นโยบายบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ มหาวิทยาลัยนเรศวร พ.ศ. ๒๕๕๕ - พ.ศ. ๒๕๕๙

จัดทำโดย
กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
มหาวิทยาลัยนเรศวร
๒ ๕

สารบัญ

เรื่อง **หน้า**

1. หลักการและเหตุผล

ตามยุทธศาสตร์เทคโนโลยีสารสนเทศและการสื่อสาร ปี พ.ศ. 2555 – 2559 ของกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร ได้จัดทำภายใต้กรอบนโยบายและแผนยุทธศาสตร์สู่เป้าหมายและแผนการดำเนินงานในช่วง ปี พ.ศ. 2552 – ปี พ.ศ. 2556 ของมหาวิทยาลัยนเรศวร และสังเคราะห์บริบทแนวโน้มด้านเทคโนโลยีสารสนเทศ แล้วนำมายกร่างเป็นยุทธศาสตร์ CITCOMS ปี พ.ศ. 2554 – 2559 ต่อมาได้ประชุมเชิงปฏิบัติการระดมความคิดเห็นบุคลากร CITCOMS เพื่อจัดทำแผนงาน/โครงการ ตามพันธกิจ จากนั้นได้นำเสนอที่ประชุมคณะกรรมการบริหารกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร ได้พิจารณาและให้ข้อคิดเห็นแล้วนำมาปรับปรุง ผนวกกับมุมมองที่ได้จากการไปศึกษาดูงานนอกสถานที่ของผู้บริหาร หัวหน้างาน และบุคลากร ผลจากการวิเคราะห์ สังเคราะห์ กระบวนการดังกล่าว ได้เป็นยุทธศาสตร์เทคโนโลยีสารสนเทศและการสื่อสาร ปี พ.ศ. 2555 – 2559 หากกองบริการเทคโนโลยีสารสนเทศและการสื่อสารไม่มีการบริหารจัดการและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ อาจส่งผลกระทบต่อการดำเนินงานและสร้างความเสียหายต่อหน่วยงานต่างๆ ได้ทั้งในด้านการพัฒนาบุคลากร และความคุ้มค่าทางงบประมาณ ดังนั้น การวางแผนและการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ จึงเป็นเรื่องสำคัญ และควรมีการเตรียมการที่ดีอีกทั้งยังต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

2. วิสัยทัศน์ (VISION)

กองบริการเทคโนโลยีสารสนเทศและการสื่อสารมีความมุ่งมั่น เพื่อเป็นหน่วยงานที่พร้อมให้บริการเทคโนโลยีสารสนเทศอย่างมืออาชีพให้สอดคล้องกับพันธกิจของมหาวิทยาลัยนเรศวร

3. พันธกิจ (MISSION)

1. พัฒนาดูแลระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยนเรศวร
2. จัดหา จัดสรร คอมพิวเตอร์และอุปกรณ์เทคโนโลยีสารสนเทศของมหาวิทยาลัยนเรศวร
3. บริหารจัดการและให้คำปรึกษาด้านเทคโนโลยีสารสนเทศสำหรับประชาคมมหาวิทยาลัยนเรศวรและสังคม

4. ยุทธศาสตร์ (STRATEGY)

ยุทธศาสตร์ที่ 1 พัฒนาเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารให้มีประสิทธิภาพ อย่างทั่วถึงและมีความมั่นคงปลอดภัย

วัตถุประสงค์ มีเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารที่มีคุณภาพและประสิทธิภาพ สะดวก รวดเร็ว มีความมั่นคงปลอดภัยโดยมีเครือข่ายครอบคลุมพื้นที่มหาวิทยาลัยนเรศวร

เป้าหมายและตัวชี้วัด

1. มีเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร (NU-NET) ที่มีประสิทธิภาพ มั่นคง ปลอดภัย ทันสมัย พร้อมใช้งานตลอดเวลา และอย่างทั่วถึง
2. มีเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร (NU-NET) แบบรวมศูนย์
3. เป็นศูนย์กลางการกระจายโอกาสด้านการเรียน การบริการวิชาการ การเรียนรู้อย่างต่อเนื่อง โดยการใช้เครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร (NU-NET) ที่มีความเร็วสูง และเป็นศูนย์กลางการกระจายข้อมูลข่าวสาร ด้านการวิจัยและบริการวิชาการที่มุ่งตอบสนองต่อความต้องการของชุมชน สนับสนุนการทำนุศิลปะและวัฒนธรรม สร้างผลงานวิชาการที่สร้างชื่อเสียงให้กับมหาวิทยาลัย

ยุทธศาสตร์ที่ 2 พัฒนาระบบสารสนเทศมาใช้ในการบริหารจัดการและบริการทุกหน่วยอย่างมีธรรมาภิบาล

