Econ
คณะเศรษฐศาสตร์
มหาวิทยาลัยเชียงใหม่

คู่มือการปฏิบัติงาน

การแก้ไขปัญหาภัยคุกคามระบบความมั่นคงปลอดภัยไซเบอร์

สำหรับผู้ปฏิบัติงาน

แนวทางการรับมือและจัดการภัยคุกคาม
อย่างเป็นระบบ รวดเร็ว และมีประสิทธิภาพ
เพื่อความมั่นคงปลอดภัยขององค์กร

ตรวจจับเร็ว
เฝ้าระวังและตรวจจับภัยคุกคาม
ได้อย่างทันท่วงที

วิเคราะห์แม่นยำ
วิเคราะห์สาเหตุและประเมินผลกระทบ
อย่างเป็นระบบ

จัดการทันที
ตอบสนองและแก้ไขปัญหา
อย่างมีประสิทธิภาพ

ป้องกันยั่งยืน
เสริมความแข็งแกร่งและป้องกัน
ไม่ให้เกิดซ้ำ

สำหรับผู้ปฏิบัติงาน

กลุ่มภารกิจเทคโนโลยีดิจิทัล
และสื่อการเรียนรู้ (DTLM)

คำนำ

คู่มือการแก้ไขปัญหาภัยคุกคามระบบความมั่นคงปลอดภัยไซเบอร์ คณะเศรษฐศาสตร์ มหาวิทยาลัยเชียงใหม่ เล่มนี้จัดทำขึ้น เพื่อให้บุคลากรในกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้สามารถแก้ไขปัญหาภัยคุกคามฯ ได้อย่างถูกต้องและมีประสิทธิภาพ เนื้อหาภายในคู่มือครอบคลุมถึงแนวทางการป้องกันความเสียหายจากภัยพิบัติ ขั้นตอนปฏิบัติในมาตรการที่สำคัญข้อปฏิบัติในการแก้ไขปัญหา แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติและขั้นตอนการดำเนินการแก้ไขปัญหากรณีเกิดภัยคุกคามฯ เพื่อให้เกิดความสะดวกและความเป็นระบบในการดำเนินการแก้ไขกรณีเกิดปัญหาภัยคุกคามฯ ได้อย่างเหมาะสม

หวังเป็นอย่างยิ่งว่าคู่มือฉบับนี้จะช่วยให้บุคลากรในกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้สามารถดำเนินการตามคู่มือฯ ดังกล่าวได้อย่างถูกต้อง และเป็นระบบ หากมีข้อเสนอแนะใด ๆ ทางหน่วยงานยินดีรับฟังเพื่อนำไปพัฒนาปรับปรุงให้ดียิ่งขึ้น

ผู้จัดทำ

กลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้

มกราคม 2569

สารบัญ

หน้า

คำนำ

1. หลักการและเหตุผล 1
2. วัตถุประสงค์ 1
3. คำจำกัดความ 1
4. ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศ 2
5. แนวทางการป้องกันความเสียหายจากภัยพิบัติ 3
6. ขั้นตอนปฏิบัติในมาตรการที่สำคัญ 6
7. ข้อปฏิบัติในการแก้ไขปัญหา 6
8. วิธีการขั้นตอนการปฏิบัติงาน 7
9. ระยะเวลาที่ใช้ในการปฏิบัติงาน 8
10. กฎหมายที่เกี่ยวข้อง 8
11. รายชื่อกรรมการแผนกู้คืนระบบสารสนเทศ 9
12. รายชื่อบริษัทติดต่อภายนอก 9
13. รายชื่อบริษัทภายนอกที่เกี่ยวกับแผน 10
14. ข้อมูลเครื่องแม่ข่ายคอมพิวเตอร์คณะเศรษฐศาสตร์ 11
15. เครื่องแม่ข่ายคอมพิวเตอร์คณะเศรษฐศาสตร์ บน Private Cloud 13
16. ระบบเครือข่ายหลักของคณะเศรษฐศาสตร์ 14
17. เครื่องมือในการตรวจสอบระบบเครือข่ายและเครื่องแม่ข่าย (Network and Server Monitoring) 14
18. การตรวจสอบระบบเครือข่ายคอมพิวเตอร์ไร้สาย Jumboplus 16

คู่มือการแก้ปัญหาภัยคุกคามระบบความมั่นคงปลอดภัยไซเบอร์
สำหรับผู้ปฏิบัติงาน

1. หลักการและเหตุผล

ระบบเทคโนโลยีสารสนเทศของคณะฯ มีความสำคัญเป็นอย่างยิ่ง ในการวางแผนพัฒนาองค์กร บริหารจัดการองค์กร และการปฏิบัติงานของบุคลากรในคณะฯ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์ กลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้ได้ตระหนักถึงความสำคัญของระบบ ซึ่งอาจมีปัจจัยจากทั้งภายในและภายนอกมากระทบทำให้ระบบเทคโนโลยีสารสนเทศของรวมถึงระบบเครือข่ายคอมพิวเตอร์ เครื่องแม่ข่ายคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ เกิดความเสียหาย และไม่สามารถใช้งานได้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถแก้ไขปัญหาภัยคุกคามฯ ได้อย่างตรงจุด ผู้จัดทำจึงได้จัดทำคู่มือการแก้ปัญหาภัยคุกคามระบบความมั่นคงปลอดภัยไซเบอร์เพื่อใช้ประกอบในการปฏิบัติงานของบุคลากรในกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้

2. วัตถุประสงค์

1. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาความปลอดภัยไซเบอร์ของระบบเทคโนโลยีสารสนเทศของคณะฯ
2. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศของคณะฯ ให้มีเสถียรภาพและพร้อมสำหรับการใช้งาน
4. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขปัญหาได้อย่างทันท่วงที
5. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร

3. คำจำกัดความ

เพื่อให้เกิดความเข้าใจที่ถูกต้องและชัดเจนเกี่ยวกับคู่มือการแก้ปัญหาภัยคุกคามระบบความมั่นคงปลอดภัยไซเบอร์คณะเศรษฐศาสตร์ มหาวิทยาลัยเชียงใหม่ คู่มือฉบับนี้จึงกำหนดคำจำกัดความของคำสำคัญต่าง ๆ ดังต่อไปนี้

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ระบบคอมพิวเตอร์ทั้งฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้ระบบ พนักงานที่เกี่ยวข้อง และผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูล

เพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์และติดตามผลการดำเนินงานขององค์กร

“ระบบเครือข่ายหลัก” หมายถึง ระบบเครือข่ายในการส่งสัญญาณที่เป็นเส้นทางหลัก มีความเร็วสูง และมีความเสถียรต่อการส่งข้อมูล ทำให้การสูญเสียของสัญญาณที่วิ่งผ่านในระยะไกลมีน้อย และหากเกิดปัญหาในการส่ง ข้อมูลก็จะมีเส้นทางสำรองในการส่งข้อมูลไว้เรียบร้อย เครือข่ายหลักถือเป็นระบบโครงสร้างพื้นฐานที่สำคัญของทุกองค์กรตั้งแต่องค์กรขนาดเล็กไปจนถึงองค์กรขนาดใหญ่

