แผนบริหารจัดการความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

กรมยุทธศึกษาทหารเรือ

130 23 ก.ย 57

กองการศึกษา ยศ.ทร.
เลขรับ 2303
วันที่ 25 ก.ย. 57
เวลา 0930

บันทึกข้อความ

ส่วนราชการ คณะทำงานย่อยหมวด ๖ (กปภ. โทร ๕๓๖๐๘)

ที่ กห ๐๕๓๔.๑๒/๒๙ **วันที่** ๒๕ ก.ย.๕๗

เรื่อง ขออนุมัติแผนบริหารความต่อเนื่องในภาวะวิกฤต และแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ยศ.ทร.

เสนอ ยศ.ทร.

๑. คณะทำงานย่อยหมวด ๖ การจัดการกระบวนการ เสนอขออนุมัติแผนบริหารความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. และแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ยศ.ทร. เพื่อให้ ยศ.ทร. สามารถดำรงการปฏิบัติงานตามภารกิจหรือกระบวนการหลักที่สร้างคุณค่าของ ยศ.ทร. ได้อย่างต่อเนื่องในภาวะฉุกเฉินหรือมีภัยพิบัติ รายละเอียดตาม (ร่าง) แผนฯ ที่แนบ จำนวน ๒ แผน

๒. คณะทำงานย่อยหมวด ๖ฯ ขอเสนอข้อมูลและมีข้อพิจารณา ดังนี้

๒.๑ พ.ร.ฎ.ว่าด้วยหลักเกณฑ์และการบริหารบ้านเมืองที่ดี พ.ศ.๒๕๔๖ มาตรา ๕๐ บัญญัติว่า "เพื่อให้การบริหารราชการเป็นไปอย่างมีประสิทธิภาพและคุ้มค่าในเชิงภารกิจของรัฐ สำนักงาน ก.พ.ร. จึงได้เสนอแนวทางการดำเนินการเตรียมความพร้อมต่อสภาวะวิกฤต และมาตรการที่เกี่ยวข้องต่อคณะรัฐมนตรีในการประชุมเมื่อ ๒๔ เม.ย.๕๕ และคณะรัฐมนตรีมีมติเห็นชอบแนวทางดังกล่าว ซึ่งกำหนดให้ทุกส่วนราชการทั้งระดับกรม จังหวัด สถาบันอุดมศึกษา องค์กรปกครองส่วนท้องถิ่น องค์การมหาชน และรัฐวิสาหกิจดำเนินการเพื่อสร้างความพร้อมให้แก่หน่วยงานเมื่ออยู่ในสภาวะวิกฤต ดังนั้น ทร. โดย สปช.ทร. จึงได้กำหนดให้ นขต.ทร. และหน่วยเฉพาะกิจ ทร. จัดทำแผนบริหารความต่อเนื่อง ทั้งนี้ สปช.ทร. ได้จัดการบรรยายพิเศษ เรื่อง "การบริหารความพร้อมต่อสภาวะวิกฤต" (Business Continuity Management : BCM) เมื่อวันศุกร์ที่ ๑๓ ธ.ค.๕๖ ณ โรงแรมรอยัลซิตี้ เขตบางพลัด กรุงเทพมหานคร และเชิญ นขต.ทร. และหน่วยเฉพาะกิจ ทร. เข้าร่วมฟังการบรรยายพิเศษฯ ดังกล่าว พร้อมทั้งให้ นขต.ทร. และหน่วยเฉพาะกิจ ทร. จัดทำร่างแผนความต่อเนื่องในสภาวะวิกฤตของหน่วย เสนอให้ สปช.ทร. ภายใน ๒๔ ม.ค.๕๗ เพื่อใช้เป็นข้อมูลเตรียมการจัดสัมมนาเชิงปฏิบัติการฯ โดยในครั้งนั้น ยศ.ทร. ได้ส่งผู้แทนเข้าร่วมสัมมนา จำนวน ๒ นาย จาก กศษ.ยศ.ทร. และ ศยร.ยศ.ทร. คือ น.อ.ชลธี นภาโชติ และ น.ท.กิติกรณ์ กาญจนวณิชย์ พร้อมทั้งได้มอบหมายให้ น.ต.จิตกร นรบัตร เป็นผู้จัดทำ (ร่าง) แผนความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. โดย กศษ.ยศ.ทร. ได้พิจารณา (ร่าง) แผนฯ ดังกล่าว เสนอให้ สปช.ทร. ใช้ประกอบการสัมมนาเชิงปฏิบัติการฯ ของ สปช.ทร. ในระหว่าง ๑๑ - ๑๓ ก.พ.๕๗ ตามสิ่งที่ส่งมาด้วย

