จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University
Pillar of the Kingdom

แผนแม่บทความปลอดภัย
ด้านเทคโนโลยีสารสนเทศของจุฬาลงกรณ์มหาวิทยาลัย
(CU IT Security Master Plan)

แผนแม่บทความปลอดภัย
ด้านเทคโนโลยีสารสนเทศของจุฬาลงกรณ์มหาวิทยาลัย
(CU IT Security Master Plan)

ฉบับที่ 1 ปี 2557-2559

สำนักบริหารเทคโนโลยีสารสนเทศ

เวอร์ชั่นที่ 2.2
วันที่ทบทวน วันที่ 26 พฤษภาคม 2558
เริ่มประกาศใช้เอกสารแผนแม่บทความปลอดภัยด้านสารสนเทศ วันที่ 2 พฤศจิกายน 2558

คำนำ

จุฬาลงกรณ์มหาวิทยาลัยได้จัดทำแผนแม่บทความปลอดภัยด้านเทคโนโลยีสารสนเทศของจุฬาลงกรณ์มหาวิทยาลัย (CU IT Security Master Plan) ฉบับที่ 1 ปี 2557-2559 ซึ่งได้มาจากการศึกษาวิเคราะห์สถานภาพปัจจุบันด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และแผนยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศของจุฬาลงกรณ์มหาวิทยาลัย ฉบับปี 2556 - 2559 ในยุทธศาสตร์นี้มุ่งเน้นการบริหารการกำกับดูแลที่ดี (IT Governance) และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามแนวทางของพระราชบัญญัติว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล (ISO/IEC 27001) เพื่อเป็นกรอบแนวทางในการกำหนดวิสัยทัศน์ พันธกิจ วัตถุประสงค์ เป้าหมายและแผนงานที่มีความเหมาะสมและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้แก่มหาวิทยาลัย รวมทั้งเป็นการยกระดับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยให้ได้ตามมาตรฐานสากลโดยมีวัตถุประสงค์ เพื่อให้ใช้เป็นกรอบในการจัดทำแผนงานด้านความมั่นคงปลอดภัยสารสนเทศ

สารบัญ

หน้า

บทที่ 1 บททั่วไป

1.1 เป้าหมาย

จุฬาลงกรณ์มหาวิทยาลัยมีเป้าหมายมุ่งสู่การเป็นมหาวิทยาลัยยุคดิจิตอล (Digital University) โดยให้บริการด้านเทคโนโลยีสารสนเทศที่ทันสมัยเพื่อจะสนับสนุนงานด้านการเรียน การสอน งานวิจัย การบริการวิชาการและงานบริหารด้านต่างๆ ของมหาวิทยาลัย

1.2 พันธกิจด้านเทคโนโลยีสารสนเทศ

1) สร้างโครงสร้างพื้นฐานเพื่อสนับสนุนการสร้างนวัตกรรมในการเรียนรู้ การวิจัย การบริการวิชาการและการบริหารจัดการเพื่อก้าวไปสู่การเป็นมหาวิทยาลัยแห่งชาติในระดับโลก (World Class National University)

2) พัฒนาระบบบริการเทคโนโลยีสารสนเทศให้ตอบสนองผู้ใช้งาน

3) ปรับปรุงระบบบริหารจัดการเทคโนโลยีสารสนเทศของมหาวิทยาลัยให้สามารถตอบสนองความต้องการอย่างมีประสิทธิผลและประสิทธิภาพ

4) ปรับปรุงกระบวนการทำงานและเชื่อมโยงระบบสารสนเทศที่สำคัญของมหาวิทยาลัยเข้าด้วยกัน เพื่อส่งเสริมการใช้สารสนเทศในการตัดสินใจและการสร้างองค์ความรู้

5) ปรับปรุงโครงสร้างพื้นฐานให้พร้อมรองรับการใช้งานระบบสารสนเทศ ทั้งในด้านเสถียรภาพ คุณภาพและความหลากหลายในการเข้าถึง

ยุทธศาสตร์ทั้ง 6 ด้านขององค์กร ปี 2556-2559

แผนแม่บทเทคโนโลยีสารสนเทศ ฉบับปี พ.ศ. 2556-2559 ได้กำหนดยุทธศาสตร์ไว้ 6 ด้าน ดังรูป

ภาพที่ 1 ยุทธศาสตร์งาน IT เพื่อสนับสนุนภารกิจงาน 6 ด้านของมหาวิทยาลัย

หนึ่งในยุทธศาสตร์คือยุทธศาสตร์ด้านการกำกับดูแลที่ดีและมีนโยบายการใช้งานเครือข่ายคอมพิวเตอร์และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เนื่องจากในปัจจุบันความก้าวหน้าด้านเทคโนโลยีมีความรวดเร็วมากและเทคโนโลยีสารสนเทศถูกนำมาใช้อย่างกว้างขวางในกิจกรรมต่างๆ นำมาซึ่งความเสี่ยงต่อการเกิดอาชญากรรมทางคอมพิวเตอร์ เช่น การโจรกรรมหรือดัดแปลงข้อมูล การแพร่ไวรัสคอมพิวเตอร์ การบุกรุกโจมตีเครือข่าย จึงมีความจำเป็นอย่างยิ่งที่จะต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และควรมีแผนแม่บทการรักษาความปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายสำหรับส่วนกลาง ส่วนงานต่างๆ ตลอดจนผู้ใช้งานระบบและเครือข่ายทั่วไป เพื่อให้การดำเนินการดังกล่าวมีกระบวนการขั้นตอนอย่างเป็นระบบ จึงได้มีการจัดทำแผนแม่บทความปลอดภัยด้านเทคโนโลยีสารสนเทศของจุฬาลงกรณ์มหาวิทยาลัยขึ้น (CU IT Security Master Plan)

