด้านข้อมูลจราจรคอมพิวเตอร์

9.5 ให้สบท. ส่งรายงานหมายเลขไอพีที่ส่วนงาน/หน่วยงานได้รับการยกเว้นและผู้ที่ได้รับมอบหมายให้ทำการแทนส่วนงาน/หน่วยงานในการขอยกเว้น ให้ส่วนงาน/หน่วยงานทราบทุกเดือน

9.6 ให้ซักซ้อมการเข้าถึงและนำส่งข้อมูลจราจรคอมพิวเตอร์ของสบท. ตลอดจนส่วนงาน/หน่วยงานต่างๆ เป็นประจำทุก 6 เดือน แล้วรายงานให้คณะกรรมการไอที (มหาวิทยาลัย) ทราบ

7 นโยบายการเข้าถึงข้อมูลและระบบสารสนเทศ

ให้มีการกำหนดแนวทางบริหาร และการควบคุมการเข้าถึงข้อมูลเพื่อลดปัญหาในเรื่องความเสี่ยงของระบบสารสนเทศและการดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และป้องกันความเสียหายอันเกิดจากการกระทำที่ไม่ถูกต้อง และให้เป็นแนวปฏิบัติงานอย่างมีประสิทธิภาพแก่บุคลากรและนิสิตของมหาวิทยาลัย

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลจัดการระบบคอมพิวเตอร์และเครือข่าย
2. ผู้ใช้ หมายถึง บุคลากรและนิสิตและ/หรือบุคคลหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์และระบบสารสนเทศของมหาวิทยาลัย

สาระสำคัญ

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ครอบคลุมการจัดการการเข้าถึงของผู้ใช้ กำหนดขึ้นเพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

    1.1 การลงทะเบียนผู้ใช้ใหม่ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้ใหม่เพื่อให้สามารถใช้งานระบบสารสนเทศและต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้ทันที ในกรณีที่มีการยกเลิกการใช้งาน เช่น การจบการศึกษาของนิสิตหรือการลาออกของบุคลากร

    1.2 การบริหารจัดการรหัสผ่านของผู้ใช้ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องบริหารจัดการรหัสผ่านของผู้ใช้ให้มีความมั่นคงปลอดภัย

    1.3 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือ เท่ากับ 8 ตัวอักษร โดยมี การผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

    1.4 ผู้ใช้ต้องลงนามสัญญาการใช้งานเครือข่ายว่าจะเก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ และไม่บอกรหัสแก่บุคคลอื่น

    1.5 การบริหารสิทธิการเข้าถึงระบบคอมพิวเตอร์และเครือข่ายของผู้ใช้ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายจะกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบตามที่ผู้บริหารมหาวิทยาลัยหรือคณะหรือสำนักงานต่างๆ เป็นผู้กำหนด

    1.6 ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศของผู้ใช้ตามระยะเวลาที่กำหนดไว้ อย่างน้อย 1 ครั้งต่อรอบ 6 เดือน

    1.7 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัย ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัยสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศได้

1.8 การจำกัดเส้นทางบนเครือข่าย ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

2. <u>การควบคุมการเข้าถึงระบบปฏิบัติการ กำหนดขึ้นด้วยวัตถุประสงค์เพื่อป้องกันการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและ/หรือการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต</u>

2.1 การจำกัดระยะเวลาการใช้งาน ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย ต้องจำกัดระยะเวลาการใช้งานสำหรับระบบสารสนเทศที่มีความสำคัญสูงหรือมีความเสี่ยงสูง

2.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้เป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

2.3 การบริหารจัดการรหัสผ่าน ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

2.4 ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องกำหนดให้ระบบให้บริการปฏิเสธการเข้าใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง

2.5 การตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย เมื่อเครื่องลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอและต้องใช้รหัสผ่านในการเข้าสู่ระบบอีกครั้ง เป็นต้น

2.6 การควบคุมการใช้งานโปรแกรมยูทิลิตี้ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงระบบฯ โดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนเข้าใช้งานต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ใครเป็นผู้ใช้งาน

2.7 ให้ติดตั้งระบบเตือนภัยให้กับผู้ใช้ที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

3. <u>การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ กำหนดขึ้นด้วยวัตถุประสงค์ เพื่อป้องกันการใช้งานระบบสารสนเทศ โดยไม่ได้รับอนุญาต</u>

3.1 การจำกัดการใช้งานสารสนเทศผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย ต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่า สารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

3.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง ต้องแยกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระบบที่เชื่อมต่อระหว่างระบบอินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานทั่วไปในมหาวิทยาลัย ออกจากการเชื่อมต่อเพื่อใช้งานระบบ ERP เป็นต้น

4. <u>การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกมหาวิทยาลัย กำหนดขึ้นด้วยวัตถุประสงค์เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนที่ได้รวมทั้งการปฏิบัติงานนอกมหาวิทยาลัยให้เป็นไปอย่างปลอดภัย</u>

   4.1 การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้กลุ่มบุคลากรต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook, Tablet หรือ Smartphone) เช่น เมื่อปฏิบัติงานอยู่นอกสถานที่ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพาและต้องเข้ารหัสข้อมูลที่สำคัญไว้ เป็นต้น

   4.2 การปฏิบัติงานนอกมหาวิทยาลัย ผู้ใช้งานระบบสารสนเทศกลุ่มบุคลากรต้องปฏิบัติตามนโยบายการปฏิบัติงานนอกสถานที่ เช่น ใช้วิธีการป้องกันสำหรับเครื่องคอมพิวเตอร์พกพา การติดต่อผ่านทางเครือข่ายจากภายนอกต้องได้รับการป้องกันการถูกลักลอบดูข้อมูล เป็นต้น

8 นโยบายการใช้อุปกรณ์ไอทีส่วนบุคคล

ให้กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยของคอมพิวเตอร์ส่วนบุคคล ซึ่งทั้งที่เป็นทรัพย์สินของมหาวิทยาลัย หรือเป็นทรัพย์สินส่วนตัวของผู้ใช้ที่นำมาใช้งานกับระบบสารสนเทศของมหาวิทยาลัย เพื่อให้การจัดการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์เป็นไปอย่างเป็นระบบ มีแบบแผนและสามารถจัดการปัญหาความปลอดภัยที่อาจจะเกิดขึ้นได้อย่างรวดเร็ว เนื่องจากการใช้งานเครื่องคอมพิวเตอร์ภายในมหาวิทยาลัยมีอยู่ในหลายคณะหลายหน่วยงานที่มีการเชื่อมต่อเครือข่ายภายในและภายนอก (ระบบเครือข่ายอินทราเน็ตและเครือข่ายอินเตอร์เน็ต) ซึ่งอาจมีการติดไวรัสคอมพิวเตอร์ หรือ malware ต่างๆและเครื่องคอมพิวเตอร์เหล่านี้อาจถูกโจมตีและเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ใช้ (User) ได้แก่ นิสิตและบุคลากรของมหาวิทยาลัยที่มีชื่ออยู่ในบัญชีผู้ได้รับสิทธิการใช้งานระบบคอมพิวเตอร์และเครือข่ายที่ประกาศโดยสำนักบริหารเทคโนโลยีสารสนเทศ
2. ผู้ดูแลระบบ (System administrator) หมายถึง ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ดูแลระบบคอมพิวเตอร์และเครือข่าย
3. คอมพิวเตอร์ส่วนบุคคล หมายถึง คอมพิวเตอร์ซึ่งเป็นทรัพย์สินของมหาวิทยาลัยซึ่งได้จัดสรรให้บุคลากรและนิสิตใช้งาน ซึ่งแบ่งเป็นสองประเภท คือ คอมพิวเตอร์ประจำตัว และคอมพิวเตอร์ให้บริการ
4. คอมพิวเตอร์ส่วนตัว หมายถึง เครื่องคอมพิวเตอร์พกพา (Notebook, Tablet หรือ Smartphone) ที่ผู้ใช้นำมาเอง

1. การจัดลำดับชั้นความมั่นคงของคอมพิวเตอร์ส่วนบุคคล

คอมพิวเตอร์ส่วนบุคคล ลำดับชั้นความมั่นคงของคอมพิวเตอร์ส่วนบุคคลแบ่งเป็นสามระดับคือ ระดับที่ 1 (ความมั่นคงสูงมาก) ระดับที่ 2 (ความมั่นคงสูง) และระดับที่ 3 (ความมั่นคงปกติ)

1.1 ระดับที่ 1 (ความมั่นคงสูงมาก) คือ คอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานและมีการจัดเก็บบันทึกข้อมูลที่มีความสำคัญ หากข้อมูลเสียหายจะส่งผลกระทบต่อการดำเนินงานของมหาวิทยาลัย ได้แก่ คอมพิวเตอร์ด้านการเงิน การบัญชี การลงทะเบียน งานบุคคล งานสารบรรณและงานพัสดุหรืองานอื่นใดที่จะกำหนดเพิ่มเติมในภายหลัง

1.2 ระดับที่ 2 (ความมั่นคงสูง) คือ คอมพิวเตอร์ที่ใช้ดูแลระบบคอมพิวเตอร์และเครือข่าย หรือใช้พัฒนาโปรแกรมของระบบสารสนเทศและคอมพิวเตอร์ของผู้บริหาร

1.3 ระดับที่ 3 (ความมั่นคงปกติ) คือ คอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานทั่วไป และคอมพิวเตอร์ให้บริการ รวมถึงคอมพิวเตอร์ส่วนตัว

2. ข้อกำหนดด้านความปลอดภัย

2.1 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

2.2 เครื่องคอมพิวเตอร์ทุกเครื่องต้องมีการลงโปรแกรม Antivirus , Antispyware และ Firewall เป็นไปตามข้อกำหนด

2.3 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องที่เป็นทรัพย์สินของมหาวิทยาลัยต้องมีการป้องกันโดยใช้ Password ในระดับ BIOS เพื่อป้องกันการแก้ไขค่าติดตั้งเบื้องต้นประจำเครื่อง

2.4 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องที่เป็นทรัพย์สินของมหาวิทยาลัยควรลงโปรแกรมการบริหารการจัดการเครื่องคอมพิวเตอร์เพื่อป้องกันการติดตั้งโปรแกรมหรือการแก้ไขค่าติดตั้งประจำเครื่อง เช่น IP address หรือ เปลี่ยนแปลงสิทธิการใช้เครื่อง เป็นต้น

2.5 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องติดตั้งระบบ Screen saver และให้ Screen saver ทำงานเมื่อเครื่อง idle เป็นระยะเวลา 5 นาทีขึ้นไป และกำหนดให้ต้องใส่รหัสผ่านในการเข้าใช้งานอีกครั้งหนึ่ง

2.6 ห้ามผู้ใช้ที่ไม่ได้รับอนุญาต ใช้งานคอมพิวเตอร์ที่มีความมั่นคงระดับที่ 1 โดยเด็ดขาด หากมีความจำเป็นต้องให้ผู้อื่นใช้ เครื่องคอมพิวเตอร์ในการปฏิบัติงาน ผู้ใช้ประจำเครื่องคอมพิวเตอร์นั้นจะต้องอนุญาตและต้องคอยเฝ้าระวังในระหว่างการใช้งาน

2.7 การเข้าถึงข้อมูลจะถูกจำกัดโดยผู้ดูแลระบบ ห้ามมิให้ผู้ใช้งานเข้าถึงข้อมูลที่ไม่อนุญาต

2.8 การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์เป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์นั้น

2.9 ห้ามนำคอมพิวเตอร์ส่วนตัวมาใช้งานในความมั่นคงระดับที่ 1 และให้ สบท. เตรียมเครื่องคอมพิวเตอร์ส่วนบุคคลให้กับผู้ว่าจ้างดูแลระบบใช้งาน หรือหากจะยกเว้นให้ผู้ว่าจ้างดูแลระบบใช้คอมพิวเตอร์ส่วนตัวต้องได้รับอนุญาตจาก สบท. และมีเจ้าหน้าที่นั่งประกบขณะปฏิบัติงาน

3. <u>ข้อกำหนดการใช้งานทั่วไป</u>

ข้อกำหนดการใช้งานสำหรับผู้ใช้

3.1 ห้ามมิให้มีการเปิดระบบแชร์แฟ้มข้อมูลหรือโฟลเดอร์ระหว่างคอมพิวเตอร์ส่วนบุคคลที่เป็นทรัพย์สินของมหาวิทยาลัยยกเว้นได้รับอนุญาตจากผู้ดูแลระบบเป็นรายกรณี