๒.๒ คณะทำงานย่อยหมวด ๖ฯ มีหน้าที่รับผิดชอบการจัดการกระบวนการของ ยศ.ทร. ให้เป็นไปตามคู่มือการประเมินองค์กรด้วยตนเองของ ทร. (RTN Excellence Guidebook) สำหรับหน่วยสถานศึกษา ซึ่งในคู่มือฯ ดังกล่าว ระบุให้หน่วยสถานศึกษาต้องจัดทำแผนสำรองฉุกเฉินหรือแผนเผชิญเหตุรองรับภัยพิบัติ/ภาวะฉุกเฉิน (PM4) โดยจะต้องมีการกำหนดสถานการณ์ภัยพิบัติและภาวะฉุกเฉินที่มีผลกระทบต่อปัจจัยสำคัญของกระบวนการทำงานของหน่วยสถานศึกษา ทำการฝึกซ้อม บันทึกปัญหาข้อขัดข้องและปรับปรุงแผน ทั้งนี้ คณะทำงานย่อยหมวด ๖ฯ พิจารณาแล้วเห็นว่า (ร่าง) แผนบริหารความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. ที่ กศษ.ยศ.ทร. เสนอให้ สปช.ทร. ใช้ประกอบการสัมมนา นั้น สอดคล้องกับแผนสำรองฉุกเฉินหรือแผนเผชิญเหตุที่ระบุในคู่มือฯ ในหมวด ๖ฯ (PM4) สามารถนำมาใช้เป็นแผนสำรองฉุกเฉินหรือแผนเผชิญเหตุของ ยศ.ทร. ได้ เพียงแต่การเสนอขอความเห็นชอบ (ร่าง) แผนบริหารความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. ...

ของ ยศ.ทร. ในครั้งนั้น เป็นการเสนอขอความเห็นชอบเพื่อเสนอ สปช.ทร. เพื่อนำไปใช้ประกอบการสัมมนาเท่านั้น ยังมิได้เสนอขออนุมัติอย่างเป็นทางการ และยังไม่ได้สำเนาแจกจ่ายให้ทุกหน่วยและบุคลากรใน ยศ.ทร. ได้รับทราบ เพื่อใช้ในการเตรียมการและเป็นแนวทางปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉิน

๒.๓ ดังนั้น เพื่อให้การเสนอขออนุมัติแผนสำรองฉุกเฉินหรือแผนเผชิญเหตุ เป็นไปตามขั้นตอนและสอดคล้องกับที่ระบุไว้ในคู่มือฯ คณะทำงานย่อยหมวด ๖ฯ จึงขอเสนออนุมัติแผนบริหารความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. สำหรับใช้เป็นแผนสำรองฉุกเฉินหรือแผนเผชิญเหตุของ ยศ.ทร. เพื่อเตรียมความพร้อมและสามารถบริหารจัดการองค์กร ให้สามารถปฏิบัติงานตามภารกิจหน้าที่หลักได้อย่างต่อเนื่อง มีประสิทธิภาพแม้ประสบสถานการณ์วิกฤตหรือภัยพิบัติต่าง ๆ อันส่งผลต่อการสร้างความเชื่อมั่นที่มีต่อ ยศ.ทร. ทั้งนี้ คณะทำงานย่อยหมวด ๖ฯ ได้ปรับรายละเอียดการวิเคราะห์หน้าที่บทบาทของแต่ละหน่วยใน ยศ.ทร. ให้ครอบคลุมกับภารกิจของแต่ละหน่วย รวมถึงได้ปรับผลการวิเคราะห์ระดับผลกระทบในการปฏิบัติงานให้สอดคล้องกับเกณฑ์การประเมิน และเพิ่มเติมรายละเอียดบางส่วนให้ครอบคลุมกับคู่มือการบริหารความพร้อมต่อสภาวะวิกฤต ของ ก.พ.ร.