“ภัยคุกคามระบบความมั่นคงปลอดภัยไซเบอร์” หมายถึง ภัยคุกคามที่มีผลทำให้ระบบของเครือข่ายและการสื่อสารขัดข้อง ไม่สามารถใช้งานระบบเครือข่ายและการสื่อสารได้ รวมทั้งการเข้าถึงอุปกรณ์เครือข่ายเพื่อปรับแต่ง และแก้ไขการทำงานโดยไม่ได้รับอนุญาต

“เครื่องคอมพิวเตอร์แม่ข่าย” หมายถึง เครื่องคอมพิวเตอร์ประมวลผลระดับสูงที่มีเสถียรภาพ ทั้งในด้านการบริหารจัดการหน่วยจัดเก็บข้อมูล หน่วยความจำ การเชื่อมต่อระบบเครือข่ายและการใช้พลังงานไฟฟ้า โดยการให้บริการระบบโปรแกรมประยุกต์ ระบบข้อมูลสารสนเทศและระบบฐานข้อมูลแก่ผู้ใช้งานผ่านเว็บไซต์หรือโปรแกรมคอมพิวเตอร์ลูกข่ายบนระบบเครือข่ายภายในและระบบเครือข่ายอินเทอร์เน็ต

“การสำรองข้อมูล” หมายถึง กระบวนการจัดเก็บข้อมูลของเครื่องคอมพิวเตอร์ทั้งระบบปฏิบัติการ ข้อมูลการตั้งค่าและข้อมูลอื่น ๆ โดยการคัดลอกข้อมูลของเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ในปัจจุบัน บนสื่อบันทึกข้อมูลภายนอกเครื่องคอมพิวเตอร์ เพื่อป้องกันข้อมูลเสียหาย และข้อมูลสูญหาย จากความตั้งใจ หรือความประมาทของผู้ใช้งาน รวมถึง การเกิดภัยพิบัติที่มีผลกระทบต่อเครื่องคอมพิวเตอร์ดังกล่าว

“การกู้คืนข้อมูล” หมายถึง กระบวนการแก้ไขปัญหาที่เกิดกับข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายจากสื่อบันทึกข้อมูลที่สำรองข้อมูลมูลสารสนเทศ

“ผู้ดูแลระบบ” หมายถึง บุคคลผู้ทำหน้าที่ดูแลและะจัดการระบบหรือเครือข่าคอมพิวเตอร์ โดยทั่วไปผู้ดูแลมักจะทำหน้าที่ติดตั้ง ตอบคำถาม ดูแลเซิร์ฟเวอร์ หรือระบบคอมพิวเตอร์อื่น รวมถึงการวางแผนงานการดูแล ควบคุมโครงการที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“ผู้ปฏิบัติงานตรวจสอบ” หมายถึง บุคคลหรือหน่วยงานที่มีหน้าที่ประเมินและตรวจสอบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ข้อมูล และการบริหารจัดการภายในองค์กร เพื่อให้มั่นใจว่ามาตรการที่ใช้อยู่นั้นมีประสิทธิภาพและสอดคล้องกับกฎหมายหรือมาตรฐานที่กำหนด

4. ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของคณะฯ สามารถจำแนกได้เป็นภัยพิบัติจากภายนอก และ ภัยพิบัติจากภายใน

4.1 ภัยพิบัติจากภายนอก

4.1.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของอุปกรณ์เครือข่ายหลัก และเครื่องแม่ข่ายคอมพิวเตอร์ของคณะฯ ได้แก่ อัคคีภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

4.1.2 การโจรกรรมอุปกรณ์คอมพิวเตอร์

4.1.3 ระบบสื่อสารหลักของคณะที่เชื่อมต่อกับระบบเครือข่ายหลักของมหาวิทยาลัยเกิดความขัดข้อง

4.1.4 ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

4.1.5 การบุกรุกหรือการโจมตีจากภายนอก เพื่อเข้าถึงเครื่องแม่ข่ายคอมพิวเตอร์หลักของคณะฯ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

4.1.6 ไวรัสคอมพิวเตอร์

4.2 ภัยพิบัติจากภายใน

4.2.1 เครื่องแม่ข่ายหลัก ที่จัดเก็บฐานข้อมูลเกิดเสียหาย หรือข้อมูลถูกทำลาย

4.2.2 ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในคณะฯ

4.2.3 เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ ทำให้ระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

5. แนวทางการป้องกันความเสียหายจากภัยพิบัติ

5.1 ภัยพิบัติจากภายนอก

5.1.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของอุปกรณ์เครือข่ายหลัก และเครื่องแม่ข่ายคอมพิวเตอร์ของคณะฯ ได้แก่ อัคคีภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

1. การป้องกันและการดำเนินการอัคคีภัย

(1.1) มีการอบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิง

(1.2) มีการติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์

(1.3) มีการจัดทำเครื่องหมายระบุความสำคัญตามลำดับอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุการณ์ฉุกเฉิน

2. การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม

(2.1) มีการเปิดเครื่องปรับอากาศ และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

5.1.2 การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เก็บข้อมูลหลักของคณะฯ

1. มีการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายที่เก็บข้อมูลของคณะฯ โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปยุ่งเกี่ยวกับอุปกรณ์ หากมีความจำเป็นให้มีเจ้าหน้าที่หน่วยเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบควบคุมดูแล

5.1.3 ระบบการสื่อสารหลักของหน่วยงาน ที่เชื่อมต่อกับระบบเครือข่ายนอกองค์กรเกิดความขัดข้อง

1. ทำการตรวจสอบระบบเครือข่ายทั้งภายใน (LAN, Wifi) และเครือข่ายภายนอก (Internet) ให้สามารถใช้งานได้ตลอดเวลา

2. ตรวจสอบ Network Traffic ของคณะได้จาก https://nms.econ.cmu.ac.th/cacti

5.1.4 ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

1. มีการติดตั้งเครื่องสำรองกระแสไฟฟ้า(UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลัก และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC)

2. ให้ผู้ใช้งานเปิดเครื่องสำรองกระแสไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองกระแสไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ ถ้ามีปัญหาการใช้งานให้แจ้งมายังกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้เพื่อดำเนินการให้สามารถใช้งานได้ตามปกติ

3. กรณีเมื่อเกิดไฟฟ้าดับ ให้ผู้ใช้งานบันทึกข้อมูลที่ยังค้างอยู่ทันที และทำการปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ

5.1.5 การบุกรุกหรือการโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

1. คณะฯ มีการติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินทราเน็ตและอินเทอร์เน็ต เข้าสู่ระบบเทคโนโลยีสารสนเทศขององค์กรได้ และสามารถทำงานอยู่ตลอดเวลา