3.2 หากคอมพิวเตอร์ส่วนบุคคลที่เป็นทรัพย์สินของมหาวิทยาลัยไม่สามารถทำงานได้ตามปกติ ผู้ใช้งานสามารถแจ้งผู้ดูแลระบบเพื่อแก้ปัญหาได้ ห้ามมิให้ผู้ใช้งานติดตั้ง ปรับแก้ และเปลี่ยนแปลงฮาร์ดแวร์และ/หรือซอฟต์แวร์ด้วยตนเอง ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบเป็นรายกรณี

3.3 ห้ามทำงานอื่นที่ไม่ได้รับมอบหมายในเครื่องคอมพิวเตอร์ที่มีความมั่นคงระดับ 1

3.4 ผู้ใช้งานต้องปฏิบัติตามคำแนะนำเมื่อผู้ดูแลระบบแจ้งให้เปลี่ยนรหัสผ่าน

3.5 ผู้ใช้งานต้องไม่เปิดอ่าน e-mail ที่ไม่มั่นใจว่าผู้ส่งมาเป็นผู้ใดเนื่องจากอาจมีโปรแกรมไวรัสคอมพิวเตอร์และโปรแกรมประเภท malware ต่างๆ ติดมาพร้อม e-mail

3.6 ห้ามไม่ให้ติดตั้งซอฟต์แวร์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานกับเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของมหาวิทยาลัย

3.7 การติดตั้งซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการทำงานโดยตรงให้ผู้ใช้งานขออนุญาตผ่านผู้บังคับบัญชา

3.8 ผู้ใช้งานต้องตรวจสอบเครื่องว่ามีโปรแกรมไวรัสคอมพิวเตอร์หรือโปรแกรมประเภท malware ในเครื่องหรือไม่

3.9 ผู้ใช้งานประจำเครื่องมีหน้าที่สำรองข้อมูล และบำรุงรักษาคอมพิวเตอร์ตามระยะเวลาที่กำหนด

3.9.1 คอมพิวเตอร์ที่มีความมั่นคงระดับที่ 1 ให้สำรองข้อมูลทุกวันตามคำแนะนำของผู้ดูแลระบบ

3.9.2 คอมพิวเตอร์ที่มีความมั่นคงระดับที่ 2 และ 3 ให้สำรองข้อมูลทุกเดือน

3.10 ในกรณีที่ข้อมูลเกิดความเสียหาย ให้ผู้ใช้งานประจำเครื่องกู้ข้อมูลตามคำแนะนำของผู้ดูแลระบบ ทั้งนี้หากเป็นคอมพิวเตอร์ส่วนบุคคลที่มีความมั่นคงระดับที่ 1 จะต้องดำเนินการโดยผู้ดูแลระบบ

3.11 รายงานสิ่งผิดปกติที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ส่วนบุคคลต่อผู้ดูแลระบบ

4. <u>ข้อกำหนดการใช้งานของผู้ดูแลระบบ</u>

4.1 กำหนดรหัสผ่านให้กับเครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องที่เป็นทรัพย์สินของมหาวิทยาลัย ผู้ดูแลระบบจะมีรหัสผ่านสองชุดเพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำรองสำหรับการใช้งานในกรณีฉุกเฉิน

4.2 ติดตั้งซอฟต์แวร์ต่างๆ ที่จำเป็นต่อการใช้งานให้เพียงพอต่อการใช้งานในแต่ละระดับ

4.3 ทำการ update โปรแกรมต่าง ๆ เช่น Windows, Antivirus และ Antispyware ทุกสัปดาห์ เพื่อให้โปรแกรมที่ใช้งานมีความทันสมัยอยู่เสมอ

4.4 ทำการ update บัญชีรายชื่อไวรัสคอมพิวเตอร์ทุกสัปดาห์ให้คอมพิวเตอร์ทุกเครื่องอยู่ในสภาพพร้อมใช้และปราศจากโปรแกรมที่ไม่พึงประสงค์

4.5 ทำการ scan ไวรัสคอมพิวเตอร์และ malware ทุกสัปดาห์

4.6 ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เช่น มีการติดไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์ส่วนบุคคลในระดับความมั่นคงทุกระดับ ทันที ที่เกิดเหตุการณ์ขึ้น

4.7 ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศเป็นประจำทุกเดือน

4.8 ผู้ดูแลระบบบันทึกผู้ใช้ที่ฝ่าฝืนข้อปฏิบัติด้านความมั่นคงคอมพิวเตอร์ส่วนบุคคลเสนอต่อผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศเป็นประจำทุกเดือน

9 นโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

ให้มีการวางระเบียบแนวทางปฏิบัติทั้งทางด้านจริยธรรม จรรยาบรรณ และความถูกต้องตามกฎหมายเพื่อป้องกันความเสียหายอันเกิดจากกระทำที่ไม่ถูกต้อง โดยกำหนดเป็นแนวปฏิบัติให้นิสิตและบุคลากรในการใช้งานเครือข่ายสารสนเทศของมหาวิทยาลัยอย่างมีประสิทธิภาพ เพื่อปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้รวมถึงการรักษาข้อมูลที่เป็นสมบัติของมหาวิทยาลัยให้มีความมั่นคงปลอดภัยในการนำมาใช้งานและรักษาภาพลักษณ์ของมหาวิทยาลัย

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ทรัพยากร (Resource) หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของมหาวิทยาลัย
2. ผู้ใช้ (User) ได้แก่ นิสิตและบุคลากรของมหาวิทยาลัย หรือบุคคลภายนอกที่มีบัญชีการใช้งานเครือข่ายคอมพิวเตอร์ที่ประกาศโดยสำนักบริหารเทคโนโลยีสารสนเทศ
3. ผู้ดูแลระบบ (System administrator) หมายถึง ผู้ซึ่งได้รับมอบหมายให้ทำหน้าที่ดูแลระบบคอมพิวเตอร์และเครือข่าย

1. ผู้ดูแลระบบ

1.1 ทำหน้าที่เฝ้าระวังการใช้งานผิดวัตถุประสงค์
1.2 มีหน้าที่รายงานเหตุการณ์ผิดปกติให้กับผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
1.3 มีหน้าที่ปรับปรุงระบบเครือข่ายและอุปกรณ์คอมพิวเตอร์ให้มีประสิทธิภาพและทันสมัยอยู่เสมอ
1.4 มีหน้าที่ป้องกันภัยจากผู้บุกรุกทั้งภายนอกและภายในมหาวิทยาลัยรวมถึงการป้องกันภัยไวรัสคอมพิวเตอร์
1.5 มีหน้าที่จัดหาและใช้ระบบบันทึก ระบบตรวจสอบและแก้ไขปัญหาความปลอดภัยของเครือข่าย
1.6 มีสิทธิยุติการทำงานของโปรเซสเซอร์ที่สร้างภาระให้ระบบ และอาจทำให้เกิดปัญหากับการใช้งานต่อผู้ใช้ส่วนรวม
1.7 มีหน้าที่แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบเพื่อบำรุงรักษาปรับปรุง หรือเปลี่ยนแปลงระบบซึ่งส่งผลให้ต้องหยุดบริการในช่วงระยะเวลาหนึ่ง แต่ในกรณีฉุกเฉินผู้ดูแลระบบอาจมีความจำเป็นต้องปิดระบบอย่างเร่งด่วนได้
1.8 มีหน้าที่จัดอบรมและแจ้งให้ผู้ใช้รับทราบถึงวิธีการรักษาความปลอดภัยของเครือข่ายและมีอำนาจที่จะเพิ่ม ลด ยุติหรือเพิกถอนสิทธิการใช้คอมพิวเตอร์และเครือข่ายโดยทันทีหากตรวจพบว่าผู้ใช้ฝ่าฝืนระเบียบหรือกระทำการที่อาจสร้างความเสียหายให้กับระบบ

2. ผู้ใช้

2.1 ต้องเข้าเรียนหรือฝึกอบรม และผ่านการสอบในหลักสูตรออนไลน์การใช้งานเครือข่ายคอมพิวเตอร์อย่างถูกต้องปลอดภัยที่ทางมหาวิทยาลัยกำหนดและนำไปปฏิบัติอย่างเคร่งครัด
2.2 กำหนดรหัสผ่านที่ปลอดภัยและรักษารหัสให้เป็นความลับอยู่ตลอดเวลา รวมถึงมีการเปลี่ยนแปลงรหัสทุกภาคการศึกษา

2.3 นำเครื่องคอมพิวเตอร์ลูกข่ายส่วนตัวที่ปลอดภัยมาใช้กับระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยตามจำนวนเครื่องที่ได้รับสิทธิที่ทางมหาวิทยาลัยกำหนด

2.4 รายงานการล่วงละเมิดความปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายให้ผู้ดูแลระบบทราบในทันที

2.5 ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ

2.6 ไม่ปลอมแปลงชื่อผู้ใช้ภายใต้ระบบบัญชี หรือ สร้างรายชื่อผู้ใช้เพื่อให้เข้าใจว่าเป็นบุคคลอื่น

2.7 ไม่เข้าใช้ เรียกดู ลบ สำเนา หรือแก้ไขข้อมูลหรือโปรแกรมของผู้อื่นโดยผู้ใช้ไม่มีสิทธิหรือได้รับอนุญาตโดยเจ้าของ

2.8 ไม่ลักลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้ใช้อื่น หรือการกระทำการอันใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

2.9 ไม่ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ใดๆที่จะตรวจค้นจุดบกพร่องของฮาร์ดแวร์หรือซอฟต์แวร์หรือทำลายกลไกรักษาความปลอดภัยระบบ

2.10 ไม่เผยแพร่ เวอร์ม (Worm, Malware) หรือโปรแกรมประเภทไวรัส

2.11 ไม่ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

2.12 ไม่ใช้คอมพิวเตอร์และเครือข่ายโดยก่อผลกระทบต่อประสิทธิภาพโดยรวม เช่น การสร้างภาระให้กับระบบจนกระทั่งส่งผลกระทบต่อผู้ใช้งานอื่น

2.13 ไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อกระจายข่าวสารที่ไม่พึงประสงค์ หรือส่งจดหมายลูกโซ่ หรือส่งจดหมายขนาดใหญ่ หรือส่งจดหมายจำนวนมาก

2.14 ไม่ส่ง เผยแพร่ หรือประกาศข้อความใดที่จะล่วงละเมิด สร้างความเดือดร้อน รบกวน ข่มขู่ หมิ่นประมาท หรือส่งคำหยาบคายต่อบุคคลหรือกลุ่มบุคคล หรือนิติบุคคลมิว่าในเรื่องเชื้อชาติ ศาสนา เพศ หรืออื่นๆ ผู้ใช้ควรใช้คอมพิวเตอร์และเครือข่ายเพื่อการสื่อสารด้วยมารยาทและจริยธรรมอันดี

2.15 ไม่ใช้เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเข้าสู่เวบไซต์ที่ไม่เหมาะสมเช่น เวบไซต์การพนัน หรือเวบไซต์ต้องห้ามต่างๆ

2.16 ไม่เผยแพร่ข้อมูลและซอฟต์แวร์ที่อยู่ภายใต้กฎหมายทรัพย์สินทางปัญญาโดยไม่ได้รับอนุญาตจากเจ้าของ

2.17 ไม่ลักลอบใช้โปรแกรมหรือฮาร์ดแวร์ในการดักจับข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาต

2.18 ไม่ใช้คอมพิวเตอร์เพื่อการกระทำที่ผิดกฎหมาย

3. <u>สิทธิการใช้เครือข่าย</u>

3.1 สิทธิการใช้เครือข่ายเป็นสิทธิพิเศษเฉพาะ (Privilege) ที่ทางมหาวิทยาลัยจัดหาให้ นิสิต บุคลากร หรือบุคคลภายนอกที่ได้รับสิทธิ ซึ่งไม่สามารถโอนสิทธิให้แก่บุคคลอื่นได้

3.2 ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้รายอื่น

3.3 ผู้ใช้ต้องใช้เครือข่ายตามมารยาทและจรรยาบรรณตามนโยบายและข้อปฏิบัติของการใช้เครือข่ายของมหาวิทยาลัยและตามหลักสากลอย่างเคร่งครัด

10 นโยบายการดำเนินงานต่อเนื่อง Business Continuity Plan (BCP) และรับเหตุการณ์ฉุกเฉิน (Disaster)

มีแผนบริหารความต่อเนื่องการดำเนินงาน (BCP) เพื่อให้มั่นใจว่าการให้บริการที่กำหนดไว้ในแผน จะสามารถดำเนินต่อไปได้เมื่อเกิดเหตุการณ์ที่จะต้องประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงาน โดยผู้ที่ได้รับมอบหมายสามารถปฏิบัติตามกระบวนการที่กำหนดไว้ได้อย่างถูกต้อง สามารถกู้คืนระบบกลับมาให้บริการต่อไปได้ โดยมีรายละเอียดในเรื่องต่างๆ ดังนี้