วัตถุประสงค์ สามารถนำระบบสารสนเทศมาใช้ในการบริหารจัดการและบริการทุกหน่วยงานอย่างมีประสิทธิภาพ เพื่อยกระดับคุณภาพบริการข้อมูลสถิติ และสารสนเทศที่มีคุณภาพ และนำมาใช้ในการวางแผนและตัดสินใจได้

เป้าหมายและตัวชี้วัด

1. มีสถาปัตยกรรมของฐานข้อมูล นิสิต บุคลากร วิจัย หลักสูตร บริการ วิชาการ รวมถึงด้านการเงินและงบประมาณ และด้านทรัพย์สินและอาคารสถานที่
2. มีฐานข้อมูลและเชื่อมโยงในด้านวิจัยและบริการวิชาการ ด้านการเงินและงบประมาณ และด้านทรัพย์สินและอาคารสถานที่
3. มีการบูรณาการฐานข้อมูลเข้าด้วยกันเพื่อรายงานตัวชี้วัดของมหาวิทยาลัยนเรศวร
4. มีระบบสารสนเทศให้เป็นระดับ Decision Support System (DSS) ในด้านวิจัยและบริการวิชาการ ด้านการเงินและงบประมาณ และด้านทรัพย์สินและอาคารสถานที่
5. มีระบบสารสนเทศในการบริหารจัดการข้อมูลคอมพิวเตอร์และอุปกรณ์เทคโนโลยีสารสนเทศเพื่อการวางแผนจัดสรรงบประมาณระบบบริหารจัดการข้อมูล คอมพิวเตอร์ และอุปกรณ์เทคโนโลยีสารสนเทศ
6. มีระบบสารสนเทศสนับสนุนการดำเนินการภายในมหาวิทยาลัยที่พัฒนาโดยใช้เทคโนโลยี Open Source

ยุทธศาสตร์ที่ 3 ส่งเสริม ให้คำที่ปรึกษา และบริการความรู้และทักษะด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ บูรณาการระบบการจัดการเรียนการสอน Online ในรูปแบบ Ubiquitous Learning ส่งเสริมและให้คำที่ปรึกษาในการผลิตสื่อการเรียนการสอนแบบ e-Learning เพื่อเข้าถึงแหล่งเรียนรู้ด้วยตนเองและให้อาจารย์กับนิสิตสามารถผลิตสื่อที่มีคุณภาพด้วยตนเอง ตลอดทั้งให้ความรู้และทักษะด้านเทคโนโลยีสารสนเทศเพื่อเตรียมความพร้อมแก่นิสิตสู่ตลาดแรงงาน

เป้าหมายและตัวชี้วัด

1. มีบริการระบบ LMS ที่สนับสนุน การจัดการเรียนการสอนระบบ รูปแบบ Ubiquitous Learning
2. ส่งเสริมและให้คำที่ปรึกษาในการผลิตสื่อการเรียนการสอนแบบ e-Learning เพื่อเข้าถึงแหล่งเรียนรู้ด้วยตนเองและให้อาจารย์กับนิสิตสามารถผลิตสื่อที่มีคุณภาพด้วยตนเอง
3. สนับสนุนและผลักดันให้อาจารย์และนิสิตมีการจัดการเรียนการสอนในรูปแบบออนไลน์
4. บริการให้ความรู้และทักษะด้านเทคโนโลยีสารสนเทศเพื่อเตรียมความพร้อมแก่นิสิตสู่ตลาดแรงงาน

ยุทธศาสตร์ที่ 4 บริหารจัดการและบริการคอมพิวเตอร์และอุปกรณ์เทคโนโลยีสารสนเทศอย่างทั่วถึง

วัตถุประสงค์ สามารถให้บริการจัดหาและจัดสรรคอมพิวเตอร์และอุปกรณ์โลยีสารสนเทศอันเป็นทรัพยากรให้มีประสิทธิภาพสูงสุดโดยคำนึงถึงผลประโยชน์ของนิสิต บุคลากร และมหาวิทยาลัยนเรศวรอย่างมีธรรมาภิบาล

