งานเทคโนโลยีสารสนเทศเพื่องานวิชาการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

สารบัญ

สารบัญตาราง

๑. หลักการและเหตุผล

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน เป็นหน่วยงานที่เกิดขึ้นจากการรวมหน่วยงานเดิมของสถาบันเทคโนโลยีราชมงคล วิทยาเขตภาคตะวันออกเฉียงหนือ ๒ หน่วยงานเข้าด้วยกัน ได้แก่ ศูนย์วิทยบริการ และศูนย์คอมพิวเตอร์ จัดตั้งขึ้นตามประกาศกระทรวงศึกษาธิการ เมื่อวันที่ ๒๔ เมษายน พ.ศ. ๒๕๕๐ อาศัยอำนาจตามความในมาตรา ๖ และมาตรา ๙ วรรคสอง แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. ๒๕๔๘ ซึ่งเป็นหน่วยงานที่ให้บริการด้านทรัพยากรสารสนเทศ เพื่อการเรียนการสอนการค้นคว้าวิจัยแก่นักศึกษา คณาจารย์ เจ้าหน้าที่ของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน และบุคคลทั่วไป โดยการนำเทคโนโลยีสารสนเทศที่ทันสมัยและเหมาะสมมาใช้ในการบริการ

เนื่องจากภาระกิจของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีความหลากหลายและรองรับการใช้งานจากหน่วยงานต่างๆ ดังนั้นจึงต้องมีการสำรวจระบบเดิมทีมีอยู่ เพื่อพิจารณาถึงปัจจัยแวดล้อมอย่างครบถ้วน เป็นเสถียรภาพของระบบฮาร์ดแวร์และเครือข่าย ระบบฐานข้อมูล โปรแกรมประยุกต์และบริการต่าง ๆ ระบบรักษาความปลอดภัยของข้อมูล การพัฒนาบุคลากรเพื่อรองรับภารกิจของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ รวมถึงการประชาสัมพันธ์สร้างความเข้าใจให้กับหน่วยงานราชการ ภาคธุรกิจเอกชน และภาคประชาชน ดังนั้นจึงต้องมีระบบบริหารความเสี่ยงของระบบสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน เพื่อหาวิธีการป้องกันปัญหาอันจะส่งผลกระทบต่อระบบสารสนเทศของมหาวิทยาลัยและเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการการบริหารงานของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน แบบบูรณาการเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายต่อระบบสารสนเทศ

๒. วัตถุประสงค์

๒.๑ เพื่อให้ความรู้แก่บุคลากรหรือเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศและเป็นแผนที่ใช้สำหรับคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริง

๒.๒ เพื่อนำแผนบริหารความเสี่ยงฉบับนี้ไปใช้ในการแก้ไขปัญหา การบำรุงรักษาระบบสารสนเทศ การป้องกันสภาวะความเสี่ยงที่ส่งผลกระทบต่อระบบสารสนเทศ การแก้ไขปัญหากรณีสภาวะความเสี่ยง

๓. คำนิยาม

๓.๑ ความเสี่ยง หมายถึง โอกาสเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๓.๒ การวิเคราะห์ความเสี่ยง หมายถึง หลังจากที่ระบุปัจจัยเสี่ยงแล้ว ขั้นต่อไปคือ การวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธี โดยทั่วไปการจะวิเคราะห์ ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิดหรือโอกาสที่จะเกิดความเสี่ยง

๓.๓ การบริหารความเสี่ยง หมายถึง เมื่อทราบความเสี่ยงที่มีนัยสำคัญและโอกาสเกิดความเสี่ยงแล้ว ต้องวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยง และพิจารณาว่าสามารถยอมรับความเสี่ยงนั้นหรือกำหนดกิจกรรมการควบคุมต่าง ๆ เพื่อป้องกัน หรือลดความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้

๔. ความเสี่ยงด้านสารสนเทศ

๔.๑ ประเภทของความเสี่ยงด้านสารสนเทศ

การควบคุมความเสี่ยงด้านสารสนเทศเมื่อพิจารณาแล้วเห็นว่าความเสี่ยงด้านสารสนเทศที่เกี่ยวข้องกับมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน แบ่งออกเป็น ๔ ประเภทหลัก ดังนี้

๔.๑.๑ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (Access Risk) เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานที่รับผิดชอบไม่ได้มีวิธีการจัดการและควบคุมความเสี่ยงด้านการเข้าถึงข้อมูล ที่รอบคอบและรัดกุมเพียงพอแล้ว ส่งผลทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และนำข้อมูลไปใช้ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็มีโอกาสถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น มีผลกระทบทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้านการเข้าถึงข้อมูล สามารถเกิดจากหลายสาเหตุ การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การไม่ได้มีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การไม่ได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์

๔.๑.๒ ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งก่อให้เกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยมีสาเหตุมาจากการที่หน่วยงานที่รับผิดชอบไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอซึ่งส่งผลให้ข้อมูลรวมทั้งการทำงานของระบบคอมพิวเตอร์ ถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็ส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

๔.๑.๓ ความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลได้ (Availability Risk) เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งทำให้การปฏิบัติงานหรือการให้บริการด้านต่างๆเกิดการหยุดชะงักได้ โดยความเสี่ยงนี้เกิดจากการที่ไม่ได้มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้ทำการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้ มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ ถ้าหากไม่ได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้วส่งผล

ให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

๔.๑.๔ ความเสี่ยงเกี่ยวกับการที่ไม่ได้จัดให้มีการบริการสารสนเทศ (Infrastructure Risk) เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานที่รับผิดชอบไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดีรวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการปฏิบัติงาน โดยความเสี่ยงนี้เกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม รวมถึงการที่ไม่ได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินงาน การมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

๔.๒ ขั้นตอนการบริหารจัดการความเสี่ยง

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องมีทั้งการวางแผนเพื่อขจัดหรือลดความเสี่ยง และการประเมินผลในการบริหารจัดการความเสี่ยง เพื่อลดโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และสามารถประเมินเป็นเชิงปริมาณหรือเชิงคุณภาพได้ ซึ่งมีขั้นตอนในการบริหารจัดการความเสี่ยง ๕ ขั้นตอนดังนี้

ขั้นตอนที่ ๑ ขั้นตอนของการระบุความเสี่ยงและผลกระทบที่มีผลกระทบต่อข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร

ขั้นตอนที่ ๒ ขั้นตอนการประเมินถึงความเป็นไปได้ที่เกิดความเสี่ยงและความรุนแรงของผลกระทบ โดยผลกระทบจากผลการประเมินความเสี่ยงที่เกิดขึ้นต่อข้อมูลสารสนเทศ โดยความเสี่ยงนั้นส่งผลกระทบต่อระบบในหลายๆ ด้าน ซึ่งแต่ละความเสี่ยงก็มีความรุนแรงอันก่อให้เกิดความเสียหายแตกต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

ขั้นตอนที่ ๓ ขั้นตอนการวางแผนกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยง เพื่อให้สามารถบรรลุเป้าประสงค์ หรือใกล้เคียงกับเป้าประสงค์ที่กำหนดไว้ ในการวางแผนต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่เกิดขึ้น เพื่อให้สามารถลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้

โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของมหาวิทยาลัยเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ รวมถึงป้องกัน แก้ไข และควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบโดยสามารถดำเนินการตามแผน

ขั้นตอนที่ ๔ ขั้นตอนการติดตามข้อมูลเพื่อทราบร่องรอยของความเสี่ยง ในขั้นตอนนี้ เจ้าหน้าที่รับผิดชอบต้องมีการรวบรวมและรายงานข้อมูลความเสี่ยงในระยะยาวและข้อมูลที่เกี่ยวข้อง เพื่อนำเสนอให้ผู้บังคับบัญชาทราบและมีการทำบันทึกไว้เป็นหลักฐาน

ขั้นตอนที่ ๕ ขั้นตอนการติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยง มีการตรวจสอบการทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของระบบ โดยมีหลักฐานประกอบการปฏิบัติหน้าที่ตามระยะเวลาที่กำหนดให้

๕. แผนบริหารและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ตามแผนบริหารความเสี่ยงของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน เพื่อบริหารจัดการความเสี่ยงด้านสารสนเทศโดยต้อง มีการบริหารความเสี่ยง เพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสื่อสาร และการสำรองและกู้คืนข้อมูลความเสียหาย (Backup and Recovery) มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่เกิดกับระบบสารสนเทศและการสื่อสาร (IT Contingency Plan) มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล ระบบ Anti-Virus ระบบไฟฟ้าสำรอง มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละดับ (Access Rights)

๕.๑ แผนบริหารความเสี่ยง

๕.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าระบบปฏิบัติการ เพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต

๕.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๕.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๕.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) ระบบสารสนเทศและการสื่อสารที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

๕.๑.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๕.๒ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

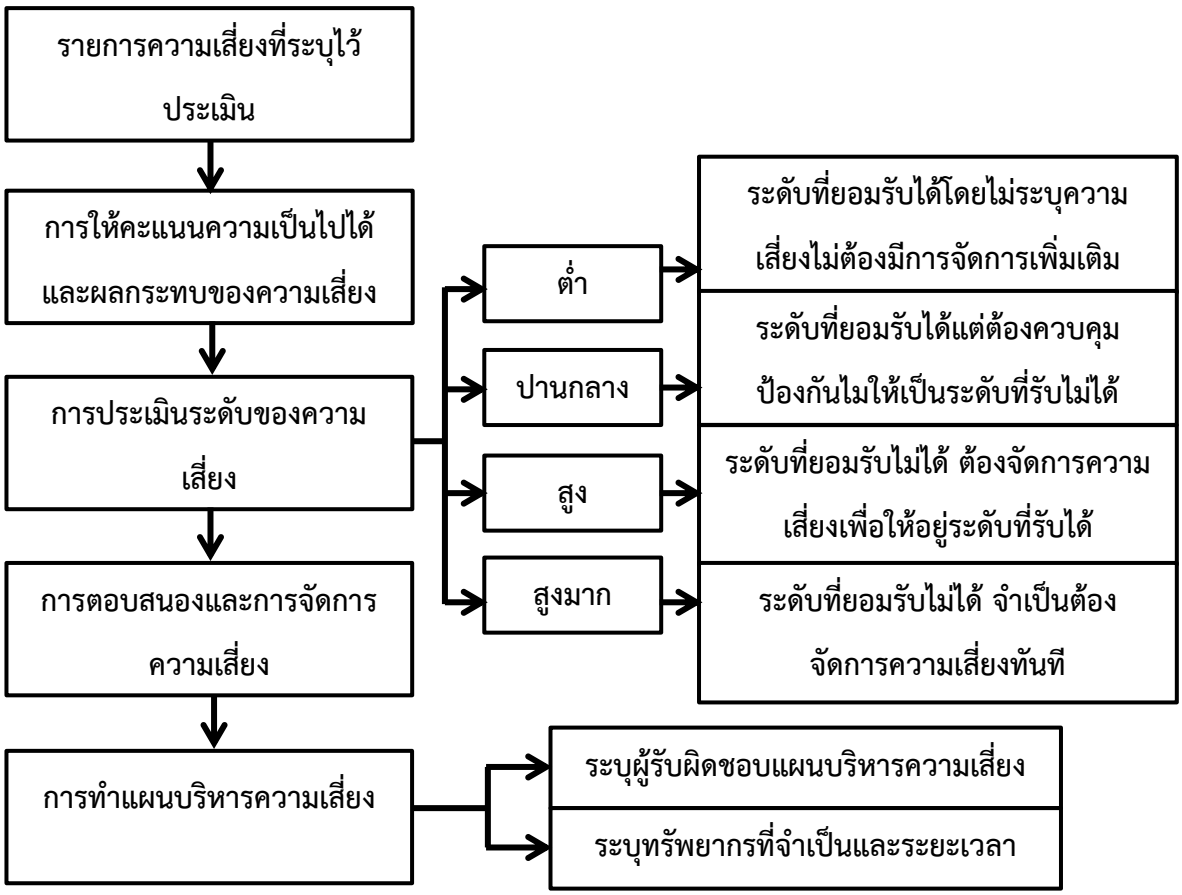
๕.๓ การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๕.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๕.๓.๒ ภัยคุกคามหรือสิ่งที่ก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๕.๓.๓ จุดอ่อนหรือช่องโหว่ที่ถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๕.๔ ขั้นตอนประเมินความเสี่ยง