- กำหนดความเสี่ยงหลักที่มีผลกระทบต่อการดำเนินงานของมหาวิทยาลัย
- กำหนดกลยุทธ์ในการลดความเสี่ยงดังกล่าว รวมถึงการดำเนินการที่เกี่ยวข้อง
- กำหนดทรัพยากรที่ต้องการใช้ในการดำเนินงานและ (งบประมาณ) ในการนำแผนมาใช้ในการดำเนินการ
- มีการซ้อมแผนและทบทวนปรับปรุงแผนทุกปี

แนวปฏิบัติตามนโยบาย ประกอบด้วย

1. ขอบเขต
2. บทบาทหน้าที่และความรับผิดชอบของคณะทำงาน
   - 2.1 คณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Steering Committee)
   - 2.2 ผู้ประสานงานคณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Coordinator)
   - 2.3 ทีมกู้คืนระบบ (Service Recovery Team)
   - 2.4 ฝ่ายสนับสนุนและแจ้งข่าวด้านระบบเทคโนโลยีสารสนเทศ (ฝ่ายบริการเทคโนโลยีสารสนเทศ)
3. การประเมินความเสี่ยงของการบริหารความต่อเนื่องการดำเนินงาน
   - 3.1 ความเสี่ยง
   - 3.2 ระดับความเสี่ยงที่ยอมรับได้ (Acceptable Risk Level)
   - 3.3 การวิเคราะห์ภัยคุกคามและการวิเคราะห์ความเสี่ยง
   - 3.4 การจัดการความเสี่ยง (Risk Treatment)
4. การวิเคราะห์ผลกระทบต่อการทำงานในการบริหารความต่อเนื่องการดำเนินงาน (BCM)
   - 4.1 วิเคราะห์และจัดลำดับความสำคัญของทรัพยากรด้านเทคโนโลยีสารสนเทศ

<u>การเตรียมการและปฏิบัติตามแผนบริหารความต่อเนื่องการดำเนินงาน (BCP)</u>

5. การเตรียมการก่อนเกิดเหตุการณ์ภัยพิบัติ

    5.1 การจัดทำสัญญาการให้บริการเกี่ยวกับการเชื่อมต่ออินเตอร์เน็ต

    5.2 กำหนดจุดรวมพล

    5.3 การกำหนดสถานที่ศูนย์สั่งการและที่ปฏิบัติงานสำรอง

    5.4 การจัดตั้งศูนย์สั่งการ และ DR Site

6. การรับมือกับเหตุการณ์ภัยพิบัติ

    6.1 การจัดการเหตุการณ์และการประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงาน BCM

    6.2 การติดต่อผู้ที่เกี่ยวข้อง

7. การจัดเตรียมสถานที่

    7.1 การจัดการความพร้อมของศูนย์สั่งการ

    7.2 การแจ้งข่าวเกี่ยวกับระบบสารสนเทศ

    7.3 การประกันภัย

8. สถานการณ์และขั้นตอนการกู้คืนระบบ

    8.1 เวลาที่ใช้ในการตอบสนองและกำลังคนที่ต้องการ

    8.2 ระยะเวลาในการเริ่มดำเนินการใหม่และการกู้ระบบ

9. แผนการจัดการความต่อเนื่องการดำเนินงาน

    9.1 แผนการจัดการความต่อเนื่องการดำเนินงาน - BCP-001

    9.2 แผนการจัดการความต่อเนื่องทางธุรกิจ - BCP-002

1. ขอบเขต

- จัดทำแผนการบริหารความต่อเนื่องการดำเนินงานตามแนวทางมาตรฐาน ISO/IEC 27001:2005: Including information security in the business continuity management process.

- แผนบริหารความต่อเนื่องการดำเนินงานจะนำมาใช้ในกรณีที่การให้บริการต้องหยุดชะงัก ซึ่งทำให้ระบบงานที่มหาวิทยาลัยเลือกให้เป็นระบบที่มีความสำคัญในการดำเนินงานต่อเนื่อง ไม่สามารถดำเนินการหรือหยุดให้บริการเป็นเวลานาน โดยกำหนดให้มีการซ้อมแผนปีละ 1 ครั้ง (เดือนมกราคม)

- ขอบเขตของแผนบริหารความต่อเนื่องการดำเนินงานนี้ครอบคลุมการวางแผนรองรับเหตุการณ์ฉุกเฉิน การวางแผนการกู้คืนระบบสำหรับระบบหรือบริการที่สำคัญให้สามารถดำเนินการได้ภายในระยะเวลาที่กำหนด โดยมี Scenario ใน 2 ลักษณะ คือ

  1.1 กรณี บุคลากรไม่สามารถเดินทางมาทำงานที่มหาวิทยาลัยได้ เป็นจำนวนมาก นับตั้งแต่มหาวิทยาลัยเริ่มประกาศปิดมหาวิทยาลัยจากเหตุฉุกเฉินต่างๆ

  1.1.1 ระบบงานหลักไม่มีปัญหา ให้บุคลากรที่จำเป็นสำหรับระบบงานหลักให้สามารถ remote เข้าระบบงานทำงาน (BCP-001)

  1.1.2 ระบบงานหลักมีปัญหา ให้บุคลากรที่จำเป็นสำหรับระบบงานหลักให้สามารถ remote เข้าใช้ระบบงานสำรอง ที่ศูนย์ IDC สำรองในมหาวิทยาลัยที่อาคารมหิตลาธิเบศร (BCP-001) แทนได้

  1.2 กรณี บุคลากรไม่สามารถเดินทางมาทำงานที่มหาวิทยาลัยได้เป็นจำนวนมาก นับตั้งแต่มหาวิทยาลัยเริ่มประกาศปิดมหาวิทยาลัยจากเหตุฉุกเฉินต่างๆ และมีปัญหาทั้งที่ระบบงานหลักและระบบงานสำรองในมหาวิทยาลัย ใช้ระบบงานสำรอง ที่ศูนย์สำรอง DR-site นอกจุฬาลงกรณ์มหาวิทยาลัย (BCP-002)

- มีการทบทวนแผนบริหารความต่อเนื่องการดำเนินงานทุกปี หรือหากมีการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นดังนี้:
  - การเปลี่ยนแปลงของสภาพแวดล้อม
  - การเปลี่ยนแปลงของมาตรการควบคุมด้านเทคนิคและสภาพแวดล้อมทางด้านเทคนิค
  - การเปลี่ยนแปลงผู้รับผิดชอบในส่วนต่างๆ
  - การเปลี่ยนแปลงใดๆ ที่มีผลต่อการดำเนินงานตามแผนบริหารความต่อเนื่อง

- มีการแต่งตั้งคณะทำงาน เพื่อให้สามารถดำเนินงานได้เมื่อมีการประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงาน ดังต่อไปนี้
  - คณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Steering Committee)
  - ผู้ประสานงานคณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Coordinator)

- ทีมกู้คืนระบบ (Service Recovery Team)
- ฝ่ายสนับสนุนและประชาสัมพันธ์

2. บทบาทหน้าที่และความรับผิดชอบของคณะทำงาน

ผู้ที่เกี่ยวข้องในแผนการบริหารความต่อเนื่องการดำเนินงาน ประกอบไปด้วยคณะทำงานต่างๆ ดังต่อไปนี้

- คณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Steering Committee)
- ผู้ประสานงานคณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Coordinator)
- ทีมกู้คืนระบบ (Service Recovery Team)
- ฝ่ายสนับสนุนและแจ้งข่าวด้านระบบเทคโนโลยีสารสนเทศ (ฝ่ายบริการเทคโนโลยีสารสนเทศ)

2.1 คณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Steering Committee)

คณะกรรมการ ประกอบด้วย

- ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ (สบท.) ประธาน
- ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ กรรมการ
- ผู้อำนวยการฝ่ายระบบเทคโนโลยีสารสนเทศ กรรมการ
- ผู้อำนวยการศูนย์การจัดการทรัพยากรของมหาวิทยาลัย (ศจท.) กรรมการ
- ผู้อำนวยการสำนักงานการทะเบียน กรรมการ
- ผู้อำนวยการศูนย์นวัตกรรมการเรียนรู้ (ศนว.) กรรมการ
- ผู้อำนวยการสำนักบริหารระบบกายภาพ (สบภ.) กรรมการ
- ผู้อำนวยการฝ่ายบริการเทคโนโลยีสารสนเทศ กรรมการและเลขานุการ

มีหน้าที่ดังต่อไปนี้

- ประเมินความเสียหายอันเกิดจากเหตุการณ์ภัยพิบัติ
- กำหนดทิศทางในการดำเนินการกู้คืนระบบ และให้การสนับสนุนการกู้คืนตลอดจนการฟื้นฟูระบบที่ได้รับความเสียหาย
- ให้ข้อมูลสถานการณ์ดำเนินการแก่ผู้ที่เกี่ยวข้อง เช่น บุคลากร และหน่วยงานที่เกี่ยวข้อง
- พิจารณาประกาศใช้แผนบริหารความต่อเนื่อง กรณีเกิดเหตุการณ์ภัยพิบัติ

2.2 ผู้ประสานงานคณะกรรมการบริหารความต่อเนื่องการดำเนินงานด้านไอที (IT BCM Coordinator) ประกอบด้วย

- ผู้อำนวยการฝ่ายบริการเทคโนโลยีสารสนเทศ หัวหน้าทีม IT BCM Coordinator
- ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ผู้ช่วยหัวหน้าทีม IT BCM Coordinator
- ผู้อำนวยการฝ่ายระบบเทคโนโลยีสารสนเทศ ผู้ช่วยหัวหน้าทีม IT BCM Coordinator

มีหน้าที่ดังต่อไปนี้

- ติดต่อ IT BCM Steering Committee เพื่อให้เข้ามาร่วมประเมินความเสียหายอันเกิดจากเหตุการณ์ภัยพิบัติ
- ติดต่อผู้ที่เกี่ยวข้องหากมีการประกาศใช้งานบริหารความต่อเนื่องการดำเนินงานด้านไอที
- ประสานงานการกู้คืนระบบ และเป็นผู้อัพเดทสถานภาพการดำเนินงานให้กับ IT BCM Steering Committee
- ตรวจสอบผลการกู้คืนระบบ

2.3 ทีมกู้คืนระบบ ประกอบด้วยบุคลากรด้านเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากฝ่ายต่างๆ ดังนี้

- ทีมงานของฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
- ทีมงานของฝ่ายระบบเทคโนโลยีสารสนเทศ
- ทีมงานของฝ่ายบริการเทคโนโลยีสารสนเทศ
- ทีมงานของสำนักบริหารระบบกายภาพ
- ทีมงานของศูนย์การจัดการทรัพยากรของมหาวิทยาลัย
- ทีมงานของสำนักงานการทะเบียน
- ทีมงานของศูนย์นวัตกรรมการเรียนรู้

มีหน้าที่ดังต่อไปนี้

- ปฏิบัติหน้าที่ตามที่ได้รับมอบหมายจากคณะทำงาน IT BCM Steering Committee
- ดำเนินการกู้คืนข้อมูลและระบบสารสนเทศที่สำคัญตามที่กำหนดไว้ในแผนการดำเนินงาน (Scenario)

2.4 ฝ่ายสนับสนุนและแจ้งข่าวด้านระบบเทคโนโลยีสารสนเทศ

ทีมงานของฝ่ายบริการเทคโนโลยีสารสนเทศ มีหน้าที่ดังต่อไปนี้

- ให้ข้อมูลแก่หน่วยงานที่เกี่ยวข้องเกี่ยวกับเรื่องการให้บริการเทคโนโลยีสารสนเทศ
- ปฏิบัติหน้าที่ตามที่ได้รับมอบหมายจากคณะทำงาน IT BCM Steering Committee
- จัดเตรียมสถานที่เพื่อใช้ในการปฏิบัติงาน สำหรับศูนย์สั่งการหรือ DR site
- จัดเตรียมอาหารและระบบสาธารณูปโภคให้พร้อมสำหรับการดำเนินงาน

3. การประเมินความเสี่ยงของการบริหารความต่อเนื่องการดำเนินงาน

3.1 ความเสี่ยง คือ

- ความเสี่ยง หมายถึง โอกาสที่ระบบงานสำคัญๆ ด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยจะเกิดความสูญเสียหรือความเสียหาย และส่งผลให้เกิดการหยุดชะงักในการดำเนินการได้
- การจัดระดับความสำคัญเพื่อใช้ในการจัดทำแผนการดำเนินการสำหรับรองรับความเสี่ยงที่ถูกระบุไว้ โดยปัญหาที่พบจะต้องถูกนำไปวิเคราะห์ และจัดทำข้อเสนอแนะเพื่อช่วยลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3.2 ระดับความเสี่ยงที่ยอมรับได้ (Acceptable Risk Level)

ระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ ได้แก่ ระดับความเสี่ยงที่อยู่ในระดับ “M” และ “L” โดยพิจารณาจากตารางดังต่อไปนี้ (กำหนดความหมายของ E, H, L, M ในตาราง)

โอกาสที่จะเกิด (Likelihood) แบ่งออกเป็น 5 ระดับ ดังนี้

5 - เกือบจะแน่นอน (100%)

4 - น่าจะเกิด (75%)

3 - เป็นไปได้ (50%)

2 - เป็นไปได้ยาก (25%)

1 - ไม่น่าจะเป็นไปได้ (< 25%)

ผลกระทบ (BC impact) แบ่งออกเป็น 4 ระดับ ดังนี้

1 - ไม่สำคัญ	ไม่มีผลต่อการใช้งานระบบ และสามารถแก้ไขได้ใน SLA ตาม Incident Management
2 - เล็กน้อย	ระบบยังพอใช้งานได้ หรือสามารถแก้ไขได้ใน SLA ตาม Incident Management
3 - สูง	ทุกระบบใช้ไม่ได้เลย แต่ทางกายภาพของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศไม่เสียหาย
4 – ภัยพิบัติ	ทุกระบบใช้ไม่ได้เลย และทางกายภาพของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศเสียหาย หรือไม่สามารถให้บริการได้

โอกาสที่จะเกิด (Likelihood)	ผลกระทบ (BC impact)			
	ไม่สำคัญ	เล็กน้อย	สูง	ภัยพิบัติ
	1	2	3	4
5 – เกือบจะแน่นอน (100%)	H	H	E	E
4 – น่าจะเกิด (75%)	M	H	H	E
3 – เป็นไปได้ (50%)	L	M	H	H
2 – เป็นไปได้ยาก (25%)	L	L	M	H
1 – ไม่น่าจะเป็นไปได้ (< 25%)	L	L	L	M

3.3 การวิเคราะห์ภัยคุกคามและการวิเคราะห์ความเสี่ยง

- เพื่อจัดกลุ่มเหตุการณ์ที่อาจเกิดขึ้น (สำหรับการจัดทำแผนบริหารความต่อเนื่อง) จะพิจารณาจากเงื่อนไขต่างๆ ดังต่อไปนี้
  - ผลกระทบของภัยพิบัตินั้นๆ คาดว่า/เกิดขึ้น จะต้องไม่น้อยกว่าค่า **MTPD (Maximum Tolerable Period of Disruption)** ของบริการนั้น ซึ่งหมายถึง ระยะเวลานานที่สุดตั้งแต่เกิดเหตุการณ์ภัยพิบัติ จนกระทั่งระบบสามารถกลับมาปฏิบัติงานหรือดำเนินงานได้ตามปกติ โดยไม่ก่อให้เกิดความเสียหาย หรือการให้บริการของมหาวิทยาลัย
  - ความเสี่ยงที่ระบุไว้ เป็นเหตุการณ์ที่เลวร้ายที่สุดที่อาจเกิดขึ้นได้ (worst case scenario)

- **โอกาสที่จะเกิด (Likelihood) แบ่งออกเป็น 5 ระดับ ดังนี้**

  5 - เกือบจะแน่นอน (100%)

  4 - น่าจะเกิด (75%)

  3 - เป็นไปได้ (50%)

  2 - เป็นไปได้ยาก (25%)

  1 - ไม่น่าจะเป็นไปได้ (< 25%)

- **ผลกระทบ (BC impact) แบ่งออกเป็น 4 ระดับ ดังนี้**

  1 - ไม่สำคัญ ไม่มีผลต่อการใช้งานระบบ และสามารถแก้ไขได้ใน SLA ตาม Incident Management

  2 - เล็กน้อย ระบบยังพอใช้งานได้ หรือสามารถแก้ไขได้ใน SLA ตาม Incident Management

3 - สูง	ทุกระบบใช้ไม่ได้เลย แต่ทางกายภาพของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศไม่เสียหาย
4 – ภัยพิบัติ	ทุกระบบใช้ไม่ได้เลย และทางกายภาพของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศเสียหาย หรือไม่สามารถให้บริการได้

- ได้มีการระบุเหตุการณ์ต่างๆ รวมถึงความเสี่ยงที่จะเกิดขึ้นของแต่ละเหตุการณ์ ไว้ในตารางดังต่อไปนี้

ลำดับ	เหตุการณ์หยุดชะงักทางธุรกิจ (Disruption Events)	ผลที่ตามมา	โอกาสที่จะเกิด (Likelihood)	ระดับของผลกระทบด้านความต่อเนื่องในการดำเนินงาน (BC impact)	ความเสี่ยง (Exposure)	การจัดการความเสี่ยง
1	พายุรุนแรง	ระบบสารสนเทศไม่สามารถให้บริการได้เนื่องจากไฟดับเป็นเวลานานกว่า 1 ชม. และบุคลากร ไม่สามารถมาปฏิบัติงานที่คณะและสำนักงานได้	2	3	M	BCP-002
2	ไฟไหม้/ระเบิด	ไม่สามารถให้บริการหรือปฏิบัติงานได้ เนื่องจากศูนย์ Data Center หลักและสำรอง หรืออุปกรณ์หลักและสำรองได้รับความเสียหายทั้งหมด	2	4	H	BCP-002
3	น้ำท่วมมาก	ระบบโครงสร้างพื้นฐานและระบบงานไม่สามารถให้บริการได้เนื่องจากไฟดับและไฟสำรองดับเป็นเวลานานกว่า 1 ชม. และ บุคลากรไม่สามารถมาปฏิบัติงานที่มหาวิทยาลัยได้	3	4	H	BCP-002
		อาคารสำนักงานเสียหาย ไม่สามารถเข้ามาปฏิบัติงานได้	2	4	H	BCP-002
4	แผ่นดินไหวมาก	อาคารสำนักงานเสียหาย ไม่สามารถเข้ามาปฏิบัติงานได้ หรือ ห้อง Data Center หลัก และสำรอง ได้รับความเสียหาย ไม่สามารถให้บริการได้	2	4	H	BCP-002

ลำดับ	เหตุการณ์หยุดชะงักทางธุรกิจ (Disruption Events)	ผลที่ตามมา	โอกาสที่จะเกิด (Likelihood)	ระดับของผลกระทบด้านความต่อเนื่องในการดำเนินงาน (BC impact)	ความเสี่ยง (Exposure)	การจัดการความเสี่ยง
5	เหตุการณ์ก่อการร้าย	ประกาศภาวะฉุกเฉิน บุคลากรไม่สามารถเข้ามาปฏิบัติงานได้	2	3	M	BCP-001
		อาคารสำนักงาน อุปกรณ์ถูกทำลาย เสียหายหรือสูญหาย และบุคลากรไม่สามารถเข้ามาปฏิบัติงานได้	1	4	M	BCP-002
6	เหตุการณ์ประท้วงหรือชุมนุมทางการเมือง	พนักงานไม่สามารถเข้ามาปฏิบัติงานได้	3	3	H	BCP-001
		อาคารสำนักงาน อุปกรณ์ถูกทำลาย เสียหายหรือสูญหาย และบุคลากรไม่สามารถเข้ามาปฏิบัติงานได้ ทำให้ไม่สามารถให้บริการได้	1	4	M	BCP-002
7	การแพร่กระจายของไวรัสคอมพิวเตอร์	ไม่สามารถให้บริการได้เนื่องจากระบบเครือข่ายล่มนานกว่า 1 ชม.	2	3	M	Incident Management
8	การโจมตีแบบ DDOS	ไม่สามารถให้บริการได้เนื่องจากระบบเครือข่ายล่มนานกว่า 1 ชม.	2	3	M	Incident Management

ลำดับ	เหตุการณ์หยุดชะงักทางธุรกิจ (Disruption Events)	ผลที่ตามมา	โอกาสที่จะเกิด (Likelihood)	ระดับของผลกระทบด้านความต่อเนื่องในการดำเนินงาน (BC impact)	ความเสี่ยง (Exposure)	การจัดการความเสี่ยง
9	ถูกโจมตีแบบ DDOS	ระบบเครือข่ายอินเตอร์เน็ตล่ม ทำให้ไม่สามารถเชื่อมต่ออินเตอร์เน็ตได้ นานกว่า 1 ชม.	2	3	M	Incident Management
10	การเชื่อมต่ออินเตอร์เน็ต (International route) ได้รับความเสียหาย	ระบบเครือข่ายอินเตอร์เน็ตล่ม ทำให้ไม่สามารถเชื่อมต่ออินเตอร์เน็ตได้ นานกว่า 1 ชม.	3	3	M	Incident Management
11	อุปกรณ์ระบบเครือข่ายชำรุดหรือได้รับความเสียหาย	ระบบเครือข่ายล่ม ทำให้ไม่สามารถเชื่อมต่ออินเตอร์เน็ตนานกว่า 1 ชม.	1	4	M	Incident Management
12	บุคลากรลาออกจำนวนมาก	บุคลากรไม่เพียงพอต่อการให้บริการ ทำให้ไม่สามารถให้บริการได้	1	4	M	
		บุคลากรที่เหลือขาดความรู้ความสามารถในการปฏิบัติงานแทน ทำให้ไม่สามารถให้บริการได้	1	4	M	

ลำดับ	เหตุการณ์หยุดชะงักทางธุรกิจ (Disruption Events)	ผลที่ตามมา	โอกาสที่จะเกิด (Likelihood)	ระดับของผลกระทบด้านความต่อเนื่องในการดำเนินงาน (BC impact)	ความเสี่ยง (Exposure)	การจัดการความเสี่ยง
13	โรคระบาด	บุคลากรติดโรคระบาดจำนวนมาก ไม่สามารถมาปฏิบัติงานได้	1	3	L	BCP-001
		บุคลากรไม่สามารถมาปฏิบัติงานได้ เนื่องจากเป็นพื้นที่กักกัน	1	3	L	BCP-002
14	บุคลากรประท้วงเนื่องจากไม่พอใจการจ้างงาน	ไม่มีผู้มาปฏิบัติงาน ทำให้ไม่สามารถให้บริการได้	1	4	M	

3.4 การจัดการความเสี่ยง (Risk Treatment)

ภายหลังการจัดลำดับความเสี่ยงของสถานการณ์แล้ว สถานการณ์ที่มีระดับความเสี่ยงสูงมาก (Extreme) และสูง (High) จะถูกกำหนดไว้ในตารางด้านล่างนี้ เพื่อให้มหาวิทยาลัยสามารถดำเนินงานได้อย่างต่อเนื่อง

ลำดับ	เหตุการณ์หยุดชะงักทางธุรกิจ (Disruption Events)	ผลที่ตามมา	ความเสี่ยง (Exposure)	การจัดการความเสี่ยง (Risk Treatment)	แผนจัดการความต่อเนื่องการดำเนินงาน
1	ไฟไหม้ / ระเบิด	ไม่สามารถให้บริการหรือปฏิบัติงานได้ เนื่องจากศูนย์ Data Center หลัก และสำรองหรือ อุปกรณ์หลักและสำรองได้รับความเสียหายทั้งหมด	H	Reduce	BCP-002
2	น้ำท่วมมาก	ไม่สามารถให้บริการได้เนื่องจากไฟดับและไฟสำรองดับเป็นเวลานานกว่า 1 ชม. และบุคลากรไม่สามารถมาปฏิบัติงานที่มหาวิทยาลัยได้ หรืออาคารสำนักงานเสียหายไม่สามารถเข้ามาปฏิบัติงานได้	H	Reduce	BCP-002
3	แผ่นดินไหวมาก	อาคารสำนักงานเสียหาย ไม่สามารถเข้ามาปฏิบัติงานได้ หรือ ศูนย์ Data Center หลัก และสำรองได้รับความเสียหาย ไม่สามารถให้บริการได้	H	Reduce	BCP-002

ลำดับ	เหตุการณ์หยุดชะงักทางธุรกิจ (Disruption Events)	ผลที่ตามมา	ความเสี่ยง (Exposure)	การจัดการความเสี่ยง (Risk Treatment)	แผนจัดการความต่อเนื่องการดำเนินงาน
4	เหตุการณ์ประท้วงหรือชุมนุมทางการเมือง	พนักงานไม่สามารถเข้ามาปฏิบัติงานได้	H	Reduce	BCP-001