เป้าหมายและตัวชี้วัด

1. มีระบบเครือข่ายคอมพิวเตอร์ สามารถรองรับการใช้งาน ความเร็วที่ 10 GB และอุปกรณ์ที่เกี่ยวข้องกับการดำเนินงานบนระบบเครือข่ายคอมพิวเตอร์มี Uptime ไม่น้อยกว่าร้อยละ 99
2. มีระบบเครือข่ายไร้สาย (Wireless LAN) ครอบคลุมการใช้งานทุกพื้น และสามารถรองรับปริมาณการใช้งานในช่วงเวลาเดียวกัน (Concurrent User) ได้ไม่น้อยกว่า 30,000 คน
3. นิสิต อาจารย์ บุคลากร ผู้บริหาร สามารถเข้าถึงและใช้ประโยชน์จากทรัพยากรเทคโนโลยีสารสนเทศของมหาวิทยาลัยได้ทุกคน
4. มีบริการซอฟท์แวร์ลิขสิทธิ์
5. มีระบบการสื่อสารแบบรวมศูนย์ (Single point Communication) สามารถรองรับการสื่อสารที่ใช้งานได้ครบทุกรูปแบบ (Unified Communication) ทั้งภาพ (Video) เสียง (Voice) และข้อมูล (Data)
6. มีความพร้อมเครือข่ายมหาวิทยาลัยให้รองรับมาตรฐาน IPv6 ทั้งระบบ
7. มีแผนงานการจัดหาและจัดสรรทรัพยากรสำหรับบุคลากรสายวิชาการและสายสนับสนุน
   (1) อุปกรณ์เทคโนโลยีสารสนเทศสำหรับบุคลากรสายวิชาการ (คนละ 20,000 บาท ภายใน 3 ปี)
   (2) เครื่องคอมพิวเตอร์ระบบเช่าสำหรับบุคลากรสายสนับสนุน คณะ/วิทยาลัย/กอง/สถาน และเครื่องคอมพิวเตอร์ สำหรับบริการการเรียนการสอนส่วนกลางของมหาวิทยาลัย

5. เป้าประสงค์ภาพรวม (Summarized Goal) (พ.ศ. 2555 – พ.ศ. 2559)

1. พัฒนาคุณภาพเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร ที่สนับสนุนการเรียนการสอน การวิจัย และบริการวิชาการ โดยใช้เทคโนโลยีเป็นฐาน (ICT-based University) สู่การเป็นมหาวิทยาลัยชั้นนำในด้านเทคโนโลยี

   1.1 มีความเร็วอินเทอร์เน็ต (Bandwidth) ภายในประเทศ (Domestic) จำนวนไม่น้อยว่า 2 Gbps

   1.2 มีความเร็วอินเทอร์เน็ต (Bandwidth) ต่างประเทศ (International) จำนวนไม่น้อยว่า 500 Mbps

   1.3 มีบริการอินเทอร์เน็ตความเร็วสูง เพื่อการสืบค้นฐานข้อมูลออนไลน์ สนับสนุนการเรียนการสอน การวิจัยและบริการวิชาการ

   1.4 มีการให้บริการระบบ Live@edu / Microsoft Office 365 for Education เพื่อสนับสนุนการเรียนการสอน การวิจัยและบริการวิชาการ

   1.5 มีการให้บริการระบบ Google Apps for Education เพื่อสนับสนุนการเรียนการสอน การวิจัย และบริการวิชาการ

   1.6 มีบริการระบบบริหารจัดการองค์ความรู้ (Knowledge Management) ให้บริการระดับคณะ/หน่วยงาน ภายในมหาวิทยาลัย

2. มีความพร้อมให้ประชาคมมหาวิทยาลัยนเรศวร เข้าถึงเทคโนโลยีการสื่อสาร ได้อย่างทั่วถึงในสถานะมหาวิทยาลัยไซเบอร์ (Cyber University)

   2.1 พัฒนาระบบเครือข่ายเทคโนโลยีการสื่อสารให้พร้อมใช้งาน

   - อุปกรณ์ที่เกี่ยวข้องกับการดำเนินงานบนระบบเครือข่ายคอมพิวเตอร์มี Uptime ไม่น้อยกว่าร้อยละ 99
   - ปรับปรุงระบบเครือข่ายคอมพิวเตอร์ สามารถรองรับการใช้งาน ความเร็วที่ 10 GB
   - มีระบบบริการรักษาความปลอดภัยจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

   2.2 มีการปรับปรุงระบบเครือข่ายคอมพิวเตอร์ไร้สาย (Wireless LAN) แบบผสมผสาน (Hybrid) รองรับการใช้งานในรูปแบบมาตรฐานเดียวกัน (Web Authentication) และสามารถบริหารจัดการได้ทั้งระบบ ครอบคลุมพื้นที่การใช้งานทั้งมหาวิทยาลัย จำนวนไม่น้อยกว่า 800 จุด

   2.3 ปรับปรุงอุปกรณ์ ที่เกี่ยวข้องกับการดำเนินงานบนระบบเครือข่ายคอมพิวเตอร์ ให้มีความทันสมัย และมีประสิทธิภาพ

   2.4 ปรับปรุงและพัฒนาระบบจดหมายอิเล็กทรอนิกส์ (NU Mail) ให้มีเสถียรภาพ ประสิทธิภาพ