๒.๔ จากการประสานกับ กบศ.ยศ.ทร. ทราบว่าได้มีการเตรียมการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ ยศ.ทร. และแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ยศ.ทร. ซึ่งแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ ยศ.ทร. เป็นการเพิ่มเติมรายละเอียดในการรองรับสถานการณ์ความไม่แน่นอนและภัยพิบัติ ด้านระบบฐานข้อมูลและสารสนเทศของ ยศ.ทร. ซึ่งเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. จึงได้นำมาผนวกให้เป็นแผนเดียวกัน สำหรับแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ยศ.ทร. ถูกระบุอยู่ในหมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ (IT6) ของคู่มือฯ เป็นความรับผิดชอบของหมวด ๔ฯ แต่อย่างไรก็ตามเพื่อเป็นการลดภาระงานของผู้บังคับบัญชา คณะทำงานย่อยหมวด ๖ฯ พิจารณาแล้วเห็นว่าควรเสนอขออนุมัติในคราวกันกับแผนความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. ที่หมวด ๖ฯ รับผิดชอบ เพื่อให้หน่วยต่าง ๆ ใน ยศ.ทร. ได้ใช้ยึดถือเป็นหลักปฏิบัติในการรองรับและเตรียมความพร้อมรับมือต่อสภาวะวิกฤตต่าง ๆ ที่อาจเกิดขึ้นได้ ให้สามารถปฏิบัติงานตามภารกิจหน้าที่หลักได้อย่างต่อเนื่อง

๓. เห็นควร

๓.๑ ให้ความเห็นชอบและอนุมัติแผนบริหารความต่อเนื่องในสภาวะวิกฤตของ ยศ.ทร. และแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ยศ.ทร. ตามข้อ ๑. และกรุณาลงนามในคำนำของแผนฯ ที่แนบ

๓.๒ ให้กองต่าง ๆ ใน บก.ฯ และ นขต.ยศ.ทร. ศึกษาขั้นตอนการปฏิบัติในแผนฯ และชี้แจงให้กำลังพลภายในหน่วยรับทราบ โดยสามารถดาวน์โหลดแผนฯ ได้ที่เว็บไซต์ ยศ.ทร.

๓.๓ กธก.ยศ.ทร. สำเนาบันทึกนี้และแผนฯ ให้กองต่าง ๆ ใน บก.ฯ นขต.ยศ.ทร. และเผยแพร่แผนฯ ในระบบสารบรรณอิเล็กทรอนิกส์ ต้นเรื่องส่งคืนคณะทำงานย่อยหมวด ๖ฯ (กปภ.ยศ.ทร.)

จึงเสนอมาเพื่อโปรดพิจารณาดำเนินการต่อไป

น.อ.

หัวหน้าคณะทำงานย่อยหมวด ๖ฯ และ

รอง เสธ.ยศ.ทร.

เสนอ ประธานคณะทำงานพัฒนาคุณภาพการบริหารจัดการภาครัฐ ยศ.ทร.

เห็นควรอนุมัติตามที่คณะทำงานย่อยหมวด ๖ การจัดการกระบวนการ เสนอในข้อ ๓ และกรุณาลงนามในคำนำแผนบริหารความต่อเนื่องในสภาวะวิกฤติของ ยศ.ทร. และคำนำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ยศ.ทร. ที่แนบ

น.อ.

เลขานุการฯและรอง เสธ.ยศ.ทร.

๒๕ ก.ย.๕๗

เสนอ

เห็นควรอนุมัติตามที่คณะทำงานย่อยหมวด ๖ การจัดการกระบวนการ เสนอในข้อ ๓ และกรุณาลงนามในคำนำแผนบริหารความต่อเนื่องในสภาวะวิกฤติของ ยศ.ทร. และคำนำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ยศ.ทร. ที่แนบ

พล.ร.ต.

ประธานคณะทำงานฯและรอง จก.ยศ.ทร.

๒๕ ก.ย.๕๗

- อนุมัติ
- ลงนามแล้ว

พล.ร.ท.