แผนจัดการความเสี่ยง (Risk Treatment Strategy) เสนอ Scenario ใน 2 ลักษณะ คือ

3.4.1 กรณี บุคลากรไม่สามารถเดินทางมาทำงานที่มหาวิทยาลัยได้ เป็นจำนวนมาก นับตั้งแต่มหาวิทยาลัยเริ่มประกาศปิดมหาวิทยาลัยจากเหตุฉุกเฉินต่างๆ

1) ระบบงานหลักไม่มีปัญหา ให้บุคลากรที่จำเป็นสำหรับระบบงานหลักให้สามารถ remote เข้าระบบงานทำงาน (BCP-001)

2) ระบบงานหลักมีปัญหา ให้บุคลากรที่จำเป็นสำหรับระบบงานหลักให้สามารถ remote เข้าใช้ระบบงานสำรอง ที่ศูนย์ IDC สำรองในมหาวิทยาลัยที่อาคารมหิตลาธิเบศร (BCP-001) แทนได้

3.4.2 กรณี บุคลากรก็ไม่สามารถเดินทางมาทำงานที่มหาวิทยาลัยได้เป็นจำนวนมาก นับตั้งแต่มหาวิทยาลัยเริ่มประกาศปิดมหาวิทยาลัยจากเหตุฉุกเฉินต่างๆ และมีปัญหาทั้งที่ระบบงานหลักและระบบงานสำรองในมหาวิทยาลัย ใช้ระบบงานสำรอง ที่ศูนย์สำรอง DR-site นอกจุฬาลงกรณ์มหาวิทยาลัย (BCP-002)

ลำดับ	กลยุทธ์ในการจัดการความเสี่ยง	รายละเอียดการดำเนินงาน
1	BCP-001	● ใช้ศูนย์ IDC สำรองในมหาวิทยาลัยที่อาคารมหิตลาธิเบศร ● นำระบบไฟสำรองมาใช้และจัดเตรียมน้ำมันให้เพียงพอต่อการใช้งานไม่น้อยกว่า 48 ชม. ● จัดหาเส้นทางการเชื่อมอินเตอร์เน็ตและ link สำรอง
2	BCP-002	● ย้ายศูนย์ IDC ไปยังศูนย์สำรอง DR-site นอกจุฬาลงกรณ์มหาวิทยาลัย

4. การวิเคราะห์ผลกระทบต่อการทำงานในการบริหารความต่อเนื่องการดำเนินงาน (BCM)

4.1 วิเคราะห์และจัดสำดับความสำคัญของทรัพยากรด้านเทคโนโลยีสารสนเทศ

ตารางดังต่อไปนี้ สรุปผลการลำดับความสำคัญของระบบงานที่เกี่ยวข้องกับการให้บริการของมหาวิทยาลัย โดยระบบที่มีผลกระทบสูง (H: High Impact) จะต้องได้รับการกู้คืนในช่วงเวลาที่เกิดเหตุการณ์ภัยพิบัติและ มี ศูนย์ IDC สำรองในมหาวิทยาลัยที่อาคารมหิตลาธิเบศร หรือ DR Site อยู่ภายนอกมหาวิทยาลัย

การประเมินระบบงานต่างๆ โดยวิเคราะห์จากระยะเวลาในการกู้คืนระบบ โดยต้องพิจารณาเวลาในแต่ละประเภทดังต่อไปนี้

- **MTPD (Maximum Tolerable Period of Disruption)** หมายถึง ระยะเวลายาวนานที่สุดตั้งแต่เกิดเหตุการณ์ภัยพิบัติ จนกระทั่งสามารถกลับมาปฏิบัติงาน หรือดำเนินธุรกิจได้ตามปกติโดยไม่ก่อให้เกิดความเสียหายต่อมหาวิทยาลัย หรือการให้บริการของมหาวิทยาลัย
- **RTO (Recovery Time Objective)** หมายถึง ระยะเวลาตั้งแต่เกิดเหตุการณ์ภัยพิบัติจนกระทั่งสามารถกู้คืนระบบให้อยู่ในระดับที่ยอมรับได้เพื่อสามารถปฏิบัติงานหรือให้บริการได้
- **RPO (Recovery Point Objective)** หมายถึง ระยะเวลามากที่สุดที่ยอมให้มีการสูญเสียของข้อมูลได้ หากเกิดเหตุการณ์ภัยพิบัติ ทั้งนี้ค่า RPO ขึ้นอยู่กับความถี่ในการสำรองข้อมูลของแต่ละบริการ

Service Lists	MTPD	RTO	RPO	Critical Impact	Remark
01 - ระบบโครงสร้างพื้นฐานที่สำคัญของ สบท.					
1.1 - DNS	1 day	4 hours	1 day	H	ไม่สามารถหา Domain Chula ได้
1.2 - LDAP & AD & RADIUS	1 day	4 hours	1 day	H	ระบบ Authentication เข้าเครือข่าย
1.3 - VM	1 day	6 hours	1 day	H	ระบบ server เสมือนของระบบงานต่างๆ ที่ฝากไว้
02 - ระบบการจัดการทรัพยากรของมหาวิทยาลัย (CU-ERP)	1 day	4 hours	Last transaction	H	RTO ขึ้นอยู่กับระบบ Authentication เข้าเครือข่าย

Service Lists	MTPD	RTO	RPO	Critical Impact	Remark
03 - ระบบบริหารจัดการข้อมูลทะเบียนนิสิต (CU-SAA)	1 day	BCP-001 - 2-3 hours BCP-002 - 5 hours	1 day	H	
04 - ระบบจัดการเรียนการสอน (LMS)	2 day	1 day	1 day	H	

Function	Function unit (Activities)	BCP-001	BCP-002
01 - ระบบโครงสร้างพื้นฐานที่สำคัญของ สบท.	DNS LDAP & AD & RADIUS VM	√	√
02 - ระบบการจัดการทรัพยากรของมหาวิทยาลัย (CU-ERP)	การงบประมาณ การพัสดุ การเงินและการบัญชี การบริหารงานบุคคล	√	√
03 - ระบบบริหารจัดการข้อมูลทะเบียนนิสิต (CU-SAA)	การทะเบียนนิสิต	√	√
04 - ระบบจัดการเรียนการสอน (LMS)	การเรียนการสอน	√	

– VM มีการจัดความสำคัญระบบงานเป็น 3 levels ในการจัดทำ BCP คือ

Level 1: ทำ data back up ใน external storage

Level 2: จัดทำให้มีระบบและข้อมูลสำรองที่ site สำรองภายในจุฬาฯ และเมื่อเกิดเหตุการณ์ภัยพิบัติใช้แผน BCP-001

Level 3: จัดทำให้มีระบบและข้อมูลสำรองที่ site สำรองภายนอกจุฬาฯ และเมื่อเกิดเหตุการณ์ภัยพิบัติใช้แผน BCP-001 และ/หรือ BCP-002

จุฬาลงกรณ์มหาวิทยาลัยมีระบบงานทั้งหมด 42 ระบบงาน 145 servers และมีการจัดลำดับความสำคัญของระบบงาน ดังนี้

ลำดับ	ชื่อระบบงาน	Level1	Level2 (BCP-001)	Level3 (BCP-002)
1	ระบบแชร์พื้นที่จัดเก็บเอกสารงานสำหรับ สนม. (File sharing)	✓	✓	✓
2	เว็บไซต์จุฬาลงกรณ์มหาวิทยาลัย www.chula.ac.th	✓	✓	✓
3	เว็บไซต์ Intranet www.intranet.chula.ac.th	✓	✓	✓
4	ระบบ e-document โครงการ Lesspaper	✓	✓	✓
5	ระบบตรวจสอบการลอกเลียนวรรณกรรมทางวิชาการ (อักขราวิสุทธิ์) -ใช้ตรวจสอบการคัดลอกวิทยานิพนธ์	✓	✓	✓
6	ระบบ Domain Controller (ระบบสำหรับจัดการสิทธิในการเข้าถึงเครื่องคอมพิวเตอร์ในสำนักงานมหาวิทยาลัย)	✓	✓	✓
7	ระบบสารสนเทศเพื่อรับมือและช่วยงานฟื้นฟู (ThaiCrisis Planner & Reporter) http://thaicrisis.chula.ac.th	✓		✓

ลำดับ	ชื่อระบบงาน	Level1	Level2 (BCP-001)	Level3 (BCP-002)
8	ระบบ chular2 สำหรับบริหารจัดการวิจัย เช่น ข้อมูลข้อเสนอโครงการการรับทุน ข้อมูลผู้ทรงคุณวุฒิ https://portal.research.chula.ac.th	✓	✓	
9	ระบบประเมินการเรียนการสอน CUCAS https://www.cas.chula.ac.th/cas/	✓	✓	
10	ระบบ Chula Mobile และ Clicker	✓	✓	
11	ระบบเครื่องแม่ข่ายและฐานข้อมูลของศูนย์ปฏิบัติการลงทุน เช่น ระบบลงทุน Online Trading	✓	✓	
12	ระบบบริหารการพิมพ์ใน สนม. สำหรับจัดการและบริหารเครื่องพิมพ์	✓	✓	
13	ระบบ DHCP (แจกหมายเลขไอพี)	✓	✓	
14	ระบบการทดสอบกลาง (e-Exam) ใช้สำหรับรับสมัครบุคลากร	✓	✓	
15	ระบบเว็บไซต์ของ ERP	✓	✓	
16	ระบบ echo (ระบบบันทึกภาพและเสียงสำหรับการเรียนการสอน)	✓	✓	
17	ระบบการจัดทำวิทยานิพนธ์อิเล็กทรอนิกส์ CU E-THESIS	✓	✓	
18	ระบบแลกเปลี่ยนไฟล์ข้อมูลระหว่างศูนย์สุขภาพและกิจการนิสิต	✓	✓	
19	ระบบจัดทำสารนิพนธ์อิเล็กทรอนิกส์ CU e-IS	✓	✓	
20	ระบบ radius สำหรับ eduroam (ใช้ดูแลควบคุมAccount สำหรับเข้าใช้ eduroam)	✓	✓	

ลำดับ	ชื่อระบบงาน	Level1	Level2 (BCP-001)	Level3 (BCP-002)
21	ระบบควบคุมการเข้า-ออก ประตูภายในสำนักบริหารเทคโนโลยีสารสนเทศและอาคารจามจุรี4	✓		
22	ระบบดูแล Wi-Fi CU iHouse	✓		
23	ระบบเว็บไซต์ ศูนย์พัฒนกิจและนิสิตเก่าสัมพันธ์ alumni.cuar.chula.ac.th	✓		
24	ระบบ Blended Learning ระบบของภาควิชาเทคโนโลยีการศึกษา	✓		
25	ระบบ CHEQA สำนักยุทธศาสตร์และประเมินผล ข้อมูลส่งให้ สกอ.	✓		
26	ระบบดูแล Wi-Fi ของมหาวิทยาลัย (Cisco Prime Infarstructure)	✓		
27	ระบบ cognos (สำหรับให้เจ้าหน้าที่ remote ให้เข้าไปทำงาน)	✓		
28	cp.sa.chula.ac.th โครงการบริหารจัดการสมรรถนะความสามารถของนิสิต	✓		
29	โครงการอบรมออนไลน์ของคณะพาณิชย์ศาสตร์และการบัญชี (CBS InnovativeBusiness Online) http://cer.lic.chula.ac.th	✓		
30	ระบบ CU GATEWAY ระบบนำเสนอผลงานทางวิชาการ งานวิจัยของคณาจารย์ และวิทยานิพนธ์ของนิสิตจุฬาลงกรณ์มหาวิทยาลัยที่น่าสนใจ นำมาผลิตเป็นสื่ออิเล็กทรอนิกส์ และเผยแพร่ไปยังประชาชนทั่วไปผ่านเครือข่ายอินเทอร์เน็ต	✓		

ลำดับ	ชื่อระบบงาน	Level1	Level2 (BCP-001)	Level3 (BCP-002)
31	ระบบรับสมัครงานนิสิตออนไลน์ CU Job http://cujob.student.chula.ac.th/	✓		
32	ระบบงานตรวจสอบภายใน	✓		
33	เว็บไซต์ศูนย์วิจัยเพื่อพัฒนาด้านนวัตกรรมเทคโนโลยีการศึกษา Innovative Educational Technology Research and Development Center	✓		
34	ระบบการจัดการองค์ความรู้ของเครือข่ายวิชาชีพสายสนับสนุน km.chula.ac.th	✓		
35	ระบบงานศูนย์กฎหมายและนิติการ เช่น ระบบติดตามงานคดี	✓		
36	ระบบ DNS จุฬาฯ (name server)	✓		
37	ระบบการรับสมัครคัดเลือกนักเรียนเข้าศึกษาในหลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาการบริหารจัดการทรัพยากรการเกษตร สำนักวิชาทรัพยากรการเกษตร (School of Aricultural Resources)	✓		
38	ระบบงานสำนักยุทธศาสตร์และการงบประมาณ www.qmis.osm.chula.ac.th	✓		
39	ระบบทุนการศึกษากิจการนิสิต	✓		
40	ระบบงานภายในคณะเภสัชศาสตร์	✓		
41	ระบบวิดีโอสตรีมมิ่งของจุฬาฯ (ใช้uploadไฟล์วีดีโอของหน่วยงานในจุฬาฯ การทำงานเหมือน youtube) Netcast.it.chula.ac.th	✓		
42	เว็บไซต์สำนักบริหารวิชาการ www.academic.chula.ac.th	✓		