   - มีพื้นที่จัดเก็บข้อมูล Mailbox เพียงพอต่อการใช้งานในปัจจุบัน พื้นที่การใช้งานโดยรวมจำนวนไม่น้อยกว่า 25 TB
   - มีระบบ Database Availability Group (DAG) เพื่อสำรองข้อมูล ระบบฐานข้อมูลใน Exchange Server

   2.5 มีบริการระบบ Call Center และบริการเว็บไซต์ Help Desk เพื่อให้ความรู้และช่วยแก้ไขปัญหาผู้ใช้งานระบบเครือข่าย NU-NET

   2.6 มีระบบการสื่อสารแบบรวมศูนย์ (Single point Communication) สามารถรองรับการสื่อสารที่ใช้งานได้ครบทุกรูปแบบ (Unified Communication) ทั้งภาพ (Video) เสียง (Voice) และข้อมูล (Data)

   2.7 มีบริการซอฟท์แวร์ลิขสิทธิ์

2.8 เตรียมความพร้อมเครือข่ายมหาวิทยาลัยให้รองรับมาตรฐาน IPv6 ทั้งระบบ

3. พัฒนาระบบแม่ข่ายบนเทคโนโลยี Cloud Computing
   3.1 ปรับเปลี่ยนเครื่องคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัย ไปสู่ Private Cloud
   3.2 ปรับปรุงเครื่องคอมพิวเตอร์แม่ข่ายบนเทคโนโลยี Private Cloud และสามารถรองรับการขยายตัวของระบบได้ในอนาคต
   3.3 มีระบบแม่ข่ายที่ใช้งานบน Public Cloud หรือ Hybrid Cloud ให้บริการ
   3.4 มีศูนย์ข้อมูลกลาง (Data Center) ที่ทันสมัย
4. มีซอฟต์แวร์ลิขสิทธิ์เพื่อการศึกษาพร้อมทั้งส่งเสริมการใช้ Open source ในการปฏิบัติงานอย่างเพียงพอ
5. มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล
6. มีระบบสารสนเทศเพื่อสนับสนุนการดำเนินงานและการตัดสินใจของผู้บริหารมหาวิทยาลัยนเรศวร (NU-MIS) และระบบคลังข้อมูล (Data Warehouse) ที่ครอบคลุมการใช้งานทั้งมหาวิทยาลัย
7. ส่งเสริมและพัฒนาการทำวิจัยสถาบันของหน่วยงาน
8. มีระบบการบริหารจัดการข้อมูลการจัดสรรคอมพิวเตอร์สำหรับสายสนับสนุนและอุปกรณ์เทคโนโลยีสารสนเทศสำหรับสายวิชาการ
9. มีการจัดโครงการหรือกิจกรรมความร่วมมือเครือข่ายสถาบันการศึกษา
10. บูรณาการระบบการจัดการเรียนการสอน Online ในรูปแบบ Ubiquitous Learning ส่งเสริมและให้คำที่ปรึกษาในการผลิตสื่อการเรียนการสอนแบบ e-Learning เพื่อเข้าถึงแหล่งเรียนรู้ด้วยตนเอง
11. จัดอบรมบุคลากรและนิสิต ให้มีความรู้ ทักษะ และสมรรถนะทางด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
12. ส่งเสริมและพัฒนาศักยภาพบุคลากร ให้สามารถตอบสนองพันธกิจของมหาวิทยาลัย
13. มีระบบบริหารจัดการพื้นที่ใช้สอยภายในอาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ

6. นโยบายในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เพื่อให้กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมีภารกิจหลักในการดูแลรักษาระบบเครือข่ายของมหาวิทยาลัยนเรศวร พัฒนาระบบสารสนเทศเพื่อสนับสนุนการดำเนินการและการตัดสินใจผู้บริหาร ให้บริการคอมพิวเตอร์และอุปกรณ์เทคโนโลยีสารสนเทศ และให้คำปรึกษา ความรู้และทักษะทักษะด้านเทคโนโลยีสารสนเทศ แก่ประชาคมมหาวิทยาลัยนเรศวรและสังคม จึงจำเป็นต้องมีระบบในการบริหารความเสี่ยง เพื่อเป็นเครื่องมือในการกำกับกระบวนการดำเนินงานด้านต่าง ๆ ได้อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น เพื่อลดความเสียหายแก่องค์กรโดยเฉพาะด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงการดำเนินงานและเป้าหมายของมหาวิทยาลัยเป็นสำคัญ

นอกจากนี้ กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร ยังได้ให้ความสำคัญอย่างยิ่งต่อการจัดทำแผนบริหารความเสี่ยง (Risk Management) เพราะหากมีการวางแผนที่ดีและมีการจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพแล้วจะลดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นได้ตามสภาวการณ์ต่างๆ อีกทั้งยังอำนวยความสะดวกในการดำเนินการ สอดคล้องกับกรอบการปฏิบัติงาน ตามพันธกิจ

