แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏสกลนคร

ระยะ 4 ปี (พ.ศ. 2568 – 2571)

มกราคม 2568
สำนักงานผู้อำนวยการ
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

คำนำ

การบริหารจัดทำความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อการดำเนินงาน เป็นอุปสรรคต่อการบรรลุพันธกิจขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม

เพื่อให้ผลการดำเนินงานขององค์กรเป็นไปตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้ อีกทั้งยังมุ่งเน้นให้เกิดการตระหนัก และเข้าใจถึงความเสี่ยงด้านต่างๆ ที่อาจเกิดขึ้นกับองค์กร โดยสามารถเลือกวิธีบริหารจัดการที่เหมาะสมในการลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ด้วยเหตุนี้ ทางสำนักฯ จึงได้นำหลักการ แนวคิด และกระบวนการบริหารความเสี่ยงมาประยุกต์ใช้เป็นเครื่องมือในการพัฒนาองค์กร โดยมุ่งปลูกฝังให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานตามภารกิจ จนเป็นวัฒนธรรมองค์กร อันจะก่อให้เกิดประโยชน์สูงสุดต่อการบรรลุเป้าหมายการดำเนินงานขององค์กรในระยะยาว

คณะกรรมการบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏสกลนคร
มกราคม 2568

สารบัญ

หน้า

บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

การบริหารจัดการความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญ ตามหลักการกำกับดูแลกิจการที่ดี ซึ่งจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ เป็นไปอย่างเหมาะสม และมีประสิทธิภาพมากขึ้น อีกทั้งยังลดการสูญเสียและโอกาสที่อาจทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งทางด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ซึ่งครอบคลุมถึงทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก่อให้เกิดความไม่แน่นอน และอาจส่งผลกระทบต่อการดำเนินงานหรือการบรรลุเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร ในปัจจุบันการวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่อาจเกิดขึ้น การจัดลำดับความสำคัญของความเสี่ยง และการกำหนดแนวทางในด้านจัดการความเสี่ยง ในการดำเนินการดังกล่าวต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสมเพื่อให้เกิดประสิทธิภาพสูงสุดในการบริหารจัดการองค์กร

1.2 วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

การจัดทำแผนบริหารความเสี่ยงมีวัตถุประสงค์ดังต่อไปนี้

1) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร

2) เพื่อกำหนดแนวทางและมาตรการในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศให้มีความเสถียรภาพ มีประสิทธิภาพและมีความพร้อมสำหรับการใช้งานอย่างต่อเนื่อง

3) เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีในกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

4) เพื่อสร้างความตระหนักและการมีส่วนร่วมในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่บุคลากรทุกระดับในองค์กร

5) เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศและการดำเนินงานของมหาวิทยาลัย

1.3 คำจำกัดความและความหมายที่เกี่ยวข้องกับการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ การกระทำใดๆ ที่ไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงลบต่อวัตถุประสงค์หรือเป้าหมายขององค์กร หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ของแผนงาน/โครงการที่จะก้าวสู่พันธกิจและวิสัยทัศน์ที่กำหนดไว้

ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุของความเสี่ยงซึ่งจะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และจะเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยงและการวิเคราะห์ความเสี่ยงเพื่อจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบต่อการบรรลุเป้าหมายขององค์กร (Impact)

ระดับความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งเป็น 5 ระดับ คือ ความเสี่ยงสูงมาก ความเสี่ยงสูง ความเสี่ยงปานกลาง ความเสี่ยงต่ำ และความเสี่ยงต่ำมาก

โอกาส (Opportunity) หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงบวกต่อวัตถุประสงค์หรือเป้าหมายขององค์กร ซึ่งผู้บริหารและผู้ที่เกี่ยวข้องควรจะได้ทบทวนถึงกลยุทธ์และแผนงานที่เหมาะสมใหม่ เพื่อสร้างคุณค่าเพิ่มให้กับองค์กรนอกเหนือจากแผนงานและโครงการที่ได้กำหนดไว้แล้ว

การควบคุมภายใน (Internal Control) หมายถึง กระบวนการปฏิบัติงานที่บุคลากรในองค์กร โดยคณะกรรมการบริหาร ผู้บริหารทุกระดับ และพนักงานทุกคนมีบทบาทร่วมกันในการจัดให้มีขึ้น เพื่อสร้างความเชื่อมั่นอย่างสมเหตุสมผลว่าการปฏิบัติงานจะบรรลุวัตถุประสงค์ของการควบคุมภายใน

การบริหารจัดการความเสี่ยง (Risk Management) หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด

การบริหารความเสี่ยงโดยองค์กร (Enterprise Risk Management : EMR) หมายถึง การบริหารความเสี่ยง โดยมีโครงสร้างองค์กร กระบวนการ และวัฒนธรรมองค์กรประกอบเข้าด้วยกัน และเป็นกลไกส่วนหนึ่งของการขับเคลื่อนไปสู่การกำกับดูแลกิจการที่ดี เพื่อบรรลุวัตถุประสงค์และการเติบโตอย่างยั่งยืนขององค์กร และเป็นที่พอใจของผู้มีผลประโยชน์ร่วม โดยครอบคลุมความเสี่ยงทั่วทั้งองค์กร ไม่ว่าจะเป็นความเสี่ยงเกี่ยวกับกลยุทธ์การดำเนินงาน การปฏิบัติตามกฎระเบียบ และการเงิน ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหาย ความไม่แน่นอน และโอกาส รวมถึงการมีผลกระทบต่อวัตถุประสงค์และความต้องการของผู้มีผลประโยชน์ร่วม

1.4 ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น และทำให้องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย

ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

1) การบริหารความเสี่ยงเป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี โดยการบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

2) การบริหารความเสี่ยงสร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร โดยเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ ซึ่งสอดคล้องกับเป้าหมาย ภารกิจหลัก และระดับความเสี่ยงที่ยอมรับได้ขององค์กร

3) การบริหารความเสี่ยงช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด ส่งผลให้ให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงด้านธรรมาภิบาล

4) การบริหารความเสี่ยงเป็นเครื่องมือที่สำคัญในการบริหารงาน ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของมหาวิทยาลัยเป็นไปตามเป้าหมายที่กำหนด และสามารถรักษาผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่องค์กร

5) การบริหารความเสี่ยงช่วยในการพัฒนาองค์กรให้เป็นไปในทิศทางเดียวกัน โดยส่งผลให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์ วัตถุประสงค์ขององค์กร แลระดับความเสี่ยงอย่างชัดเจน

6) การบริหารความเสี่ยงช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล โดยการจัดสรรทรัพยากรจะพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรมและการเลือกใช้มาตรการในการบริหารความเสี่ยงที่เหมาะสม ทำให้การใช้ทรัพยากรเป็นไปอย่างคุ้มค่าและเหมาะสมกับระดับความเสี่ยงของแต่ละกิจกรรม

บทที่ 2

แนวทางการบริหารความเสี่ยง

2.1 หลักการบริหารความเสี่ยง

มหาวิทยาลัยราชภัฏสกลนคร ดำเนินการตามหลักการบริหารความเสี่ยงโดยใช้กระบวนการบริหารความเสี่ยงตามมาตรฐานของ COSO (The Committee of Sponsoring Organization of the Tread way Commission) ซึ่งกำหนดกรอบการจัดการความเสี่ยงในแนวทาง COSO : ERM (Enterprise Risk management) ประกอบด้วยหลักการสำคัญ 8 องค์ประกอบ เพื่อให้เกิดการบรรลุวัตถุประสงค์ของการบริหารความเสี่ยง ดังรูปที่ 1

รูปที่ 1 COSO : ERM (Enterprise Risk Management)

2.2 แนวทางในการบริหารความเสี่ยง (ERM : Enterprise Risk Management)

การบริหารความเสี่ยงเป็นเครื่องมือที่สำคัญที่ทำให้เกิดความมั่นใจว่าความเสี่ยงทั้งหมด ที่มีผลกระทบสำคัญทั้งจากภายในและภายนอก ที่มีต่อการบรรลุวัตถุประสงค์ขององค์กรจะได้รับการพิจารณาและจัดการให้หมดไปหรือลดน้อยลง ซึ่งจะทำให้ผลการดำเนินงานมีประสิทธิภาพและประสิทธิผล แต่ทั้งนี้การบริหารความเสี่ยงดังกล่าว นอกจากจะต้องมีการดำเนินการทั่วทั้งองค์กรแบบบูรณาการแล้ว หากยังต้องให้ความสำคัญในการกำหนดผู้รับผิดชอบต่อกิจกรรมการควบคุม (Control Activities) เพื่อพิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน หรือพิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิภาพของการจัดการความเสี่ยง มีการติดตาม (Monitoring) เพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยง มีคุณภาพ มีความเหมาะสม และการบริหารความเสี่ยงได้นำไปใช้ทุกระดับขององค์การ มีการรายงานความเสี่ยงทั้งหมดที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กรต่อผู้บริหารที่รับผิดชอบ และท้ายสุดมีสารสนเทศและการสื่อสาร (Information & Communication) แก่บุคลากรทุกคนให้ได้รับรู้และเข้าใจอย่างทั่วถึง จะสามารถช่วยให้บุคลากรที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพยิ่งขึ้น

เพื่อให้การจัดการของมหาวิทยาลัยเป็นไปตามระบบการบริหารความเสี่ยงที่ควบคุมปัจจัย กิจกรรม และกระบวนการดำเนินงานที่อาจเป็นมูลเหตุของความเสียหาย ให้ระดับความเสี่ยงและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่ยอมรับและควบคุมได้ ตลอดจนเพื่อป้องกันหรือบรรเทาความรุนแรงของปัญหา รวมทั้งการมีแผนสำรองต่อภาวะฉุกเฉินเพื่อให้มีความมั่นใจว่าระบบงานต่าง ๆ มีความพร้อมใช้งาน มีการปรับปรุงระบบอย่างต่อเนื่อง และทันต่อการเปลี่ยนแปลงเพื่อให้บรรลุเป้าหมายของยุทธศาสตร์ของมหาวิทยาลัย

มหาวิทยาลัยราชภัฏสกลนคร ได้ดำเนินการตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน *COSO (The Committee of Sponsoring Organizations of the Tread way Commission)