2. คณะฯ มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดตอย่างสม่ำเสมอ และมี Dashboard สำหรับตรวจสอบ เฝ้าระวังเครื่องคอมพิวเตอร์ที่มีปัญหา

5.1.6 ไวรัสคอมพิวเตอร์

1. คณะฯ มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดตอย่างสม่ำเสมอ และมี Dashboard สำหรับตรวจสอบ เฝ้าระวังเครื่องคอมพิวเตอร์ที่มีปัญหา

2. ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ

(2.1) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(2.2) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

3. ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ระวังภัยจากการเปิดไฟล์จาก E-mail

(3.1) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

(3.2) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

4. ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต

(4.1) ไม่เปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่าง ๆ

(4.2) ไม่เปิดเว็บไซต์ที่แนบมาทาง E-mail

(4.3) ไม่ดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ

(4.4) หลีกเลี่ยงการแชร์ไฟล์

(4.5) ติดตามการแจ้งเตือนการโจมตีของไวรัสต่าง ๆ อย่างสม่ำเสมอ

5.2 ภัยพิบัติภายใน

5.2.1 เครื่องแม่ข่ายหลัก ที่จัดเก็บฐานข้อมูลเกิดเสียหาย หรือข้อมูลถูกทำลาย

1. ดำเนินการสำรองข้อมูลอัตโนมัติ ทุกวัน โดยสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ดำเนินการสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน สามารถเรียกกู้ข้อมูลย้อนหลังได้อย่างน้อย 7 วัน

2. ดำเนินการสำรองฐานข้อมูลโดยอัตโนมัติอีกชุดหนึ่ง สำรองไว้บน NAS ของคณะทุกวัน

3. ทดสอบการกู้คืน เครื่องแม่ข่ายหลัก เพื่อทดสอบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

5.2.2 ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

1. มีการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย ให้ทันสมัย และอัพเดตอย่างสม่ำเสมอ

2. หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

5.2.3 เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ ทำให้ระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

1. มีการฝึกอบรมให้ความรู้ เกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ต่าง ๆ ระบบสารสนเทศ รวมไปถึงการใช้งานอุปกรณ์ห้อง Smart Classroom และห้องเรียนที่มี Interactive Board อย่างถูกต้องปลอดภัยไซเบอร์

2. มีการฝึกอบรมการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ของคณะเป็นประจำทุกปี

6. ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

6.1 การสำรองข้อมูล (Back Up)

มีการสำรองข้อมูลเครื่องแม่ข่ายหลักของคณะฯ โดยสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่เป็นประจำทุกวัน โดยสำรองข้อมูลและบันทึกข้อมูลลงในสื่อบันทึกข้อมูล นอกจากนั้นยังมีการสำรองฐานข้อมูลเก็บไว้บน One Drive ซึ่งเป็น Cloud ของ Microsoft ในส่วนของเครื่องลูกข่ายของเจ้าหน้าที่ให้ทำการสำรองไฟล์ไว้บน One Drive ด้วย

6.2 การกู้ข้อมูล (Recovery)

ทดสอบการกู้ข้อมูลที่ได้สำรองไว้ อย่างน้อย ปีละ 1 ครั้ง

7. ข้อปฏิบัติในการแก้ไขปัญหา

7.1 กรณีเครื่องลูกข่าย

1. กรณีที่มีเหตุให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้ผู้ใช้งานแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือผู้ดูแลระบบทราบ

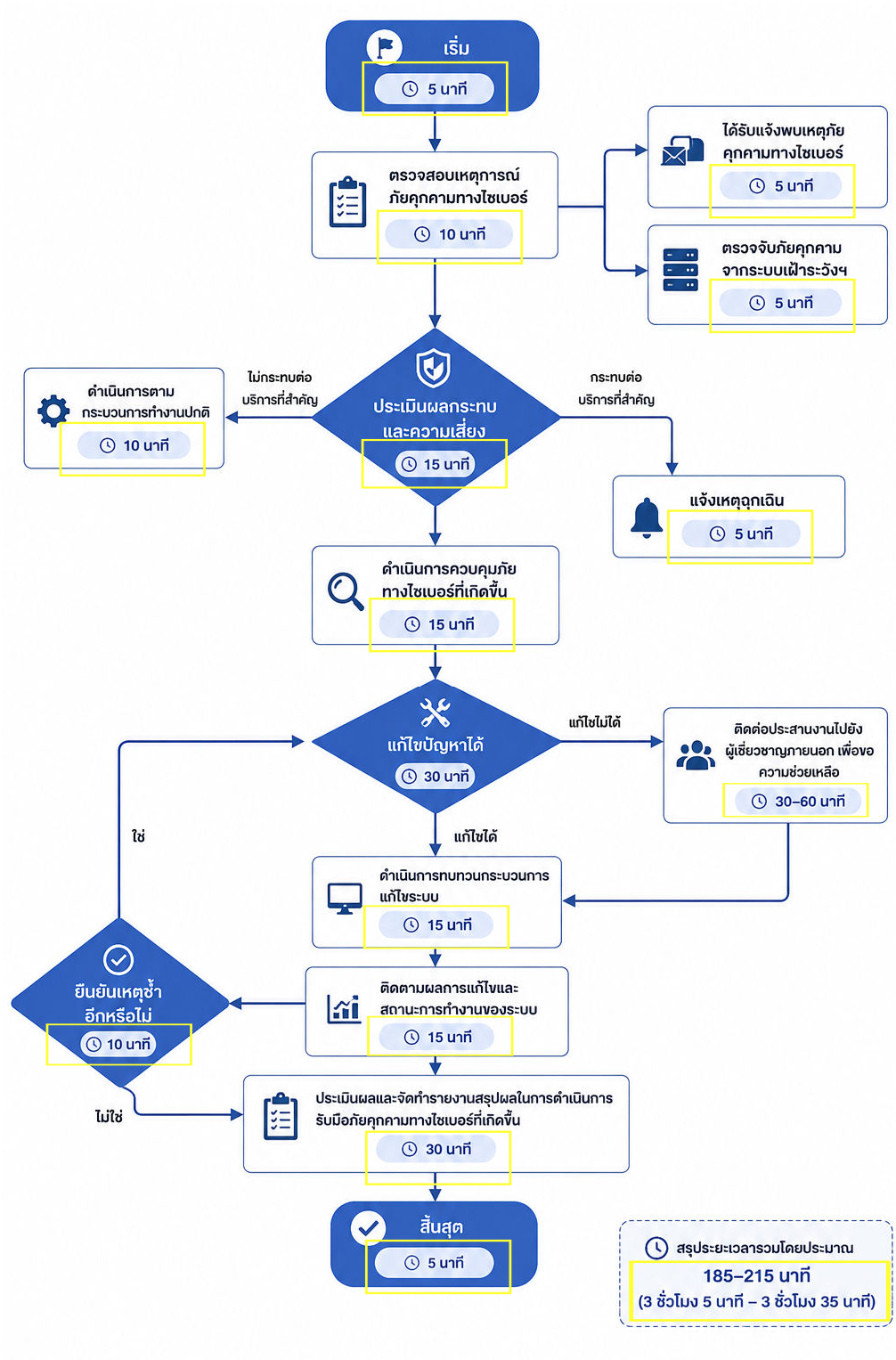
2. กรณีจากไวรัสคอมพิวเตอร์ ให้ทำการตัดการเชื่อมต่อระบบเครือข่ายของเครื่องนั้นออกจากระบบเครือข่ายหลัก และทำการตรวจสอบหาสาเหตุ