รูปที่ ๑ ขั้นตอนการประเมินความเสี่ยง

๖. เกณฑ์การประเมินความเสี่ยง

ตารางที่ ๑ ระดับความเสี่ยง

Risk Assessment Matrix	ระดับโอกาส (ความเป็นไปได้)				
	น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
	๑	๒	๓	๔	๕

ผลกระทบ							
	สูงมาก	๕	๕	๑๐	๑๕	๒๐	๒๕
	สูง	๔	๔	๘	๑๒	๑๖	๒๐
	ปานกลาง	๓	๓	๖	๙	๑๒	๑๕
	น้อย	๒	๒	๔	๖	๘	๑๐
	น้อยมาก	๑	๑	๒	๓	๔	๕

ตารางที่ ๒ เกณฑ์การยอมรับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วยแถบสี	ความหมาย
ต่ำ	๑-๓	เขียว	ระดับที่ยอมรับได้ ไม่ต้องควบคุมความเสี่ยง ไม่ต้องจัดการเพิ่มเติม
ปานกลาง	๔-๙	เหลือง	ระดับที่ยอมรับได้แต่ต้องควบคุมป้องกันไม่ให้เป็นระดับที่รับไม่ได้
สูง	๑๐-๑๖	ส้ม	ระดับที่ยอมรับไม่ได้ ต้องจัดการความเสี่ยงเพื่อให้อยู่ระดับที่รับได้
สูงมาก	๑๗-๒๕	แดง	ระดับที่ยอมรับไม่ได้ จำเป็นต้องจัดการความเสี่ยงทันที เพื่อให้อยู่ระดับที่รับได้

ตารางที่ ๓ ระดับโอกาส (ความเป็นไปได้)

ระดับโอกาส (ความเป็นไปได้)	คำนิยาม
๑	นาน ๆ ครั้ง (แทบไม่เกิด)
๒	ไม่บ่อย (มีโอกาสเกิดทุก ๆ ๕ ปี)
๓	ปานกลาง (มีโอกาสเกิดขึ้นทุกปี)
๔	บ่อย (มีโอกาสเกิดขึ้นทุกเดือน)
๕	บ่อยมาก (มีโอกาสเกิดขึ้นทุกวัน)

ตารางที่ ๔ ผลกระทบ (ความรุนแรง)

ผลกระทบ (ความรุนแรง)	คำนิยาม
๑	กระทบต่อความเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการ น้อยมาก (แทบไม่มีผลกระทบ)
๒	กระทบต่อความเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการ น้อย (เจ้าหน้าที่ถูกตำหนิ)
๓	กระทบต่อความเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการ ปานกลาง (เจ้าหน้าที่ถูกร้องเรียน)
๔	กระทบต่อความเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใชบริการ มาก (ผู้บริหารถูกร้องเรียน)
๕	กระทบต่อความเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใชบริการ มากที่สุด (ผู้บริหารถูกลงโทษทางวินัย)

๗. แผนจัดการความเสี่ยง (Risk management action plan)

การจัดการความเสี่ยงจำเป็นต้องคำนึงถึงลำดับความสำคัญและความเร่งด่วนในการจัดการความเสี่ยง โดยให้ความสำคัญและจัดการโดยเร่งด่วนกับกลุ่มความเสี่ยงมาก (สีแดง) ก่อนกลุ่มอื่น ส่วนกลุ่มความเสี่ยงต่ำ ต้องออกมาตราการควบคุม กำกับดูแล ให้อยู่ในระดับที่สามารถยอมรับได้

๗.๑ องค์ประกอบความเสี่ยง

๗.๑.๑ ด้านบุคคลากร

ตารางที่ ๕ องค์ประกอบความเสี่ยงด้านบุคคลากร

องค์ประกอบ	สถานการณ์	ระดับโอกาส	ผลกระทบ	ระดับสี
ผู้ปฏิบัติหน้าที่ด้านสารสนเทศ	ป่วย/ ขาดงานโดยไม่แจ้ง	๓	๑	เขียว
	อุบัติเหตุ	๓	๑	เขียว
	ติดภารกิจด่วน	๒	๑	เขียว
	ทำผิดขั้นตอนจนระบบเสียหาย	๓	๓	เหลือง
	ย้าย/เพิ่ม/แก้ไข ข้อมูลผิดพลาด	๒	๔	เหลือง
	มอบสิทธิ์ให้ผู้ไม่เกี่ยวข้อง	๑	๔	เหลือง
ผู้ดูแลระบบสารสนเทศ	ป่วย/ ขาดงานโดยไม่แจ้ง	๑	๒	เขียว
	อุบัติเหตุ	๒	๔	เหลือง
	ติดภารกิจด่วน	๒	๒	เหลือง
	ไม่ตรวจสอบการสำรองข้อมูล	๒	๕	ส้ม

องค์ประกอบ	สถานการณ์	ระดับโอกาส	ผลกระทบ	ระดับสี
	Start up ระบบผิดพลาด	๒	๔	เหลือง
	ประมาทในการรักษาความปลอดภัย	๒	๕	ส้ม
	มอบสิทธิ์ให้ผู้ไม่เกี่ยวข้อง	๑	๔	เหลือง
	ไม่ดูแลรักษาอุปกรณ์ที่เกี่ยวข้อง	๒	๕	ส้ม
	ไม่ตรวจสอบประสิทธิภาพของระบบ	๑	๔	เหลือง
บุคคลภายนอก	เข้ามาใช้โดยไม่มีสิทธิ์	๑	๕	เหลือง
	เข้ามาโจมตีระบบ	๔	๕	แดง
	เข้ามาทำลายข้อมูล	๓	๕	ส้ม
	แพร่กระจายไวรัสคอมพิวเตอร์	๒	๕	ส้ม