5. การเตรียมการก่อนเกิดเหตุการณ์ภัยพิบัติ

5.1 การจัดทำสัญญาการให้บริการเกี่ยวกับการเชื่อมต่ออินเตอร์เน็ต

จะต้องปรับแก้สัญญาการให้บริการระหว่าง มหาวิทยาลัย และ Internet Service Provider (ISP) โดยมีรายละเอียดดังต่อไปนี้

- กำหนดระยะเวลาในการกู้คืนการเชื่อมต่ออินเตอร์เน็ต โดยจะต้องสามารถเชื่อมต่อได้ภายในเวลา 4 ชม.
- การจัดหา link สำรอง ในกรณีที่ไม่สามารถกู้คืนการเชื่อมต่ออินเตอร์เน็ตได้ในระยะเวลาที่กำหนดไว้ในข้อแรก

5.2 กำหนดจุดรวมพล

- กำหนดให้มีสถานที่เป็นจุดรวมพลเมื่อมีเหตุการณ์ภัยพิบัติเกิดขึ้น เช่น
  - สบท. ได้กำหนดจุดรวมพลที่ บริเวณลานโพธิ์ หน้าอาคารจามจุรี 4
- มีหมายเลขโทรศัพท์สำหรับเหตุการณ์ฉุกเฉิน ติดประกาศไว้ตามสถานที่ต่างๆ

ชื่อหน่วยงาน	เบอร์โทรศัพท์
สำนักงานรักษาความปลอดภัยแห่งจุฬาฯ • หน่วยรักษาความปลอดภัยของจุฬาฯ	02-218-0000
เหตุด่วนเหตุร้าย • สถานีตำรวจนครบาลบางรัก • สถานีตำรวจนครบาลปทุมวัน	191 02-234-0242 02-215-2991
ไฟไหม้ • สถานีดับเพลิงกรุงเทพมหานคร	199
ไฟฟ้าขัดข้อง • ไฟฟ้านครหลวง	1130
ธนาคารเลือด • โรงพยาบาลจุฬาลงกรณ์ • ศูนย์บริการโลหิตแห่งชาติ สภากาชาดไทย	 02-256-4214 02-263-9600

5.3 การกำหนดสถานที่ศูนย์สั่งการและที่ปฏิบัติงานสำรอง

- ให้กำหนดที่ตั้งของศูนย์สั่งการและหมายเลขโทรศัพท์ติดต่อฉุกเฉิน 24 ชั่วโมง เช่น
  - **BCP-001** สบท. กำหนดไว้ที่ ชั้น 8 อาคารมหิตลาธิเบศร
- ให้แจ้งถึงที่ตั้งของสถานที่ปฏิบัติงานสำรอง (Disaster Recovery Site) และหมายเลขโทรศัพท์ติดต่อฉุกเฉิน 24 ชั่วโมง
  - **BCP-002** สบท. ยังไม่ได้กำหนดสถานที่

5.4 การจัดตั้งศูนย์สั่งการ และ DR Site

จะต้องมีการจัดเตรียมอุปกรณ์และเอกสารต่างๆ ที่จำเป็นไว้ที่ศูนย์สั่งการและ DR Site เพื่อให้สามารถประชุมและสั่งการได้เมื่อเกิดเหตุการณ์ภัยพิบัติ โดยจะต้องจัดเตรียมสิ่งต่างๆ ดังต่อไปนี้

รายการเอกสารที่จะต้องจัดเตรียมไว้ที่ศูนย์สั่งการและ DR Site

ลำดับ	รายการ	จำนวน	จัดเตรียมโดย
1	แผนบริหารความต่อเนื่องการดำเนินงาน	1	IT BCM Coordinator
2	รายชื่อและหมายเลขโทรศัพท์ติดต่อเจ้าหน้าที่ที่เกี่ยวข้องและผู้รับบริการ	1	IT BCM Coordinator
3	คู่มือการตั้งค่าเครื่องปั่นไฟฟ้าสำรอง	1	IT BCM Coordinator
4	คู่มือการตั้งค่าอุปกรณ์เครือข่าย	1	IT BCM Coordinator
5	เอกสารประกันภัย (ถ้ามี)	-	-

รายชื่อบุคคล/ส่วนงานที่จะต้องถือครองเอกสารแผนบริหารความต่อเนื่องการดำเนินงาน (Business Continuity Management Plan) ประกอบด้วย

ลำดับ	รายชื่อ/ ส่วนงาน	จัดเตรียมโดย
1	IT BCM Steering Committees	IT BCM Coordinator
2	IT BCM Coordinator	IT BCM Coordinator
3	Service Recovery Team	IT BCM Coordinator

จัดเตรียมเอกสารและข้อมูลที่สำคัญโดยทำสำเนาและจัดเก็บไว้ ณ สถานที่ปฏิบัติงานสำรอง รวมถึงรายชื่อบุคคล/ ส่วนงานที่จะต้องถือครองเอกสารแผนบริหารความต่อเนื่องการดำเนินงาน และจะต้องตรวจสอบให้เอกสารดังกล่าวเป็นเอกสารฉบับปัจจุบันเสมอ หรืออย่างน้อยทุก 1 ปี

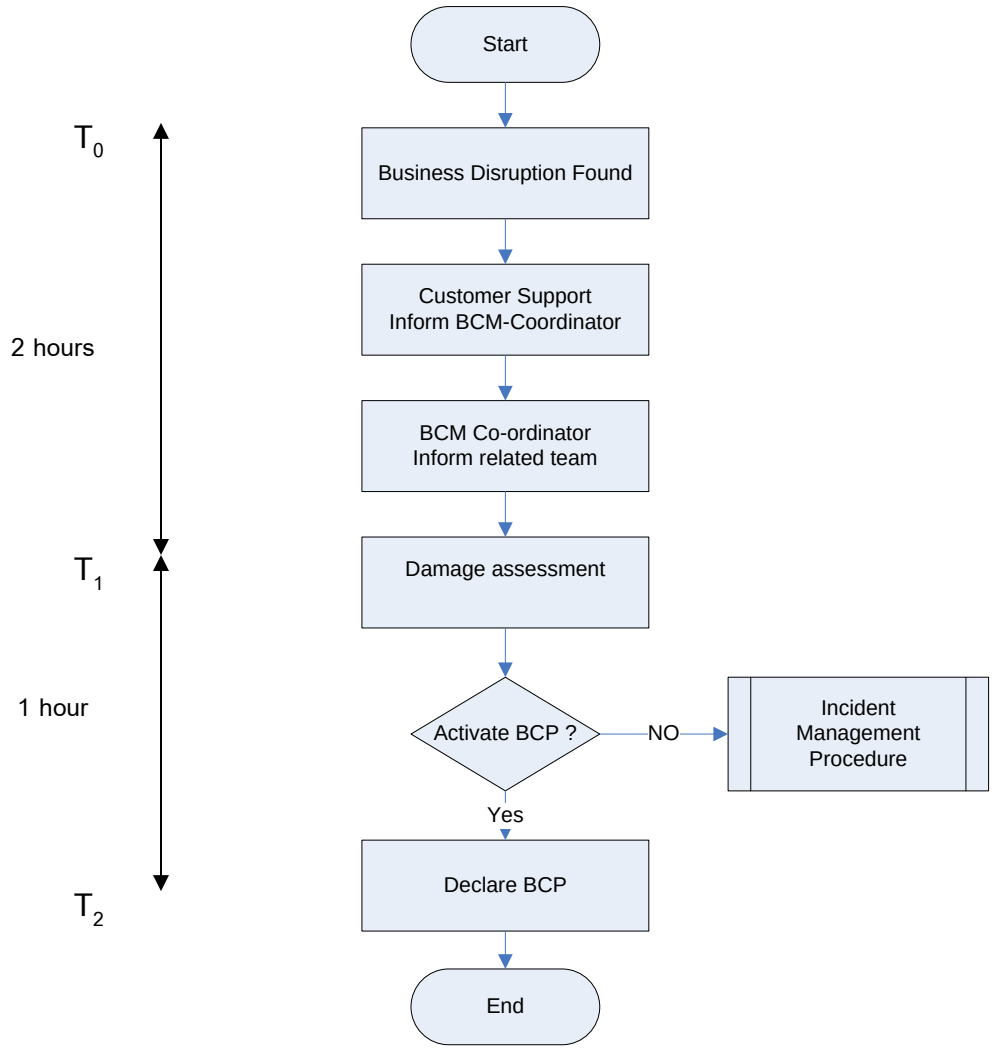
<u>อุปกรณ์อื่นๆ ที่ต้องจัดเตรียมเพื่อใช้งานที่ศูนย์สั่งการ</u>

ลำดับ	รายการ	จำนวน	จัดเตรียมโดย
1	Printer	1	ฝ่ายสนับสนุน
2	Power Extension Cord	3	ฝ่ายสนับสนุน
3	Projector	1	ฝ่ายสนับสนุน
4	White Board	1	ฝ่ายสนับสนุน
5	Wireless Access Point	1	ฝ่ายสนับสนุน
6	PC Notebook	1	ฝ่ายสนับสนุน
7	สาย Console (RS 232)	1	ฝ่ายสนับสนุน
8	สาย Ethernet	1	ฝ่ายสนับสนุน

อุปกรณ์สนับสนุนดังแสดงในตารางข้างต้นให้จัดเตรียมไปที่ศูนย์สั่งการและ DR Site ภายหลังจากเกิดเหตุการณ์ภัยพิบัติ

6. การรับมือกับเหตุการณ์ภัยพิบัติ

6.1 การจัดการเหตุการณ์และการประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงาน BCM



ISO 22301 : Business Continuity Management System

เมื่อพบเหตุการณ์ภัยพิบัติให้แจ้ง Customer Support (ฝ่ายบริการเทคโนโลยีสารสนเทศของ สบท. โทร. 02-218-3314) ซึ่งฝ่ายบริการฯ จะแจ้ง IT BCM Coordinator (T_0) เพื่อให้เข้ามาประเมินความเสียหายที่เกิดขึ้น

IT BCM Coordinator ติดต่อผู้ที่เกี่ยวข้องดังต่อไปนี้

- แจ้งคณะกรรมการ IT BCM Steering Committee อย่างน้อย 1 ท่าน ภายใน 2 ชั่วโมง เพื่อให้เข้ามาร่วมประเมินความเสียหายที่เกิดขึ้น
- แจ้งทีมกู้คืนระบบให้เข้าร่วมประเมินความเสียหาย
- คณะกรรมการ IT BCM Steering Committee ต้องทำการประเมินเพื่อดำเนินการตาม BCP หรือ Incident Management ภายใน 1 ชั่วโมง
- แจ้งสถานที่ประชุมแก่คณะกรรมการ IT BCM Steering Committee และทีมกู้คืนระบบ

คณะกรรมการ IT BCM Steering Committee และ IT BCM Coordinator จะต้องมาถึงสถานที่เกิดเหตุภายใน 2 ชั่วโมง (T_1) จากนั้นคณะกรรมการดังกล่าวจะร่วมกันทำการประเมินสถานการณ์ความเสียหาย โดยจะต้องดำเนินการให้แล้วเสร็จภายใน 1 ชั่วโมง (T_2) โดยใช้เกณฑ์ดังต่อไปนี้ในการพิจารณาความเสียหายที่พบ

ความรุนแรง (Severity)	**เกณฑ์การพิจารณา (Criteria)**
4	■ ทุกระบบใช้ไม่ได้เลย และทางกายภาพของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศเสียหาย หรือไม่สามารถให้บริการได้ ■ ไม่สามารถปฏิบัติงานได้
3	■ ทุกระบบใช้ไม่ได้เลย แต่ทางกายภาพของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศไม่เสียหาย ■ ไม่สามารถปฏิบัติงานได้
2	■ ระบบยังพอใช้งานได้ หรือสามารถแก้ไขได้ใน SLA ตาม Incident Management
1	■ ไม่มีผลต่อการใช้งานระบบ และสามารถแก้ไขได้ใน SLA ตาม Incident Management