7.2 กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

1. กรณีที่เครื่องแม่ข่ายไม่สามารถใช้งานได้ ให้ทำการตรวจสอบหาสาเหตุ และทำการแก้ไข

2. กรณีจากไวรัสคอมพิวเตอร์ ให้ทำการตัดการเชื่อมต่อของเครื่องแม่ข่ายจากระบบเครือข่ายหลัก ทำการหาสาเหตุ และทำการแก้ไข

8. วิธีการขั้นตอนการปฏิบัติงาน



9. ระยะเวลาที่ใช้ในการปฏิบัติงาน

ลำดับ	ช่วงการทำงาน	ขั้นตอนปฏิบัติงาน	ระยะเวลา	หมายเหตุ / เงื่อนไข
1	ตรวจจับ & ประเมิน (รวม 30 นาที)	• เริ่มต้นกระบวนการ • ตรวจสอบเหตุการณ์ • ประเมินความเสี่ยง	5 นาที 10 นาที 15 นาที	-รับแจ้งหรือเฝ้าระวัง (ช่องทางละ 5 นาที) - กระทบสำคัญ: แจ้งฉุกเฉิน (+5 นาที) - ไม่กระทบ: ทำงานปกติ (+10 นาที)
2	ควบคุม & แก้ไข (รวม 45–105 นาที)	• ควบคุมภัยคุกคาม • ดำเนินการแก้ไขปัญหา	15 นาที 30 นาที	**กรณีแก้ไขไม่ได้:** ต้องประสานผู้เชี่ยวชาญภายนอก (+30–60 นาที)
3	ตรวจสอบ & ติดตาม (รวม 30 นาที)	• ทบทวนกระบวนการแก้ไข • ติดตามผลและสถานะระบบ	15 นาที 15 นาที	
4	สรุป & ปิดงาน (รวม 45 นาที)	• ตรวจสอบการเกิดเหตุซ้ำ • จัดทำรายงานสรุปผล • สิ้นสุดกระบวนการ	10 นาที 30 นาที 5 นาที	หากเกิดเหตุซ้ำ (ใช่) ให้วนกลับไปขั้นตอนแก้ไข

สรุปเวลารวมทั้งหมด

1. เวลารวมขั้นต่ำ: 185 นาที (3 ชั่วโมง 5 นาที) — กรณีแก้ไขได้เอง ไม่เกิดซ้ำ

2. เวลารวมสูงสุด: 215 นาที (3 ชั่วโมง 35 นาที) — กรณีต้องให้ผู้เชี่ยวชาญภายนอกช่วย

10. กฎหมายที่เกี่ยวข้อง

ในประเทศไทยมีกฎหมายหลัก 3 ฉบับที่องค์กรและบุคคลต้องระบุให้ชัดเจน:

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (Cybersecurity Act) เน้นการป้องกันและรับมือภัยคุกคามที่กระทบต่อความมั่นคงของรัฐและโครงสร้างพื้นฐานสำคัญ (CII) เช่น พลังงาน สาธารณสุข การเงิน และขนส่ง

หน้าที่: หน่วยงาน CII ต้องมีมาตรฐานขั้นต่ำในการรักษาความปลอดภัย และรายงานเหตุภัยคุกคามต่อ สกมช. (NCSA)

2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เน้นการคุ้มครองสิทธิของเจ้าของข้อมูล (Data Subject)

หน้าที่: หากเกิด "ข้อมูลรั่วไหล" ต้องแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง และต้องแจ้งเจ้าของข้อมูลหากมีความเสี่ยงสูง

3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Crime Act) เน้นการลงโทษผู้กระทำความผิดและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log files)

หน้าที่: ผู้ให้บริการต้องเก็บ Log ไว้ไม่น้อยกว่า 90 วัน เพื่อใช้เป็นหลักฐานในการดำเนินคดี

11. รายชื่อกรรมการแผนกู้คืนระบบสารสนเทศ

บุคลากรที่ได้รับการคัดเลือกให้ปฏิบัติหน้าที่ตามแผนกู้คืนระบบสารสนเทศ กรณีฉุกเฉินนั้น เป็นผู้ที่มีความรู้ความเชี่ยวชาญในหน้าที่ที่ได้รับมอบหมายให้รับผิดชอบในแต่ละหน่วย

ตาราง รายชื่อคณะกรรมการกู้คืนระบบสารสนเทศ

ชื่อ-นามสกุล	ตำแหน่ง	หมายเลขโทรศัพท์	E-mail
ผศ. ดร.ทัชชา สุตตสันต์	ประธาน	053942212	tatcha.s@cmu.ac.th
นายนิติรัฐ สาลี	กรรมการ	0818823003	nitirat.sal@cmu.ac.th
นายสุพัฒน์ ศรีญาณลักษณ์	กรรมการ	0816359553	supat.sr@cmu.ac.th
นางสาววชิราภรณ์ คำไชยลึก	กรรมการ	0959549690	wachiraporn.k@cmu.ac.th
นายวีรศักดิ์ เหมือนฟู	กรรมการ	0959549187	weerasak.m@cmu.ac.th
นายชลวิทย์ เพ็ญวิจิตร	กรรมการ	0807708593	chonlawit.pe@cmu.ac.th

12. รายชื่อติดต่อบริษัทภายนอก

ในการดำเนินการจัดทำแผนกู้คืนระบบสารสนเทศกรณีฉุกเฉิน ได้มีข้อตกลงในการใช้บริการดังนี้

1. สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ให้บริการด้านเครื่องแม่ข่าย อุปกรณ์เครือข่ายหลัก การสำรองข้อมูลของเครื่องแม่ข่ายของคณะฯ บน Private Cloud ทุกวัน ระบบเทคโนโลยีสารสนเทศหลักของมหาวิทยาลัย
2. บริษัทชิชางคอมพิวเตอร์ ให้บริการด้านเครื่องแม่ข่าย เครื่องคอมพิวเตอร์(PC) และ เครื่องคอมพิวเตอร์แบบพกพา (Laptop) อุปกรณ์ต่อพ่วง อุปกรณ์เครือข่ายและอุปกรณ์ป้องกันเครือข่าย (Firewall) เครื่องพิมพ์ หมึกพิมพ์
3. บริษัทลานนาคอม ให้บริการด้านเครื่องแม่ข่าย อุปกรณ์ห้องเรียนอัจฉริยะ จอสัมผัสในห้องเรียน
4. บริษัทไอโอนอน ให้บริการเครื่องคอมพิวเตอร์ (PC) และ เครื่องคอมพิวเตอร์แบบพกพา (Laptop)
5. บริษัท Undefined Co.,ltd ให้บริการด้านระบบสารสนเทศสำหรับงานวิจัย