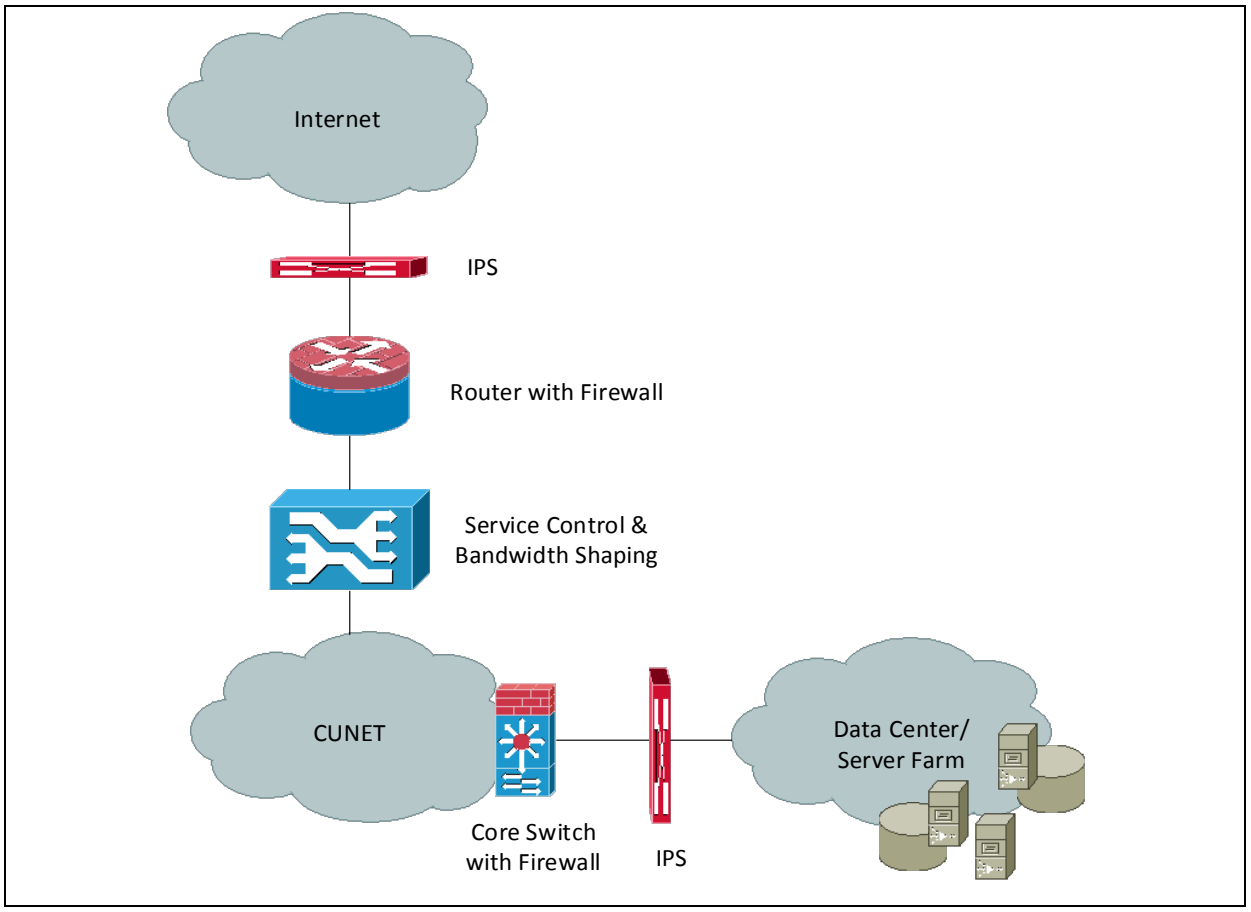
บทที่ 2 การวิเคราะห์สถานภาพความปลอดภัยด้านเทคโนโลยีสารสนเทศในปัจจุบัน

<u>บทวิเคราะห์สภาพแวดล้อมภายในและภายนอก</u>

ปัจจุบันสำนักบริหารเทคโนโลยีสารสนเทศมีการดำเนินการในส่วนการรักษาความปลอดภัย แบ่งเป็น 6 ส่วน ได้แก่

1. การรักษาความปลอดภัยระบบเครือข่ายหลักของมหาวิทยาลัย ณ Gateway และอุปกรณ์เครือข่ายหลัก ดำเนินการโดย
   1.1 ติดตั้งระบบ Firewall ณ Gateway ของมหาวิทยาลัยเพื่อป้องกันการบุกรุก โจมตีระบบเครือข่ายและระบบคอมพิวเตอร์จากภายนอกมหาวิทยาลัย
   1.2 ติดตั้งระบบ IPS (Intrusion Prevention System) ณ Gateway ของมหาวิทยาลัยเพื่อป้องกันการโจมตีในระดับ service จากภายนอก รวมทั้งป้องกันการใช้ระบบคอมพิวเตอร์ของมหาวิทยาลัยเป็นฐานในการโจมตีผู้อื่น
   1.3 ติดตั้งระบบ Bandwidth Shaping ณ Gateway ของมหาวิทยาลัยเพื่อจัดความสำคัญและควบคุมปริมาณการใช้งานบริการต่างๆ ผ่านระบบเครือข่าย
   1.4 สร้าง Access Control List เพื่อควบคุมบริการที่มีความเสี่ยงหรืออาจถูกใช้เป็นเครื่องมือในการโจมตีระบบคอมพิวเตอร์ ณ จุดเชื่อมต่อระหว่างอุปกรณ์หลักของมหาวิทยาลัยไปยังคณะ และหน่วยงานต่างๆ