รูปที่ 2 กระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO

โดยคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้วิเคราะห์สภาพแวดล้อมของหน่วยงานเพื่อวางแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

1) สภาพแวดล้อมภายในองค์กรด้านเทคโนโลยีสารสนเทศ (Internal Environment) ได้แก่

- ระบบฐานข้อมูลสารสนเทศ (Database & Software) เช่น เว็บไซต์มหาวิทยาลัยราชภัฏสกลนครและหน่วยงานภายในมหาวิทยาลัย ภายใต้อินเทอร์เน็ตโดเมน snru.ac.th และฐานข้อมูลเว็บไซต์ดังกล่าว เป็นต้น
- ระบบฐานข้อมูลสำหรับการบริหารงานภายใน (Back Office) ได้แก่ ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ (e-document) ฐานข้อมูลระบบสารสนเทศทรัพยากรบุคคล (n-eport) ฐานข้อมูลครุภัณฑ์ ฐานข้อมูลระบบบริหารงบประมาณ ฐานข้อมูระบบบริหารพัสดุ ฐานข้อมูลระบบจัดการเรียนการสอนออนไลน์ เป็นต้น
- ระบบฐานข้อมูลวิทยานิพนธ์ฉบับเต็ม (TDC) ระบบสหบรรณานุกรมห้องสมุดสถาบันอุดมศึกษาไทย (UCTAL) ระบบลงทะเบียนเพื่อสมัครสมาชิกบนฐานข้อมูลสหบรรณานุกรม e-Journal เป็นต้น
- ระบบให้บริการเครือข่าย ได้แก่ ระบบเครือข่ายภายใน (LAN) ระบบเครือข่ายอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wi-Fi) ระบบเครือข่ายเสมือน (VPN) https://snru.ac.th/vpn

- อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบสารสนเทศ (Web Application Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น
- ระบบรักษาความปลอดภัย ได้แก่ โปรแกรตรวจสอบและป้องกันไวรัส Firewall IPS (Instruction Prevention System) และ Web Application Fire wall

2) วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

1) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร

2) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศให้มีความเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

3) เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3) การบ่งชี้หรือการระบุความเสี่ยง (Event Identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันบ่งชี้หรือระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบเหตุการณ์ที่เป็นความเสี่ยงที่อาจจะมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
- การใช้ Checklist
- การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
- การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- การรวบรวมปัญหาที่เกิดขึ้นแล้ว

ในขั้นตอนนี้มีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จและปัญหาอุปกรณ์ซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

4) การประเมินความเสี่ยง (Risk Assessment) ประกอบด้วย 4 ขั้นตอน คือ

4.1 การกำหนดเกณฑ์ประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงกำหนดเกณฑ์ของหน่วยงานขึ้น โดยกำหนด เกณฑ์เชิงปริมาณ และเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเกณฑ์ 5 ระดับ คือ สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และน้อยมาก ส่วนระดับของความเสี่ยงกำหนดเป็นเกณฑ์ 5 ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก

4.2 การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้น และประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนด เพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของมหาวิทยาลัย โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบและมิติของโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ มีดังนี้

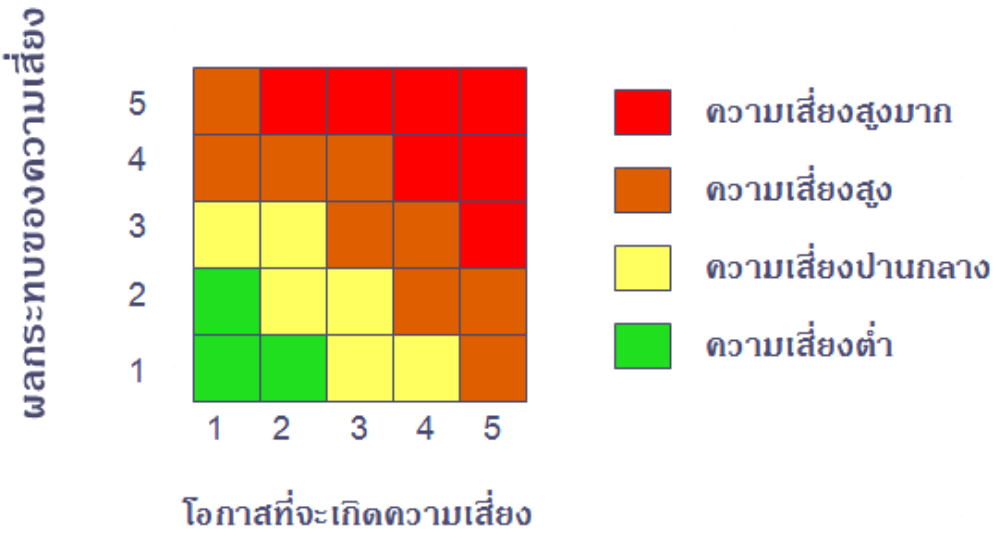
ระดับ	การประเมิน
1	น้อยมาก
2	น้อย
3	ปานกลาง
4	สูง
5	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง มีดังนี้

ระดับ	การประเมิน
1	โอกาสเกิดขึ้นน้อยมาก
2	โอกาสเกิดขึ้นน้อย
3	โอกาสปานกลาง
4	โอกาสสูง
5	โอกาสสูงมาก

การประเมินความเสี่ยง

ระดับของความเสี่ยง (Degree of Risk) COSO ERM 2017



รูปที่ 3 ระดับความเสี่ยง (Degree of Risk) COSO ERM 2017

5) การตอบสนองความเสี่ยง (Risk Response) เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว คณะกรรมการบริหารความเสี่ยงต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับ เพื่อให้การบริหารความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับ เพื่อให้การบริหารเสี่ยงมีประสิทธิผล ผู้บริหารอาจจะต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดโอกาสที่จะเกิดขึ้น และผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการสอบสนองความเสี่ยงมี 4 ประการ คือ

5.1 การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับนำมาซึ่งการเสียโอกาสของหน่วยงานได้

5.2 การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

5.3 การลด/การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาด

5.4 การกระจาย/การถ่ายโอน (Transfer/Sharing) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์ เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกันหรือสัญญาการบำรุงรักษาหลังการขาย

6) กิจกรรมควบคุมความเสี่ยง (Control Activities)

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบความเสี่ยง เพื่อให้สามารถบรรลุเป้าหมายหรือใกล้เคียงกับเป้าที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงอาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภท คือ

6.1 ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

6.2 การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุม เพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

6.3 การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

6.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว

จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง และประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

(1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมากหรือสูง มากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

(2) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

(3) ถ้ามีการควบคุมแล้วให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามต้องการหรือไม่

7) ข้อมูลสารสนเทศและการติดต่อสื่อสาร (Information & Communication)

เป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมินและการบริหารจัดการความเสี่ยง ดังนั้นมหาวิทยาลัยราชภัฏสกลนคร ได้รวบรวมและบันทึกข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งภายนอกและภายในตลอดจนเปิดเผยและสื่อสารอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อช่วยให้บุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยข้องสามารถตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ

8) การติดตาม รายงาน และประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงเมื่อองค์กรทราบความเสี่ยงยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายทางเลือกเพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

8.1 พิจารณาว่ายอมรับความเสี่ยงหรือจะกำหนดกิจกรรมควบคุมเพื่อความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

8.2 เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

8.3 กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

8.4 ในรอบปีต่อไป ให้พิจารณาผลการติดตามการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่นับว่าสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใดและมีวิธีจัดการความเสี่ยงนั้นอย่างไรเสนอผู้บริหารเพื่อทราบและสั่งการ

2.3 ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามแนวทางของ COSO (Committee of Sponsoring Organization) เป็น 8 ประเภท ดังนี้

1) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Rist)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2) ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงเกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม

3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

4) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากการระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Harker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งทำมหาวิทยาลัยฯ อาจถูกฟ้องร้องให้ชำระค่าละเมิดลิขสิทธิ์เป็นต้น

5) ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานนข้มูลต่างๆ ในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูลเพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

6) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศ ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

7) ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

8) ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยงเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนในการดำเนินงานที่ดี

2.3 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร ได้แก่

2.3.1 ปัจจัยภายนอก ได้แก่

1) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่อาจกระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย (Server) ของระบบฐานข้อมูล เช่น ไฟไหม้ และภัยพิบัติ

2) การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่ใช้เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

3) การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

4) ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

5) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

6) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.3.2 ปัจจัยภายใน ได้แก่

1) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2) การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

3) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

2.4 การประเมินความเสียหาย

การประเมินความเสียหายมาจากการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง โดยประเมินโอกาสและผลกระทบที่เกิดขึ้น ที่อาจส่งให้ต้องหยุดระบบประมวลผลทั้งระบบ ตัวอย่างความเสียหายร้ายแรง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส เป็นต้น

2.5 ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยราชภัฏสกลนคร ได้พัฒนาอย่างต่อเนื่องเพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่าย มหาวิทยาลัยราชภัฏสกลนครเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยระบบหลักตั้งอยู่ที่อาคารศูนย์สารสนเทศ (Data Center) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร ถนนสกล-อุดร ตำบลธาตุเชิงชุม อำเภอเมืองสกลนคร จังหวัดสกลนคร

มหาวิทยาลัยราชภัฏสกลนคร ได้มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกัน เพื่อป้องการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่ง ใช้ในการกรอง (Filer Package) ที่ผ่านเข้ามาภายในระบบของมหาวิทยาลัยราชภัฏสกลนคร จากเครือข่ายภายนอก เช่น เครือข่าย Uninet และเครือข่ายของผู้ให้บริการอินเทอร์เน็ตเอกชน นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ที่ทำหน้าที่ป้องกันการบุกรุกในส่วน DMZ ที่ดูแลเครื่องแม่ข่ายทั้งหมดของมหาวิทยาลัยราชภัฏสกลนคร รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่อง

คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือขายของมหาวิทยาลัยราชภัฏสกลนคร มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของมหาวิทยาลัยราชภัฏสกลนคร มีการแบ่ง Subnet เพื่อให้เป็นระบบกลุ่มบรอดคลาสส์โดเมน (Broadcast Domian) เดียวกัน ประกอบกับกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ โดยเฉพาะกรณีเกิดปัญหาการใช้งาน