๗.๑.๒ ด้านเครื่องแม่ข่ายและอุปกรณ์

ตารางที่ ๖ องค์ประกอบความเสี่ยงด้านเครื่องแม่ข่ายและอุปกรณ์

องค์ประกอบ	สถานการณ์	ระดับโอกาส	ผลกระทบ	ระดับสี
Server	Server ไม่ทำงาน/ ไม่ Start up	๒	๕	ส้ม
	หยุดทำงานโดยไม่ทราบสาเหตุ	๒	๕	ส้ม
	ภายในห้องมีอุณหภูมิสูง	๒	๔	เหลือง
	ภายในห้องมีฝุ่นละอองเยอะ	๒	๒	เหลือง
	อุบัติเหตุจากภัยทางธรรมชาติ	๑	๕	เหลือง
Switch/ Router	จุดต่อหลุดโดยอุบัติเหตุ	๑	๓	เขียว
	Switch เสีย	๒	๕	เหลือง
	ช่อง Port เสีย	๒	๒	เหลือง
External Hard disk	Disk เกิด Bad	๒	๒	เหลือง
	ห้องมีอุณหภูมิสูง	๒	๔	เหลือง
	Connect ไป Server ไม่ได้	๒	๓	เหลือง
	อุปกรณ์ต่อพ่วงใช้งานไม่ได้	๑	๑	เขียว
เครื่องสำรองไฟ	เกิดข้อผิดพลาดในการจ่ายไฟฟ้า	๒	๕	ส้ม
	ไม่มีการสำรองไฟเมื่อเกิดไฟดับ	๔	๕	แดง
	ห้องมีอุณหภูมิสูง	๒	๔	เหลือง

๗.๑.๓ ด้านการเชื่อมโยงเครือข่าย

ตารางที่ ๗ องค์ประกอบความเสี่ยงด้านการเชื่อมโยงเครือข่าย

องค์ประกอบ	สถานการณ์	ระดับโอกาส	ผลกระทบ	ระดับสี
สาย LAN	สาย LAN โดนความร้อน/ ไฟ	๑	๓	เขียว
	สาย LAN ขาดใน	๑	๓	เขียว
	สาย LAN ถูกหนู/ แมลง กัดสาย	๑	๓	เขียว
Wireless	Wireless ไม่สามารถส่งสัญญาณได้	๒	๔	เหลือง
	Wireless ไม่สามารถรับสัญญาณได้	๒	๔	เหลือง
	AP ไม่สามารถ Connect WLC ได้	๒	๔	เหลือง
Lead Line	ไม่สามารถเชื่อมต่อสัญญาณได้	๒	๕	ส้ม

๗.๑.๔ ด้านโปรแกรม

ตารางที่ ๘ องค์ประกอบความเสี่ยงด้านโปรแกรม

องค์ประกอบ	สถานการณ์	ระดับโอกาส	ผลกระทบ	ระดับสี
Software ระบบ	Software License Expire	๒	๔	เหลือง
	Software ละเมิดลิขสิทธิ์	๒	๔	เหลือง
	Software ล้าสมัย	๑	๔	เหลือง
	Software ติดไวรัส	๒	๔	เหลือง
Software ประยุกต์	Software License Expire	๒	๔	เหลือง
	Software ละเมิดลิขสิทธิ์	๓	๔	ส้ม
	Software ล้าสมัย	๑	๔	เหลือง

๗.๑.๕ ด้านระบบงานและข้อมูล

ตารางที่ ๙ องค์ประกอบความเสี่ยงด้านระบบงานและข้อมูล

องค์ประกอบ	สถานการณ์	ระดับโอกาส	ผลกระทบ	ระดับสี
ระบบสารสนเทศ	มี File โดนลบ / ทำลาย	๒	๕	ส้ม
	ระบบติดไวรัส	๑	๔	เหลือง
	ระบบหยุดทำงานโดยไม่ทราบสาเหตุ	๑	๕	เหลือง
	ข้อผิดพลาด Application	๑	๔	เหลือง
ระบบฐานข้อมูล	โดน Hacker ลบ/แก้ไข ข้อมูล	๒	๕	ส้ม
	ไม่สามารถสำรองข้อมูลได้	๒	๕	ส้ม

	ไม่สามารถกู้คืนข้อมูลได้	๓	๕	ส้ม
	ข้อมูลไม่ถูกต้อง	๒	๔	เหลือง

๗.๑.๖ ด้านกายภาพและสิ่งแวดล้อม

ตารางที่ ๑๐ องค์ประกอบความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

องค์ประกอบ	สถานการณ์	ระดับโอกาส	ผลกระทบ	ระดับสี
ระบบปรับอากาศ	ระบบปรับอากาศไม่ทำงาน	๒	๔	เหลือง
	เครื่องไม่ทำความเย็น	๒	๔	เหลือง
	ไฟฟ้าลัดวงจร	๑	๕	เหลือง
	เกิดการชำรุดเสียหาย	๒	๕	ส้ม
ภัยธรรมชาติ	น้ำท่วม	๑	๔	เหลือง
	ไฟไหม้	๒	๕	ส้ม
	พายุ	๒	๔	เหลือง
	แผ่นดินไหว	๑	๕	เหลือง
ภัยสงคราม	เกิดวินาศกรรม	๑	๕	เหลือง
	เกิดการจลาจล	๑	๔	เหลือง
	การประท้วงปิดที่ทำการ	๑	๔	เหลือง

๗.๒ แผนจัดการความเสี่ยง

แผนจัดการความเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของการควบคุมมีอยู่ด้วยกัน ๓ ด้าน คือด้านการดำเนินงาน (O) ด้านการเงิน (F) และด้านการปฏิบัติ กฎหมาย กฎระเบียบ (C)

ตารางที่ ๑๑ แผนจัดการความเสี่ยงด้านบุคคลากร

องค์ประกอบ	เหตุการณ์	มาตราการป้องกัน	ผู้รับผิดชอบ
ผู้ปฏิบัติหน้าที่ด้านสารสนเทศ	ป่วย/ ขาดงานโดยไม่แจ้ง อุบัติเหตุ ติดภารกิจด่วน	มีเจ้าหน้าที่ทำงานทดแทน	หน่วยงานต้นสังกัด
	ทำผิดขั้นตอนจนระบบเสียหาย	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
	ย้าย/เพิ่ม/แก้ไข ข้อมูลผิดพลาด	จัดอบรมให้ความรู้เพิ่เติม	หน่วยงานต้นสังกัด
	มอบสิทธิ์ให้ผู้ไม่เกี่ยวข้อง	กำหนดผู้รับผิดชอบอย่างชัดเจน	ผู้ดูแลระบบ