ของมหาวิทยาลัยนเรศวร มีแนวทางป้องกันและแก้ไขความเสี่ยงที่อาจจะเกิดขึ้นได้ ซึ่งจะช่วยให้การบริหารงานและให้บริการแก่นิสิตและบุคลากรได้อย่างมีประสิทธิภาพสูงสุดที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่าตลอดจนความสามารถพัฒนาคุณภาพบริการที่ดีให้แก่ผู้รับบริการ ดังนั้น กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดแนวทางและแผนในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยพิจารณาจากแนวทางด้านการพัฒนาฐานข้อมูลและสารสนเทศของมหาวิทยาลัยที่มีระบบงานหลัก ดังนี้ ระบบคอมพิวเตอร์แม่ข่าย (Server System) ระบบเครือข่าย (Network System) ระบบเครื่องคอมพิวเตอร์และอุปกรณ์ (Hardware System) ระบบฐานข้อมูลสารสนเทศและโปรแกรมการดำเนินงาน (Database & Software) และระบบบุคลากร (People ware System)

7. วัตถุประสงค์ของการจัดทำนโยบายบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศของมหาวิทยาลัยนเรศวร
2. เพื่อเป็นแนวทางในการวางแผน ดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และพร้อมสำหรับการใช้งาน
3. เพื่อให้การปฏิบัติงานเป็นระบบและต่อเนื่อง สามารถแก้ไขสถานการณ์ต่าง ๆ ได้ทันท่วงที ในกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ
4. เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุด และลดโอกาสความเสียหายที่อาจเกิดขึ้น
5. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงของระบบฐานข้อมูลด้านเทคโนโลยีสารสนเทศของกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร ให้หน่วยงานต่างๆ นำไปใช้ประโยชน์
6. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจโดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

8. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

1. ระบบฐานข้อมูลสารสนเทศและโปรแกรมการดำเนินงาน (Database & Software) เช่น ระบบสารสนเทศสนับสนุนการดำเนินงานภายในมหาวิทยาลัยนเรศวร (NU-IS) ระบบสารสนเทศสนับสนุนการตัดสินใจผู้บริหาร (NU-MIS) ระบบสารสนเทศด้านการเงินและงบประมาณ ระบบสารสนเทศสนับสนุนด้านกิจกรรมนิสิต เป็นต้น

2. ระบบเครือข่าย (Network System) เช่น การให้บริการระบบเครือข่ายภายในมหาวิทยาลัยนเรศวร (NU Net) การให้บริการระบบเครือข่ายแบบไร้สาย (NU Wireless) โปรแกรมระบบจัดการเครือข่าย (Network Software) โปรแกรมป้องกันไวรัส (AntiVirus) เครื่องคอมพิวเตอร์ป้องกันการโจมตีจากบุคคลภายนอก (Firewall) เป็นต้น

3. อุปกรณ์คอมพิวเตอร์แม่ข่าย (Server System) เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) ตู้สำหรับจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ (ตู้ Rack) เป็นต้น
4. เครื่องคอมพิวเตอร์และอุปกรณ์ (Hardware) เช่น เครื่องคอมพิวเตอร์ (PC/Notebook) เครื่องพิมพ์ (Printer) เครื่องสแกนเนอร์ (Scanner) อุปกรณ์สำรองไฟฟ้า (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายแบบไร้สาย (Wireless Access Point) เป็นต้น

9. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ในปัจจุบัน เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานของมหาวิทยาลัยนเรศวรรวมถึงในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล การใช้เครื่องคอมพิวเตอร์แม่ข่าย การจัดทำและพัฒนาระบบเทคโนโลยีสารสนเทศในภาพรวม มุ่งหวังที่จะให้ระบบสารสนเทศ ช่วยในการปฏิบัติงานของหน่วยงานมีความสะดวก รวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น แต่การนำเทคโนโลยีสารสนเทศมาใช้ ย่อมมีความเสี่ยงหลายประการด้วยกัน ดังนั้น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงต้องมีทั้งการวางแผน การประเมินทั้งโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้น และสามารถประเมินเป็นเชิงปริมาณ หรือเชิงคุณภาพได้

9.1 ความเสี่ยงด้านเทคโนโลยีสารสนเทศของกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร สามารถระบุได้ 7 ประเภท ดังนี้

1 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม อายุการใช้งานของอุปกรณ์ อุปกรณ์ชำรุด อุปกรณ์ไม่รองรับการเปลี่ยนแปลงของเทคโนโลยี เป็นต้น