13. รายชื่อบริษัทภายนอกที่เกี่ยวกับแผน

ชื่อบริษัท หน่วยงาน	ผู้ติดต่อ	ระบบ	โทรศัพท์	E-mail
สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่				
ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	คุณสัจจะ ตันจันทร์พงศ์	เครือข่ายอินเทอร์เน็ต	41781	chairat.c@cmu.ac.th
	คุณนวิน ธรรมรักษ์		43853	nawin.t@cmu.ac.th
	คุณปฐมพงศ์ แผ้วสาสน์	เครือข่ายไร้สาย JumboPlus	41778	pathompong.p@cmu.ac.th
	ว่าที่ร้อยตรีศุภวิทย์ วรรณภิละ	VPS, Guestaccount, Firewall	43853	supawit.w@cmu.ac.th
	คุณสันติ เซี่ยงวงษ์	Backup, Antivirus	41778	santi.s@cmu.ac.th
	คุณอนุรักษ์ ศรีชัยวิทย์	Oauth		anurak.s@cmu.ac.th
	คุณจริยา ลิ้มจีระจรัส	VOC	43832	jariya.lim@cmu.ac.th
	คุณจริยา ลิ้มจีระจรัส	MIS	43832	kanokwan.w@cmu.ac.th
	คุณเยาวภา จรัสสันติจิต	E-MEETING	43836	yaowapa.j@cmu.ac.th
	คุณณัฏฐ์วลัช นันทิสิงห์	E-DOCUMENT	43832	nathwarat.n@cmu.ac.th
	คุณวรากร คิดคำนวณ	CMU Software License, CMU WEB	43809	warakon.kid@cmu.ac.th
	คุณโอภาส หมื่นแสน	CSOC	41784	opas.m@cmu.ac.th
บริษัทชิชางคอมพิวเตอร์	คุณกฤษณา วงศ์เสน่ห์	Computer, Accessories and Peripheral	053280150 ต่อ 817	product@chichang.com
	คุณสุชาติ รัตนา	Firewall, Switch	053280150 ต่อ 805	suchat@chichang.com
บริษัทลานนาคอม	คุณนัฐวุฒิ ศิริกุลสัมพันธ์	Smart Classroom	053441480	natthawuts@lanna.co.th
	คุณธีรัชริน ขันอัศวะ	Smart Classroom	085-2162772	teeratcharink@lanna.co.th
บริษัทไอโอนอน	คุณคิว	PC	089-7557793	

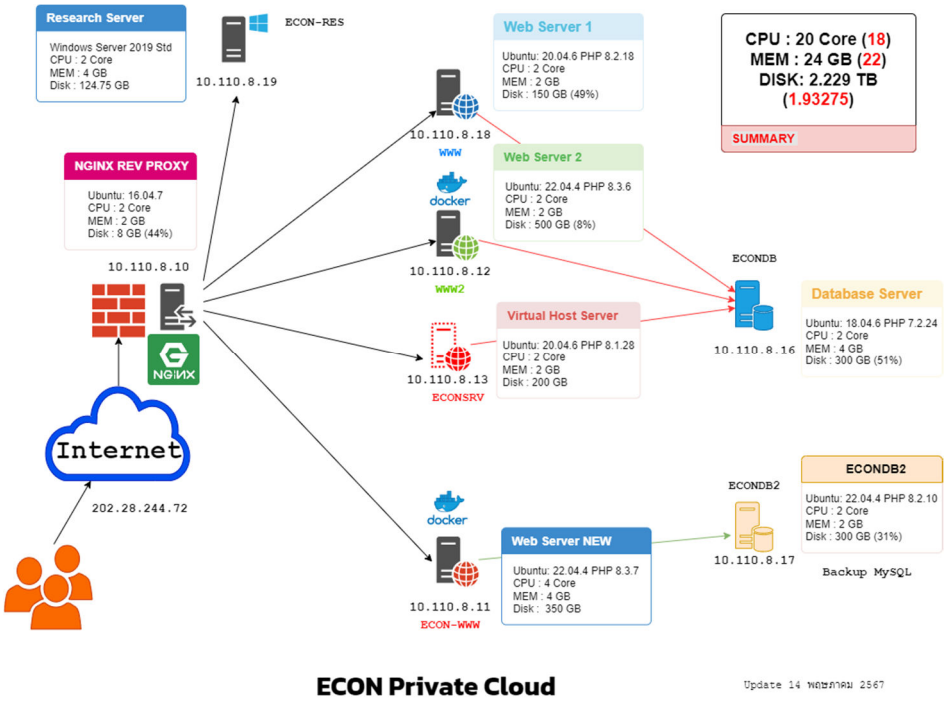
14. ข้อมูลเครื่องแม่ข่ายคอมพิวเตอร์คณะเศรษฐศาสตร์

สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ได้ให้บริการศูนย์จัดเก็บข้อมูลเทคโนโลยีสารสนเทศ (Data Center) ที่ได้รับการรับรองมาตรฐาน ISO27001 ซึ่งได้ให้บริการเป็นแบบ Virtual Private Cloud (VPS) บน Nutanix Platform เป็นแพลตฟอร์มที่ผสานรวมทรัพยากรของ Server และ Storage เข้าด้วยกันสำหรับการทำงานในสภาพแวดล้อมของ Virtualization โดยคณะฯได้รับการจัดสรรทรัพยากรจากสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ดังนี้

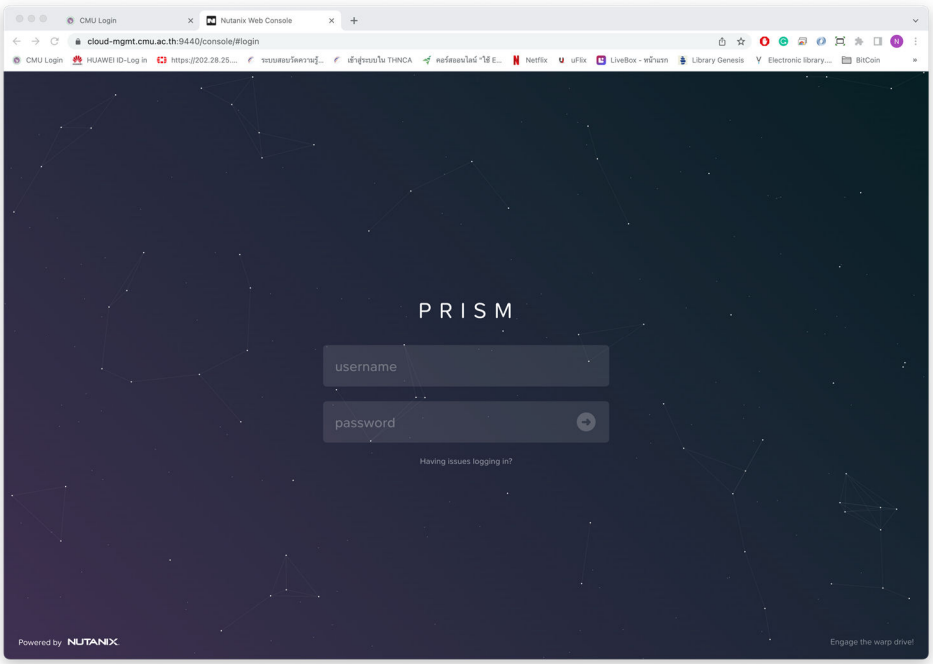
คณะ	Disk(GB)	vCPU(Cores)	RAM(GB)
คณะเศรษฐศาสตร์	2,229	20	24