จก.ยศ.ทร.

๒๕ ก.ย.๕๗

ปิ่นทัศน์
นงต., กองกลาง
- งานทั้งหมดแผนกกรรมวิธี ดำเนินการลงระบบเรียบร้อยแล้ว ธุรการ
(นต. พีระ)

- ส่งทางระบบงานสารบรรณอิเล็กทรอนิกส์ทหารเรือ 26/9/57

คำนำ

เนื่องด้วยภารกิจของ ยศ.ทร. มีหน้าที่ อำนวยการ ประสานงาน แนะนำ กำกับการ และดำเนินการเกี่ยวกับการฝึกหัดศึกษาและตำรา การอนุศาสนาจารย์ งานประวัติศาสตร์และพิพิธภัณฑ์ทหาร การศึกษา วิเคราะห์ จัดทำ ประเมินยุทธศาสตร์ และกำหนดหลักนิยมของ ทร. ตลอดจนการฝึก การศึกษา วิชาการทหารเรือ และวิทยาการที่เกี่ยวข้องของสถานศึกษาในบังคับบัญชาและสถานศึกษาในกำกับ โดยมี จก.ยศ.ทร. เป็นผู้บังคับบัญชารับผิดชอบนั้น เทคโนโลยีสารสนเทศและการสื่อสาร จึงเข้ามามีบทบาทสำคัญที่ช่วยสนับสนุนในการบริหารจัดการ และปฏิบัติราชการของทุก นขต.ยศ.ทร. ให้บรรลุ “ภารกิจ” และประสบผลสัมฤทธิ์ตามตัวชี้วัด และเป้าหมายที่ได้กำหนดไว้ จึงถือได้ว่าเทคโนโลยีสารสนเทศและการสื่อสารเป็น “เครื่องมือสำคัญ” ที่มีความจำเป็นต้องดูแล ปรับปรุง บำรุงรักษา เพื่อให้สามารถสนับสนุนการบริหารจัดการและปฏิบัติงานได้อย่างต่อเนื่อง

ยศ.ทร. จึงได้จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้การจัดการภายในหน่วยงาน มีประสิทธิภาพและมีความยืดหยุ่น ลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ สามารถรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ จึงหวังเป็นอย่างยิ่งว่าแผนฉบับนี้ จะเป็นประโยชน์ต่อเจ้าหน้าที่ที่รับผิดชอบได้ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการความเสี่ยงด้านสารสนเทศของ ยศ.ทร. ต่อไป

พล.ร.ท.
จก.ยศ.ทร.
๒๕ ก.ย.๕๗

สารบัญ

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
กรมยุทธศึกษาทหารเรือ

๑. <u>หลักการและเหตุผล</u>

การบริหารจัดการความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้อง “ภารกิจ” ของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยง ควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน โดยมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชาและผู้ดูแลระบบของหน่วยงาน

หน่วยงานจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยงและเพื่อความสามารถในการดำเนินภารกิจของหน่วยงานให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเพียงเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุเป้าประสงค์และภารกิจที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานของหน่วยงาน ที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่า

๒. <u>ความหมายของการบริหารความเสี่ยง</u>

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด เกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการเพื่อให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง อยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

๒. การระบุความเสี่ยงต่าง ๆ (Event Identification)

๓. การประเมินความเสี่ยง (Risk Assessment)

๔. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

๕. กิจกรรมการบริหารความเสี่ยง (Control Activities)

๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

๗. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

กระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประกอบด้วย ๕ ขั้นตอน ดังนี้

๑. การประเมินความเสี่ยง (Risk assessment) ประกอบด้วย กระบวนการวิเคราะห์ความเสี่ยงและการประเมินค่าความเสี่ยง

๑.๑ การวิเคราะห์ความเสี่ยง (Risk analysis) ประกอบด้วย ๓ ขั้นตอน ดังนี้

๑.๑.๑ การชี้ระบุความเสี่ยง (Risk identification)

๑.๑.๒ ลักษณะรายละเอียดของความเสี่ยง (Risk description)

๑.๑.๓ การประมาณความเสี่ยง (Risk estimation)