2 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การควบคุมอุณหภูมิและความชื้น การปรับปรุงสถานที่ การไม่มีระบบรักษาความปลอดภัยของห้องคอมพิวเตอร์แม่ข่าย การก่อการร้ายและการโจรกรรม เป็นต้น

3 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ช่องโหว่ของซอฟแวร์ที่พัฒนาขึ้น ถูกผู้ไม่หวังดีทำลายระบบ มัลแวร์และไวรัสคอมพิวเตอร์ เป็นต้น

4 ความเสี่ยงด้านระบบสารสนเทศและข้อมูลสารสนเทศ หมายถึง ความเสี่ยงที่เกิดกับระบบสารสนเทศและข้อมูลสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย ระบบหยุดทำงานหรือไม่สามารถใช้งานได้ ข้อมูลถูกทำลาย การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล การโจรกรรมข้อมูล การสำรองข้อมูลที่ไม่เหมาะสม

5 ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ การวางแผน การตรวจสอบ การทำงาน ความไม่พร้อมของบุคลากรในการปฏิบัติงาน เช่น การเจ็บป่วย การกำหนดหน้าที่และสิทธิของบุคลากร/คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการทำงาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึงบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งเป็นความเสี่ยงทั้งสิ้น

6 ความเสี่ยงด้านกลยุทธ์ หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายผู้บริหาร เนื่องจากการเปลี่ยนแปลงผู้บริหารในด้านเทคโนโลยีสารสนเทศ ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

7 ความเสี่ยงด้านพัสดุและการเงิน หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ การเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา กระบวนการจัดซื้อจัดจ้างไม่เป็นไปตามแผน

9.2 แนวทางการบริหารจัดการความเสี่ยงของกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร

1. **การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ**

(1) ความเสี่ยงในเรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงานและขององค์กร ที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ ให้เหมาะสมตามลักษณะของโครงการและเหมาะสมกับงบประมาณ

(2) ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ซึ่งโอกาสที่จะเกิดความเสี่ยง 2 ด้าน คือ

(2.1) ด้านการบำรุงรักษาและลดความเสี่ยง

(2.1.1) สามารถแก้ไขปัญหาเบื้องต้นของเครื่องคอมพิวเตอร์ได้โดย Administrator และ User และการดูแลอย่างถูกต้องและต่อเนื่อง

(2.1.2) ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว

(2.1.3) มีการตรวจเช็คไวรัส และกำจัดอย่างสม่ำเสมอ

(2.1.4) การติดตั้ง Firewall เพื่อป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยนเรศวรได้

(2.1.5) การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ

(2.1.6) ฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงาน เกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ เช่น การกำหนดรหัสผู้ใช้ การใช้รหัสผ่าน

(2.1.7) การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ

(2.1.8) การสำรองข้อมูล (Backup) สารสนเทศ

(2.2) ด้านการรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย

(2.2.1) กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์ และระบบเครือข่าย

(2.2.2) ติดตั้งโปรแกรมระบบรักษาความปลอดภัย

(2.2.3) ทำการทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

2. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

(1) การกำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยงสูง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น เครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย หน้าต่างระบายความร้อน ถังดับเพลิง เป็นต้น

(2) การควบคุมการเข้า – ออก Network Operation Center (NOC) ห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง เป็นพื้นที่เขตหวงห้ามเฉพาะ โดยกำหนดสิทธิการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง โดยหน่วยงานระบบเครือข่าย หัวหน้างานระบบเครือข่าย รับผิดชอบ

(3) การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม โดยทำการติดตั้งระบบดับเพลิงอัตโนมัติด้วยสารเคมีห้องปฏิบัติการคอมพิวเตอร์เครือข่ายของกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร

(4) การป้องกันความเสี่ยงจากระบบไฟฟ้าขัดข้อง โดยมีการติดตั้งเครื่องสำรองไฟสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และการติดตั้งระบบสายดินที่ได้มาตรฐานอุปกรณ์ป้องกันไฟ

(5) การป้องกันความเสี่ยงจากระบบควบคุมอุณหภูมิและความชื้นให้เหมาะสม โดยการติดตั้งอุณหภูมิเครื่องปรับอากาศและค่าความชื้นให้มีระดับเหมาะสมกับคุณลักษณะของระบบคอมพิวเตอร์

(6) ความเสี่ยงในเรื่องงบประมาณที่จะดำเนินการได้อย่างมีประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง

(7) ความเสี่ยงในเรื่องประเด็นนโยบายของผู้บริหาร ที่ให้น้ำหนักและความสำคัญเกี่ยวกับเทคโนโลยีสารสนเทศ หากมีการเปลี่ยนแปลงจะส่งผลกระทบต่อการปฏิบัติงานและแนวทางในการดำเนินการขั้นตอนต่อไป