ระบบเครือข่ายหลักของมหาวิทยาลัยราชภัฏสกลนคร (Core Network) ตั้งอยู่ที่อาคารศูนย์สารสนเทศ (Data Center) ห้องคอมพิวเตอร์แม่ข่ายกลาง (Server Room) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏสกลนคร เป็นศูนย์การเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่ายภายในระดับกอง/สำนักงาน ในความเร็ว 10 Gbps และระบบเครือข่ายภายนอกที่สามารถทดแทนกันได้ (Redundant Network) เพื่อแก้ปัญหาระบบเครือข่ายศูนย์กลางล่ม (Single Point of Failure) และแก้ปัญหาคอขวดในการเข้าถึงข้อมูล (Bottle neck) เพื่อรองรับภารกิจของมหาวิทยาลัยราชภัฏสกลนคร ซึ่งลักษณะงานต้องใช้อุปกรณ์เครือข่ายที่มีประสิทธิภาพสูงสามารถรองรับการเชื่อมต่อกับระบบเครือข่ายภายในและภายนอกแบบ 24 x 7 เพื่อใช้ระบบงานฐานข้อมูลที่สำคัญของมหาวิทยาลัยราชภัฏสกลนคร พร้อมทั้งเชื่อมโยงไปยังอุปกรณ์ Distributed Switch (L3) และ Access Switch (L2) ไปยังอาคารต่างๆ ซึ่งเป็นที่ตั้งของหน่วยงานในมหาวิทยาลัยราชภัฏสกลนคร

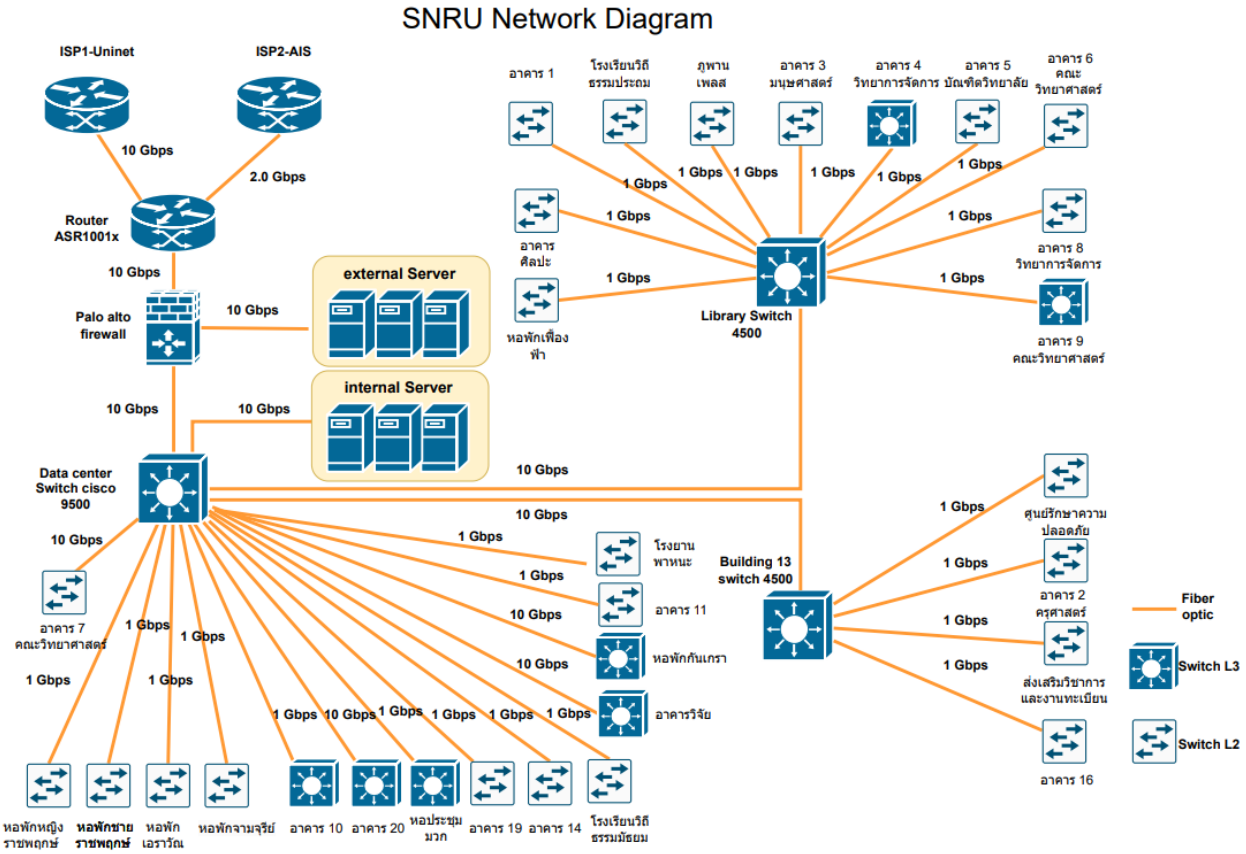
---

[1]Government Information Network (Gin)

[2]โซนเครื่องคอมพิวเตอร์แม่ข่าย (Demilitarized Zone)

[3]มีการแบ่งหมายเลข IP Address เป็นกลุ่มย่อย (Subnet Mask)

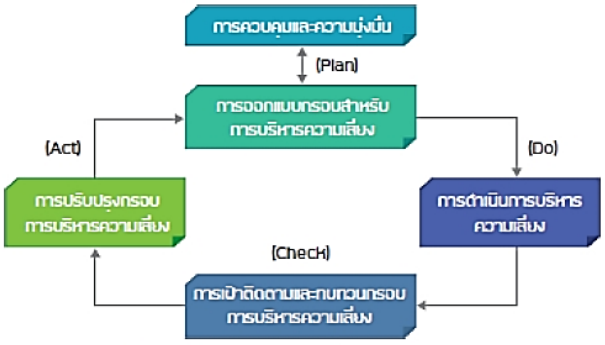
[4]หมายเลขภายใน (Private Address)



รูปที่ 4 แสดงโครงข่ายคอมพิวเตอร์สารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร

2.6 กรอบการบริหารจัดการความเสี่ยง

กรอบการบริหารจัดการความเสี่ยง (Framework for Managing Risk) ตามมาตรฐานการบริหารจัดการความเสี่ยงสากล ISO 31000 แบ่งออกเป็น 4 ส่วน โดยขับเคลื่อนผ่านวงจร PDCA ประกอบด้วย 1) การวางแผน (Plan) 2) การลงมือทำ (Do) 3) การตรวจสอบ (Check) 4) การปรับปรุงแก้ไข (Act)



รูปที่ 5 กรอบการบริหารความเสี่ยง ตามมาตรฐาน ISO31000

2.6.1 การออกแบบกรอบเพื่อการบริหารความเสี่ยง (Plan)

เป็นขั้นตอนการทำงานเข้าใจสภาพแวดล้อมขององค์กร การบริหารความเสี่ยงขององค์กรจะเริ่มต้นจากการทำความเข้าใจในภาพแวดล้อมทั้งภายในและภายนอกขององค์กร โครงสร้างองค์กร การกำหนดนโยบายความต่อเนื่องทางธุรกิจ (Business continuity policy) รวมถึงวัตถุประสงค์ เป้าหมาย กระบวนการและวิธีการปฏิบัติงานที่เกี่ยวข้องกับการจัดการกับความเสี่ยง เพื่อให้สามารถสร้างผลลัพธ์ที่สอดคล้องกับนโยบายและวัตถุประสงค์โดยรวมขององค์กร

2.6.2 การดำเนินการบริหารความเสี่ยง (Do)

การดำเนินการตามกรอบการบริหารความเสี่ยง จะเป็นการลงมือดำเนินการตามนโยบายการควบคุม กระบวนการ และวิธีปฏิบัติ กำหนดช่วงเวลาและกลยุทธ์ที่เหมาะสมสำหรับการดำเนินการ การนำนโยบายและกระบวนการบริหารจัดการความเสี่ยงมาใช้ในกระบวนการต่างๆ การจัดทำเอกสาร การฝึกอบรม การสื่อสารองค์กร ดำเนินการเพื่อให้มั่นใจว่ากระบวนการบริหารความเสี่ยงต่างๆ ได้รับการนำไปปฏิบัติในทุกระดับและหน้าที่งานที่เกี่ยวข้องในองค์กร โดยเป็นส่วนหนึ่งของการปฏิบัติงานขององค์กรและกระบวนการทางธุรกิจ

2.6.3 การเฝ้าติดตามและทบทวนกรอบการบริหารความเสี่ยง (Check)

ในขั้นตอนนี้จะเป็นการประเมินและการวัดผลการดำเนินงานของแต่ละกระบวนการ วัดความก้าวหน้าเทียบแผนการบริหารความเสี่ยงเป็นระยะๆ การทบทวนถึงกรอบการบริหารความเสี่ยง นโยบายและแผนงานอย่างสม่ำเสมอ การจัดทำรายงานความเสี่ยง ความก้าวหน้าของแผนการบริหารความเสี่ยงและการดำเนินการสอดคล้องกับนโยบายการบริหารความเสี่ยง การจัดทำรายงานความเสี่ยง ความก้าวหน้าของแผนการบริหารความเสี่ยง และการดำเนินการสอดคล้องกับนโยบายการบริหารความเสี่ยง การรายงานผลลัพธ์ที่ได้เพื่อนำไปสู่การทบทวนโดยฝ่ายบริหารต่อไป