ผู้ดูแลระบบสารสนเทศ	ป่วย/ ขาดงานโดยไม่แจ้ง อุบัติเหตุ/ ติดภารกิจด่วน	มีเจ้าหน้าที่ทำงานทดแทน	หน่วยงานต้นสังกัด
	ไม่ตรวจสอบการสำรองข้อมูล	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
	Start up ระบบผิดพลาด	จัดอบรมให้ความรู้เพิ่เติม	หน่วยงานต้นสังกัด
	ประมาทในการรักษาความปลอดภัย	ติดตั้งระบบรักษาความปลอดภัย	ผู้ดูแลระบบ
	มอบสิทธิ์ให้ผู้ไม่เกี่ยวข้อง	กำหนดผู้รับผิดชอบอย่างชัดเจน	หน่วยงานต้นสังกัด
	ไม่ดูแลรักษาอุปกรณ์ที่เกี่ยวข้อง	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
	ไม่ตรวจสอบประสิทธิภาพของระบบ	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
บุคคลภายนอก	เข้ามาใช้โดยไม่มีสิทธิ์	กำหนดสิทธิ์การใช้งาน	ผู้ดูแลระบบ
	เข้ามาโจมตีระบบ	ติดตั้งระบบรักษาความปลอดภัย	ผู้ดูแลระบบ
	เข้ามาทำลายข้อมูล	ติดตั้งระบบรักษาความปลอดภัย	ผู้ดูแลระบบ
	แพร่กระจายไวรัสคอมพิวเตอร์	ติดตั้งโปรแกรมป้องกันไวรัส	ผู้ดูแลระบบ

ตารางที่ ๑๒ แผนจัดการความเสี่ยงด้านเครื่องแม่ข่ายและอุปกรณ์

องค์ประกอบ	เหตุการณ์	มาตราการป้องกัน	ผู้รับผิดชอบ
Server	Server ไม่ทำงาน/ ไม่ Start up	มีเครื่องสำรองให้บริการ	ผู้ดูแลระบบ
	หยุดทำงานโดยไม่ทราบสาเหตุ	ดูแลให้พร้อมใช้งานอยู่เสมอ	ผู้ดูแลระบบ
	ภายในห้องมีอุณหภูมิสูง	ใช้ระบบปรับอากาศที่มีมาตราฐาน	หน่วยงานต้นสังกัด
	ภายในห้องมีฝุ่นละอองเยอะ	กำหนดผู้รับผิดชอบอย่างชัดเจน	หน่วยงานต้นสังกัด
	อุบัติเหตุจากภัยทางธรรมชาติ	จัดให้มีระบบสำรองข้อมูล	หน่วยงานต้นสังกัด
Switch/ Router	จุดต่อหลุดโดยอุบัติเหตุ	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	ผู้ดูแลระบบ
	Switch เสีย	มีเครื่องสำรองให้บริการ	ผู้ดูแลระบบ
	ช่อง Port เสีย	มี Port สำรองให้บริการ	ผู้ดูแลระบบ

External Hard disk	Disk เกิด Bad	จัดให้มีระบบสำรองข้อมูล	ผู้ดูแลระบบ
	ห้องมีอุณหภูมิสูง	ใช้ระบบปรับอากาศที่มีมาตราฐาน	หน่วยงานต้นสังกัด
	Connect ไป Server ไม่ได้	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
	อุปกรณ์ต่อพ่วงใช้งานไม่ได้	จัดให้มีอุปกรณ์สำรอง	หน่วยงานต้นสังกัด
เครื่องสำรองไฟ	เกิดข้อผิดพลาดในการจ่ายไฟฟ้า	ติดตั้งระบบตัดวงจรอัตโนมัติ ติดตั้งระบบสายดิน	หน่วยงานต้นสังกัด
	ไม่มีการสำรองไฟเมื่อเกิดไฟดับ	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
	ห้องมีอุณหภูมิสูง	ใช้ระบบปรับอากาศที่มีมาตราฐาน	หน่วยงานต้นสังกัด

ตารางที่ ๑๓ แผนจัดการความเสี่ยงด้านการเชื่อมโยงเครือข่าย

องค์ประกอบ	เหตุการณ์	มาตราการป้องกัน	ผู้รับผิดชอบ
สาย LAN	สาย LAN โดนความร้อน/ไฟ	กำหนดผังแนวเดินสาย LAN	ผู้ดูแลระบบ
	สาย LAN ขาดใน	เดินท่อร้อยสาย LAN	ผู้ดูแลระบบ
	สาย LAN ถูกหนู/ แมลงกัดสาย	จัดหาอุปกรณ์ป้องกันและกำจัด	ผู้ดูแลระบบ
Wireless LAN	Wireless ไม่สามารถส่งสัญญาณได้	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	ผู้ดูแลระบบ
	Wireless ไม่สามารถรับสัญญาณได้	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	ผู้ดูแลระบบ
	AP ไม่สามารถ Connect WLC ได้	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	ผู้ดูแลระบบ
Lead line	ไม่สามารถเชื่อมต่อสัญญาณได้	มีระบบ Monitoring	ผู้ดูแลระบบ

ตารางที่ ๑๔ แผนจัดการความเสี่ยงด้านด้านโปรแกรม

องค์ประกอบ	เหตุการณ์	มาตราการป้องกัน	ผู้รับผิดชอบ
Software	Software License Expire	จัดทำโครงการจัดซื้อซอฟต์แวร์	หน่วยงานต้นสังกัด

	Software ละเมิดลิขสิทธิ์	จัดทำระเบียบ มาตราการที่ชัดเจน	หน่วยงานต้นสังกัด
	Software ล้าสมัย	มั่นอัพเดทให้เป็นปัจจุบัน	ผู้ดูแลระบบ
	Software ติดไวรัส	ติดตั้งโปรแกรมป้องกันไวรัส	ผู้ดูแลระบบ

ตารางที่ ๑๕ แผนจัดการความเสี่ยงด้านระบบงานและข้อมูล

องค์ประกอบ	เหตุการณ์	มาตราการป้องกัน	ผู้รับผิดชอบ
ระบบสารสนเทศ	มี File โดนลบ / ทำลาย	จัดให้มีระบบสำรองข้อมูล	หน่วยงานต้นสังกัด
	ระบบติดไวรัส	ติดตั้งโปรแกรมป้องกันไวรัส	ผู้ดูแลระบบ
	ระบบหยุดทำงานโดยไม่ทราบสาเหตุ	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
	ข้อผิดพลาด Application	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	ผู้ดูแลระบบ
ระบบฐานข้อมูล	โดน Hacker ลบ/แก้ไขข้อมูล	ติดตั้งระบบรักษาความปลอดภัย	ผู้ดูแลระบบ
	ไม่สามารถสำรองข้อมูลได้	จัดให้มีระบบสำรองข้อมูล	หน่วยงานต้นสังกัด
	ไม่สามารถกู้คืนข้อมูลได้	ทดสอบระบบสำรองข้อมูลเป็นระยะ	ผู้ดูแลระบบ
	ข้อมูลไม่ถูกต้อง	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด

ตารางที่ ๑๖ แผนจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

องค์ประกอบ	เหตุการณ์	มาตราการป้องกัน	ผู้รับผิดชอบ
ระบบปรับอากาศ	ระบบปรับอากาศไม่ทำงาน	จัดทำคู่มือขั้นตอนการปฏิบัติงาน	หน่วยงานต้นสังกัด
	เครื่องไม่ทำความเย็น	จัดทำแผนบำรุงรักษา	ผู้ดูแลระบบ
	ไฟฟ้าลัดวงจร	จัดทำระบบตัดวงจรอัตโนมัติ	หน่วยงานต้นสังกัด
	เกิดการชำรุดเสียหาย	จัดทำแผนบำรุงรักษา	หน่วยงานต้นสังกัด
ภัยธรรมชาติ	น้ำท่วม	เลือกสถานที่ตั้งให้เหมาะสม	หน่วยงานต้นสังกัด
	ไฟไหม้	จัดให้มีระบบดับเพลิง	หน่วยงานต้นสังกัด
	พายุ	โครงสร้างอาคารป้องกันพายุ	หน่วยงานต้นสังกัด
	แผ่นดินไหว	โครงสร้างอาคารรองรับแผ่นดินไหว	หน่วยงานต้นสังกัด
ภัยสงคราม	เกิดวินาศกรรม	จัดให้มีศูนย์คอมพิวเตอร์สำรอง	หน่วยงานต้นสังกัด
	เกิดการจลาจล	จัดให้มีศูนย์คอมพิวเตอร์สำรอง	หน่วยงานต้นสังกัด

องค์ประกอบ	เหตุการณ์	มาตราการป้องกัน	ผู้รับผิดชอบ
	การประท้วงปิดที่ทำการ	จัดให้มีศูนย์คอมพิวเตอร์สำรอง	หน่วยงานต้นสังกัด

๘. แนวทางกำกับดูแลป้องกันความเสี่ยง

๘.๑ ด้านบุคคลากร

๘.๑.๑ ผู้ดูแลระบบสารสนเทศและผู้ปฏิบัติหน้าที่ด้านสารสนเทศ มีแนวทางกำกับดูแลป้องกันความเสี่ยงดังนี้

๑) จัดตั้งคณะทำงานผู้รับผิดชอบด้านต่างๆ

๒) จัดโครงสร้างสายการปฏิบัติงานและมอบหมายงานให้ชัดเจน

๓) ฝึกอบรมเจ้าหน้าที่เฉพาะด้านเพื่อให้เกิดความเชี่ยวชาญ

๔) กำหนดผู้รับผิดชอบร่วมในเรื่องที่ยังขาดความชำนาญ

๕) จัดให้มีการติดตามและประเมินผล

๘.๑.๒ ผู้ใช้งานทั่วไปและบุคคลภายนอก มีแนวทางกำกับดูแลป้องกันความเสี่ยงดังนี้

๑) จำแนกกลุ่มผู้ใช้ให้ชัดเจน

๒) จัดทำคู่มือและวิธีการใช้งาน

๓) ติดตั้งระบบรักษาความปลอดภัย ป้องกันการถูกโจมตี

๔) ติดตั้งโปรแกรมป้องกันไวรัส

๕) กำหนดนโยบายรักษาความปลอดภัยที่เหมาะสม

๖) กำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้

๘.๒ ด้านเครื่องแม่ข่ายและอุปกรณ์

๘.๒.๑ Server เมื่อเครื่องแม่ข่ายหยุดการให้บริการ เสียหาย ไม่สามารถใช้งานได้ตามปกติ ให้ตรวจสอบ ฮาร์ดแวร์และระบบไฟฟ้า ตรวจสอบระบบปฏิบัติการ ถ้าระบบปฏิบัติการไม่สามารถทำงานได้ให้ทำการติดตั้งระบบปฏิบัติการใหม่ ติดตั้งโปรแกรมประยุกต์ทั้งหมด ติดตั้งข้อมูลที่สำรองไว้กลับสู่ระบบแล้ว ตรวจสอบเซอร์วิสต่างๆ และทดสอบการทำงานของเครื่องแม่ข่าย

๘.๒.๒ Switch ตัวกระจายสัญญาณเสียหาย ไม่สามารถใช้งานได้ตามปกติ ให้ตรวจสอบ ฮาร์ดแวร์และระบบไฟฟ้า เมื่อพบอุปกรณ์ชำรุดให้จัดหาอุปกรณ์สำรองทดแทน

๘.๒.๓ เครื่องสำรองไฟฟ้า จัดหาอุปกรณ์ ไฟฟ้าสำรอง (UPS) สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างเพียงพอ ติดตั้งระบบสายดิน ติดตั้งระบบป้องกันไฟกระชาก ตรวจเช็คระบบให้สามารถใช้ได้อย่างสม่ำเสมอ

๘.๓ ด้านการเชื่อมโยงเครือข่าย

๘.๓.๑ สาย LAN ตรวจเช็คสายนำสัญญาณอย่างสม่ำเสมอ เมื่อเดินสายสัญญาณใหม่ต้องร้อยท่อป้องกันสาย จัดหาสายนำสัญญาณและอุปกรณ์สำรองต่อการซ่อมแซมและขยายจุดเชื่อมต่อ

๘.๓.๒ Wireless ตรวจสอบอุปกรณ์การรับส่งสัญญาณได้เป็นปกติ เมื่อพบอุกรณ์ไม่ทำงานให้ทำการตรวจเช็คตัวอุปกรณ์ระบบไฟฟ้าและอัพเดทซอฟต์แวร์ให้เป็นปัจจุบัน เพื่อเชื่อมต่อไปยัง Controller หากอุปกรณ์ที่เป็น Stand alone ให้กำหนดเงื่อนไขการใช้งานชัดเจนเพื่อไม่ให้ส่งผลกระทบต่อระบบเครือข่ายในภาพรวมทั้งหมด