(8) ความเสี่ยงในเรื่องของการบริหารจัดการ โดยสามารถวางแผนบริหารความเสี่ยงและดำเนินการเพื่อลดความเสี่ยงได้ ดังนี้

(8.1) จัดทำแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศ

(8.2) บริหารจัดการ ติดตาม ควบคุม กำกับดูแล และให้คำปรึกษา แก้ไขปัญหาระบบ

(8.3) ติดตาม จัดทำ ควบคุม กำกับ ดูแล และให้คำปรึกษา แก้ไขปัญหาระบบการจัดการและไหลเวียนเอกสารไร้กระดาษ ให้หน่วยงานต่างๆ ของมหาวิทยาลัยนเรศวร

(8.4) ศึกษา วิเคราะห์ และจัดทำระบบข้อมูลเพื่อการบริหารงานและสนับสนุนการตัดสินใจของผู้บริหารระดับสูง

(8.5) จัดการประเมินผลแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศและการสื่อสาร

(8.6) ศึกษา วิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อการวางแผน และคาดการณ์แนวโน้มความต้องการบุคลากรด้านเทคโนโลยีสารสนเทศ

(8.7) ให้บริการฝึกอบรมเพื่อพัฒนาความรู้และทักษะด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศแก่บุคลากรและนิสิตของมหาวิทยาลัยนเรศวร

3. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

(1) มีการทดสอบระบบที่พัฒนาขึ้น (Software Testing) ก่อนเปิดใช้งานจริง

(2) มีการเข้ารหัสข้อมูลระหว่างเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งาน (SSL)

(3) มีการติดตั้งซอฟต์แวร์แอนติไวรัสและปรับปรุง patch อย่างสม่ำเสมอทั้งที่เครื่องแม่ข่ายและเครื่องลูกข่าย

4. ความเสี่ยงด้านระบบสารสนเทศและข้อมูลสารสนเทศ

(1) มีการรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย

(2) มีการบำรุงรักษาอุปกรณ์เครือข่ายและระบบคอมพิวเตอร์

(3) มีการพัฒนาระบบสารสนเทศในลักษณะรวมศูนย์เพื่อลดความซ้ำซ้อนในการพัฒนาระบบสารสนเทศและฐานข้อมูลของหน่วยงานต่างๆ ในมหาวิทยาลัย

(4) มีการวางแผนเพื่อกำหนดมาตรฐานกลางในการแลกเปลี่ยนข้อมูลเพื่อให้ข้อมูลสามารถอ้างอิงได้จากที่เดียว

(5) มีการกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูล

(6) มีการสำรองข้อมูลพร้อมทั้งทดสอบการรีสโตร์ฐานข้อมูลอย่างสม่ำเสมอและการเตรียมความพร้อมในกรณีฉุกเฉิน โดยครอบคลุมปัจจัยเสี่ยงที่จะเกิดความเสียหายดังนี้

(6.1) ปัจจัยภายใน ได้แก่

1) ระบบฐานข้อมูลหลักเสียหายหรือข้อมูลถูกทำลาย

2) การโดนไวรัสโจมตี

3) การถูกเจาะหรือลักลอบเข้าระบบฐานข้อมูลโดยไม่ได้รับอนุญาต

(6.2) ปัจจัยภายนอก ได้แก่

1) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องแม่ข่ายหลักของระบบฐานข้อมูล

2) การขโมยเครื่องแม่ข่ายของระบบฐานข้อมูล

3) การขำรุดเสียหายของเครื่องแม่ข่ายของระบบฐานข้อมูล

4) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

(7) มีการกำหนดสิทธิในการเข้าถึงข้อมูลระหว่างผู้ใช้งานและผู้ดูแลระบบเทคโนโลยีสารสนเทศ การกำหนดสิทธิ เปลี่ยนแปลง เพิ่มเติม หรือแก้ไขสิทธิในการเข้าถึงข้อมูลผู้ใช้งานระบบสารสนเทศ และผู้ดูและระบบเทคโนโลยีสารสนเทศนั้น จะทำโดยผู้ดูแลระบบสารสนเทศ ดังนี้

(7.1) เพิ่มข้อมูลการกำหนดสิทธิ์เมื่อเข้ามาทำงานใหม่

(7.2) ปรับปรุงข้อมูลการกำหนดสิทธิเมื่อโยกย้ายตำแหน่ง หรือหน่วยงาน

(7.3) ลบข้อมูลการกำหนดสิทธิเมื่อเกษียณอายุหรือลาออกจากงาน

5 การบริหารจัดการความเสี่ยงด้านบุคลากร

(1) การกำหนดโครงสร้าง/มอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศที่มีความเหมาะสมตรงตามอัตราและตำแหน่งภาระหน้าที่ คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีสารสนเทศด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