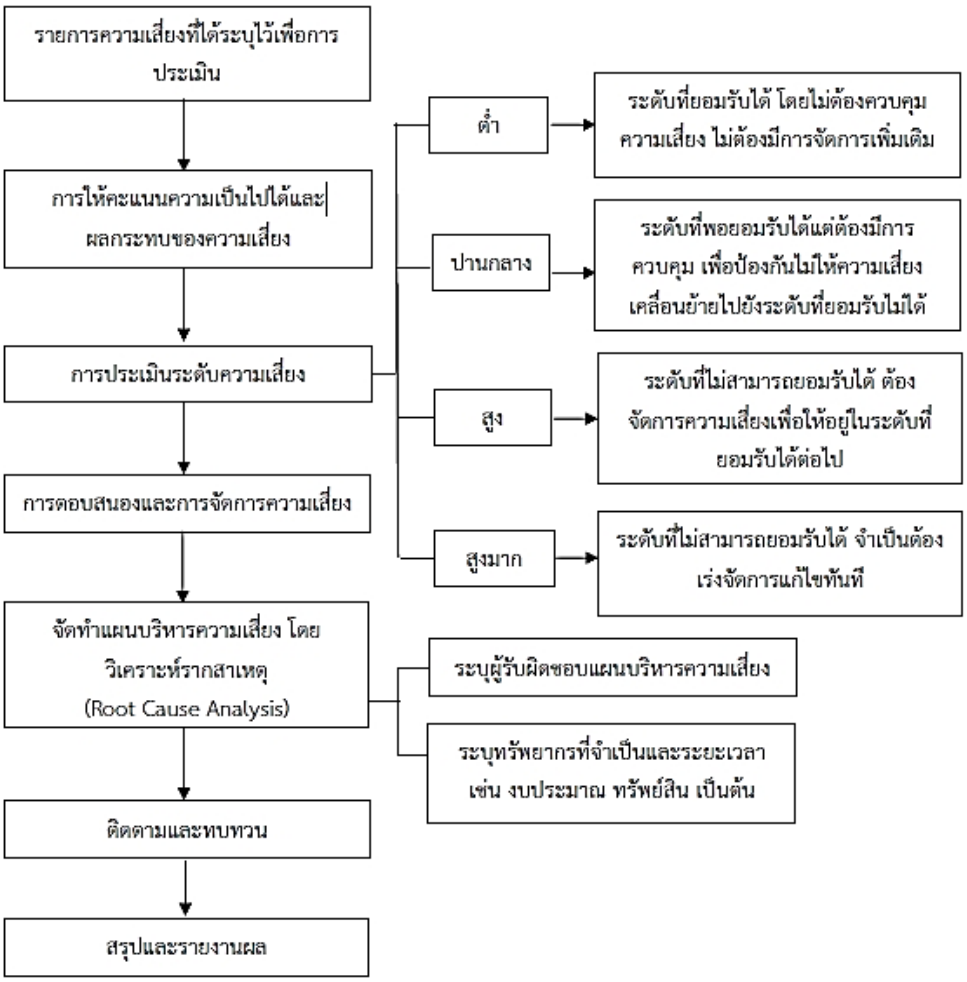
2.6.4 การปรับปรุงกรอบการบริหารความเสี่ยง (Act)

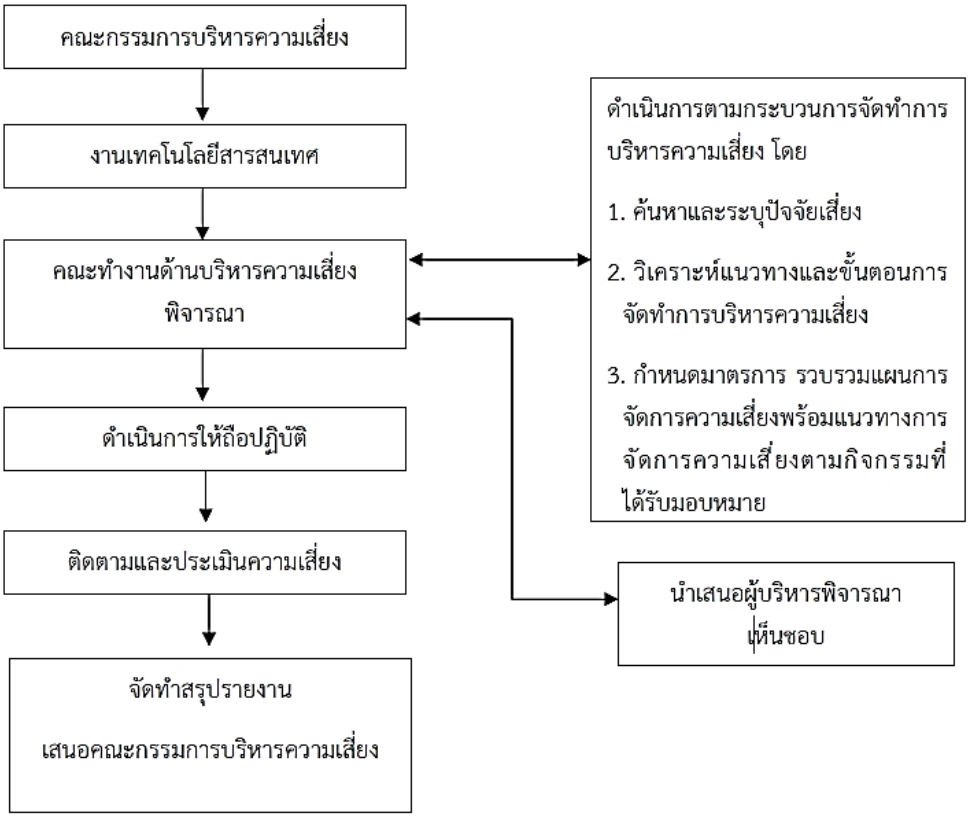
เป็นการดำเนินการปฏิบัติการแก้ไขและป้องกันจากผลการทบทวนโดยฝ่ายบริหาร รวมถึงการดำเนินการปรับปรุงระบบการจัดการความเสี่ยง (Risk Management) ด้วย

บทที่ 3
กระบวนการบริหารความเสี่ยง

มหาวิทยาลัยราชภัฏสกลนคร ได้ตระหนักถึงความสำคัญของข้อมูลและการทำงานของระบบเครือข่ายที่สนับสนุนการปฏิบัติงานของหน่วยงานที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่าง ๆ จึงมอบหมายให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พ.ศ. 2567 – 2570 ให้สอดคล้องกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยงที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

3.1 แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง





มหาวิทยาลัยราชภัฏสกลนคร มีการดำเนินงานในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย และผู้ที่เกี่ยวข้อง ได้แก่ สำนักวิทยบริการและเทคโนโลยี (งานด้านเทคโนโลยีสารสนเทศ) คณะทำงานด้านการบริหารความเสี่ยง ในการดำเนินการตามกระบวนการจัดการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ 3 ขั้นตอน คือ

1. คณะทำงานด้านการบริหารความเสี่ยง พิจารณาในการค้นหาและระบุปัจจัยเสี่ยง วิเคราะห์แนวทางและขั้นตอนการจัดทำการบริหารความเสี่ยง และกำหนดมาตรการ รวบรวมแผนการจัดการความเสี่ยงพร้อมแนวทางการจัดการความเสี่ยงตามกิจกรรมที่ได้รับมอบหมาย
2. คณะทำงานด้านการบริหารความเสี่ยง นำเสนอแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศพร้อมแนวทางการจัดการความเสี่ยงเสนอผู้บริหารพิจารณา
3. คณะกรรมการบริหารความเสี่ยงในระดับมหาวิทยาลัย พิจารณาแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
4. ประกาศใช้และถือปฏิบัติตามแผนบริหารความเสี่ยงและแนวทางการจัดการความเสี่ยง
5. คณะกรรมการบริหารความเสี่ยงระดับมหาวิทยาลัยติดตามและประเมินความเสี่ยง
6. คณะทำงานด้านการบริหารความเสี่ยงจัดทำสรุปรายงานเสนอคณะกรรมการบริหารความเสี่ยงระดับมหาวิทยาลัย

3.2 กำหนดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ในส่วนของมหาวิทยาลัยราชภัฏสกลนคร โดยสำนักวิทยบริการและเทคโนโลยีสารสนเทศ (หน่วยงานผู้ดูแล) ได้วิเคราะห์แล้วว่ามีความเสี่ยงใน 5 ด้าน คือ 1) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม 2) ความเสี่ยงด้านบุคลากร 3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ 4) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ 5) ความเสี่ยงด้านระบบข้อมูล ดังนี้

ลำดับที่	ประเภทความเสี่ยง	ความเสี่ยง
1	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	1. ภัยธรรมชาติ ได้แก่ อัคคีภัย น้ำท่วม แผ่นดินไหว ฟ้าผ่า เป็นต้น
		2. ความชื้นอุณหภูมิห้องคอมพิวเตอร์แม่ข่ายกลาง
2	ความเสี่ยงด้านบุคลากร	3. การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย
		4. การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)
		5. ระบบกระแสไฟฟ้าขัดข้อง
		6. ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย
3	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	7. ระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหายเสื่อมสภาพ
		8. ให้บริการระบบเครือข่ายไร้สายภายนอกหยุดให้บริการ
		9. การถูกโจมตีเครื่องแม่ข่าย (Sever) ทำให้ไม่สามารถให้บริการได้ (Denial of Service-Dos)
		10. การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์
		11. แมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์หรือสายไฟฟ้าสายสัญญาณ
		12. การใช้เข้าเครือข่ายอินทราเน็ตโดยไม่ได้รับอนุญาต
		13. การใช้คอมพิวเตอร์/ระบบเครือข่ายผิดวัตถุประสงค์
4	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	14. การถูกโจมตีระบบจากเครือข่ายภายใน
		15. การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
		16. การถูกบุกรุกจากผู้ไม่ประสงค์ดี/ปล่อยไวรัสคอมพิวเตอร์ (Malware)
		17. การถูกโจรกรรมฐานข้อมูล
		18. การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง
5	ด้านระบบข้อมูล	19. ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้
		20. มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร
		21. การสูญหายของข้อมูล
		22. การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนการบริหารความต่อเนื่อง

ลำดับที่	ประเภทความเสี่ยง	ความเสี่ยง
6	ความเสี่ยงด้านกลยุทธ์	1. กลยุทธ์ด้านการพัฒนาทางเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลง
		2. การกำหนดกลยุทธ์ด้านเทคโนโลยีไม่สอดคล้องกับโลกที่เปลี่ยนแปลงในปัจจุบัน
7	ความเสี่ยงด้านการเงิน	1. งบประมาณสนับสนุนการปรับเปลี่ยนระบบเทคโนโลยีสารสนเทศไม่เพียงพอ
		2. การเบิกจ่ายงบประมาณการจัดซื้อจัดจ้างวัสดุครุภัณฑ์ทางเทคโนโลยีสารสนเทศไม่ทันตามกำหนดเวลา
8	ความเสี่ยงด้านการบริหารจัดการ	1. การบริหารจัดการด้านเทคโนโลยีไม่รัดกุม
		2. ขาดแผนการดำเนินการด้านเทคโนโลยีสารสนเทศที่เหมาะสม