๑.๒ ประเมินค่าความเสี่ยง (Risk evaluation)

๒. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

๓. กระบวนการบำบัดความเสี่ยง (Risk treatment)

๔. การรายงานความเสี่ยงตกค้าง (Residual risk reporting)

๕. การเฝ้าสังเกต (Monitoring)

๓. <u>วัตถุประสงค์</u>

๓.๑ เพื่อให้การจัดการภายในหน่วยงาน มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

๓.๒ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของหน่วยงาน

๓.๓ เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓.๔ เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๕ เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน การเงิน กฎ ระเบียบ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

๔. <u>ขอบเขตการดำเนินการ</u>

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ฉบับนี้มีขอบเขตครอบคลุมเฉพาะการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของ ยศ.ทร. เท่านั้น

๕. <u>การประเมินความเสี่ยง</u> (Risk assessment)

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของ ยศ.ทร. สามารถแยกประเภทความเสี่ยง เป็น ๔ ประเภท ดังนี้

๕.๑ **ความเสี่ยงด้านเทคนิค** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker หรือถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๕.๒ **ความเสี่ยงจากผู้ปฏิบัติงาน** เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของ ยศ.ทร. เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๕.๓ **ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน** เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๕.๔ **ความเสี่ยงด้านการบริหารจัดการ** เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตาราง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน/ ระบบสารสนเทศ ระบบฐานข้อมูล
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำเครื่องส่วนตัว, wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายโดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่น ๆ ที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่าย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ/ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT03	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ/ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ
๔. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT04	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	-นโยบายการบริหารจัดการกำลังพลสายวิทยาการสารสนเทศและการสื่อสารของ สสท.ทร.	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	-การโยกย้ายกำลังพลประจำปี	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	-นโยบายการบริหาร/การจัดสรรงบประมาณประจำปี	ผู้ใช้งาน ผู้ดูแลระบบ/ ระบบฐานข้อมูล ระบบสารสนเทศ
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT08	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ เกิดความเสียหายทั้งชีวิตและทรัพย์สิน	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ/ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT09	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ และถูกบุกยึดสถานที่ทำงาน อุปกรณ์ต่าง ๆ ได้รับความเสียหาย	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ/ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT10	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ/ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ
๑๑.ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT11	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU, Hard disk, Ram ฯลฯ ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

๖. <u>การประมาณความเสี่ยง</u> (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไร และผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณความเสี่ยง เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	๕ ครั้ง/ปี
๔	สูง	๔ ครั้ง/ปี
๓	ปานกลาง	๓ ครั้ง/ ปี
๒	น้อย	๒ ครั้ง/ปี
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	> ๑๐ ล้านบาท หรือเกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
๔	สูง	> ๕ แสนบาท - ๑๐ ล้านบาท หรือเกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	> ๒.๕ แสนบาท - ๕ แสนบาท หรือระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	> ๑ แสนบาท - ๒.๕ แสนบาท หรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	ไม่เกิน ๑ แสนบาท หรือเกิดเหตุร้ายที่ไม่มีความสำคัญ

การประมาณความเสี่ยง แสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ	ความถี่	ความรุนแรง
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน/ระบบสารสนเทศ ระบบฐานข้อมูล	๕	๔
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำเครื่องส่วนตัว wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่าย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่าย ไม่สามารถใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่น ๆ ที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่าย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ/ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย	๕	๓
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT03	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่อง	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์แม่แม่ข่าย	๕	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ	ความถี่	ความรุนแรง
			แม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วน เกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ		อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ		
๔. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT04	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์/แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์ แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๔
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	-นโยบายการบริหารจัดการกำลังพลสายวิทยาการสารสนเทศ และการสื่อสารของ สสท.ทร.	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ	ความถี่	ความรุนแรง
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	-การโยกย้ายกำลังพลประจำปี	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๑
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	-นโยบายการบริหาร/การจัดสรรงบประมาณประจำปี	ผู้ใช้งาน ผู้ดูแลระบบ/ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT08	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหว จนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ เกิดความเสียหายทั้งชีวิตและทรัพย์สิน	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผู้ได้รับผลกระทบ/ผลกระทบ	ความถี่	ความรุนแรง
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT09	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ และถูกบุกยึดสถานที่ทำงาน อุปกรณ์ต่าง ๆ ได้รับความเสียหาย	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๔
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT10	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย	๓	๔
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT11	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU, Hard disk, Ram ฯลฯ ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ/เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย	๑	๕