๘.๓.๓ Leased line สัญญาณการเชื่อมต่อจัดให้มีระบบ Monitoring สถานะการทำงานของเครือข่าย เมื่อไม่สามารถเชื่อมต่อสัญญาณได้ ให้หาสาเหตุแล้วแจ้งผู้เกี่ยวข้องดำเนินการแก้ไขทันที

๘.๔ ด้านด้านโปรแกรม

๘.๔.๑ โปรแกรมระบบปฏิบัติการ จัดหาโปรแกรมลิขสิทธิ์ให้เหมาะสมเพียงพอต่อการใช้งาน อัพเดทปรับปรุงซอฟต์แวร์ให้เป็นปัจจุบันเสมอ จัดหาซอฟต์ Open source เพื่อลดค่าใช้จ่ายและทดแทนโปรแกรมลิขสิทธิ์ และติดตั้งโปรแกรมป้องกันไวรัส

๘.๔.๒ โปรแกรมประยุกต์ จัดหาโปรแกรมประยุกต์ให้เหมาะสมเพียงพอต่อการใช้งาน อัพเดทปรับปรุงซอฟต์แวร์ให้เป็นปัจจุบันเสมอ จัดหาซอฟต์ Open source เพื่อลดค่าใช้จ่ายและทดแทนโปรแกรมลิขสิทธิ์ และติดตั้งโปรแกรมป้องกันไวรัส

๘.๕ ด้านระบบงานและข้อมูล

๘.๕.๑ ระบบสารสนเทศ ตรวจสอบการทำงานของระบบอย่างเสมอ ทำการสำรองข้อมูลแบบ Full backup ทำการทดสอบการสำรองข้อมูลให้สามารถนำกลับมาใช้งานได้ในกรณีเกิดเหตุฉุกเฉิน ติดตั้งระบบรักษาความปลอดภัยและโปรแกรมป้องกันไวรัส

๘.๕.๒ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลสม่ำเสมอ จัดให้มีการเชื่อมกันระหว่างฐานข้อมูล ปรับปรุงข้อมูลให้เป็นปัจจุบัน ทำการสำรองข้อมูลแบบ Full backup ทำการทดสอบการสำรองข้อมูลให้สามารถนำกลับมาใช้งานได้ในกรณีเกิดเหตุฉุกเฉิน ติดตั้งระบบรักษาความปลอดภัยและโปรแกรมป้องกันไวรัส

๘.๖ ด้านกายภาพและสิ่งแวดล้อม

๘.๖.๑ ระบบปรับอากาศ กำหนดระยะเวลาการใช้งานแต่ละเครื่องสลับเวลาการทำงานสำหรับเครื่องปรับอากาศแบบแยกส่วน ทำความสะอาดแผ่นกรองอากาศอย่างสม่ำเสมอ ทำการบันทึกในสมุดการบำรุงรักษาประจำเครื่องทุกครั้ง กรณีที่เครื่องชำรุด ติดต่อประสานงานผู้ชำนาญการโดยเร่งด่วนทันที

๘.๖.๒ ภัยธรรมชาติ เลือกสถานที่ตั้งให้ปลอดภัยต่อภัยธรรมชาติ วางอุปกรณ์สื่อสารและเครื่องคอมพิวเตอร์แม่ข่ายในห้องที่น้ำท่วมไม่ถึง ติดตั้งระบบป้องกันอัคคีภัย กรณีที่เกิดอัคคีภัย ให้ทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายเป็นอันดับแรก

๘.๖.๓ ภัยสงคราม วางอุปกรณ์สื่อสารและเครื่องคอมพิวเตอร์แม่ข่ายในตู้ที่ทนทานต่อแรงกระแทก กรณีเกิดการจลาจลไม่สามารถเข้าไปปฏิบัติงานในสถานที่ได้ จัดให้มีศูนย์สารสนเทศสำรองที่สามารถทำงานทดแทนสถานที่หลักได้

๙. หน่วยงานผู้รับผิดชอบด้านสารสนเทศ

๙.๑ ศูนย์กลาง นครราชสีมา

ที่อยู่ ๗๔๔ ถ.สุรนารายณ์ อ.เมือง จ.นครราชสีมา ๓๐๐๐๐ โทรศัพท์: ๐๔๔ ๒๓๓๐๐๐ โทรสาร ๐๔๔ ๒๓๓๐๕๒

๙.๑.๑ นายประกาย นาดี รองผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเพื่องานวิชาการ
การติดต่อ E-Mail: prakai@rmuti.ac.th เบอร์โทร ๒๘๘๘

๙.๑.๒ นายชัยวัฒน์ แดงจันทึก หัวหน้างานเทคโนโลยีสารสนเทศเพื่องานวิชาการ
การติดต่อ E-Mail: chaiwat.d@rmuti.ac.th เบอร์โทร ๒๘๘๒

๙.๑.๓ แผนกงาวิศวกรรมเครือข่าย

๑) นายชัยวัฒน์ แดงจันทึก หัวหน้าแผนกงาวิศวกรรมเครือข่าย
การติดต่อ E-Mail: chaiwat.d@rmuti.ac.th เบอร์โทร ๒๘๘๒

๒) นายพลากร ชาญสูงเนิน วิศวกร
การติดต่อ E-Mail: palagon.ch@rmuti.ac.th เบอร์โทร ๒๘๘๒