3.3 วิเคราะห์และประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏสกลนคร ได้ระบุความเสี่ยง (Risk identification) โดยชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ผลสรุปการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้และผลกระทบ มีดังนี้

3.2.1 ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) กำหนดไว้ 5 ระดับ ดังนี้

ระดับ	โอกาสที่จะเกิด	เชิงคุณภาพ	เชิงปริมาณ
1	น้อยมาก	มีโอกาสเกิดเกือบทุกครั้ง	ไม่เกิน 1 ครั้งต่อปี
2	น้อย	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ	2 ครั้งต่อปี
3	ปานกลาง	มีโอกาสเกิดบางครั้ง	3 ครั้งต่อปี
4	สูง	อาจมีโอกาสเกิดแต่นานๆ ครั้ง	4 ครั้งต่อปี
5	สูงมาก	มีโอกาสเกิดในกรณียกเว้น	มากกว่า 4 ครั้งต่อปี

3.2.2 ระดับความรุนแรงของผลกระทบ (Impact) กำหนดผลกระทบไว้ 4 ด้าน แต่ละด้านกำหนดเกณฑ์ไว้ 5 ระดับ ดังนี้

(1) ผลกระทบเชิงปริมาณ ด้านการเงิน (Financial)

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
1	น้อยมาก	มีมูลค่าความเสี่ยง ≤ 300,000 บาท
2	น้อย	มีมูลค่าความเสี่ยง › 300,000 ≤ 800,000 บาท
3	ปานกลาง	มีมูลค่าความเสี่ยง › 800,000 ≤ 2,000,000 บาท
4	สูง	มีมูลค่าความเสี่ยง › 2,000,001 ≤ 6,000,000 บาท
5	สูงมาก	มีมูลค่าความเสี่ยง › 6,000,000 บาท

(2) ผลกระทบเชิงคุณภาพ ด้านการดำเนินงานการให้บริการ (Operation)

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
1	น้อยมาก	การให้บริการยังดำเนินการได้ แต่มีแนวโน้มจะหยุดชะงัก ดำเนินการแก้ไขได้ภายใน 15 นาที
2	น้อย	การให้บริการยังดำเนินการได้ แต่มีแนวโน้มจะหยุดชะงัก ดำเนินการแก้ไขได้ภายใน › 15 ≤ 30 นาที
3	ปานกลาง	การให้บริการหยุดชะงัก ดำเนินการแก้ไขได้ภายใน › 30 นาที ≤ 1 ชั่วโมง
4	สูง	การให้บริการหยุดชะงัก ดำเนินการแก้ไขได้ภายใน › 1 ชั่วโมง ≤ 4 ชั่วโมง
5	สูงมาก	การให้บริการหยุดชะงัก ดำเนินการแก้ไขได้ภายใน › 4 ชั่วโมง

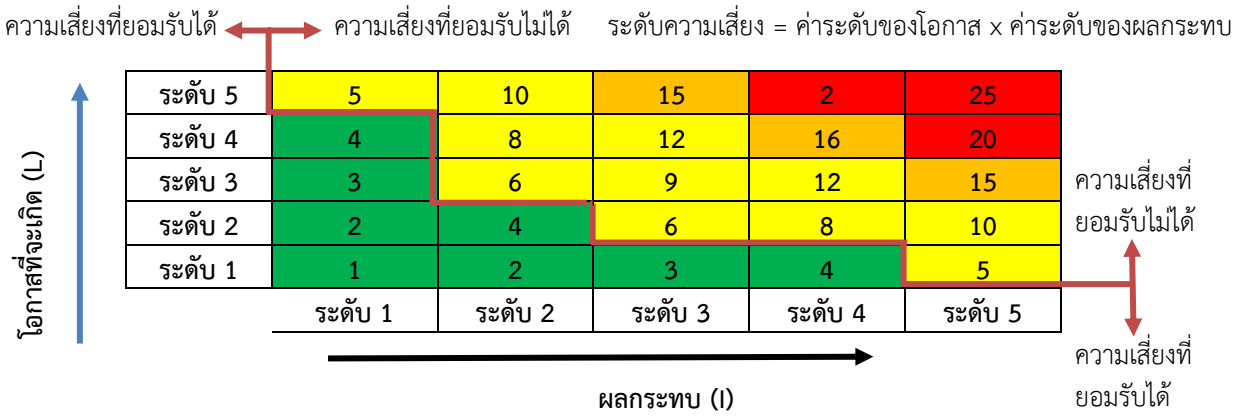
(3) ผลกระทบเชิงคุณภาพ ด้านภาพลักษณ์องค์กร (Reputation)

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
1	น้อยมาก	มีการเผยแพร่ข่าวในวงจำกัดภายในงานที่รับผิดชอบ และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย
2	น้อย	มีการเผยแพร่ข่าวในวงจำกัดภายในสำนักวิทยบริการฯ และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย
3	ปานกลาง	มีการเผยแพร่ข่ายในระดับมหาวิทยาลัย และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย
4	สูง	มีการเผยแพร่ข่าวทั่วทั้งมหาวิทยาลัย และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย
5	สูงมาก	มีการเผยแพร่ข่ายภายนอกมหาวิทยาลัย และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย

(4) ผลกระทบเชิงคุณภาพ ด้านพนักงาน (Employee)

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
1	น้อยมาก	เกิดเหตุการณ์ แต่ไม่ก่อให้เกิดการบาดเจ็บ
2	น้อย	เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บเล็กน้อยหรือพักงาน ≤ 3 วัน
3	ปานกลาง	เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บ พักงาน ≤ 1 เดือน
4	สูง	เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บสาหัส พักงาน ≥ 1 เดือน
5	สูงมาก	เกิดเหตุการณ์ ก่อให้เกิดการเสียชีวิต/สูญเสียอวัยวะ/ทุพพลภาพ

3.2.3 ระดับความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะเกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน



3.2.4 จัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

ตารางที่ 1 เกณฑ์การประเมินระดับความรุนแรงของความเสี่ยง

ระดับ ความรุนแรง	ค่าความเสี่ยง (โอกาส x ผลกระทบ)	เกณฑ์การประเมิน
น้อยมาก	1 - 4	อยู่ในระดับที่ยอมรับได้ ไม่ต้องควบคุมความเสี่ยง ไม่ต้องการมีการจัดการเพิ่มเติม
ปานกลาง	5 - 12	ระดับที่พอยอมรับได้แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	13 - 26	อยู่ในระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้
สูงมาก	17 - 25	อยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการแก้ไขทันที

ตารางที่ 2 ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ	ความเสี่ยง	โอกาสที่จะเกิด	ผลกระทบ				ระดับความเสี่ยง
			การเงิน (F)	การดำเนินงาน (O)	ภาพลักษณ์ (R)	พนักงานงาน (E)	
1	การถูกบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ (Malware)	5	1	1	1	1	ปานกลาง 5x1=5
2	การถูกโจรกรรมฐานข้อมูล	2	5	4	5	1	ปานกลาง 2x5=10
3	การถูกโจมตีเครื่องแม่ข่าย (Sever) ทำให้ไม่สามารถให้บริการได้ (Denial of Service-Dos)	4	5	5	5	1	สูงมาก 4x5=20

ลำดับ	ความเสี่ยง	โอกาสที่จะเกิด	ผลกระทบ				ระดับความเสี่ยง
			การเงิน (F)	การดำเนินงาน (O)	ภาพลักษณ์ (R)	พนักงานงาน (E)	
4	การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์	1	1	5	1	1	ปานกลาง 1x5=5
5	การถูกโจมตีระบบจากเครือข่ายภายใน	5	1	3	2	1	สูง 5x3=15
6	การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)	2	5	3	4	1	ปานกลาง 2x5=10
7	ความชื้น อุณหภูมิห้องคอมพิวเตอร์แม่ข่ายกลาง	1	4	3	1	1	ต่ำ 1x4=4
8	ระบบกระแสไฟฟ้าขัดข้อง	4	4	2	1	3	ปานกลาง 4x4=8
9	ภัยธรรมชาติ เช่น อัคคีภัย น้ำท่วม แผ่นดินไหว ฟ้าผ่า ฯลฯ	2	1	5	1	4	ปานกลาง 2x5=10
10	แมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์หรือสายไฟฟ้า สายสัญญาณ	2	1	5	2	1	ปานกลาง 2x5=10
11	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	2	1	3	5	1	ปานกลาง 2x5=10
12	ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	2	1	1	5	1	ปานกลาง 2x5=10
13	การใช้เข้าเครือข่ายอินทราเน็ตโดยไม่ได้รับอนุญาต	3	1	1	3	1	ปานกลาง 3x3=9
14	มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	3	1	4	4	1	ปานกลาง 3x4=12
15	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนการบริหารความต่อเนื่อง	1	1	4	4	1	ต่ำ 1x4=4
16	การสูญหายของข้อมูล	2	5	4	5	1	ปานกลาง 2x5=10
17	การใช้คอมพิวเตอร์/ระบบเครือข่ายผิดวัตถุประสงค์	3	1	1	2	1	ปานกลาง 3x2=6
18	ระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหายเสื่อมสภาพ	5	4	5	3	1	สูงมาก 5x5=25
19	การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	3	4	1	5	1	สูง 3x5=15
20	ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	3	1	1	1	1	ต่ำ 3x1=3
21	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	3	2	1	5	1	สูง 3x5=15
22	ผู้ให้บริการระบบเครือข่ายไร้สายภายนอกหยุดให้บริการ	5	3	5	5	1	สูงมาก 5x5=25