โครงสร้างการรักษาความปลอดภัยระบบเครือข่ายหลักของมหาวิทยาลัย แสดงดังในภาพที่ 2

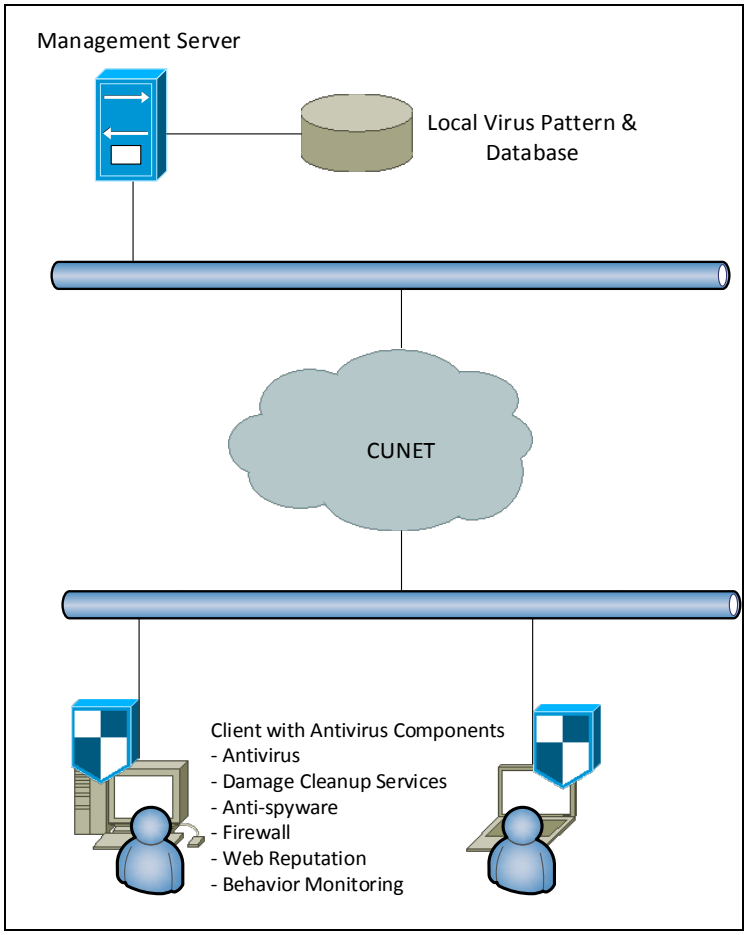


ภาพที่ 2 โครงสร้างการรักษาความปลอดภัยระบบเครือข่ายหลักของมหาวิทยาลัย

2. การรักษาความปลอดภัยระบบเครื่องแม่ข่าย และระบบงานให้บริการต่างๆ
   2.1 ติดตั้งระบบ Firewall ป้องกันระบบเครือข่าย สำหรับเครื่องแม่ข่ายระบบงานต่างๆ
   2.2 ติดตั้งระบบ IPS ระหว่างอุปกรณ์เครือข่ายหลักไปยัง ห้อง Data Center เพื่อป้องกันการโจมตีบุกรุก เครื่องแม่ข่ายระบบงานต่างๆ
   2.3 ติดตั้งระบบ Antivirus บนเครื่องแม่ข่ายระบบ File sharing เพื่อป้องกันและจัดการ malware หรือ virus ที่แอบแฝงมากับแฟ้มข้อมูลใช้งานรูปแบบต่างๆ
   2.4 ติดตั้งระบบ VPN เพื่อเพิ่มระดับความปลอดภัยและจำกัดการเข้าถึงระบบงานสำคัญของมหาวิทยาลัย อาทิ ระบบ ERP
   2.5 ติดตั้งระบบ Mail Gateway เพื่อตรวจจับและกำจัดไวรัส ที่ติดมากับ e-mail รวมทั้งกรอง e-mail ที่ส่งมาจากแหล่งที่เป็นอันตรายและ e-mail ขยะที่ส่งมาจากแหล่งต่างๆ

3. การรักษาความปลอดภัยระดับบุคคล
   3.1 จัดหาระบบ Enterprise Antivirus เพื่อให้ ส่วนงาน/คณะ/หน่วยงาน/ผู้ใช้ นำไปติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่าย เพื่อป้องกัน malware หรือ virus ที่สามารถแพร่กระจายผ่านแฟ้มข้อมูลและระบบเครือข่าย ดังแสดงในภาพที่ 3 ระบบ Enterprise Antivirus ของมหาวิทยาลัย

3.2 จัดหาซอฟต์แวร์ถูกต้องตามลิขสิทธิ์ อาทิ ระบบปฏิบัติการ Microsoft Windows, Microsoft Office, SPSS (Statistical Package for the Social Sciences) เป็นต้น เพื่อป้องกันการนำซอฟต์แวร์ละเมิดลิขสิทธิ์ที่มี malware หรือ virus แฝงมาแพร่กระจายในมหาวิทยาลัย



ภาพที่ 3 ระบบ Enterprise Antivirus ของมหาวิทยาลัย

4. การรักษาความปลอดภัยระดับกายภาพ
   4.1 ติดตั้งระบบ CCTV เพื่อเฝ้าระวังและบันทึกเหตุการณ์ ต่างๆ ณ ห้อง Data Center
   4.2 ติดตั้งระบบ Access Control เพื่อควบคุมและจำกัดสิทธิ การเข้าถึงระบบเครื่องแม่ข่าย ณ ห้อง Data Center
   4.3 ควบคุมการเข้าถึงอุปกรณ์เครือข่ายที่ติดตั้งอยู่ ณ อาคารต่างๆ โดยติดตั้งอยู่ในตู้อุปกรณ์ที่สามารถปิดล็อคได้
5. การปฏิบัติตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2555
   5.1 จัดหาระบบ Log Server กลาง เพื่อเก็บข้อมูลการใช้งาน (log) ของระบบต่างๆ ตาม พรบ.
   5.2 จัดทำระบบระบุและแสดงตัวตนของผู้ใช้งาน เพื่อให้ผู้ใช้งานแสดงตนก่อนเข้าใช้งานระบบเครือข่ายสู่ภายนอกมหาวิทยาลัย

6. การประสานงานและให้คำแนะนำการแก้ไขปัญหา

6.1 ประสานงานไปยังคณะหรือหน่วยงานกรณีได้รับแจ้งเหตุผิดปกติของการใช้งานระบบเครือข่ายและระบบเครื่องแม่ข่าย อาทิ การถูกใช้เป็นฐานไปโจมตีผู้อื่น โดยให้คำแนะนำและร่วมมือในการแก้ไขปัญหา

บทวิเคราะห์สภาพแวดล้อมภายในและภายนอกของระบบเครือข่ายสารสนเทศ (SWOT Analysis)

จุดแข็ง (Strengths)

- ได้รับการสนับสนุนการดำเนินการและงบประมาณจากมหาวิทยาลัย
- มีคณาจารย์ผู้ทรงคุณวุฒิและบุคลากรภายในมหาวิทยาลัยที่มีความรู้ความเชี่ยวชาญ
- เริ่มมีการลงทุนระบบและเครื่องมือในส่วนของ IT Security
- มีการบริหารจัดการระบบเทคโนโลยีสารสนเทศแบบกระจายศูนย์ ทำให้สามารถพัฒนาและจัดทำ IT Security ให้เหมาะสมกับศาสตร์และลักษณะของแต่ละหน่วยงานได้
- มีสมาชิกเครือข่ายวิชาชีพเพื่อแลกเปลี่ยนเรียนรู้ด้านเทคโนโลยีสารสนเทศ และให้ความช่วยเหลือกัน

จุดอ่อน (Weaknesses)

- ยังไม่มีนโยบายที่ชัดเจนในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงมาตรฐานขั้นตอน ปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งของผู้ใช้งาน บริการด้านเทคโนโลยีสารสนเทศ และบุคลากรผู้ให้บริการ
- ขาดกระบวนการทำงานที่มีประสิทธิภาพของบุคลากรกับอุปกรณ์และ solution ด้าน IT Security ที่ได้ลงทุนไป เช่น การ set up IPS ในระดับ service, การ monitor แบบ day to day ของ IPS, network monitoring, web gateway, mail gateway รวมทั้งขาดการดูแลอย่างสม่ำเสมอของเครื่องคอมพิวเตอร์ส่วนบุคคล เช่น การ update patch หรือ firmware ของโปรแกรมต่างๆ รวมถึง Antivirus software เป็นต้น และขาดการจัดทำ report อย่างสม่ำเสมอจากอุปกรณ์เหล่านี้เพื่อการป้องกันและแก้ไขปัญหา
- ไม่มีแผนงานการตรวจสอบช่องโหว่ด้านความปลอดภัยเทคโนโลยีสารสนเทศเป็นประจำ
- ยังไม่มีการดำเนินงานด้านการรักษาความปลอดภัยของข้อมูลสารสนเทศตามความสำคัญของระบบงานในแต่ละระดับ เช่น การมีระบบ Backup Site มีการซ้อมปฏิบัติการแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง BCP (Business Continuity Plan) และมีแผนเตรียมรับสถานการณ์ฉุกเฉินด้านความปลอดภัยสารสนเทศ (Disaster Recovery Plan) เป็นประจำทุกปี