โดยผู้ดูแลระบบจะสามารถบริหารจัดการระบบประมวลผลได้ด้วยตนเองผ่านหน้า Website ที่ทางสำนักฯ ได้จัดสรรให้ ซึ่งทำให้สะดวกในการบริหารจัดการเครื่องแม่ข่าย และการกู้คืนระบบได้อย่างรวดเร็ว โดยในปัจจุบันหน่วยเทคโนโลยีสารสนเทศได้ดำเนินสร้างเครื่องแม่ข่ายเสมือนไว้บน Virtual Private Cloud (VPS) ของสำนักบริการเทคโนโลยีสารสนเทศ จำนวนทั้งสิ้น 8 เครื่อง ดังนี้

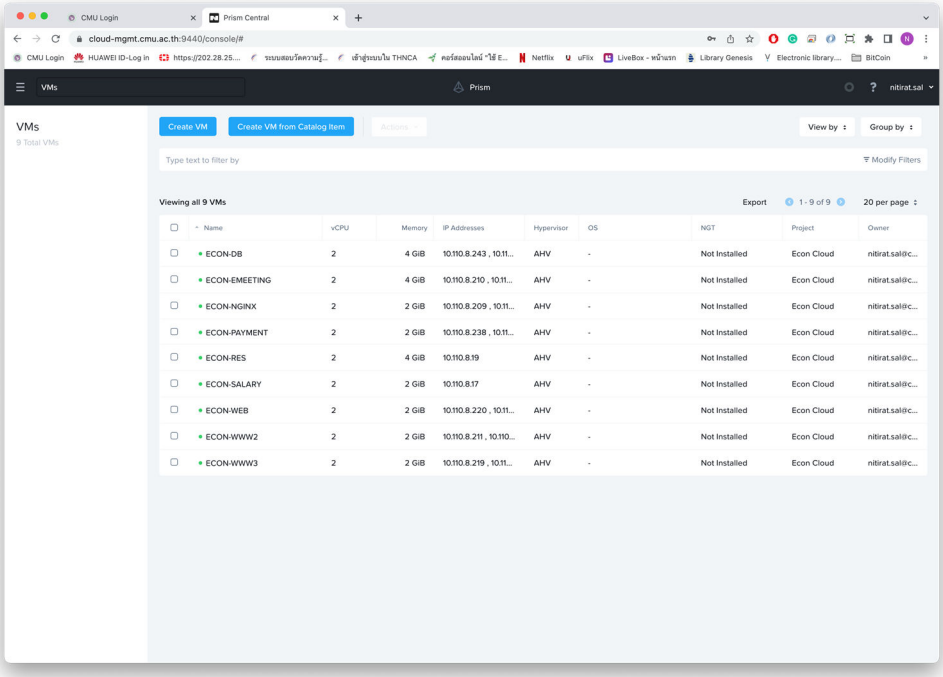
Server	Os	IP	Disk(GB)	vCPU(Cores)	RAM(GB)
ECON-NGINX	Ubuntu	10.110.8.10	8	2	2
ECON-WEB	Ubuntu	10.110.8.18	500	2	2
ECON-WWW1	Ubuntu	10.110.8.11	350	4	4
ECON-WWW2	Ubuntu	10.110.8.12	500	2	2
ECON-WWW3	Ubuntu	10.110.8.13	200	2	2
ECON-DB	Ubuntu	10.110.8.16	300	2	4
ECON-DB2	Ubuntu	10.110.8.17	300	2	2
ECON-RES	Windows	10.110.8.19	124.75	2	4
			1932.75	18	22



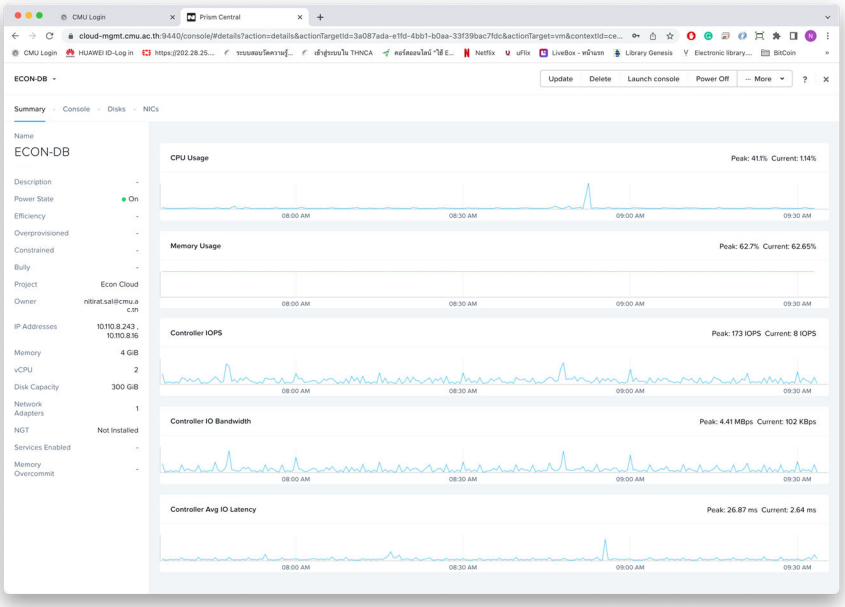
และการใช้งาน Private Cloud สามารถจัดการเครื่องแม่ข่ายแบบเสมือน ได้ผ่านหน้าเว็บไซต์ด้วยตนเอง Self Service Portal https://cloud-ssp.cmu.ac.th ซึ่งการจะบริหารจัดการได้ต้องได้รับสิทธิ์การใช้งานก่อน



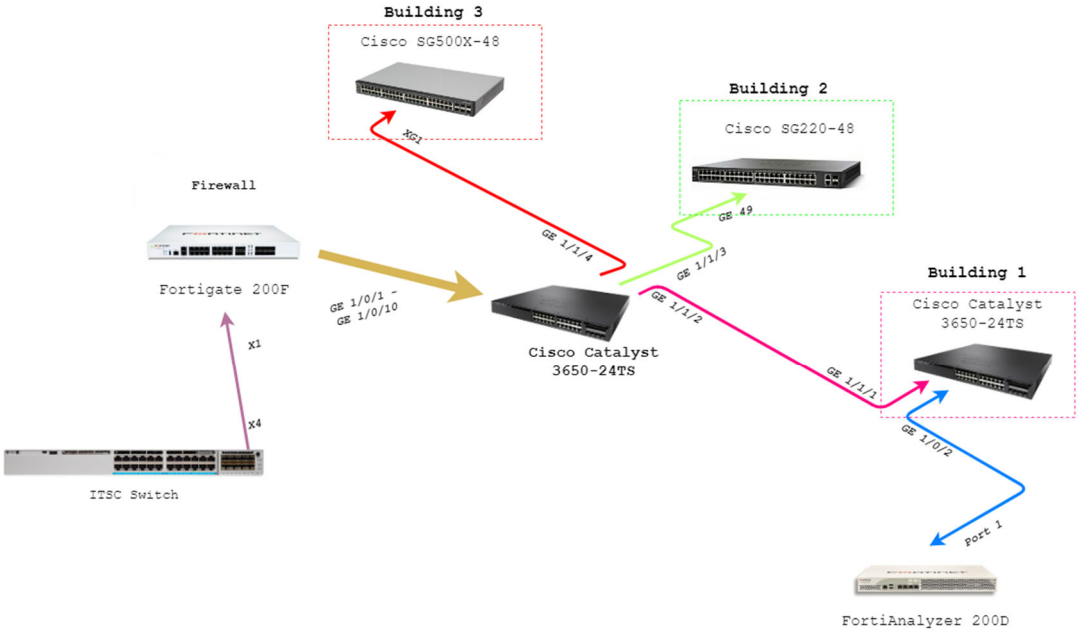
15. เครื่องแม่ข่ายคอมพิวเตอร์คณะเศรษฐศาสตร์ บน Private Cloud



สามารถตรวจสอบสถานะของเครื่องคอมพิวเตอร์แม่ข่ายบน Private Cloud ได้ ถ้าเป็น สีเขียว แสดงว่าเครื่องคอมพิวเตอร์แม่ข่ายทำงานอยู่ สีแดง แสดงว่าเครื่องคอมพิวเตอร์แม่ข่ายหยุดทำงาน สามารถเข้าไปตรวจสอบประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละตัวได้โดยการคลิกเข้าไปที่เครื่องคอมพิวเตอร์แม่ข่ายแต่ละตัว ดังภาพ



16. ระบบเครือข่ายหลักของคณะเศรษฐศาสตร์

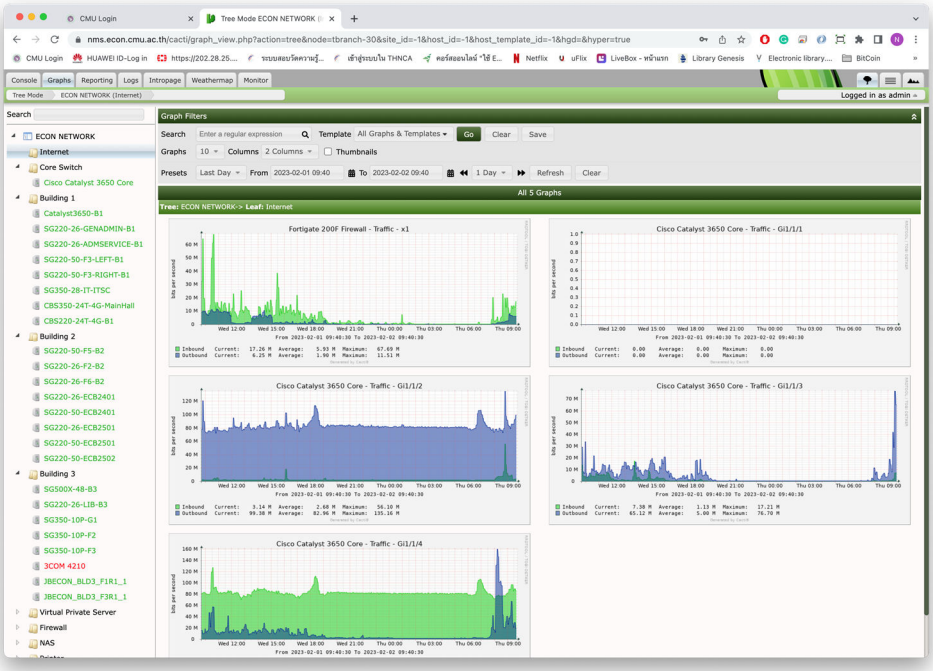


Main Network Econ Update 1 กุมภาพันธ์ 2566

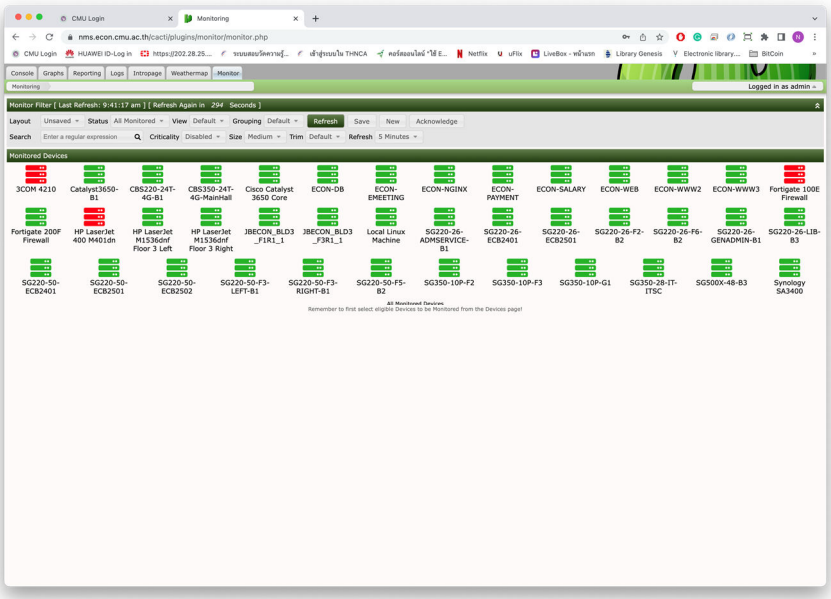
อุปกรณ์สลับสัญญาณ	รุ่น	IP Address	สถานที่ตั้ง
1. Core Switch	Cisco Catalyst 3650	10.150.126.1	ห้องอุปกรณ์เครือข่าย ITSC
2. Switch อาคาร 1	Cisco Catalyst 3650	10.150.126.11	ห้องเครื่องแม่ข่ายคณะ
3. Switch อาคาร 2	Cisco SG220-48	10.150.126.21	ห้องอุปกรณ์เครือข่ายชั้น 5 อาคาร 2 ECB2502
4. Switch อาคาร 3	Cisco SG500X-48	10.150.126.31	ห้องอุปกรณ์เครือข่ายชั้น 3 อาคาร 3

17. เครื่องมือในการตรวจสอบระบบเครือข่ายและเครื่องแม่ข่าย (Network and Server Monitoring)