3.4 ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ระดับความเสี่ยงสูงมาก							
ด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk)	1. ระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหายเสื่อมสภาพ	การทำงานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ขัดข้อง	1. ระบบทำงานไม่สามารถใช้ได้ตามปกติ 2. ข้อมูลเสียหาย	สูงมาก 5x5=25	1.ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล 2.บริหารจัดการสัญญา maintenance ให้เหมาะสม 3.จัดหา Server ใหม่ 4.สร้างระบบ Cluster ขึ้นใช้งาน	การถ่ายโอน (Transfer)	หน.งานพัฒนาระบบสารสนเทศ
ด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk)	2. ผู้ให้บริการระบบเครือข่ายไร้สายภายนอกหยุดให้บริการ	ไม่สามารถใช้งานเครือข่ายได้	1. ลดความน่าเชื่อถือของมหาวิทยาลัย 2. ถูกฟ้องร้องโดยผู้มีส่วนได้ส่วนเสีย	สูงมาก 5x5=25	1. มีระบบเครือข่ายสำรองไว้บริการ	การถ่ายโอน (Transfer)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน
ด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk)	3. การถูกโจมตีเครื่องแม่ข่าย (Sever) ทำให้ไม่สามารถให้บริการได้ (Denial of Service-Dos)	1. โปรแกรมหรือข้อมูลถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูล	1. ข้อมูลสูญหาย 2. สูญเสียรายได้	สูงมาก 4x5=20	1.ทำการ monitor จราจรของระบบเครือข่ายอย่างสม่ำเสมอ เพื่อให้สามารถ Blocked การโจมตีได้ทัน (แผนรับมือเหตุภัยคุกคามทางไซเบอร์) 2.บริหารจัดการสัญญา maintenance ให้เหมาะสม เพื่อให้ได้ข้อมูลเกี่ยวกับ site ที่ทำการโจมตี Dos ที่ใหม่อยู่เสมอ 3.ติดตาม update ฐานข้อมูล Black list ของ Domain ที่เข้าข่ายเป็น Spammer อย่างสม่ำเสมอ	การลดความเสี่ยง (Reduction)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน หน.งานพัฒนาระบบสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ระดับความเสี่ยงสูง							
					4. สำรองข้อมูลระบบและสำรองฐานข้อมูลอย่างสม่ำเสมอ (แผนรองรับสถานการณ์ฉุกเฉิน ปรับปรุงปี 2566) 5. เพิ่มประสิทธิภาพของ firewall โดยทำการเลือกซื้อเครื่องใหม่ให้มี firewall throughput สูงมากขึ้น		
ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	1. การถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครือลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ตั้งใจและตั้งใจ	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้ได้หรือใช้ได้แต่ช้ามาก	สูง 5x3=15	1. กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ 2. การควบคุมด้วยระบบ Desktop Management 3. ทำการ monitor จราจรของระบบเครือข่ายภายในอย่างสม่ำเสมอ เพื่อให้สามารถ Blocked การโจมตีได้ทัน (แผนรับมือเหตุภัยคุกคามทางไซเบอร์)	การควบคุม (Treat)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน
ความเสี่ยงด้านบุคลากร (Human Risk)	2. การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	สิทธิ์ฐานข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศไม่เป็นปัจจุบัน (เนื่องจากผู้ใช้งานมีการลาออก โอน ย้าย สิ้นสุดการจ้างตลอดเวลา)	1.หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน ข้อมูลอาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางที่ผิดกฎหมาย	สูง 3x5=15	1.หน่วยงานในมหาวิทยาลัยดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย (ในกรณีที่ ผู้ใช้งาน ลาออก โอน ย้าย หรือสิ้นสุดการจ้าง) ให้แจ้ง สวท./ผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	การควบคุม (Treat)	-หน่วยงานภายในมหาวิทยาลัยราชภัฏสกลนคร -สำนักวิทยบริการและเทคโนโลยีสารสนเทศ -หน.งานพัฒนาระบบเครือข่ายฯ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
			2.ข้อมูลที่เป็นความลับถูกเผยหรือนำไปใช้จะนำมาซึ่งการขาดความน่าเชื่อถือของหน่วยงานฯ				
ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	3. การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	1.หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	สูง 3x5=15	1.จัดหาซอฟต์แวร์ลิขสิทธิ์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2.สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	การยอมรับความเสี่ยง (Accept)	-หน.งานพัฒนาสมรรถนะดิจิทัลและเรียนรู้สมัยใหม่ -หน.งานบริการคอมพิวเตอร์และฝึกอบรม
ระดับความเสี่ยงปานกลาง							
ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	1.การถูกบุกรุกจากผู้ไม่ประสงค์ดี/ปล่อยไวรัสคอมพิวเตอร์ (Malware)	การถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1.อาจทำให้ระบบเครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย	ปานกลาง 5x1=5	1.ใช้ระบบปฏิบัติการที่ถูกลิขสิทธิ์ซึ่งจะมีโปรแกรมป้องกันไวรัสมาให้ด้วย และ patch อย่างสม่ำเสมอ (แผนรับมือเหตุภัยคุกคามทางไซเบอร์) 2.ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ 3.ติดตั้งระบบป้องและเตือนภัย Spam, Virus, Malware, Trojan	การควบคุมความเสี่ยง (Treat)	งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน
			2.ระบบ/ข้อมูลอาจถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพบน Web Site ของมหาวิทยาลัย 3.อาจถูกโจรกรรมข้อมูลที่เป็นความลับ		1.ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ 2.ติดตั้ง patch ของระบบปฏิบัติการสม่ำเสมอ 3.จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ/เฝ้าระวัง		

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	2. การถูกโจรกรรมฐานข้อมูล	เสี่ยงต่อการสูญหายของข้อมูล	- ข้อมูลสูญหาย - สูญเสียรายได้	ปานกลาง 2x5=10	1.ใช้ระบบปฏิบัติการของ Server ที่ถูกลิขสิทธิ์ซึ่งจะมีโปรแกรมป้องกันไวรัสมาให้ด้วย และ patch อย่างสม่ำเสมอ 2. patch ระบบปฏิบัติการและ service ที่ให้บริการให้ทันสมัยอยู่เสมอ 3. ปิด Service ที่ไม่ใช้งานทั้งหมด 4. เข้ารหัสในการติดต่อสื่อสารกับฐานข้อมูลทุกครั้ง 5. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย	การลดความเสี่ยง (Reduction)	หน.งานพัฒนาระบบสารสนเทศ
ด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk)	3. การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	1.เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง 2.เสียเวลาในการกู้ระบบ 3.เสียภาพลักษณ์ของมหาวิทยาลัยฯ	ปานกลาง 1x5=5	1.ติดตั้งระบบรักษาความปลอดภัยปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย 2.จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน 3.ควบคุมการเข้า-ออกและขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคารตลอดเวลา 4.ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ๆ ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	การบควบคุมความเสี่ยง (Treat)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน หน.งานบริการคอมพิวเตอร์และฝึกอบรม