- ขาดบุคลากรส่วนกลางที่รับผิดชอบดูแลด้านงานความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยตรง เพื่อแนะนำแก้ไขปัญหาในภาพรวมของมหาวิทยาลัยและเผยแพร่ข่าวสารความปลอดภัยด้านเทคโนโลยีสารสนเทศให้บุคลากรทราบ

- ขาดการประสานงานด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพระหว่างหน่วยงานในแต่ละระบบงาน ทำให้การบริหารจัดการและการดูแลงาน Security ยังไม่ทั่วถึง

- ขาดการให้และเผยแพร่ความรู้แก่บุคลากรเรื่องความปลอดภัย ด้านเทคโนโลยีสารสนเทศ เช่น เว็บไซต์และเว็บบอร์ดที่ให้ข้อมูลทางความปลอดภัยด้านเทคโนโลยีสารสนเทศ ฝึกอบรมความรู้ด้าน Security และสัมมนาให้แก่บุคลากร

โอกาส (Opportunities)

- มีกฎหมายด้านเทคโนโลยีสารสนเทศเพิ่มมากขึ้น และกำหนดบทลงโทษไว้อย่างชัดเจน เช่น พรบ. ว่า ด้วยการกระทำผิดทางคอมพิวเตอร์ ส่งผลให้มหาวิทยาลัยต้องให้ความสำคัญกับประเด็นดังกล่าวมากขึ้น

- เทคโนโลยีสารสนเทศ มีการพัฒนาอย่างรวดเร็ว ทำให้มีเทคโนโลยีใหม่ๆ ซึ่งมีการผนวกความสามารถความปลอดภัยด้านเทคโนโลยีสารสนเทศเพิ่มเข้ามา ทำให้สามารถเลือกใช้เทคโนโลยีใหม่เหล่านี้มาปิดช่องโหว่เดิมได้

- มีหน่วยงานของภาครัฐและเอกชน เป็นแหล่งข้อมูลข่าวสารความปลอดภัยด้านเทคโนโลยีสารสนเทศ ส่งเสริมการเผยแพร่ข่าวสารด้าน ICT Security

- มีมาตรฐานด้านการรักษาความปลอดภัยตามมาตรฐานสากล เช่น ISO/IEC 27001 เพื่อให้มหาวิทยาลัยนำมาใช้เป็นแนวทางปฏิบัติได้

อุปสรรค (Threats)

- ภัยคุกคามและอาชญากรรมทางด้าน IT เพิ่มขึ้น รวมทั้งมีความซ้ำซ้อนและหลากหลายขึ้นทำให้มหาวิทยาลัยมีแนวโน้มจะถูกโจมตีสูงขึ้น

- เทคโนโลยีความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงอย่างรวดเร็ว ส่งผลต่อการปรับตัวของมหาวิทยาลัยและทำให้มหาวิทยาลัยต้องใช้งบประมาณในการปรับเปลี่ยนอุปกรณ์และพัฒนาบุคลากรมากขึ้นเมื่อคำนึงถึงความปลอดภัยของข้อมูลและระบบการให้บริการของมหาวิทยาลัย

- บุคลากรที่มีความเชี่ยวชาญด้านความปลอดภัยมีจำนวนน้อย

- มีกฎหมายด้านเทคโนโลยีสารสนเทศเพิ่มมากขึ้น และกำหนดบทลงโทษไว้อย่างชัดเจน เช่น พรบ. ว่า ด้วยการกระทำผิดทางคอมพิวเตอร์ ก่อให้เกิดความเสี่ยงต่อมหาวิทยาลัยมากขึ้นต่อการกระทำผิดกฎหมาย เนื่องจากผู้ใช้บริการในมหาวิทยาลัยมีความหลากหลาย

<u>ผลการวิเคราะห์สภาพแวดล้อมภายในและภายนอก</u>

กลยุทธ์ไปข้างหน้า

- การที่มีกฎหมายด้านเทคโนโลยีสารสนเทศและบทลงโทษที่ชัดเจน ทำให้สามารถวางนโยบายด้านความปลอดภัยเทคโนโลยีสารสนเทศและนำไปสู่การปฏิบัติได้มากขึ้นสะดวกขึ้น ตามมาตรฐานและกรอบของกฎหมาย

- การมีมาตรฐานสากล เช่น ISO/IEC 27001 ทำให้ผู้บริหารเห็นความสำคัญของการควบคุมและดูแลความปลอดภัยระบบสารสนเทศ และเพิ่มประสิทธิภาพการบริหารจัดการงานด้านความปลอดภัย

- การมีแหล่งความรู้จากภายนอกและมาตรฐานสากล ทำให้บุคลากรด้าน IT Security มีโอกาสศึกษาหาความรู้และนำความรู้มาประยุกต์ใช้งานและเผยแพร่ได้มากขึ้น รวมถึงสามารถติดตามเรียนรู้ระบบและเครื่องมือในการบริหารความปลอดภัยที่ดีด้วยเทคโนโลยีใหม่ๆ

- กำหนดทีมงานและกระบวนการทำงานกับระบบคอยเฝ้าระวัง เพื่อรับผิดชอบดูแลและประสานงานด้าน IT Security และเตือนภัยแก่บุคลากรรวมทั้งการบริหารจัดการระบบและอุปกรณ์ด้านความปลอดภัยให้มีประสิทธิภาพ

- วางนโยบาย มาตรฐานและขั้นตอนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยที่ชัดเจน จะช่วยลดผลกระทบจากการเปลี่ยนแปลงของเทคโนโลยีที่ส่งผลให้มหาวิทยาลัยต้องใช้งบประมาณในการจัดซื้ออุปกรณ์เพื่อป้องกันระบบ

- วางมาตรการควบคุมการใช้งานทรัพยากรทางด้านเทคโนโลยีสารสนเทศให้มีความปลอดภัยและมีประสิทธิภาพ เพื่อลดภัยคุกคามและอาชญากรรมคอมพิวเตอร์ใหม่ๆที่เกิดขึ้น

- เพิ่มจำนวนบุคลากรที่ปฏิบัติงานด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

บทที่ 3 เป้าหมายและยุทธศาสตร์ความปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.1 วิสัยทัศน์ความปลอดภัยด้านเทคโนโลยีสารสนเทศ

มุ่งมั่นพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยสำหรับการให้บริการด้านเทคโนโลยีสารสนเทศในงานด้านต่างๆของมหาวิทยาลัย พร้อมทั้งปลูกจิตสำนึกการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศให้บุคลากรภายในปี 2559

3.2 พันธกิจความปลอดภัยด้านเทคโนโลยีสารสนเทศ

1) รักษาความมั่นคงปลอดภัยระบบสารสนเทศของมหาวิทยาลัย

2) ปลูกจิตสำนึกให้ผู้ใช้งานตระหนักถึงการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

3) สร้างกระบวนการและมาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ

4) สร้างความร่วมมือระหว่างส่วนงานและคณะต่างๆ ทั่วทั้งมหาวิทยาลัยให้ปฏิบัติตามระเบียบและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย

3.3 เป้าหมายโดยรวมของความปลอดภัยด้านเทคโนโลยีสารสนเทศ

1) มีการบริหารจัดการด้านความปลอดภัยเทคโนโลยีสารสนเทศที่ดีตามแนวมาตรฐาน

2) มีระบบเครือข่ายที่มีเสถียรภาพและปลอดภัย

3) พัฒนาความรู้ความสามารถด้านความปลอดภัยเทคโนโลยีสารสนเทศของบุคลากร

3.4 ยุทธศาสตร์ความปลอดภัย ด้านเทคโนโลยีสารสนเทศ

ยุทธศาสตร์ที่ 1 ยกระดับกระบวนการทำงานด้านการรักษาความปลอดภัยให้เป็นไปตามมาตรฐาน

<u>เป้าหมายของยุทธศาสตร์ที่ 1</u>

กำหนดให้มีนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้ง 10 ด้าน โดยการจัดทำเอกสารชุดนโยบายด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เพื่อช่วยให้ผู้ปฏิบัติงานทราบถึงนโยบายและข้อปฏิบัติ เพื่อปกป้องระบบและข้อมูลที่มีความสำคัญต่อการดำเนินงาน ลดปัจจัยเสี่ยง รวมถึงเป็นการพัฒนาบุคลากรและนิสิตให้สามารถปฏิบัติงานและใช้งานได้สอดคล้องกับหลักการรักษาความปลอดภัยตามแนวทางและมาตรฐานสากลภายในปี 2559 โดยมีเอกสาร จำนวน 10 ฉบับ ประกอบด้วย

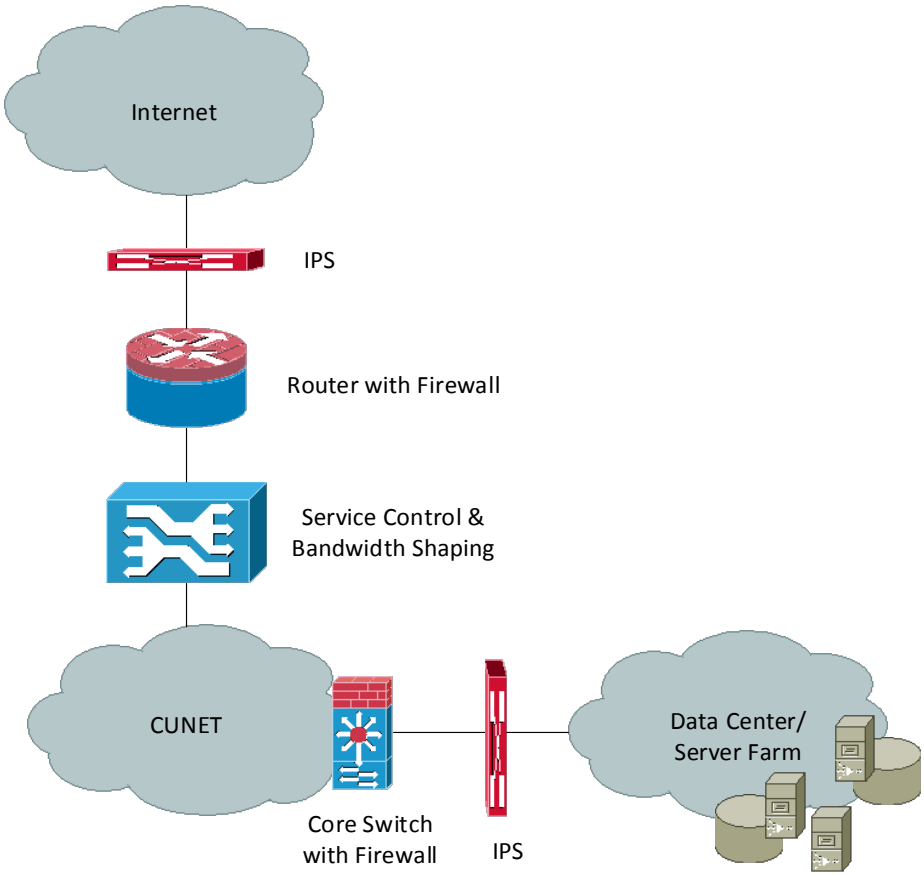
1. นโยบายความมั่นคงปลอดภัยด้านกายภาพ ครอบคลุมการรักษาความมั่นคงปลอดภัยทางกายภาพของห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ การควบคุมการเข้าออก การกำหนดสิทธิผู้ผ่านเข้าออกและความปลอดภัยทางกายภาพของเครือข่ายสื่อสัญญาณภายในมหาวิทยาลัย
2. นโยบายการจัดเตรียมระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมมาตรการและแนวปฏิบัติในการดำเนินการติดตั้งอุปกรณ์เครือข่ายและคอมพิวเตอร์ (Hardware) ระบบปฏิบัติการและระบบงานต่างๆ (Software) เพื่อเชื่อมต่อกับระบบสารสนเทศของมหาวิทยาลัย
3. นโยบายการจำแนกและการบริหารข้อมูล ครอบคลุมการกำหนดมาตรฐานในการจัดระดับชั้นความลับของข้อมูลและวิธีการจัดการข้อมูล เพื่อให้มีหลักปฏิบัติที่ใช้ในการจัดการกับข้อมูลอย่างถูกต้องเหมาะสม
4. นโยบายการสำรองข้อมูลและกู้คืน ครอบคลุมทั้งในคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคล เพื่อให้มีชุดข้อมูลสำรองกรณีเกิดความเสียหายกับข้อมูลและสามารถกู้กลับคืนมาได้อย่างมีประสิทธิภาพ
5. นโยบายการบริหารความเปลี่ยนแปลง ครอบคลุมการบริหารความเปลี่ยนแปลงในระดับการปรับปรุง (Patch/Upgrade) และระดับการเปลี่ยนแปลง (Change) ระบบงานหรือระบบปฏิบัติการ เพื่อให้มีข้อปฏิบัติก่อนดำเนินการเปลี่ยนแปลงเพื่อลดความเสี่ยงในการหยุดให้บริการ
6. นโยบายการบริหารระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมการบริหารระบบเครือข่ายทั้งระบบข้อกำหนดเกี่ยวกับ การจัดการไอพีแอดเดรส การเข้าถึงระบบจากระยะไกล การตรวจสอบระบบการซ่อมบำรุง และการดำเนินการเมื่อระบบขัดข้อง
7. นโยบายการเข้าถึงข้อมูลและระบบสารสนเทศ ครอบคลุมการบริหารบัญชีรายชื่อผู้ใช้งานระบบการกำหนดรหัสผ่าน การกำหนดสิทธิเฉพาะผู้ที่ได้รับอนุญาต
8. นโยบายการใช้อุปกรณ์ไอทีส่วนบุคคล ครอบคลุมการใช้งานคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพาและ สมาร์ทโฟน (Notebook, Tablet, Mobile computing and IT gadgets) โดยกำหนดแนวทางการใช้งาน ข้อกำหนดที่ผู้ใช้งานต้องดำเนินการ เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส
9. นโยบายการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ ครอบคลุมสิ่งที่ผู้ใช้เครือข่ายคอมพิวเตอร์ต้องปฏิบัติตาม
10. นโยบายการดำเนินงานต่อเนื่อง Business Continuity Plan (BCP) และรับเหตุการณ์ฉุกเฉิน (Disaster)

ยุทธศาสตร์ที่ 2 เพิ่มประสิทธิภาพความปลอดภัยระบบสารสนเทศของมหาวิทยาลัย

<u>เป้าหมายของยุทธศาสตร์ที่ 2</u>

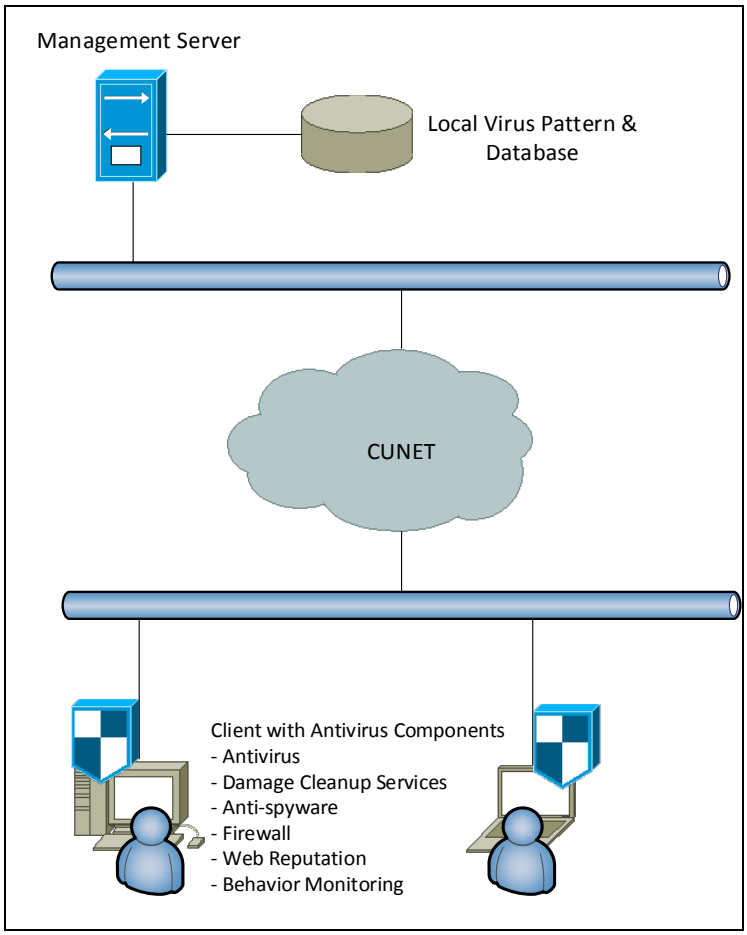
สร้างเกราะป้องกันการโจมตีระบบคอมพิวเตอร์ เพื่อเพิ่มประสิทธิภาพความปลอดภัยของระบบสารสนเทศของมหาวิทยาลัยภายในปี 2559 โดย

1. มีการปรับปรุง เปลี่ยนแปลงหรือเพิ่มเติมอุปกรณ์ด้าน IT Security เข้าไปในระบบสารสนเทศของมหาวิทยาลัย



ภาพที่ 4 โครงสร้างการรักษาความปลอดภัยระบบเครือข่ายหลักของมหาวิทยาลัย

2. มีการปรับปรุง เปลี่ยนแปลงหรือเพิ่มเติม Software Antivirus (Campus License) เข้ากับเครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัย



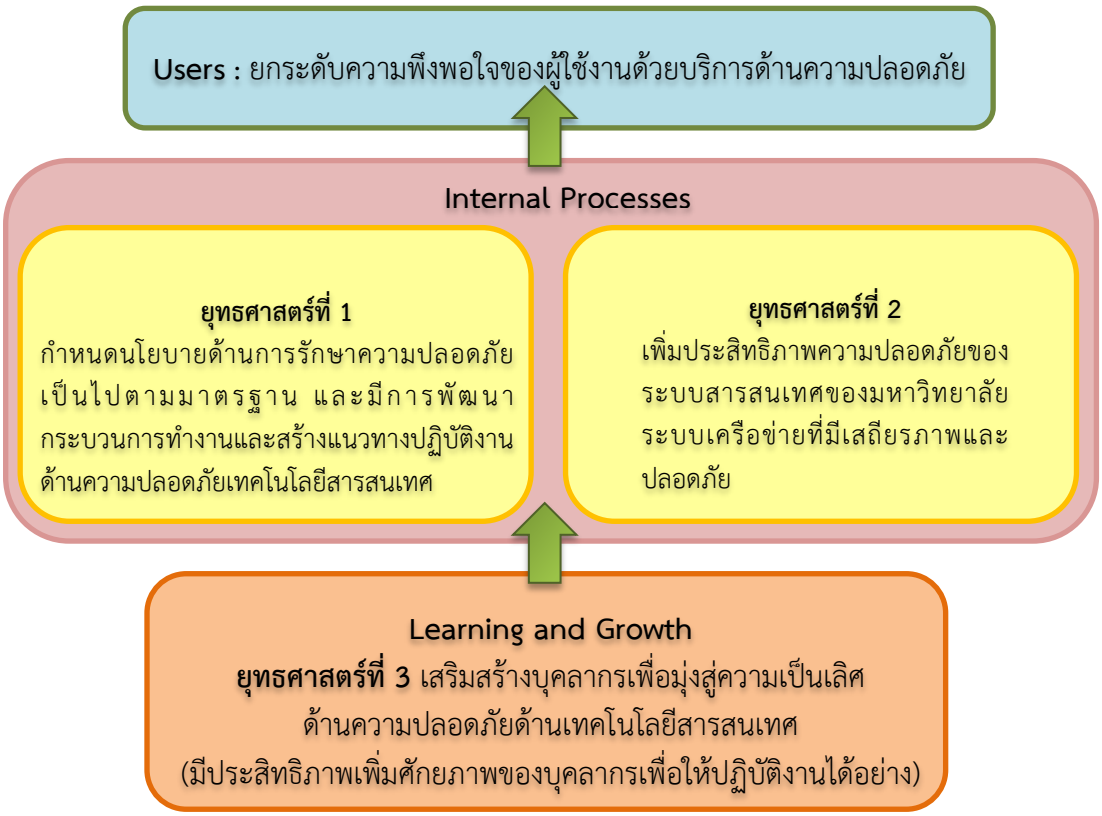
ภาพที่ 5 ระบบ Enterprise Antivirus ของมหาวิทยาลัย