๗. <u>การประเมินค่าความเสี่ยง</u> (Risk evaluation)

การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ

กลยุทธ์ในการจัดการความเสี่ยง ประกอบด้วย ๔ รูปแบบ คือ

๑. Risk Acceptance การยอมรับความเสี่ยง เหตุผลคือค่าใช้จ่ายจะสูงกว่าผลที่ได้รับ จึงใช้แผนและมาตรการกำกับดูแล

๒. Risk Reduction/Control การลด/การควบคุม ความเสี่ยงด้วยมาตรการต่าง ๆ

๓. Risk Avoidance การหลีกเลี่ยงความเสี่ยง โดยการปรับ/เปลี่ยนแปลงรูปแบบการทำงาน

๔. Risk Sharing การกระจายความเสี่ยงด้วยการโอนย้ายความเสี่ยง ไปให้หน่วยงานอื่นรับผิดชอบ เช่น การจ้างผู้อื่นดูแลบำรุงรักษา

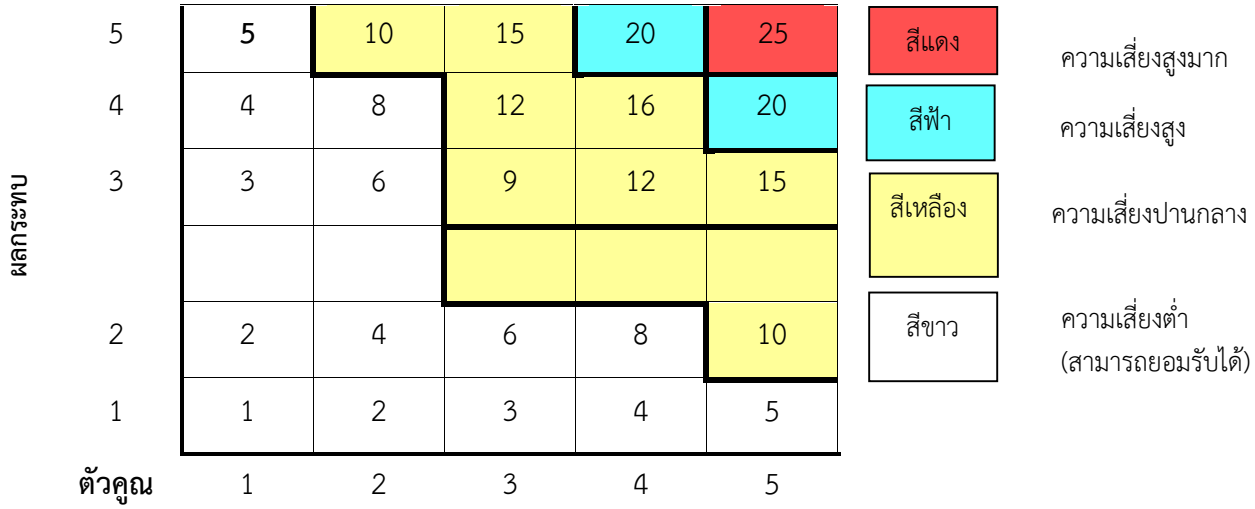
ลำดับความเร่งด่วนในการจัดการความเสี่ยง (กลั่นกรอง)

โดยการให้ความสำคัญและการจัดการโดยเร่งด่วนกับกลุ่มรายการที่มีค่าระดับคะแนนความเสี่ยงมากที่สุด จัดเป็นระดับความเสี่ยงสูงมาก เป็นลำดับแรก และจัดกลุ่มรองลงมาตามคะแนน ได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ ซึ่งเกณฑ์ในการจัดแบ่งแสดงได้ดังนี้

ระดับคะแนนความ	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ - ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๙ - ๑๖	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗ - ๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความ	ฟ้า
≥ ๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