หากพบว่ามีระดับความรุนแรงอยู่ที่ระดับ 3-4 ให้พิจารณาประกาศใช้แผนบริหารจัดการความต่อเนื่อง โดย ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศเป็นผู้ประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงาน (T_2)

จากนั้น IT BCM Coordinator แจ้งรายละเอียดให้ผู้ที่เกี่ยวข้องทราบ ดังต่อไปนี้

a. สถานะของเหตุการณ์ภัยพิบัติที่เกิดขึ้น
b. สิ่งที่ต้องดำเนินการ หรือการเตรียมพร้อมจนกว่าจะได้รับการติดต่อเพื่อแจ้งให้ทราบถึงขั้นตอนที่ต้องดำเนินการต่อไป หรือ
c. ไปรายงานตัวที่.....(สถานที่).....และ.....(เวลา)..... โดยนำบัตรประจำตัวและบัตรผ่านต่างๆ ไปด้วย

6.2 การติดต่อผู้ที่เกี่ยวข้อง

เมื่อมีการประกาศใช้แผนบริหารความต่อเนื่องการดำเนินงานแล้ว ให้ IT BCM Coordinator ติดต่อฝ่ายต่างๆที่เกี่ยวข้อง ดังนี้

- IT BCM Steering Committee ที่เหลือ
- ทีมกู้คืนระบบ
- ฝ่ายสนับสนุนและแจ้งข่าวสารงานสารสนเทศ

6.2.1 จัดทำรายชื่อและหมายเลขโทรศัพท์ติดต่อ IT BCM Steering Committee

	รายชื่อ	**หมายเลขโทรศัพท์ติดต่อ**
รักษาการแทนผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ	ผศ. บุญชัย โสวรรณวณิชกุล	081-035-7788
ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	นายวีรเดช เพ็งกระจ่าง	089-202-9057
ผู้อำนวยการฝ่ายระบบเทคโนโลยีสารสนเทศ	นายรุ่งโรจน์ กิตติถาวรกุล	081-849-7838
ผู้อำนวยการฝ่ายบริการเทคโนโลยีสารสนเทศ	นายเลิศพงษ์ เลิศไพศาลวงศ์	081-303-2788
ผู้อำนวยการสำนักงานการทะเบียน	รศ. วัลภา ประกอบผล	081-643-4614
ผู้อำนวยการศูนย์นวัตกรรมการเรียนรู้	นางประไพพิศ มงคลรัตน์	088-809-6590
ผู้อำนวยการสำนักบริหารระบบกายภาพ (สบภ.)	รศ.ดร.วีระศักดิ์ ลิขิตเรืองศิลป์	085-136-5655

6.2.2 จัดรายชื่อและหมายเลขโทรศัพท์ติดต่อทีมกู้คืนระบบ (Service Recovery Team Contacts)

	รายชื่อ	**หมายเลขโทรศัพท์ติดต่อ**
ทีมงานของฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	นางสาวปณิตา บุญมา นายจรูญ เดชากุล นายบุญชัย โชติไพบูลย์พันธุ์	081-535-7727 089-476-5826 089-478-4141
ทีมงานของฝ่ายระบบเทคโนโลยีสารสนเทศ	นางชุติมา ตั้งใจขจร นายชัยวัฒน์ มิ่งขวัญสกุล นางสาวจินตนา เสริมพณิชกุล	081-927-9193 085-088-3008 081-424-6278
ทีมงานของฝ่ายบริการเทคโนโลยีสารสนเทศ	นายประสิทธิ์ หาญเสน่ห์ลักษณ์ นายณัฐชัย พิสุทธิวงษ์ นายนิเวศ พรวรรณะศิริเวช	089-696-3070 086-984-8291 081-889-3816
ทีมงานของสำนักบริหารระบบกายภาพ (สบภ.)	นายวิเชียร เจริญไชย คุณบังอร เรือนจันทร์ทึก (ผู้จัดการอาคารจามจุรี 9)	088-193-8199 081-644-3993
ทีมงานของศูนย์การจัดการทรัพยากรของมหาวิทยาลัย	นายพิศาล คำณูนธรรม นายณัฐพล คุ้มครอง นางสาววรรณิสา ทำไร่ นายอัฐพงษ์ สว่างวรรณากร นายกิตติพงษ์ พงษ์กิตติหล้า นางสาววิมลทรา มาหา นางสาวณัฐารัตน์ วงศ์ธนากาญจน์ นางสาวสไวรินท์ ทิพย์คง นางสาวอัมพร กิตติรุจิระพันธ์ นางสาวอรววรรณ ธัญตระกูล	087-912-3285 086-661-6840 081-444-9839 089-114-9991 086-700-0927 085-061-0234 081-890-8840 081-654-5425 087-553-9889 089-119-9359

	รายชื่อ	หมายเลขโทรศัพท์ติดต่อ
ทีมงานของสำนักงานการทะเบียน	คุณสุเมธ สุขศรี เจ้าหน้าที่วิเคราะห์ (ระบบคอมพิวเตอร์)	085-087-1217
	คุณทรงพล สามกษัตริย์ เจ้าหน้าที่วิเคราะห์ (ระบบคอมพิวเตอร์)	081-412-3926
	คุณกิตติพงษ์ คำเคน เจ้าหน้าที่บริการการศึกษา (คอมพิวเตอร์)	083-433-7979
	คุณธงชัย สุภานิชย์ พนักงานคอมพิวเตอร์	081-612-2446
ทีมงานของศูนย์นวัตกรรมการเรียนรู้	นายชัยวัฒน์ มิ่งขวัญสกุล (ตัวแทน)	085-088-3008

6.2.3 จัดทำรายชื่อและหมายเลขโทรศัพท์ติดต่อฝ่ายสนับสนุนและแจ้งข่าวสารงานด้านสารสนเทศ

	รายชื่อ	หมายเลขโทรศัพท์ติดต่อ
ทีมงานของฝ่ายบริการเทคโนโลยีสารสนเทศ	นายประสิทธิ์ หาญเสน่ห์ลักษณ์	089-696-3070
	นายณัฐชัย พิสุทธิวงษ์	086-984-8291
	นายมานะ ชมวงษ์	086-991-4358

6.2.4 จัดทำรายชื่อและหมายเลขโทรศัพท์ติดต่อบุคคลากรของผู้ให้บริการ Data Center (DR site)

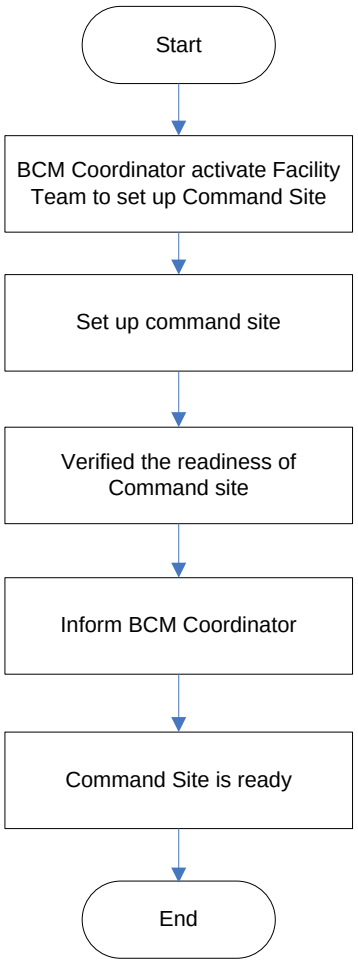
	รายชื่อ	**หมายเลขโทรศัพท์ติดต่อ**

6.2.5 จัดทำรายชื่อและหมายเลขโทรศัพท์ติดต่อพนักงานที่เกี่ยวข้อง (Internal Key Person)

	รายชื่อ	**หมายเลขโทรศัพท์ติดต่อ**
ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	นายวีรเดช เพ็งกระจ่าง	089-202-9057
ผู้อำนวยการฝ่ายระบบเทคโนโลยีสารสนเทศ	นายรุ่งโรจน์ กิตติถาวรกุล	081-849-7838
ผู้อำนวยการฝ่ายบริการเทคโนโลยีสารสนเทศ	นายเลิศพงษ์ เลิศไพศาลวงศ์	081-303-2788
ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศสำนักงานการทะเบียน	นายชูศักดิ์ คงมณี	081-575-2555
ผู้อำนวยการสำนักการจัดการทรัพยากรของมหาวิทยาลัย	นายวิโรจน์ เฉลิมเวโรจน์	081-310-1436

7. การจัดเตรียมสถานที่

7.1 การจัดตั้งศูนย์สั่งการ



Adapted from ISO 22301 : Business Continuity Management System

7.1.1 เมื่อมีการประกาศเหตุการณ์ภัยพิบัติและจำเป็นจะต้องมีการเตรียมสถานที่สำหรับศูนย์สั่งการ ให้ IT BCM Coordinator แจ้งฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและฝ่ายบริการเทคโนโลยีสารสนเทศให้เดินทางไปยังสถานที่ตั้งของศูนย์สั่งการ ภายใน 2 ชั่วโมง

7.1.2 ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศประสานงานเพื่อจัดเตรียมสถานที่และระบบสาธารณูปโภคอื่นๆ ให้พร้อมสำหรับการดำเนินงาน เช่น ระบบน้ำ ระบบไฟ ระบบปรับอากาศ โดยจะต้องจัดเตรียมให้เสร็จภายใน 1 ชั่วโมงนับจากที่เดินทางไปถึงสถานที่

7.1.3 ฝ่ายบริการเทคโนโลยีสารสนเทศตรวจสอบความพร้อมของสถานที่เพื่อใช้ในการปฏิบัติงาน เช่น อาหาร เครื่องดื่ม อุปกรณ์สำหรับการประชุม เป็นต้น โดยจะต้องจัดเตรียมให้เสร็จภายใน 1 ชั่วโมงนับจากที่เดินทางไปถึงสถานที่

7.1.4 ฝ่ายบริการเทคโนโลยีสารสนเทศแจ้งให้ IT BCM Coordinator ทราบ

7.2 การแจ้งข่าวเกี่ยวกับระบบสารสนเทศ

ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศจะเป็นผู้เตรียมข้อมูลและมอบหมายการแจ้งข้อมูลที่จะสื่อสารกันในระหว่างเกิดเหตุการณ์ภัยพิบัติ

7.3 การประกันภัย

ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศจะมอบหมายผู้ประสานงานเกี่ยวกับการประกันภัย โดยจะต้องติดต่อกับผู้ที่เกี่ยวข้องและฝ่ายกฎหมาย เพื่อดำเนินการเกี่ยวกับการขอรับประกันภัย

8. สถานการณ์และขั้นตอนการกู้คืนระบบ

8.1 เวลาที่ใช้ในการตอบสนองและกำลังคนที่ต้องการ

เวลาสูงสุดในการตอบสนองเมื่อได้รับแจ้งประกาศใช้แผน BCP และกำลังคนขั้นต่ำที่ต้องการในเวลาปกติและเวลาที่เกิดวิกฤติการณ์ แสดงไว้ในตารางด้านล่างนี้

ทีมกู้คืนระบบ	เวลาที่ใช้ในการตอบสนอง (Response Time)	จำนวนคนที่ต้องการใช้ในเวลาปกติ	จำนวนคนที่ต้องการใช้ในเวลาเกิดวิกฤติการณ์
ทีมงานฝ่ายโครงสร้างพื้นฐานและฝ่ายระบบเทคโนโลยีสารสนเทศ (สบท.)	4 - 6 ชม.	5 คน	3 คน
System Team			
- ERP	4 ชม.	23 คน	10 คน
- ระบบงานการทะเบียน	2 - 5 ชม.	7 คน	3 คน
- LMS	24 ชม.	1 คน	1 คน
Facility Team (สบภ.)	1 ชม.	2 คน	2 คน

8.1.1 กลยุทธ์ในการกู้คืนในแต่ละระบบ

หน่วยงาน	ระบบ	BCP	รายละเอียด
สำนักบริหารเทคโนโลยีสารสนเทศ	1.ระบบโครงสร้างพื้นฐานที่สำคัญของ (สบท.)		
	1.1 ระบบ DNS	BCP01, BCP02	สร้างระบบสำรองที่ Cloud/Co-location ข้างนอก ทำงานแบบ Master-Slave
	1.2 ระบบ LDAP & AD & RADIUS		
	-ระบบ AD	BCP01, BCP02	ระบบเป็นแบบ Active-Active (Multi Master)
	-ระบบ LDAP	BCP01	ระบบหลักอยู่ที่อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่อาคารมหิตลาธิเบศร ชั้น 8 ทำงานแบบ Active-Standby โดยต้องมีเจ้าหน้าช่วยในการเปิดระบบสำรอง
		BCP02	ระบบหลักอยู่ที่อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่ Cloud/Co-location ทำงานแบบ Active-Active แบบอัตโนมัติ
	-ระบบ RADIUS	BCP01	ระบบหลักอยู่ที่อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่อาคารมหิตลาธิเบศร ชั้น 8 ทำงานแบบ Active-Active แบบอัตโนมัติ
	-ระบบ RADIUS	BCP02	ระบบหลักอยู่ที่อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่ Cloud/Co-location ทำงานแบบ Active-Active แบบอัตโนมัติ