(2) บุคลากรของมหาวิทยาลัยนเรศวร ขาดความรู้ความเข้าใจในเรื่องของระบบเทคโนโลยีสารสนเทศโดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรมและนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะประสานงานและรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงในประเด็นนี้โดยการส่งเจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศ ให้มีความรู้ความเข้าใจในเชิงเทคนิคและนวัตกรรมให้สามารถนำมาพัฒนางาน

(3) กำหนดให้มีการฝึกอบรมในด้านที่เกี่ยวข้องกับระบบฐานข้อมูลสารสนเทศ สำหรับบุคลากรใน 2 ระดับ คือ ระดับผู้ดูแลระบบ และผู้ใช้งานทั่วไป

6 ความเสี่ยงด้านกลยุทธ์

(1) มีแผนบริหารจัดการเทคโนโลยีสารสนเทศและการสื่อสารที่ตอบสนองกลยุทธ์ของมหาวิทยาลัยนเรศวร

(2) มีการนำแผนการบริหารจัดการความเสี่ยงสู่การปฏิบัติได้

(3) ความเข้าใจและควมร่วมมือจากทุกส่วนงานที่เกี่ยวข้อง

7 ความเสี่ยงด้านพัสดุและการเงิน

(1) มีการจัดทำแผนบริหารจัดการการใช้จ่ายงบประมาณ

(2) การติดตามงบประมาณรายจ่ายอย่างต่อเนื่อง

(3) มีกระบวนการบริหารรายรับ – รายจ่าย อย่างโปร่งใส ตรวจสอบได้

(4) มีระบบการบริหารพัสดุและการเงินตามระเบียบข้อบังคับมหาวิทยาลัย

(5) มีการประกันภัยความมั่นคงปลอดภัยของทรัพย์สินเทคโนโลยีสารสนเทศ

10. นิยาม

10.1) ความเสี่ยง (Risk)

หมายถึง เหตุการณ์ การกระทำใด ๆ ที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบ หรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุวัตถุประสงค์และเป้าหมายตามภารกิจหลัก และตามแผนปฏิบัติการของกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในระดับองค์การ ระดับหน่วยงานและระดับบุคคลได้

ลักษณะของความเสี่ยง สามารถแยกออกเป็น 3 ส่วนดังนี้

1. ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง
2. เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงานหรือนโยบาย และ
3. ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

10.2) ปัจจัยเสี่ยง (Risk Factor)

หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

10.3) การประเมินความเสี่ยง (Risk Assessment)

หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

- โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง
- ผลกระทบ (Impact) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง
- ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

10.4) การบริหารความเสี่ยง (Risk Management)

หมายถึง การบริหารปัจจัยและควบคุมพฤติกรรม รวมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดมูลเหตุแต่ละโอกาสที่จะทำให้เกิดความเสียหาย เพื่อให้ระดับและขนาดของความเสียหาย และผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้ อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายการจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการประจำปีเป็นสำคัญ การบริหารความเสี่ยงจะอาศัยขั้นตอนที่ต่อเนื่อง เนื่องจากการระบุความเสี่ยงที่จะส่งผลกระทบจากความเสี่ยง และกำหนดแนวทางในการจัดการความเสี่ยงนั้นได้ถูกดำเนินการตามแผนที่วางไว้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก ดังนี้

1. การยอมรับ (Take, Accept) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องดำเนินการใดๆ เช่น กรณีที่มีความเสี่ยงในระดับไม่รุนแรงและไม่คุ้มค่าที่จะดำเนินการใดๆ ให้ขออนุมัติหลักการรับความเสี่ยงไว้และไม่ดำเนินการใด ๆ

2. การควบคุม (Treat) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้แต่ต้องมีการแก้ไขวิธีการควบคุม หรือมีการควบคุมเพิ่มเติม เพื่อให้มีการควบคุมที่เพียงพอและเหมาะสม เช่น การปรับปรุงกระบวนการดำเนินงาน การจัดทำมาตรฐานการควบคุม (Risk Based Internal Control)

3. การยกเลิก (Terminate) หรือ หลีกเลี่ยง (Avoid) หมายถึง การที่ความเสี่ยงนั้นไม่สามารถยอมรับได้และต้องจัดการให้ความเสี่ยงนั้นไปอยู่นอกเงื่อนไขของการดำเนินงาน เช่น การหยุดดำเนินงานหรือกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้น การเปลี่ยนแปลงวัตถุประสงค์ในการดำเนินงาน การลดขนาดของงานหรือกิจกรรมลง

4. การโอนย้าย (Transfer) หรือ แบ่ง (Share) หมายถึง การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น การจ้างบุคคลภายนอกมาดำเนินการแทน การทำประกันภัย

.....