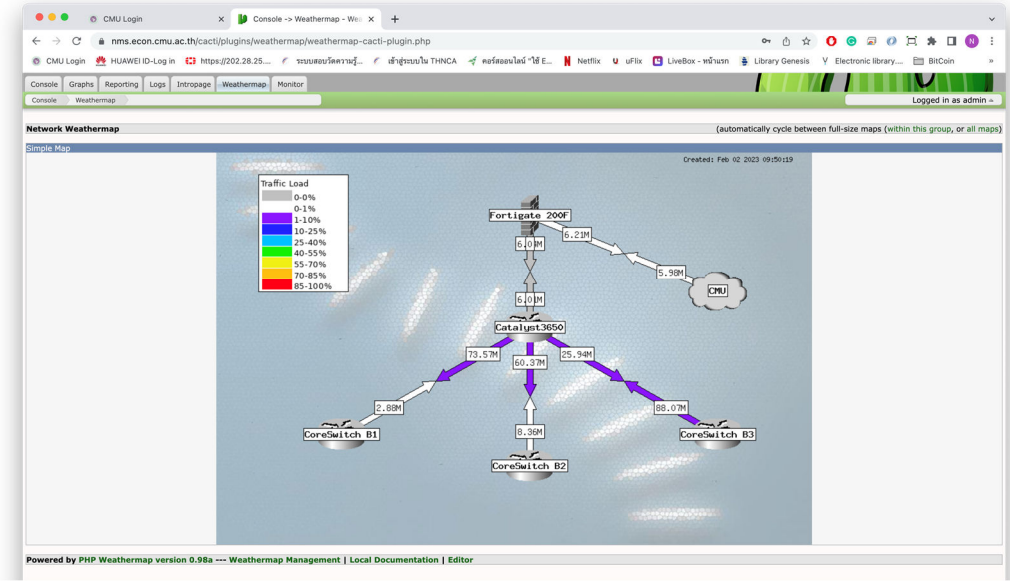
ทางกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้ได้ดำเนินการติดตั้งเครื่องมือในการตรวจสอบระบบเครือข่ายและเครื่องแม่ข่าย เพื่อใช้ในการตรวจสอบประสิทธิภาพของระบบเครือข่ายและเครื่องแม่ข่ายในรูปแบบของกราฟ โดยใช้เครื่องมือที่ชื่อว่า cacti ซึ่งมีการทำงานร่วมกับ RRDTool สำหรับการสร้างกราฟ เพื่อใช้ในการวิเคราะห์ ติดตามการทำงานของอุปกรณ์เครือข่าย เครื่องแม่ข่าย CPU Load, Network Bandwidth, Memory Usage, Disk Space เป็นต้น สามารถตรวจสอบได้ที่ url : https://nms.econ.cmu.ac.th/cacti



ใน Cacti สามารถเพิ่มเติม Plugin เพื่อเป็นการขยายความสามารถของ Cacti ได้ ดังภาพจะเป็นการเพิ่มประสิทธิภาพของ Cacti โดยใช้ Plugin : Monitor ในการตรวจสอบว่าอุปกรณ์เครือข่ายหรือเครื่องแม่ข่ายเครื่องใดไม่สามารถเชื่อมต่อได้ ถ้าการทำงานเป็นปกติจะเป็นสีเขียว ถ้าผิดปกติจะเป็นสีแดง



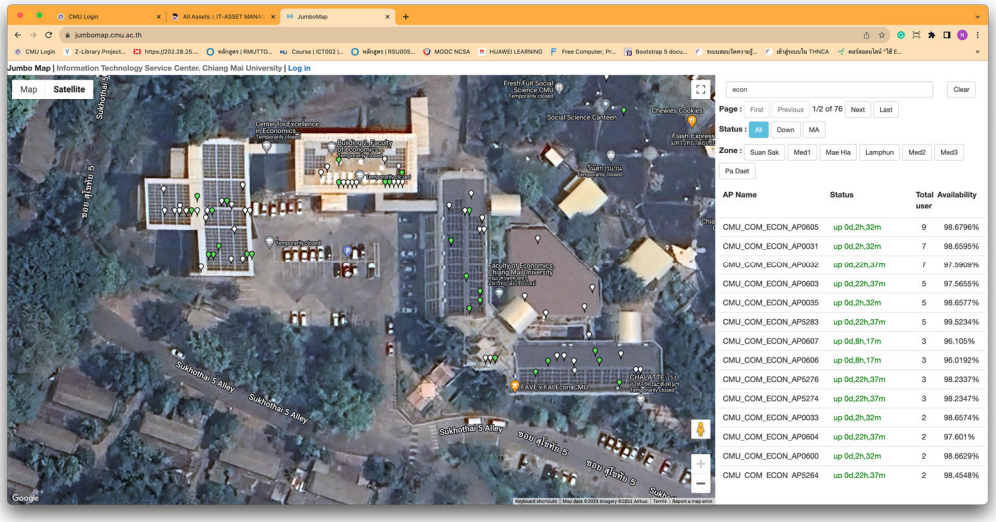
ดังภาพจะเป็นการเพิ่มประสิทธิภาพของ Cacti โดยใช้ Plugin : Weathemap คือแผนที่ของระบบเครือข่ายหลักที่สามารถแสดงสถานะในช่วงเวลาหนึ่ง ๆ โดยจะสามารถบอกได้ว่าการรับส่งข้อมูลระหว่างอุปกรณ์เครือข่าย อยู่ในระดับใด แสดงเป็นเปอร์เซ็นต์



โดยเราสามารถใช้เครื่องมือ cacti ในการตรวจสอบการทำงานของระบบเครือข่ายทำให้ทราบว่าอุปกรณ์ใดที่มีปัญหา ทำให้สามารถแก้ไขปัญหาได้อย่างรวดเร็ว แม่นยำ

18. การตรวจสอบระบบเครือข่ายคอมพิวเตอร์ไร้สาย JumboPlus

การตรวจสอบระบบเครือข่ายคอมพิวเตอร์ไร้สาย JumboPlus สามารถตรวจสอบได้จากเว็บไซต์ https://jumbomap.cmu.ac.th ซึ่งจะดูสถานะได้ว่าอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ตัวไหน Down อยู่ ติดตั้งอยู่ที่อาคารไหน



คู่มือการปฏิบัติงานกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้

การแก้ไขปัญหาภัยคุกคามระบบความมั่นคงปลอดภัยไซเบอร์
สำหรับผู้ปฏิบัติงาน

(ลงชื่อ).....ผู้รายงาน (ลงชื่อ).....ผู้รับรองรายงาน

(นายนิติรัฐ สาลี) (รองศาสตราจารย์ ดร.รสริน โอสถานันต์กุล)

หัวหน้ากลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้ คณบดีคณะเศรษฐศาสตร์

หมายเหตุ: ให้ผู้บริหารสูงสุดของหน่วยงานหรือผู้รักษาราชการแทน เป็นผู้รับรองรายงานการเผยแพร่ลงเว็บไซต์


Econ
คณะเศรษฐศาสตร์
มหาวิทยาลัยเชียงใหม่