ยุทธศาสตร์ที่ 3 เสริมสร้างทักษะให้นิสิต และบุคลากรด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยง

<u>เป้าหมายของยุทธศาสตร์ที่ 3</u>

1. สร้างจิตสำนึกให้นิสิต และบุคลากรตระหนักถึงหน้าที่ที่ต้องปฏิบัติในเรื่องความปลอดภัยสารสนเทศ ภายในปี 2559 โดยจัดทำหลักสูตรการเรียน Online ด้าน IT Security
2. เพิ่มบุคลากรที่มีทักษะและความเชี่ยวชาญเฉพาะด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อพร้อมรับมือกับภัยคุกคามใหม่ๆอย่างมีประสิทธิภาพ ภายในปี 2559

<u>ความสัมพันธ์ของยุทธศาสตร์</u>



<u>เป้าหมายและแผนงานที่สามารถบรรลุยุทธศาสตร์</u>

ซึ่งได้จัดทำเป้าหมายและแผนงานขึ้นและมีการจัดลำดับความสำคัญของแผนงาน/โครงการ/การจัดกลุ่ม/ลำดับความสำคัญของแผนงาน/โครงการ โดยคำนึงถึงปัจจัยหลายอย่าง เช่น จำนวนบุคลากร เวลา งบประมาณ ประกอบการพิจารณาเป็นหลักเกณฑ์การแบ่งกลุ่มที่เหมาะสม เพื่อให้ทราบว่าแผนงาน/โครงการใดควรจะดำเนินการก่อนหรือหลังโดยมีหลักเกณฑ์ที่นำมาใช้ในการพิจารณาเพื่อจัดลำดับความสำคัญคือ วัตถุประสงค์ของแผนงาน แบ่งระดับได้ดังนี้

ระดับสูง (3) = การปฏิบัติตามนโยบายและข้อกำหนดด้านความปลอดภัย

ปานกลาง (2) = ลดความเสี่ยงที่อาจเกิดความเสียหายหรือกระทบการดำเนินงาน

ต่ำ (1) = เพิ่มประสิทธิภาพและสนับสนุนการปฏิบัติงานภายใน

แผนงาน/โครงการ

ยุทธศาสตร์ที่ 1 ยกระดับกระบวนการทำงานด้านรักษาความปลอดภัย ให้เป็นไปตามมาตราฐาน

แผนงาน/โครงการ	หน่วยงานที่เกี่ยวข้อง	ตัวชี้วัด	เป้าหมาย				ระยะเวลา		สาระสำคัญ
			2557	2558	2559	2560	เริ่ม	สิ้นสุด	
1.1 จัดทำ/ทบทวน/ปรับปรุง นโยบายและขั้นตอนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (3)	IT Steering Committee	จำนวนครั้งในการทบทวน/ปรับปรุงนโยบาย มาตรฐานและขั้นตอนปฏิบัติ	จัดทำแผนความมั่นคงปลอดภัยสารสนเทศและขั้นตอนปฏิบัติ	มีการทบทวน/ปรับปรุงมาตราฐานและขั้นตอนปฏิบัติอย่างน้อยปีละ1ครั้ง	มีการทบทวน/ปรับปรุงมาตราฐานและขั้นตอนปฏิบัติอย่างน้อยปีละ1ครั้ง	มีการทบทวน/ปรับปรุงมาตราฐานและขั้นตอนปฏิบัติอย่างน้อยปีละ1ครั้ง	2557	2560	มีนโยบาย มาตรฐานและขั้นตอนปฏิบัติที่เป็นมาตราฐานและทันกับสถานการณ์
1.2 การประเมินการรับรู้และปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (2)	บุคลากรและนิสิตของจุฬาลงกรณ์มหาวิทยาลัย	ระดับการรับรู้และการปฏิบัติตามนโยบายและข้อกำหนด	จัดทำแบบแผนประเมินการรับรู้นโยบายความมั่นคงปลอดภัยสารสนเทศ	มีบุคลากรและนิสิตรับรู้และปฏิบัติตามอย่างน้อย 40% ของกลุ่มตัวอย่าง	มีบุคลากรและนิสิตรับรู้และปฏิบัติตามอย่างน้อย 50% ของกลุ่มตัวอย่าง	มีบุคลากรและนิสิตรับรู้และปฏิบัติตามอย่างน้อย 75% ของกลุ่มตัวอย่าง	2557	2560	จัดกิจกรรมและหลักสูตรเผยแพร่นโยบาย IT Security และและจัดทำการประเมินผลการรับรู้และปฏิบัติตามนโยบายและขั้นตอนปฏิบัติการรักษาความปลอดภัยสารสนเทศ

ยุทธศาสตร์ที่ 2 เพิ่มประสิทธิภาพความปลอดภัยระบบสารสนเทศของจุฬาลงกรณ์มหาวิทยาลัย

แผนงาน/โครงการ	หน่วยงานที่เกี่ยวข้อง	ตัวชี้วัด	เป้าหมาย				ระยะเวลา		สาระสำคัญ
			2557	2558	2559	2560	เริ่ม	สิ้นสุด	
2.1 การประเมินระบบสารสนเทศ (2)	สบท. และหน่วยงานต่างๆ ของมหาวิทยาลัย	จำนวนระบบที่ได้รับการตรวจสอบความต้านทาน (Penetration Test)	-	ทำ Penetration Test 1 ระบบ	ทำ Penetration Test 1 ระบบ	ทำ Penetration Test 2 ระบบ	2557	2560	ประเมินระบบสารสนเทศเพื่อทดสอบความต้านทานของระบบต่อการถูกโจมตีผ่านช่องทางต่างๆ
2.2 แผนรองรับการดำเนินงานอย่างต่อเนื่อง (2)	สบท. และหน่วยงานต่างๆ ของมหาวิทยาลัย	จัดทำ/ปรับปรุงและซ้อมแผนการดำเนินงานงานอย่างต่อเนื่อง	มีการจัดทำแผนรองรับการดำเนินงานอย่างต่อเนื่อง BCP	ซ้อมตามแผนและปรับปรุงทบทวนอย่างน้อย ปีละ 1 ครั้ง	ซ้อมตามแผนและปรับปรุงทบทวนอย่างน้อย ปีละ 1 ครั้ง	ซ้อมตามแผนและปรับปรุงทบทวนอย่างน้อย ปีละ 1 ครั้ง	2557	2560	เป็นการเตรียมการรองรับเหตุการณ์ภัยพิบัติและเหตุไม่คาดคิด เพื่อลดผลกระทบและป้องกันความเสี่ยงที่อาจกระทบการดำเนินงาน และสามารถกู้คืนระบบได้ตามระยะเวลาที่กำหนด