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ด้านบุคลากร (Human Risk)	4.การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)	การดำเนินการไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ข้อมูลถูกละเมิดอาจก่อให้เกิดอันตรายทั้งต่อร่างกายหรือต่อทรัพย์สิน	ปานกลาง 2x5=10	1.แต่งตั้งคณะกรรมการอำนวยการและคณะกรรมการดำเนินการที่เกี่ยวข้องกับ พรบ.ข้อมูลส่วนบุคคล 2.อบรมให้ความรู้ความเข้าใจเกี่ยวกับนโยบาย ระเบียบและแนวปฏิบัติแก่บุคลากรตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล 3.จัดทำนโยบายระเบียบและแนวปฏิบัติในการจัดการข้อมูลส่วนบุคคล รวมทั้งทบทวนแนวปฏิบัติปีละ 1 ครั้ง	การลดความเสี่ยง (Reduction)	หน.งานพัฒนาสมรรถนะดิจิทัลและเรียนรู้สมัยใหม่
ด้านบุคลากร (Human Risk)	5.ระบบกระแสไฟฟ้าขัดข้อง	1.ระบบกระแสไฟฟ้าขัดข้อง 2.UPS มีอายุการใช้งานมาก ไม่มีระบบการสำรองไฟ/ไม่มีระบบการแจ้งเตือนที่รวดเร็ว	1.ระบบไม่สามารถทำงานได้ 2.ข้อมูล/อุปกรณ์เสียหาย 3.ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายเสียหาย ต้องมีการติดตั้งใหม่	ปานกลาง 4x4=8	1.ตรวจสอบการทำงานระบบสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ 2.วางแผนการจัดหาและติดตั้ง UPS และเครื่องกำเนิดไฟฟ้า (Electrical Generator)	การควบคุมความเสี่ยง (Treat)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	6.ภัยธรรมชาติ ได้แก่ อัคคีภัย น้ำท่วม แผ่นดินไหว ฟ้าผ่า เป็นต้น	1.คอมพิวเตอร์และเครือข่ายถูกทำลาย 2.ข้อมูลถูกทำลาย 3.ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล 3.การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่	1.ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ 2.การให้บริการขาดความต่อเนื่อง 3.เสียงบประมาณการจัดหาระบบทดแทน 4.ไม่สามารถใชงานระบบหว่างที่มีการจัดหาระบบทดแทน	ปานกลาง 2x5=10	1.ตรวจสอบอุปกรณ์ดับเพลิง 2.มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ 3.จัดทำแผนสำรองฉุกเฉินเพื่อรับมือ (ขั้นตอนปฏิบัติ) 4.วางแผนจัดหาและติดตั้งระบบตรวจจับควัน/แจ้งเตือนไฟไหม้ระบบดับเพลิง 5.สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด Dr-Site	การลดความเสี่ยง (Reduction)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน หน.งานพัฒนาระบบสารสนเทศ หน.งานอาคารสถานที่ฯ
ด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk)	7. แมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์หรือสายไฟฟ้า/สายสัญญาณ	เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	1.เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน 2.ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ปานกลาง 2x5=10	1.ไม่ปล่อยให้สายไฟฟ้า/สายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack 2.ไม่นำอาหารหรือเครื่องดื่มมาทาน หรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การลดความเสี่ยง (Reduction)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน หน.งานพัฒนาระบบสารสนเทศ
ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	8.การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	1.ไม่สามารถใช้งานระบบงานของมหาวิทยาลัยผ่านเครือข่ายอินทราเน็ตได้ 2.ไม่สามารถเชื่อมต่อภายนอกมหาวิทยาลัยผ่านเครือข่ายอินเทอร์เน็ตได้	1.ขัดขว้างการปฏิบัติงานของผู้บริหารงาน และเจ้าหน้าที่ 2.บุคคลภายนอกไม่สามารถเข้าใช้ web Server หรือค้นหาข้อมูลที่ต้องการได้	ปานกลาง 2x5=10	1.ควรใช้ผู้บริการอินเทอร์เน็ตอย่างน้อย 2 ผู้ให้บริการ 2.มีแผนในการบำรุงรักษาเครือข่ายภายในองค์กร (Intranet) อย่างสม่ำเสมอ 3.ตรวจสอบระบบเครือข่ายสื่อสารหลัก	การยอมรับความเสี่ยง (Acceptance)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	9.ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องเสีย เช่น Hard Disk หรืออุปกรณ์สำรองข้อมูลประเภทต่างๆ	1.ข้อมูลที่อยู่ในขั้นความลับ รั่วไหลทำให้เสียหายต่อความเชื่อถือของมหาวิทยาลัย 2.ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	ปานกลาง 2x5=10	1.หน่วยงานในมหาวิทยาลัยต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ (ในกรณีที่ผู้ใช้งาน ลาออก โอน ย้าย หรือสิ้นสุดการจ้าง) ให้แจ้ง สวท./หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน 2.มีการบริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk อุปกรณ์สำรองข้อมูลประเภทต่างๆ ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือทำลายข้อมูลบนอุปกรณ์นั้นๆ ก่อนจำหน่าย	การยอมรับความเสี่ยง (Take)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน หน.งานพัฒนาสมรรถนะดิจิทัลและเรียนรู้สมัยใหม่
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware and Data Risk)	10.การใช้เข้าเครือข่ายอินทราเน็ตโดยไม่ได้รับอนุญาต	1.ไม่สามารถใช้งานระบบระบบของมหาวิทยาลัยผ่านเครือข่ายอินเทอร์เน็ตได้ 2.ไม่สามารถเชื่อมต่อภายนอกมหาวิทยาลัยเครือข่ายอินเทอร์เน็ตได้	1.เจ้าหน้าที่ ผู้บริหารมหาวิทยาลัยไม่สามารถใช้งานระบบอินเทอร์เน็ตสำหรับปฏิบัติงานได้ 2.บุคคลภายนอกไม่สามารถเข้าใช้งานข้อมูลสารสนเทศของหน่วยงานผ่านเครือข่าย	ปานกลาง 3x3=9	1.หน่วยงานในมหาวิทยาลัยต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ (ในกรณีที่ผู้ใช้งาน ลาออก โอน ย้าย หรือสิ้นสุดการจ้าง) ให้แจ้ง สวท./ผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	การควบคุมความเสี่ยง (Treat)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					2.ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการเครือข่ายอินเทอร์เน็ตสม่ำเสมอ 3.ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ		
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	11.มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1. การถูกขโมยข้อมูล 2. โปรแกรมเสียหาย 3. การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง	1.ลดความน่าเชื่อถือต่อมหาวิทยาลัยหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2.กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหาต่อมหาวิทยาลัยเป็นอย่างยิ่ง	ปานกลาง 3x4=12	1.ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำ OWASP-Top10 Web Application Security Risks เพื่อลดความเสี่ยง 2.ตั้งมาตรฐานในการดูแลรักษาซอฟต์แวร์ เพื่อให้มีความปลอดภัยตลอดอายุการใช้งาน 1.มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ 2.ตรวจสอบช่องโหว่และดำเนินการปิดช่องโหว่	การยอมรับความเสี่ยง (Acceptance)	หน.งานพัฒนาระบบสารสนเทศ
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	12.การสูญหายของข้อมูล	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล/ดำเนินการสำรองข้อมูล ไม่ต่อเนื่อง	1.ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน 2.ระบบเสียหายไม่สามารถใช้งานและบริการข้อมูลได้	ปานกลาง 2x5=10	1.หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ 2.มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	การควบคุมความเสี่ยง (Treat)	หน.งานพัฒนาระบบสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware and Data Risk)	13.การใช้คอมพิวเตอร์/ระบบเครือข่ายผิดวัตถุประสงค์	1.เสี่ยงต่อการใช้งานในทางที่ผิดหรือเปล่าประโยชน์ เช่น การฟัง วิทยุหรือดูโทรทัศน์ออนไลน์ เป็นต้น 2.การใช้ Resource ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรมภาพยนตร์หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	1.สูญเสีย Bandwidth ในเครือข่าย ทำให้ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี 2.อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	ปานกลาง 3x2=6	1. บริหารจัดการด้วยข้อแนะนำ Ten Ways to Protect Your Network From Insider Threats เพื่อลดความเสี่ยง	การลดความเสี่ยง (Reduction)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน
ระดับความเสี่ยงต่ำ							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	1.ความชื้นอุณหภูมิห้องคอมพิวเตอร์แม่ข่ายกลาง	ระบบปรับอากาศที่ไม่ได้มาตรฐานสำหรับห้องคอมพิวเตอร์แม่ข่าย	การทำงานของเครื่องอายุและอุปกรณ์สั้นลง	ต่ำ 1x4=4	1.ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศ ที่มีอยู่เดิมอย่างสม่ำเสมอ 2.วางแผนจัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	การลดความเสี่ยง (Reduction)	หน.งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	2.การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนการบริหารความต่อเนื่อง	1.เสี่ยงต่อการถูกขโมยข้อมูล 2.เสี่ยงต่อการทำความเสียหายแก่โปรแกรม 3.ไม่สามารถแก้ไขข้อบกพร่องได้เอง	1.ลดความน่าเชื่อถือต่อมหาวิทยาลัย หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2.กรณีเป็นข้อมูลลับอาจสร้างความเสียหายต่อมหาวิทยาลัยอย่างยิ่ง	ต่ำ 1x4=4	1. การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level 2. การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล ER Diagram 3. กำหนดให้ Outsource ต้องส่งมอบ source code และคู่มือในการพัฒนาซอฟต์แวร์แก่หน่วยงานที่จ่ายพัฒนา	การยอมรับความเสี่ยง (Acceptance)	หน.งานพัฒนาระบบสารสนเทศ
ด้านบุคลากร (Human Risk)	3.ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	1.เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อย่างปลอดภัย 2.การใช้ทรัพยากรของหน่วยงานทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	1.ระบบเสียหาย หยุดชะงักการทำงาน 2.สูญเสีย Bandwidth ในเครือข่ายทำให้ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี 3.อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	ต่ำ 3x1=3	1.อบรม สร้างความรู้ความเข้าใจในการใช้งานที่ถูกวิธี 2.กำหนด Policy ของอุปกรณ์รักษา ความปลอดภัยของหน่วยงานให้มีปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอ และการเปิด Port เท่าที่จำเป็น 3.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุมความเสี่ยง (Treat)	หน.งานพัฒนาระบบสารสนเทศ หน.งานพัฒนาสมรรถนะดิจิทัลและเรียนรู้สมัยใหม่

3.5 แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ระยะ 4 ปี (พ.ศ. 2568 – 2571)

หน่วยงาน : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร

ระดับความเสี่ยง ที่จัดทำแผนการบริหารความเสี่ยง : สูง – สูงมาก

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏสกลนคร บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ผู้รับผิดชอบ : งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน งานพัฒนาระบบสารสนเทศ

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงปม. 2568 ต.ค.67 - ก.ย.68			ปีงปม.2569 ต.ค.67 - ก.ย.69			ปีงปม.2570 ต.ค.67 - ก.ย.70			ปีงปม.2571 ต.ค.70 - ก.ย.71			งบประมาณ (บาท)	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
1. ระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย เสื่อมสภาพ	1.ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล	ทุกเดือน	←	–	–	–	–	–	–	–	–	–	–	→	ไม่มีค่าใช้จ่าย	ลดระดับความเสี่ยงลงจาก 25 (สูงมาก) เหลือ 15 (สูง)
	2.บริหารจัดการสัญญา maintenance ให้เหมาะสม	ทุก 6 เดือน					↔			↔			↔		700,000	
	3.จัดหา Server ใหม่	ทุก 3 ปี											↔		350,000	
	4.สร้างระบบ Cluster ขึ้นใช้งาน (เครื่อง Sever แบบที่ 1 /6 ตัว) Server แบบที่ 2/4 ตัว, Storage 2 ชุด)	ระยะ 3 ปี	←	–	–	–	–	–	–	–	–	–	–	→	2,100,000	
2. ผู้ให้บริการระบบเครือข่ายไร้สายภายนอกหยุดให้บริการ	1. มีระบบเครือข่ายสำรองไว้บริการ (วางระบบ access point ทั้งมหาวิทยาลัย จำนวน 1,000 จุด)	ระยะ 3 ปี		←	–	–	–	–	–	–	–	–	–	→	15,000,000	ลดระดับความเสี่ยงลงจาก 25 (สูงมาก) เหลือ 10 (ปานกลาง)
3. การถูกโจมตีเครื่องแม่ข่าย (Sever) ทำให้ไม่สามารถให้บริการได้ (Denial of Service-Dos)	1.ทำการ monitor จราจรของระบบเครือข่ายอย่างสม่ำเสมอ เพื่อให้สามารถ Blocked การโจมตีได้ทัน	ทุกวัน	←	–	–	–	–	–	–	–	–	–	–	→	ไม่มีค่าใช้จ่าย	ลดระดับความเสี่ยงลงจาก 20 (สูงมาก) เหลือ 10 (ปานกลาง)

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงปม. 2568 ต.ค.67 - ก.ย.68			ปีงปม.2569 ต.ค.67 - ก.ย.69			ปีงปม.2570 ต.ค.67 - ก.ย.70			ปีงปม.2571 ต.ค.70 - ก.ย.71			งบประมาณ (บาท)	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
	2.บริหารจัดการสัญญา maintenance ให้เหมาะสม เพื่อให้ได้ข้อมูลเกี่ยวกับ site ที่ทำการโจมตี Dos ที่ใหม่อยู่เสมอ	ทุก 6 เดือน					↔			↔			↔		1,800,000	
	3.ติดตาม update ฐานข้อมูล Black list ของ Domain ที่เข้าข่ายเป็น Spammer อย่างสม่ำเสมอ	ทุก สัปดาห์	←	—	—	—	—	—	—	—	—	—	—	→	ไม่มีค่าใช้จ่าย	
	4. สำรองข้อมูลระบบและสำรองฐานข้อมูลอย่างสม่ำเสมอ (แผนรองรับสถานการณ์ฉุกเฉิน ปรับปรุงปี 2566)	ทุกปี	←	—	—	—	—	—	—	—	—	—	—	→	ไม่มีค่าใช้จ่าย	
	5. เพิ่มประสิทธิภาพของ firewall โดยทำการเลือกซื้อเครื่องใหม่ให้มี firewall throughput สูงมากขึ้น	รอบ 4 ปี											↔		6,000,000	
4. การถูกโจมตีระบบจากเครือข่ายภายใน	1. กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์	ทุกปี	←	—	—	—	—	—	—	—	—	—	—	→	ไม่มีค่าใช้จ่าย	ลดระดับความเสี่ยงลงจาก 15 (สูง) เหลือ 10 (ปานกลาง)
	2. การควบคุมด้วยระบบ Desktop Management	ทุกวัน	←	—	—	—	—	—	—	—	—	—	—	→	ไม่มีค่าใช้จ่าย	
	3. ทำการ monitor จราจรของระบบเครือข่ายภายในอย่างสม่ำเสมอ เพื่อให้สามารถ Blocked การโจมตีได้ทัน	ทุกวัน	←	—	—	—	—	—	—	—	—	—	—	→	ไม่มีค่าใช้จ่าย	