แผนภูมิความเสี่ยง (Risk Map)
การวัดระดับความเสี่ยง

การประเมินความเสี่ยง



โอกาสที่จะเกิด

การประเมินค่าความเสี่ยง แสดงดังตารางต่อไปนี้

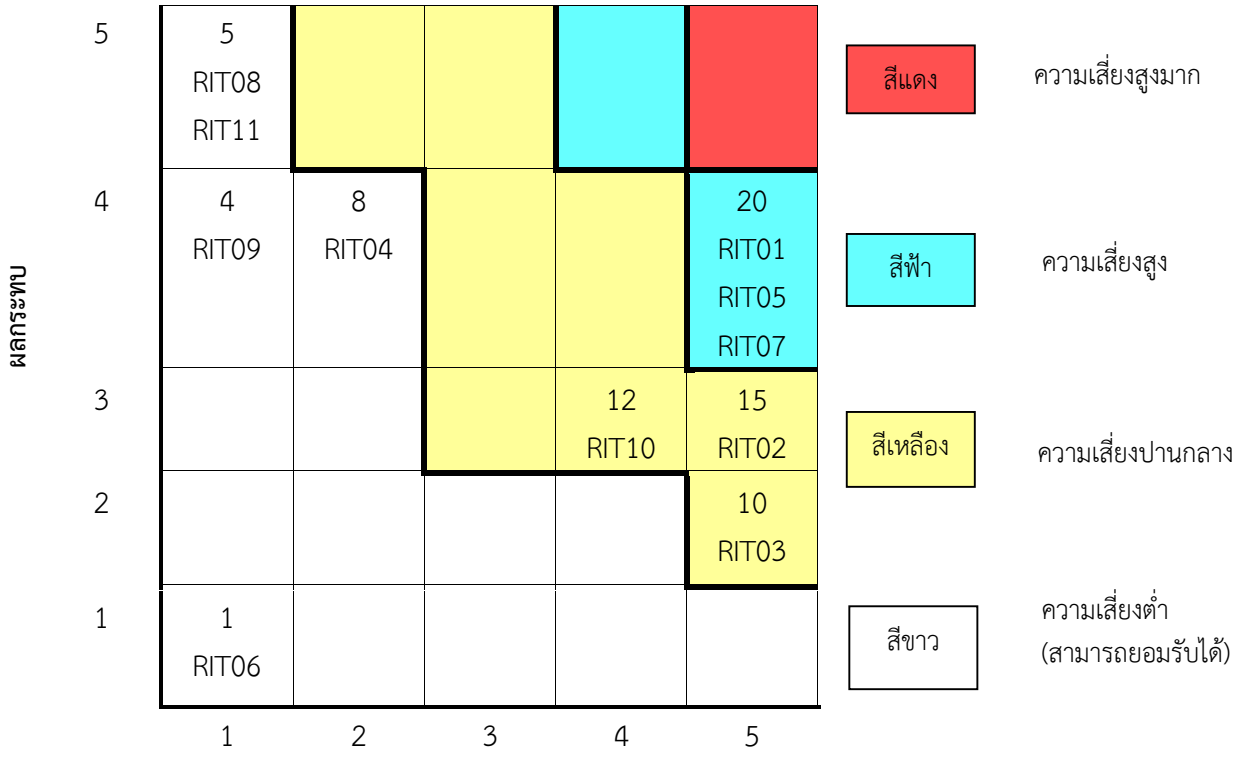
ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๕	๔	๒๐
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำเครื่องส่วนตัว wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายโดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัยทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่น ๆ ที่รับสัญญาณได้ เชื่อมต่อ	๕	๓	๑๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
			เข้ากับระบบเครือข่าย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย			
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT03	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๕	๒	๑๐
๔. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	RIT04	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	๒	๔	๘
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๕	๔	๒๐
๖. ความเสี่ยงจากการเปลี่ยนแปลง	RIT06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการ	๑	๑	๑