แผนงาน/โครงการ	หน่วยงานที่เกี่ยวข้อง	ตัวชี้วัด	เป้าหมาย				ระยะเวลา		สาระสำคัญ
			2557	2558	2559	2560	เริ่ม	สิ้นสุด	
2.3 บริหารจัดการระบบ IPS, Firewall และ Mail Gateway ให้ทำงานอย่างมีประสิทธิภาพ (3)	สบท.	ระบบ IPS, Firewall และ Mail Gateway ทำงานอย่างมีประสิทธิภาพ	ระบบ IPS, Firewall และ Mail Gateway ให้ทำงานอย่างมีประสิทธิภาพอย่างน้อย 99% หมายเหตุ วิกฤตแต่ละครั้งแก้ไขไม่เกิน 24 ชั่วโมง	ระบบ IPS, Firewall และ Mail Gateway ให้ทำงานอย่างมีประสิทธิภาพอย่างน้อย 99% หมายเหตุ วิกฤตแต่ละครั้งแก้ไขไม่เกิน 24 ชั่วโมง	ระบบ IPS, Firewall และ Mail Gateway ให้ทำงานอย่างมีประสิทธิภาพอย่างน้อย 99% หมายเหตุ วิกฤตแต่ละครั้งแก้ไขไม่เกิน 24 ชั่วโมง	ระบบ IPS, Firewall และ Mail Gateway ให้ทำงานอย่างมีประสิทธิภาพอย่างน้อย 99% หมายเหตุ วิกฤตแต่ละครั้งแก้ไขไม่เกิน 24 ชั่วโมง	2557	2560	1. มีการทำ MA อย่างต่อเนื่อง 2. มีการทบทวนนโยบายการบริหารจัดการ 3. มีการปรับปรุงข้อมูลรูปแบบการโจมตีอย่างสม่ำเสมอ
2.4 ตรวจสอบและติดตั้ง Software Antivirus เครื่องลูกข่าย (3)	สบท. และหน่วยงานต่างๆ ของมหาวิทยาลัย	ร้อยละของเครื่องลูกข่ายที่ได้รับการปรับปรุงฐานข้อมูลอย่างสม่ำเสมอ	เครื่องลูกข่ายในส่วนกลางที่ติดตั้ง Antivirus ได้รับการ update อย่างน้อย 80%	เครื่องลูกข่ายทั้งจุฬาฯ ที่ติดตั้ง Antivirus ได้รับการ update อย่างน้อย 99%	เครื่องลูกข่ายทั้งจุฬาฯ ที่ติดตั้ง Antivirus ได้รับการ update อย่างน้อย 99%	เครื่องลูกข่ายทั้งจุฬาฯ ที่ติดตั้ง Antivirus ได้รับการ update อย่างน้อย 99%	2557	2560	ตรวจสอบ ติดตั้ง upgrade Antivirus ของเครื่องลูกข่าย และ upgrade เป็น Campus License
2.5 แผนติดตั้งระบบป้องกันของเครือข่ายและระบบงานต่างๆ (2)	สบท.	ร้อยละของระบบงานที่ได้รับการประเมินและมีการป้องกันรักษาความปลอดภัย	ตรวจสอบจำนวนระบบงานและความปลอดภัยของระบบงานว่ามีหรือไม่	ระบบงานที่ได้รับการประเมินและมีการป้องกันรักษาความปลอดภัยอย่างน้อย 90%	ระบบงานที่ได้รับการประเมินและมีการป้องกันรักษาความปลอดภัยอย่างน้อย 95%	ระบบงานที่ได้รับการประเมินและมีการป้องกันรักษาความปลอดภัยอย่างน้อย 100%	2557	2560	ระบบงานต่างๆ มีการป้องกันรักษาความปลอดภัยอย่างเหมาะสม

ยุทธศาสตร์ที่ 3 เสริมสร้างบุคลากรเพื่อมุ่งสู่ความเป็นเลิศความปลอดภัยด้านเทคโนโลยีสารสนเทศ

แผนงาน/โครงการ	หน่วยงานที่เกี่ยวข้อง	ตัวชี้วัด	เป้าหมาย				ระยะเวลา		สาระสำคัญ
			2557	2558	2559	2560	เริ่ม	สิ้นสุด	
3.1 โครงการสร้างจิตสำนึกแก่นิสิต (2)	สบท.	จำนวนนิสิตที่ได้รับ permanent password	จัดทำหลักสูตรด้าน IT Security online	จำนวนนิสิตที่ได้ permanent password 10,000 คน	จำนวนนิสิตที่ได้ permanent password 30,000 คน	จำนวนนิสิตที่ได้ permanent password 40,000 คน	2557	2560	สร้างหลักสูตร IT security online เพื่อให้นิสิตตระหนักถึงการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย
3.2 แผนฝึกอบรมด้าน IT Security (1)	สบท.	จำนวนบุคลากรจุฬาฯ เข้าร่วมอบรม IT Security online	จัดทำหลักสูตรด้าน IT Security online	มีบุคลากรจุฬาฯ เข้าร่วมอบรมอย่างน้อย 50%	มีบุคลากรจุฬาฯ เข้าร่วมอบรมอย่างน้อย 75%	มีบุคลากรจุฬาฯ เข้าร่วมอบรมอย่างน้อย 100%	2557	2560	สร้างหลักสูตร IT Security online เพื่อพัฒนาศักยภาพบุคลากรด้าน IT Security
		จำนวนบุคลากรด้านไอที เข้าอบรมเป็นผู้เชี่ยวชาญด้าน IT Security	มีผู้เชี่ยวชาญเพิ่มขึ้นปีละ 1 คน	มีผู้เชี่ยวชาญเพิ่มขึ้นปีละ 1 คน	มีผู้เชี่ยวชาญเพิ่มขึ้นปีละ 1 คน	มีผู้เชี่ยวชาญเพิ่มขึ้นปีละ 1 คน	2557	2560	เพิ่มจำนวนบุคลากรผู้เชี่ยวชาญด้าน IT Security ของจุฬาฯ

บทที่ 4 การบริหารจัดการและการติดตามประเมินผล

4.1 การจัดทำ/ปรับปรุงแผนแม่บทความปลอดภัย ด้านเทคโนโลยีสารสนเทศ

1) คณะกรรมการ IT Steering Committee มอบนโยบายและกรอบแนวทางการจัดทำ ปรับปรุง และอนุมัติแผนแม่บทความปลอดภัยด้านเทคโนโลยีสารสนเทศ

2) สำนักบริหารเทคโนโลยีสารสนเทศและหน่วยงานต่างๆ ที่เกี่ยวข้องมีหน้าที่นำนโยบาย ไปจัดทำข้อปฏิบัติด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

4.2 การติดตามประเมินผล

ให้มีการติดตามประเมินผลด้านความปลอดภัยเป็นประจำทุกเดือน โดยนำหลักการ PDCA (Plan, Do, Check, Act) มาใช้วางแผน ปฏิบัติตามแผน ตรวจสอบ และปรับปรุงแก้ไข โดยมีการนำเสนอผลการตรวจสอบ ปรับปรุงและแก้ไขระบบความปลอดภัยต่อคณะกรรมการ IT Steering Committee เป็นประจำทุกปี