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงปม. 2568 ต.ค.67 - ก.ย.68			ปีงปม.2569 ต.ค.67 - ก.ย.69			ปีงปม.2570 ต.ค.67 - ก.ย.70			ปีงปม.2571 ต.ค.70 - ก.ย.71			งบประมาณ (บาท)	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
5. การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	1.หน่วยงานในมหาวิทยาลัยต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ (ในกรณีที่ผู้ใช้งาน ลาออก โอน ย้าย หรือสิ้นสุดการจ้าง) ให้แจ้ง สวท./หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	ทุก 6 เดือน		↔			↔			↔			↔			ไม่มีค่าใช้จ่าย	ลดระดับความเสี่ยงลงจาก 15 (สูง) เหลือ 9 (ปานกลาง)
6. การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	1.จัดหาซอฟต์แวร์ลิขสิทธิ์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น	ทุกปี			↔			↔			↔			↔	2,500,000	ลดระดับความเสี่ยงลงจาก 15 (สูง) เหลือ 6 (ปานกลาง)
	2.สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ทุกปี	↔			↔			↔			↔			ไม่มีค่าใช้จ่าย	

บทที่ 4

สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานขององค์กรเพื่อให้องค์กรสามารถลดความเสียหายจากความเสี่ยงที่อาจเกิดขึ้นได้มากที่สุด เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานกลไกอันทรงพลังในการขับเคลื่อนการดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานทุกหน่วยงานภายในมหาวิทยาลัย ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาล ข้อมูลเหล่านี้ก็มีความเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายหรือสูญหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กร โดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น ทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้มีมาตรฐานด้านความปลอดภัย ซึ่งก็คือการจัดการความเสี่ยงในองค์กร นั่นเอง

4.1 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

คณะกรรมการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้วิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ มหาวิทยาลัยเผชิญอยู่มีความเสี่ยงอยู่ในระดับสูง และระดับสูงมาก จำนวน 6 ความเสี่ยง จึงได้กำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงในระดับสูงมากและสูง สรุปได้ดังนี้

ความเสี่ยง	แนวทางปฏิบัติ
1. ระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหายเสื่อมสภาพ	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล
	2. บริหารจัดการสัญญา maintenance ให้เหมาะสม
	3. จัดหา Server ใหม่
	4. สร้างระบบ Cluster ขึ้นใช้งาน
2. ผู้ให้บริการระบบเครือข่ายไร้สายภายนอกหยุดให้บริการ	1. มีระบบเครือข่ายสำรองไว้บริการ
3. การถูกโจมตีเครื่องแม่ข่าย (Sever) ทำให้ไม่สามารถให้บริการได้ (Denial of Service-Dos)	1.ทำการ monitor จราจรของระบบเครือข่ายอย่างสม่ำเสมอ เพื่อให้สามารถ Blocked การโจมตีได้ทัน
	2.บริหารจัดการสัญญา maintenance ให้เหมาะสม เพื่อให้ได้ข้อมูลเกี่ยวกับ site ที่ทำการโจมตี Dos ที่ใหม่อยู่เสมอ
	3.ติดตาม update ฐานข้อมูล Black list ของ Domain ที่เข้าข่ายเป็น Spammer อย่างสม่ำเสมอ
	4. สำรองข้อมูลระบบและสำรองฐานข้อมูลอย่างสม่ำเสมอ (แผนรองรับสถานการณ์ฉุกเฉิน ปรับปรุงปี 2566)
4. การถูกโจมตีระบบจากเครือข่ายภายใน	1. กำหนดแนวปฏิบัติการจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์
	2. การควบคุมด้วยระบบ Desktop Management
	3. ทำการ monitor จราจรของระบบเครือข่ายภายในอย่างสม่ำเสมอ เพื่อให้สามารถ Blocked การโจมตีได้ทัน

ความเสี่ยง	แนวทางปฏิบัติ
5. การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	1.หน่วยงานในมหาวิทยาลัยต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ (ในกรณีที่ผู้ใช้งาน ลาออก โอน ย้าย หรือสิ้นสุดการจ้าง) ให้แจ้ง สวท./หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน
6. การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	1.จัดหาซอฟต์แวร์ลิขสิทธิ์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น
	2. สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์ และถูกต้องตามกฎหมาย

4.2 สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

1) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร

2) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศให้มีความเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

3) เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

4.3 ข้อเสนอแนะ

1) การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมโดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมมีความรับผิดชอบ ดังนี้

(1) พิจารณาประสิทธิภาพของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

(2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิภาพของการจัดการความเสี่ยงนั้น

(3) กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

2) การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่อง และดำเนินการอย่างสม่ำเสมอ เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ เป็นไปตามหลักการ PDCA

ภาคผนวก ก

คำสั่งมหาวิทยาลัยราชภัฏสกลนคร ที่ ๖๙๐/๒๕๖๗
เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏสกลนคร
สั่ง ณ วันที่ ๕ กรกฎาคม พ.ศ. ๒๕๖๗

คำสั่งมหาวิทยาลัยราชภัฏสกลนคร

ที่ ๖๙๐/๒๕๖๗

เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏสกลนคร

ด้วยมหาวิทยาลัยราชภัฏสกลนคร ได้คำนึงถึงความสำคัญของการใช้ข้อมูลสารสนเทศ การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติระบบเทคโนโลยีสารสนเทศต่างๆ ซึ่งอาจมีสภาวะความไม่แน่นอนที่ส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงได้แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏสกลนคร เพื่อจัดการความเสี่ยงอย่างเป็นระบบ เตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร

เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏสกลนคร มีการดำเนินการอย่างเป็นรูปธรรมมีความสอดคล้องตรงตามเป้าหมาย จึงแต่งตั้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยราชภัฏสกลนคร ประกอบด้วย

๑. คณะกรรมการอำนวยการ ประกอบด้วย

๑.๑ อธิการบดีมหาวิทยาลัยราชภัฏสกลนคร	ประธานกรรมการ
๑.๒ รองอธิการบดีทุกสายงาน	กรรมการ
๑.๓ คณบดีทุกคณะ	กรรมการ
๑.๔ ผู้อำนวยการสำนัก สถาบัน ทุกสำนัก สถาบัน	กรรมการ
๑.๕ ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	กรรมการและเลขานุการ
๑.๖ หัวหน้าสำนักงานผู้อำนวยการ (สำนักวิทยบริการฯ)	กรรมการและผู้ช่วยเลขานุการ
๑.๗ หัวหน้าหน่วยวินัยและนิติการ	ผู้ช่วยเลขานุการ

หน้าที่

๑) อำนวยการ ประสานงาน สนับสนุน กำกับ ดูแลและให้ความช่วยเหลือในการปฏิบัติตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒) เป็นศูนย์กลางประสานงานความร่วมมือระหว่างหน่วยงานกับคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๓) พิจารณาแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร เพื่อประกาศใช้และถือปฏิบัติ

๒. คณะกรรมการดำเนินงาน ประกอบด้วย

๒.๑ ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	ประธานกรรมการ
๒.๒ รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	กรรมการ
๒.๓ หัวหน้าสำนักงานผู้อำนวยการ (สำนักวิทยบริการฯ)	กรรมการ
๒.๔ หัวหน้างานพัฒนาทรัพยากรสารสนเทศ (สำนักวิทยบริการฯ)	กรรมการ
๒.๕ หัวหน้างานพัฒนาสมรรถนะทักษะดิจิทัลและเรียนรู้สมัยใหม่ (สำนักวิทยบริการฯ)	กรรมการ

/๒.๗ หัวหน้างาน...

๒.๖ หัวหน้างานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน (สำนักวิทยบริการฯ) กรรมการและเลขานุการ

๒.๗ หัวหน้างานพัฒนาระบบสารสนเทศ (สำนักวิทยบริการฯ) กรรมการและผู้ช่วยเลขานุการ

หน้าที่รับผิดชอบ ดังนี้

๑) พิจารณาในการค้นหาและระบุปัจจัยเสี่ยง วิเคราะห์แนวทางและขั้นตอนการจัดทำแผนการบริหารความเสี่ยง กำหนดมาตรการ รวบรวมแผนการจัดการความเสี่ยงพร้อมแนวทางการจัดการความเสี่ยงตามกิจกรรมที่ได้รับมอบหมาย

๒) ประสานการดำเนินงานในการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสเทศ ของมหาวิทยาลัยราชภัฏสกลนคร

๓) แต่งตั้งคณะทำงานเพื่อจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร

๓) นำเสนอแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศพร้อมแนวทางการจัดการความเสี่ยงประกาศใช้และถือปฏิบัติตามแผนบริหารความเสี่ยงและแนวทางการจัดการความเสี่ยง

๔) สรุปรายงานด้านการบริหารความเสี่ยงระดับมหาวิทยาลัย

ทั้งนี้ ตั้งแต่บัดนี้ เป็นต้นไป

สั่ง ณ วันที่ ๕ กรกฎาคม พ.ศ. ๒๕๖๗

(ผู้ช่วยศาสตราจารย์ชาคริต ชาญชิตปรีชา)
อธิการบดีมหาวิทยาลัยราชภัฏสกลนคร