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
นโยบายผู้บริหาร			บริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ			
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๕	๔	๒๐
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT08	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร น้ำท่วม กระแสไฟฟ้าถูกตัดขาด ไฟดับ แผ่นดินไหว จนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ เกิดความเสียหายทั้งชีวิตและทรัพย์สิน	๑	๕	๕
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT09	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ และถูกบุกยึดสถานที่ทำงาน อุปกรณ์ต่าง ๆ ได้รับความเสียหาย	๑	๔	๔
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT10	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	๓	๔	๑๒
๑๑. ความเสี่ยงจากการโจรกรรม	RIT11	ความเสี่ยงด้านการบริหารจัดการ/	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์	๑	๕	๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
เครื่องคอมพิวเตอร์และอุปกรณ์		ความเสี่ยงจากผู้ปฏิบัติงาน	คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU, Hard disk, Ram ฯลฯ ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้			

แผนภูมิความเสี่ยง



๘. <u>การรายงานผลการวิเคราะห์ความเสี่ยง</u> (Risk reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศในการบริหารจัดการได้อย่างมีประสิทธิภาพ ดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	RIT01 ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๒๐

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๒	RIT05 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๒๐
๓	RIT07 ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๒๐
๔	RIT02 ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำเครื่องส่วนตัว wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายโดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่าย ไม่สามารถใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่น ๆ ที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่าย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	๑๕
๕	RIT10 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	๑๒
๖	RIT03 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์	๑๐

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
			อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	
๗	RIT04 ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	๘
๘	RIT08 ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร น้ำท่วม แผ่นดินไหว จนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ เกิดความเสียหายทั้งชีวิตและทรัพย์สิน	๕
๙	RIT11 ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU, Hard disk, Ram ฯลฯ ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๕
๑๐	RIT09 ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ และถูกบุกยึดสถานที่ทำงาน อุปกรณ์ต่าง ๆ ได้รับความเสียหาย	๔
๑๑	RIT06 ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๑

๙. <u>แผนจัดการความเสี่ยง</u> (Risk Management Action Plan)

นโยบายของ ยศ.ทร. ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ ๙

สำนักงาน ก.พ.ร. กำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้

ผลกระทบต่อวัตถุประสงค์ของการควบคุม มี ๓ ด้าน คือ

๑. ด้านการดำเนินงาน (O)

๒. ด้านการเงิน (F)

๓. ด้านการกำกับการปฏิบัติตามกฎหมาย กฎเกณฑ์ ระเบียบ (C)

ตารางแสดงแผนจัดการความเสี่ยง

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	ผลกระทบต่อวัตถุประสงค์ของการควบคุม	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑	RIT01 ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๒๐	O, C	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - จัดทำแผนการฝึกศึกษาอบรมประจำปี
๒	RIT05 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๒๐	O, C	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- บริหารจัดการกำลังพลเพื่อรองรับงานอย่างเหมาะสม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้
๓	RIT07 ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๒๐	O, F, C	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศเพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ
๔	RIT02 ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๑๕	O, C	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	ผลกระทบต่อวัตถุประสงค์ของการควบคุม	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
					- ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย
๕	RIT10 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	๑๒	O, F, C	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- หาทางป้องกัน/กำจัดสัตว์กัดแทะอุปกรณ์ ในการเดินสายสัญญาณสื่อสารควรร้อยใส่ท่อที่ป้องกันสัตว์กัดแทะ - จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
๖	RIT03 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๑๐	O, C	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	ผลกระทบต่อวัตถุประสงค์ของการควบคุม	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๗	RIT04 ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	๘	O, C	- ยอมรับความเสี่ยง	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
๘	RIT08 ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	๕	O, F, C	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
๙	RIT11 ความเสี่ยงจากการโจรกรรมเครื่อง	๕	O, F, C	- ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจสอบระบบการ

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	ผลกระทบต่อวัตถุประสงค์ของการควบคุม	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
	คอมพิวเตอร์และอุปกรณ์				ป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง
๑๐	RIT09 ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๔	O, C	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้
๑๑	RIT06 ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๑	O, C	- ยอมรับความเสี่ยง	- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศเพื่อให้เกิดความต่อเนื่องในการบริหารจัดการ

๑๐. <u>การทบทวน ตรวจสอบ และปรับปรุงแผน</u>

คณะกรรมการ คทส.ยศ.ทร. ทำการทบทวน ตรวจสอบและปรับปรุง และขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยควรจัดทำให้เสร็จสิ้นภายในไตรมาสแรกของปีงบประมาณ

.....