หน่วยงาน	ระบบ	BCP	รายละเอียด
	1.3 ระบบ VM	BCP01	ระบบหลักอยู่ที่อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่อาคารมหิตลาธิเบศร ชั้น 8 ทำงานแบบ Active-Standby อัตโนมัติ
		BCP02	ระบบหลักอยู่ที่อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่อาคารมหิตลาธิเบศร ชั้น 8 ทำงานแบบ Active Standby ต้องอาศัยเจ้าหน้าที่ไปเซ็ตค่าต่างๆ ในระบบ เพื่อเปิดระบบสำรอง
ศูนย์การจัดการทรัพยากรของมหาวิทยาลัย	2. ระบบการจัดการทรัพยากรของมหาวิทยาลัย (CU-ERP)	BCP01	ระบบอยู่ที่ห้อง Data Center อาคารจามจุรี 9 ชั้น 4 และห้อง Data Center อาคารมหิตลาธิเบศร ชั้น 8 มีระบบสำรองแบบ Active-Standby ระหว่างสองอาคาร โดยต้องมีเจ้าหน้าที่ช่วยในการเปิดระบบสำรอง
		BCP02	ระบบสำรองบน DR Site จะเป็นแบบ Active-Standby โดยต้องมีเจ้าหน้าที่ช่วยในการเปิดระบบสำรอง
สำนักบริหารกิจการนิสิต	3.ระบบบริหารจัดการข้อมูลทะเบียนนิสิต (CU-SAA)	BCP01	ระบบหลักอยู่ที่ห้อง Data Center อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่ห้อง Data Center อาคารมหิตลาธิเบศร ชั้น 8 ทำงานแบบ Active-Standby โดยต้องมีเจ้าหน้าที่ช่วยในการเปิดระบบสำรอง
		BCP02	ระบบหลักอยู่ที่ห้อง Data Center อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่ห้อง Data Center ภายนอกจุฬาฯ ทำงานแบบ Active-Standby โดยต้องมีเจ้าหน้าที่ช่วยในการเปิดระบบสำรอง

หน่วยงาน	ระบบ	BCP	รายละเอียด
ศูนย์นวัตกรรมการเรียนรู้	4.ระบบจัดการเรียนการสอน (LMS)		
	-ระบบ Blackboard	BCP01	ระบบหลักอยู่ที่อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่อาคารมหิตลาธิเบศร ชั้น 8 ระบบจะทำงานแบบ Active – Active แบบ share load
	-ระบบ Echo	BCP01	ระบบหลักอยู่ที่ อาคารจามจุรี 9 ชั้น 4 ระบบสำรองอยู่ที่ อาคารมหิตลาธิเบศร ชั้น 8 ทำงานแบบ Active-Stanby เปิดระบบสำรองโดยต้องมีเจ้าหน้าที่ช่วยในการเปิดระบบสำรอง

9. แผนการจัดการความต่อเนื่องการดำเนินงาน

9.1 แผนการจัดการความต่อเนื่องการดำเนินงาน - BCP-001

Description of Scenario: BCP-001			
บุคลากรไม่สามารถให้บริการหรือปฏิบัติงานได้ และ/หรือ ระบบงานหลักเสียหาย แต่ยังสามารถใช้ระบบงานสำรองที่ Data Center ในอาคารมหิตลาธิเบศร			
สมมติฐาน			
มี Generator พร้อมน้ำมันสำรองสำหรับการใช้งาน 24-48 ชม. และสามารถจัดหาเชื้อเพลิงได้ และมีการติดตั้ง Server ของระบบงานสำรองไว้ที่ Data Center ในอาคารมหิตลาธิเบศร			
เป้าหมายในการกู้คืน (Target Recovery Time)			
5 ชม. (T_2+2)			
การจัดเตรียม / รายการสิ่งของที่ต้องการในช่วง Pre-Crisis			
• คู่มือการตั้งค่าเครื่องปั่นไฟฟ้าสำรอง • ปริมาณน้ำมันในเครื่องปั่นไฟ (Generator) มีเพียงพอต่อการให้บริการต่อเนื่องไม่น้อยกว่า 10 ชม. • ผู้ที่เกี่ยวข้องสามารถเข้า ออกห้องไฟฟ้ากำลัง (Power House) ได้			
Resumption & Recovery Procedure			
Time (hr)	**Crisis Activation Procedure**	**Remarks / Doc Ref**	**Action By**
T_2 + 1.0	เจ้าหน้าที่ Facility Admin และเจ้าหน้าที่ที่เกี่ยวข้องเดินทางมาถึงสถานที่ ห้องทำงาน และห้อง Data Center ชั้น 8 อาคารมหิตลาธิเบศร		IT BCM Coordinator
T_2 + 1.5	ตรวจสอบการทำงานของเครื่องปั่นไฟ (Generator) สำหรับห้อง Data Center ในอาคารมหิตลาธิเบศร	ปฏิบัติตามคู่มือการตั้งค่าเครื่องปั่นไฟฟ้าสำรอง	สำนักบริหารระบบกายภาพ (สบภ.)
T_2 + 2.0	แจ้งรถน้ำมันให้เตรียมพร้อมเพื่อเข้ามาเตรียมพร้อม Standby		สำนักบริหารระบบกายภาพ (สบภ.)

Resumption & Recovery Procedure			
Time (hr)	**Crisis Activation Procedure**	**Remarks / Doc Ref**	**Action By**
T_2 + 1.5	ตรวจสอบระบบปรับอากาศ (Air Conditioning) ในห้องกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย (Server Farm)		สำนักบริหารระบบกายภาพ (สบภ.)
T_2 + 2.0	ตรวจสอบระบบไฟและอุณหภูมิภายในห้องกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย Server	ประสานกับสำนักบริหารระบบกายภาพ (สบภ.)	ฝ่ายบริการเทคโนโลยีสารสนเทศ
T_2 + 4.0	รถน้ำมันเข้ามาเตรียมพร้อม standby		สำนักบริหารระบบกายภาพ (สบภ.)

การกลับเข้าสู่กระบวนการทำงานปกติ

1. เมื่อการไฟฟ้าจ่ายไฟได้ตามปกติ เป็นระยะเวลา 15 นาที
   1.1 ตรวจสอบการสลับแหล่งจ่ายไฟของเครื่องปั่นไฟ (Generator) ให้กลับสู่แหล่งจ่ายไฟหลัก
   1.2 ตรวจการหยุดทำงานของเครื่องปั่นไฟ Generator
2. ตรวจสอบระบบปรับอากาศ (Air Conditioning) ในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ site สำรอง
3. ตรวจสอบระบบไฟและอุณหภูมิภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ site สำรอง
4. ตรวจสอบความเสียหายของ Main Site
5. ทำการฟื้นฟูระบบและอุปกรณ์ของ Main Site
6. ตรวจสอบความพร้อมของระบบสารสนเทศของ Main Site
7. ทดสอบการให้บริการระบบสารสนเทศที่ Main Site
8. กลับมาให้บริการจาก Main Site

บุคลากรและนิสิต

1. บุคลากรที่ไม่เกี่ยวข้องในแผน ให้ทำงานผ่าน online จากภายนอกมหาวิทยาลัยได้
2. บุคลากรที่ไม่สามารถเชื่อมต่อ internet เนื่องจากไม่มี Wi-Fi ให้ใช้จากภายนอกมหาวิทยาลัยหรือที่บ้าน ให้จัดหาและใช้งานผ่าน 3G USB Modem
3. สำหรับอาจารย์ผู้สอนและนิสิต ให้ใช้การเรียนการสอนผ่านระบบ LMS จากภายนอกมหาวิทยาลัย

9.2 แผนการจัดการความต่อเนื่องทางธุรกิจ- BCP-002

Description of Scenario: BCP-002
บุคลากรไม่สามารถให้บริการหรือปฏิบัติงานได้ เนื่องจากศูนย์ข้อมูล (Data Center) ทั้ง 2 แห่งในจุฬาลงกรณ์มหาวิทยาลัยเสียหายทั้งหมด หรือโครงข่ายการเชื่อมต่อหลักของมหาวิทยาลัยได้รับความเสียหาย หรือ ไม่สามารถให้บริการได้เนื่องจากไฟดับรวมถึงไฟสำรองหยุดจ่ายเป็นเวลานานกว่า 1 ชม.
Assumptions
1. มีพื้นที่สำรอง (DR site) ที่อยู่ภายนอกมหาวิทยาลัย 2. มีการเช่าอุปกรณ์ระบบเครือข่ายที่มีประสิทธิภาพใกล้เคียงหรือเทียบเท่าอุปกรณ์ของ Main Site
Target Recovery Time
8 ชม. (T_2+5)
Preparation / Items Request During Pre-Crisis
1. มีห้องทำงานของหน่วยงานด้านสารสนเทศของระบบสำคัญๆ 2. มีอุปกรณ์ระบบเครือข่ายสำรองที่ DR Site 3. มีระบบควบคุมการเข้าถึงพื้นที่ใน DR Site 4. คู่มือการตั้งค่าอุปกรณ์เครือข่าย 5. บัตรเข้าออกพื้นที่

Resumption & Recovery Procedure

Time (hr)	Crisis Activation Procedure	Remarks / Doc Ref	Action By
T_2+ 2.0	แจ้งเจ้าหน้าที่ที่เกี่ยวข้องและเจ้าหน้าที่ของหน่วยงานที่ดูแลระบบต่างๆ ถึงสถานที่ทำงานและการเตรียมการทำงานที่ DR site	รายชื่อบุคลากร	IT BCM Coordinator
T_2+2.0	เจ้าหน้าที่ฝ่ายบริการเทคโนโลยีสารสนเทศและเจ้าหน้าที่ที่เกี่ยวข้องเดินทางมาถึง DR Site		ฝ่ายบริการเทคโนโลยีสารสนเทศ

Resumption & Recovery Procedure			
Time (hr)	**Crisis Activation Procedure**	**Remarks / Doc Ref**	**Action By**
T_2 + 3.0	เจ้าหน้าที่จัดเตรียมความพร้อมของที่ทำงานและระบบสารสนเทศที่ DR Site		ฝ่ายบริการเทคโนโลยีสารสนเทศ
T_2 + 3.0	ตรวจสอบความพร้อมของระบบสาธารณูปโภค (ระบบไฟฟ้า, ระบบ Air Condition)		ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
T_2 + 3.0	ตั้งค่าอุปกรณ์ระบบเครือข่าย	คู่มือการตั้งค่าอุปกรณ์เครือข่าย	ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
T_2 + 4.0	ทดสอบการเชื่อมต่อระบบเครือข่ายและระบบงาน ERP และระบบงานการทะเบียน		ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ, เจ้าหน้าที่ระบบงาน ERP และเจ้าหน้าที่ระบบงานการทะเบียน
T_2 + 5.0	แจ้งบุคลากรให้ทราบถึงการให้บริการจาก DR Site	รายชื่อบุคคลากรที่เกี่ยวข้อง	ฝ่ายบริการเทคโนโลยีสารสนเทศ

การกลับเข้าสู่กระบวนการทำงานปกติ

1. ตรวจสอบความเสียหายของ Main Site
2. ทำการฟื้นฟูระบบและอุปกรณ์ของ Main Site
3. ตรวจสอบความพร้อมของระบบสารสนเทศของ Main Site
4. ทดสอบการให้บริการระบบสารสนเทศที่ Main Site
5. กลับมาให้บริการจาก Main Site

บุคลากรและนิสิต

1. ให้บุคลากรที่มีรายชื่อดังต่อไปนี้ กลับเข้าทำงานตามปกติ

   1.1 บุคลากรของสำนักบริหารเทคโนโลยีสารสนเทศ

   1.2 บุคลากรของสำนักงานการทะเบียน

   1.3 บุคลากรของศูนย์การจัดการทรัพยากรของมหาวิทยาลัย

   1.4 คณะผู้บริหารมหาวิทยาลัย

   1.5 บุคคลอื่นๆ ที่เกี่ยวข้อง

2. อาจารย์ผู้สอนและนิสิตให้รอการกู้คืน Main Site (อาคารจามจุรี 9) หรือ ศูนย์สำรองที่ Data Center ในอาคารมหิตลาธิเบศร และใช้การเรียนการสอนผ่านระบบ LMS