๓) นายมงคล ทองคำ วิศวกร
การติดต่อ E-Mail: mongkol.th@rmuti.ac.th เบอร์โทร ๒๘๘๒

๙.๑.๔ แผนกงานเทคโนโลยีคอมพิวเตอร์

๑) นางปวีณา นาดี หัวหน้าแผนกงานเทคโนโลยีคอมพิวเตอร์

การติดต่อ E-Mail: paweena@rmuti.ac.th เบอร์โทร ๒๘๘๑

๒) นางสาวอาภาพร สุประดิษฐ์ นักวิชาการศึกษา

การติดต่อ E-Mail: arpaporn@rmuti.ac.th เบอร์โทร ๒๘๘๑

๓) นางสาวมยุรี รุนสูงเนิน นักวิชาการคอมพิวเตอร์

การติดต่อ E-Mail: mayuree.ru@rmuti.ac.th เบอร์โทร ๒๘๘๑

๔) นายเชิดชัย คนรู้ นักวิชาการคอมพิวเตอร์

การติดต่อ E-Mail: cherdchai.kh@rmuti.ac.th เบอร์โทร ๒๘๘๖

๙.๑.๕ แผนกงานสารสนเทศ

๑) นายสายชล สารสนอก หัวหน้าแผนกงานสารสนเทศ

การติดต่อ E-Mail: saichon.sa@rmuti.ac.th เบอร์โทร ๒๘๘๗

๒) นายธีรธรรม์ โรจนสถิตย์ นักวิชาการคอมพิวเตอร์

การติดต่อ E-Mail: thanit.ro@rmuti.ac.th เบอร์โทร ๒๘๘๗

๓) นายทิวธวัช เมฆวิชัย นักวิชาการศึกษา

การติดต่อ E-Mail: tewtawat.me@rmuti.ac.th เบอร์โทร ๒๘๘๗

๙.๑.๖ แผนกงานอีเลิร์นนิ่งและเทคโนโลยีการศึกษา

๑) นายรัญชน์ แถวโสภา หัวหน้าแผนกงานอีเลิร์นนิ่งและเทคโนโลยีการศึกษา

การติดต่อ E-Mail: rann.th@rmuti.ac.th เบอร์โทร ๒๘๗๑

๒) นายปิยวัฒน์ ชัยวงษ์ นักวิชาการโสตทัศนศึกษา

การติดต่อ E-Mail: piyawat.ch@rmuti.ac.th เบอร์โทร ๒๘๗๐

๓) นายตรีทศ ศุภคติสันติ์ นักวิชาการโสตทัศนศึกษา

การติดต่อ E-Mail: threetoss.su@rmuti.ac.th เบอร์โทร ๒๘๗๐

๔) นายวิโรจน์ ธรรมวัฒร์ นักวิชาการโสตทัศนศึกษา

การติดต่อ E-Mail: wirot.ta@rmuti.ac.th เบอร์โทร ๒๘๗๒

๕) นางสาวเมธวดี กรองโพธิ์ นักวิชาการคอมพิวเตอร์

การติดต่อ E-Mail: medwadee.kr@rmuti.ac.th เบอร์โทร ๒๘๗๐

๖) นางสาวอาจารี จรานุวัฒน์ นักวิชาการศึกษา

การติดต่อ E-Mail: archaree.ca@rmuti.ac.th เบอร์โทร ๒๘๗๒

๙.๒ วิทยาเขต ขอนแก่น

ที่อยู่ ๑๕๐ ถ.ศรีจันทร์ ต.ในเมือง อ.เมือง จ.ขอนแก่น ๔๐๐๐๐ โทรศัพท์ ๐๔๓-๓๓๖๓๗๐-๑ โทรสาร ๐๔๓-๒๓๗๔๘๓

๑) นายอาทิตย์ วงษ์พระลับ หัวหน้าแผนกเทคโนโลยีสารสนเทศเพื่องานวิชาการ
การติดต่อ E-Mail: artith.wo@rmuti.ac.th เบอร์โทร ๑๕๓๑

๒) นายสัญญา ม่วงมณี นักวิชาการคอมพิวเตอร์
การติดต่อ E-Mail: sanya.mo@rmuti.ac.th เบอร์โทร ๑๕๓๑

๓) นายนายกฤษณะ ภูผาเผย ช่างเทคนิคคอมพิวเตอร์
การติดต่อ E-Mail: kitsana.pu@rmuti.ac.th เบอร์โทร ๑๕๓๑

๙.๓ วิทยาเขต สกลนคร

ที่อยู่ ๑๙๙ หมู่ ๓ ถนนพังโคน-วาริชภูมิ ตำบลพังโคน อำเภอพังโคน จังหวัดสกลนคร ๔๗๑๖๐ โทรศัพท์ ๐-๔๒๗๗-๒๒๘๕ โทรสาร ๐-๔๒๗๗-๒๑๕๘

๑) นายเติมศักดิ์ แสนเพียง หัวหน้าแผนกเทคโนโลยีสารสนเทศเพื่องานวิชาการ
การติดต่อ E-Mail: termsak.sa@rmuti.ac.th เบอร์โทร ๑๖๐๕

๒) ว่าที่ร้อยตรีเด่นภา แสนเพียง นักวิชาการศึกษา
การติดต่อ E-Mail: denpha.sa@rmuti.ac.th เบอร์โทร ๑๖๐๕

๓) นายชัชวาลย์ คำมุงคุณ ช่างเทคนิค
การติดต่อ E-Mail: chatchawan.kh@rmuti.ac.th เบอร์โทร ๑๖๐๕

๙.๔ วิทยาเขต สุรินทร์

ที่อยู่ ๑๔๕ ม.๑๕ ถ.สุรินทร์-ปราสาท ต.นอกเมือง อ.เมืองสุรินทร์ จ.สุรินทร์ ๓๒๐๐๐ โทรศัพท์ ๐๔๔-๑๕๓๐๖๒ โทรสาร ๐๔๔-๕๒๐๗๖๔

๑) นายธนพล เริ่มปลูก หัวหน้าแผนกเทคโนโลยีสารสนเทศ
การติดต่อ E-Mail: tanaphon.ro@rmuti.ac.th เบอร์โทร ๑๔๐๐

๒) นายวสุพล เริ่มปลูก นักวิชาการคอมพิวเตอร์
การติดต่อ E-Mail: wasuphon.re@rmuti.ac.th เบอร์โทร ๑๔๐๐

๓) นายภูมินทร์ บุญสอน เจ้าหน้าที่เทคนิคและซ่อมคอมพิวเตอร์
การติดต่อ E-Mail: phumin.bo@rmuti.ac.th เบอร์โทร ๑๔๐๐

เอกสารอ้างอิง

ส่วนเทคโนโลยีสารสนเทศ, **การบริหารความเสี่ยงของระบบสารสนเทศสำนักงานปลัดกระทรวงมหาดไทยประจำปี พ.ศ. ๒๕๕๕**, ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย. จำนวน ๔๓ หน้า

กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร, **แผนบริหารความเสี่ยง แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ด้านเทคโนโลยีสารสนเทศจังหวัด จังหวัดเพชรบุรี**, สำนักงานจังหวัด กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดเพชรบุรี. จำนวน ๕๕ หน้า.

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร, **แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา(ฉบับสมบูรณ์),** สำนักงานเลขาธิการวุฒิสภา. จำนวน ๔๗ หน้า.

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน