



# คู่มือ

## การจัดทำแผนบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานสภาเกษตรกรแห่งชาติ



กองสื่อสารและสารสนเทศ  
สำนักงานสภาเกษตรกรแห่งชาติ

คู่มือ

การจัดทำแผนบริหารความเสี่ยง  
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร  
สำนักงานสภาเกษตรกรแห่งชาติ

## สารบัญ

	หน้า
ระเบียบและนโยบายด้านความมั่นคงที่เกี่ยวข้อง	๑
ความหมายของการบริหารความเสี่ยง	๑
วัตถุประสงค์ของการบริหารจัดการความเสี่ยง	๒
ทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๓
การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๓
การประเมินความเสี่ยง	๓
การประเมินค่าความเสี่ยง	๕
การบรรเทาความเสี่ยง	๗
การควบคุมความเสี่ยง	๘
ประเภทของการควบคุมความเสี่ยง	๙
กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๑๑
การเฝ้าสังเกต	๑๑
แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศและการสื่อสาร	๑๒

## คู่มือการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เนื่องจากภารกิจของสำนักงานสภาเกษตรกรแห่งชาติ ได้นำเอาระบบเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานของหน่วยงาน ฉะนั้นเพื่อให้การนำระบบเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานเกิดประโยชน์สูงสุด และลดโอกาสความเสียหายที่อาจเกิดขึ้น จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน การบริหารจัดการความเสี่ยงระบบสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาตินี้ มีวัตถุประสงค์เพื่อใช้เป็นแนวทางตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศของหน่วยงานขึ้นตรงสำนักงานสภาเกษตรกรแห่งชาติ ด้วยการคาดการณ์ล่วงหน้าในกรณีที่มีความเสี่ยงนั้นเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในดำเนินการ เป็นการช่วยเสริมสร้างความมั่นคงปลอดภัยระบบสารสนเทศและความมั่นคงปลอดภัยทางด้านไซเบอร์ให้มีความแข็งแกร่งต่อการถูกโจมตีจาก Hacker และช่วยให้การพัฒนาทางด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสภาเกษตรกรแห่งชาติ มีขีดความสามารถในการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางตามยุทธศาสตร์สำนักงานสภาเกษตรกรแห่งชาติ

### ระเบียบและนโยบายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

๑. ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
๓. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒
๔. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาติ

### ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบต่อหรือสร้างความหรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายของหน่วยงาน ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน งบประมาณ และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด ทำไม และเกิดขึ้นได้อย่างไรทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง 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 ปานกลางและต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง อยู่ในระดับที่หน่วยงานยอมรับได้ ซึ่งการจัดการความเสี่ยงอาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง ดังนี้

การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง

การลด/การควบคุมความเสี่ยง (Risk Reduction) เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

การกระจายความเสี่ยงหรือการโอนความเสี่ยง (Risk Sharing) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งความรับผิดชอบไป

การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการกับความเสี่ยงที่อยู่ในระดับสูงและ หน่วยงานไม่อาจยอมรับได้จึงต้องตัดสินใจยกเลิกโครงการ/กิจกรรมนั้นไป

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

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Treadway Commission) และ ISO ๒๗๐๐๑ 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)

### วัตถุประสงค์ของการบริหารจัดการความเสี่ยง

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และการสื่อสารของหน่วยงาน
๒. เพื่อให้สามารถวางแผนควบคุมและแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ
๓. เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุด และลดโอกาสที่อาจเกิดความเสียหาย

๔. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศของหน่วยงานให้เจ้าหน้าที่ที่เกี่ยวข้องนำไปใช้ประโยชน์

๕. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่า จะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับ ความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

### ทรัพยากรด้านเทคโนโลยีและการสื่อสาร (ICT Resources)

๑. ระบบงาน (Application System) ได้แก่ ขั้นตอนและกระบวนการปฏิบัติงาน
๒. เทคโนโลยี (Technology) ได้แก่ เครื่องคอมพิวเตอร์ (Hardware) โปรแกรมระบบ (Operating System) ระบบบริหารฐานข้อมูล (Database Management System) ระบบเครือข่าย (Network) และระบบมัลติมีเดีย
๓. องค์กรประกอบ (Facilities) ได้แก่ ทรัพยากรต่าง ๆ ที่ใช้เป็นสถานที่ติดตั้งหรือจัดวาง ตลอดจน สาธารณูปโภคที่จำเป็น เพื่อการปฏิบัติงานของระบบสารสนเทศ
๔. บุคลากร (People) ได้แก่ บุคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงานสำหรับการ ดูแลและจัดระบบ รวมถึงผู้ใช้งานทั่วไป
๕. ข้อมูล (Data) ได้แก่ ข้อมูลในรูปแบบต่าง ๆ ทั้งที่มีโครงสร้างและไม่มีโครงสร้างข้อมูลด้านกราฟิก และข้อมูลที่เป็นมัลติมีเดีย

### การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

#### ๑. การประเมินความเสี่ยง (Risk assessment)

การวิเคราะห์ความเสี่ยง การวิเคราะห์ความเสี่ยงประกอบด้วย ๓ กระบวนการ คือ

๑.๑ การชี้ระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงที่หน่วยงานเผชิญอยู่ กระบวนการนี้จำเป็นต้องอาศัยความรู้ความเข้าใจหน่วยงาน ภารกิจและกิจกรรมสิ่งแวดล้อมด้านกฎหมาย สังคม การเมืองและวัฒนธรรม พัฒนาการและปัจจัยที่มีต่อความสำเร็จของหน่วยงานรวมทั้งโอกาสและภัยคุกคามที่มีต่อ หน่วยงาน การชี้ระบุความเสี่ยงควรได้ดำเนินการอย่างทั่วถึงครอบคลุมกิจกรรมในทุก ๆ ด้านของหน่วยงาน สาเหตุ สำคัญของความเสี่ยงคือการมีภัยคุกคาม (Threat) ที่อาจส่งผลให้เกิดการละเมิดความมั่นคงสารสนเทศและส่งผล เสียตามมา

การชี้ระบุความเสี่ยง (Risk identification) อาจพิจารณาถึงเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วใน อดีตกับหน่วยงานนั้นหรือหน่วยงานอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้ กระบวนการในการชี้ระบุความเสี่ยงอาจใช้วิธีการต่าง ๆ ร่วมกันดังนี้ เช่น

- การระดมสมอง (brain storming)
- การออกแบบสอบถาม (questionnaire)
- การวิเคราะห์กระบวนการทำงานหรือกิจกรรมในภารกิจ (business process analysis)
- การวิเคราะห์สภาพการณ์เหตุการณ์ละเมิดความมั่นคง (scenario analysis)

- การประชุมเชิงปฏิบัติการด้านการประเมินความเสี่ยง (risk assessment workshop)
- การสืบสวนเหตุการณ์ละเมิดความมั่นคงสารสนเทศ (incident investigation)
- การตรวจสอบและการตรวจสอบสภาพระบบ (auditing and inspection)
- การวิเคราะห์ HAZOP (hazard and operability studies)
- การวิเคราะห์สถานการณ์ (SWOT analysis)

๑.๒ ลักษณะรายละเอียดของความเสี่ยง (Description of risk) เมื่อชี้ระบุความเสี่ยงได้แล้ว และนำมาบรรยายรายละเอียดและลักษณะของความเสี่ยงนั้น ได้แก่

- ชื่อความเสี่ยง (Name)
- ขอบเขต (Scope)
- ลักษณะความเสี่ยง (Nature)
- ผู้ที่มีผลกระทบ
- ลักษณะเชิงปริมาณ
- การยอมรับความเสี่ยง
- การบำบัดและการควบคุม
- แนวทางการปรับปรุง
- การพัฒนากลยุทธ์และนโยบาย

๑.๓ การประมาณความเสี่ยง (Risk estimation) ขั้นตอนนี้เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

โอกาส หรือ ความน่าจะเป็น (Probability or Likelihood) หรือความบ่อยครั้งของการเกิดเหตุ หรือเหตุการณ์ อาจแบ่งแบบง่าย ๆ เป็น ๕ ระดับจากน้อยไปหามาก เช่น

- บ่อย (frequent) พบได้บ่อยครั้งเป็นประจำ
- เป็นไปได้ (probable)
- ตามโอกาส (occasional)
- น้อยครั้งมาก (remote)
- แทบไม่เกิดเลย (improbable)

หมายเหตุ บางหน่วยงานแบ่งความบ่อยครั้งของการเกิดเหตุออกเป็น ๓ ระดับ เท่านั้น ซึ่งแล้วแต่ความต้องการเพื่อความเหมาะสมของแต่ละหน่วยงาน

- ความรุนแรงของสิ่งที่เกิดขึ้นตามมา (Severity of consequence) อาจแบ่งเป็น ๔ ระดับคือ
- สูงมาก (severe)
  - สูง (high)
  - ปานกลาง (moderate)
  - ต่ำ (low)

จากการวิเคราะห์ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศสามารถแยกประเภทความเสี่ยงเป็น ๔ ด้าน ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี (Malware) ถูกก่อวินาศกรรมจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการทำงานด้านสารสนเทศ

## ๒. การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยของขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้น ทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

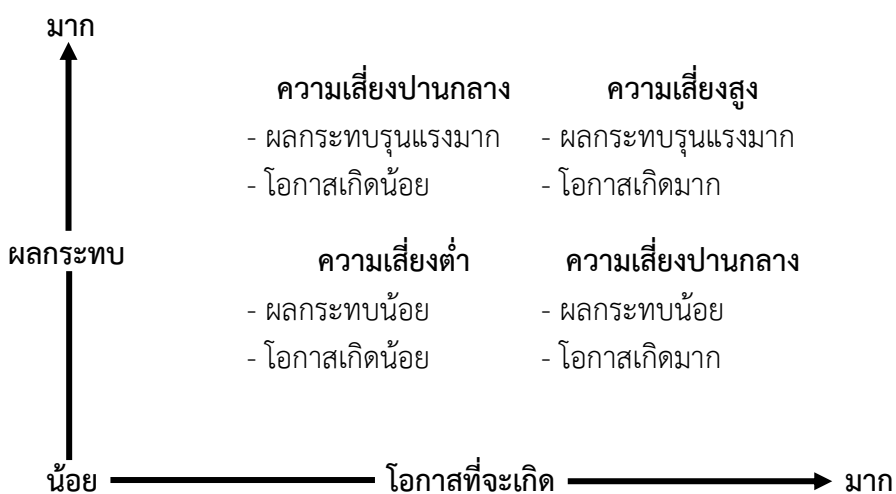
ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ × ความรุนแรงของเหตุการณ์ต่าง ๆ  
ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

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

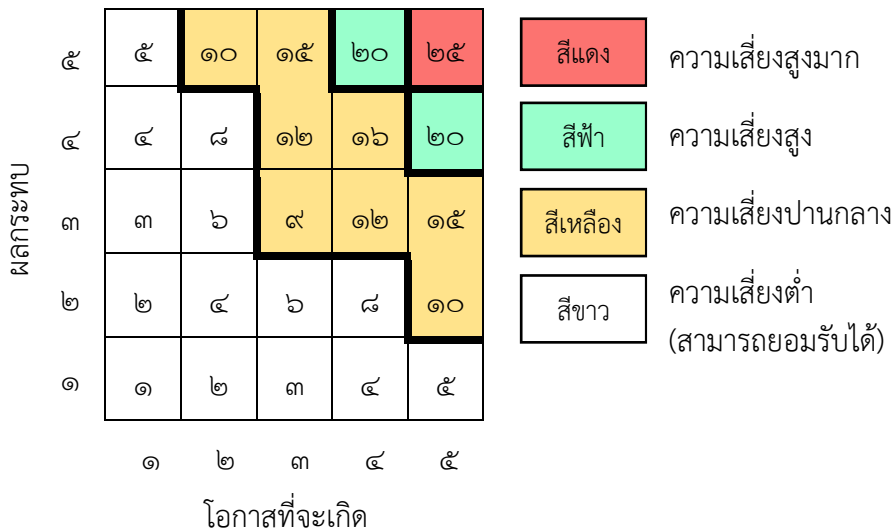


### แผนภูมิความเสี่ยง (Risk Map)

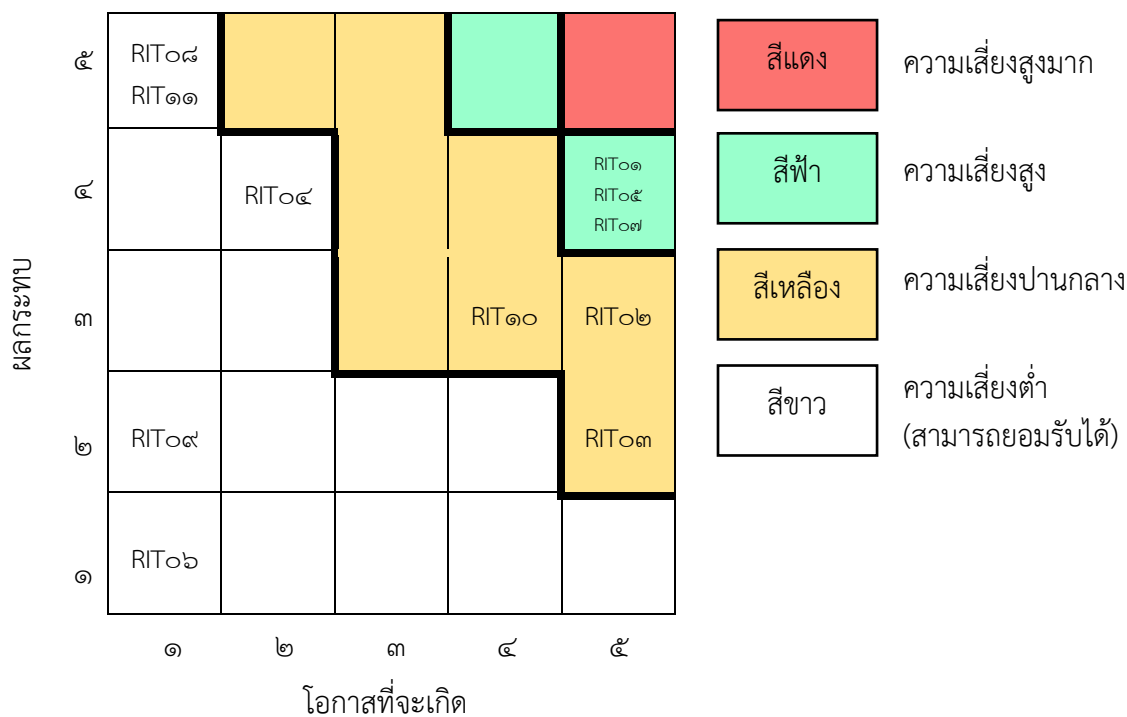
การวัดระดับความเสี่ยงโดยจัดลำดับจากผลกระทบและความเป็นไปได้ที่จะเกิดขึ้น



### การประเมินความเสี่ยง



## การประเมินค่าความเสี่ยงแสดงตารางต่อไปนี้ แผนภูมิความเสี่ยง



### ๓. การบรรเทาความเสี่ยง (Risk mitigation)

การบรรเทาความเสี่ยงเกี่ยวข้องกับการจัดลำดับ การคำนวณความเสี่ยง และการลงมือควบคุมการลดความเสี่ยงอย่างเหมาะสมตามแนวทางที่มาจากประเมินความเสี่ยง เนื่องจากการที่จะกำจัดความเสี่ยงในระบบทั้งหมดนั้นเป็นเรื่องที่ทำได้ยาก ผู้บังคับบัญชาของหน่วยจะต้องเป็นผู้รับผิดชอบการทำงานนี้ด้วยเงื่อนไขในการใช้งบประมาณที่สมดุล เพื่อให้เกิดประสิทธิภาพสูงสุด และใช้วิธีการควบคุมที่เหมาะสมที่สุดเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยส่งผลกระทบต่อภารกิจและทรัพยากรของหน่วยให้น้อยที่สุด

ทางเลือกเพื่อการบรรเทาความเสี่ยง สามารถแบ่งออกเป็น ๕ ประเภทดังนี้

๑. การยอมรับความเสี่ยง (Risk Acceptance) คือการยอมรับความเสี่ยงในระดับที่เป็นอยู่และให้ระบบข้อมูลสารสนเทศดำเนินงานไปตามปกติ ซึ่งเป็นการยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวตนเพียงใช้ชื่อผู้ใช้งานและรหัสผ่าน มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การใช้ Biometrics เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า หน่วยงานอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปและปรับปรุงเมื่อมีโอกาส

๒. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือการหลีกเลี่ยงความเสี่ยงด้วยการกำจัดสาเหตุของความเสี่ยง เช่น เมื่อพบว่าปัจจุบันหน่วยงาน มีการสำรองข้อมูลเพียง ๑ ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การหลีกเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล ๒ ชุด และแยกเก็บในสถานที่ที่ต่างกันหรือระบบด้านยุทธการที่มีชั้นความลับ ลับมาก ต้องห้ามมีการเชื่อมต่อกับอินเทอร์เน็ต เพื่อหลีกเลี่ยงภัยจาก Hacker เป็นต้น

๓. การจำกัดความเสี่ยง (Risk Limitation) คือ การทำระบบควบคุมเพื่อให้เกิดผลกระทบจากการถูกคุกคามระบบหรือจากความไม่มั่นคงของระบบให้น้อยที่สุด เช่น การใช้ Firewall ป้องกันระบบจากภัยคุกคามในอินเทอร์เน็ต

๔. การวิจัยและการรับรู้ความเสี่ยง (Research and Acknowledgement) คือการลดความสูญเสียที่เกิดจากความเสียหายโดยการตรวจสอบเพื่อรับทราบความอ่อนแอของระบบและค้นคว้าวิจัยให้ได้วิธีการควบคุมเพื่อเสริมความมั่นคงให้แก่ระบบ

๕. การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การถ่ายโอนความเสี่ยงด้วยการหาทางเลือกอื่นเพื่อชดเชยความสูญเสีย เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน หน่วยงานอาจเลือกซื้อประกัน หรือสัญญาการซ่อมบำรุง เป็นต้น

#### ๔. การควบคุมความเสี่ยง (Risk control)

เมื่อต้องมีการควบคุมเกิดขึ้นสิ่งที่ต้องปฏิบัติคือระบุความเสี่ยงที่เกิดขึ้นให้มากที่สุด แล้วพยายามหาวิธีลดความเสี่ยงด้วยวิธีที่มีต้นทุนต่ำและส่งผลกระทบต่อภารกิจอื่น ๆ ของหน่วยงานให้น้อยที่สุดกระบวนการในการบรรเทาความเสี่ยงสรุปได้ดังนี้

๑. จัดลำดับความสำคัญของการปฏิบัติงาน (Prioritize Actions) จากผลการจัดลำดับความเสี่ยง ในกระบวนการประเมินความเสี่ยง นำไปสู่การจัดลำดับการลงมือปฏิบัติงานด้วย ภายใต้ทรัพยากรที่มีอยู่ลำดับแรกสุดควรจะต้องเลือกลงมือกับความเสี่ยงที่มีระดับความเสี่ยงสูง ซึ่งต้องการการแก้ไขในทันทีเพื่อปกป้อง ภารกิจของหน่วยผลลัพธ์ที่ได้คือลำดับการลงมือจัดการความเสี่ยง

๒. ประเมินทางเลือกในการควบคุม (Evaluate recommended Control Options) วิธีการควบคุมที่ถูกเสนอในกระบวนการประเมินความเสี่ยงอาจไม่ใช่วิธีที่เหมาะสมที่สุดหรือเป็นทางเลือกที่เป็นไปได้ที่สุดสำหรับแต่ละหน่วยงาน ขั้นตอนนี้จึงเป็นการเลือกวิธีการที่มีความเป็นไปได้มากที่สุดที่จะสามารถบรรเทาความเสี่ยงได้ ผลลัพธ์ที่ได้คือรายชื่อของวิธีการควบคุม

๓. วิเคราะห์ผลประโยชน์ที่ได้รับ (Conduct Cost-Benefit Analysis) การวิเคราะห์ผลประโยชน์นี้จะช่วยให้ผู้บังคับบัญชาสามารถตัดสินใจและเลือกวิธีการควบคุมที่มีประสิทธิภาพ

๔. เลือกวิธีการควบคุม (Select Control) จากพื้นฐานผลลัพธ์ที่ได้จากการวิเคราะห์ผลประโยชน์ ผู้บังคับบัญชาสามารถตรวจสอบวิธีควบคุมทั้งหมดและเลือกวิธีที่ครอบคลุมทั้งการควบคุมเชิงเทคนิค, เชิงปฏิบัติการ และเชิงบริหารเพื่อให้มั่นใจความเพียงพอต่อความต้องการความปลอดภัยของระบบและหน่วยงาน

๕. มอบหมายความรับผิดชอบ (Assign Responsibility) คือการเลือกบุคคลที่เหมาะสมซึ่งมีความเชี่ยวชาญและมีทักษะในการลงมือควบคุม พร้อมมอบหมายหน้าที่รับผิดชอบ

๖. พัฒนาแผนการปฏิบัติงานเพื่อการป้องกัน (Develop a Safeguard Implementation Plan) อย่างน้อยที่สุด แผนงานควรจะประกอบด้วยข้อมูลดังต่อไปนี้

- ๖.๑ ความเสี่ยงและระดับความเสี่ยง
- ๖.๒ วิธีการควบคุมที่ได้รับการแนะนำ
- ๖.๓ การปฏิบัติงานที่ได้รับการจัดลำดับไว้
- ๖.๔ การเลือกวิธีการควบคุม
- ๖.๕ ทรัพยากรที่ต้องการใช้ในการลงมือควบคุม

๖.๖ รายชื่อผู้มีหน้าที่รับผิดชอบ

๖.๗ กำหนดวันที่เริ่มลงมือปฏิบัติ

๖.๘ กำหนดวันเสร็จสิ้นการปฏิบัติ

๖.๙ รายละเอียดการดูแลรักษาระบบ

๗. ลงมือปฏิบัติตามวิธีการควบคุมที่เลือก (Implement Selected Controls) ขึ้นอยู่กับแต่ละสถานการณ์ บางครั้งการควบคุมอาจจะลดความเสี่ยงได้ แต่ไม่สามารถกำจัดความเสี่ยงนั้นออกจากระบบหรือหน่วยงานได้ ซึ่งอาจทำให้มีความเสี่ยงที่ยังเหลืออยู่แต่เป็นความเสี่ยงที่หน่วยงานสามารถยอมรับได้

### ประเภทของการควบคุม (Control Category)

ในการใช้วิธีการควบคุมเพื่อบรรเทาความเสี่ยง หน่วยงานควรจะต้องพิจารณาวิธีการทั้งในแง่ของเชิงเทคนิค เชิงการบริหารจัดการ และการรักษาความปลอดภัยในเชิงกายภาพ เพื่อให้การควบคุมมีประสิทธิภาพสูงสุด การควบคุมความปลอดภัยสามารถที่จะป้องกัน จำกัด และยับยั้งความเสียหายที่อาจเกิดขึ้นแก่หน่วยงาน

๑. การควบคุมความปลอดภัยเชิงเทคนิค (Technical Security Controls) การควบคุมนี้เพื่อให้ป้องกันภัยคุกคามที่อาจเกิดขึ้น ซึ่งการควบคุมสามารถจัดช่วงได้ตั้งแต่ที่มีวิธีการอย่างง่าย ๆ ไปจนถึง วิธีที่มีความสลับซับซ้อน และโดยปกติการควบคุมนี้จะเกี่ยวข้อง โครงสร้างสถาปัตยกรรมของระบบ วินัยในการพัฒนาโปรแกรม และการรักษาความปลอดภัยโดยรวมของอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และเฟิร์มแวร์ วิธีการเหล่านี้ควรจะปฏิบัติควบคู่กันไป และสามารถแบ่งประเภทหลัก ๆ ได้ ๓ ประเภทตามวัตถุประสงค์พื้นฐานได้ดังนี้

๑.๑ การควบคุมแบบสนับสนุน (Support) เป็นการควบคุมแบบทั่วไปสำหรับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ได้แก่ การระบุตัวตน (Identification), การจัดการโดยใช้กุญแจเข้ารหัสลับ (Cryptographic Key) , การบริหารความปลอดภัย (Security Management) และการปกป้องระบบ (System Protections)

๑.๒ การควบคุมแบบป้องกัน (Prevent) เป็นการควบคุมที่ป้องกันช่องโหว่ซึ่งเกิดจากจุดที่เคยเกิดความไม่ปลอดภัยขึ้นครั้งแรก สำหรับการควบคุมในทางเทคนิคได้แก่ การตรวจสอบชื่อผู้ใช้งานและรหัสผ่าน (Authentication), การตรวจสอบสิทธิการอนุญาตใช้งาน (Authorization), การบังคับใช้การควบคุมการเข้าถึงข้อมูล (Access Control Enforcement), การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation), การสื่อสารที่ได้รับการปกป้อง (Protected communication) โดยการใช้วิธีเข้ารหัสข้อมูลและใช้เทคโนโลยีการเข้ารหัสลับ, การรักษาความปลอดภัยส่วนตัวเกี่ยวกับรายการข้อมูลที่มีการเปลี่ยนแปลง (Transaction Privacy)

๑.๓ การควบคุมแบบเฝ้าระวัง ตรวจสอบและกู้คืน (Monitor, Detect and Recover) เป็นการควบคุมเพื่อตรวจจับช่องโหว่ในระบบพร้อมทั้งกู้ข้อมูลกลับคืน วิธีการควบคุมได้แก่ การตรวจสอบระบบ (Audit), การตรวจจับการบุกรุกระบบ (Intrusion Detection), การฟื้นฟูระบบให้กลับสู่สถานะที่ปลอดภัย (Restore Secure State) และการตรวจจับและกำจัดไวรัส (Virus detection and Eradication)

๒. การควบคุมความปลอดภัยเชิงการจัดการ (Management Security Controls) เป็นการปฏิบัติ งานเพื่อจัดการและลดความสูญเสียซึ่งเกิดจากความเสียหาย การควบคุมเชิงการจัดการมุ่งเน้นที่ข้อกำหนดตามนโยบาย

การปกป้องข้อมูลและมาตรฐานของหน่วยงาน ซึ่งนำไปสู่กระบวนการปฏิบัติที่ตอบสนองต่อเป้าหมายและกำลังพลของหน่วยงาน

๒.๑ การควบคุมเชิงการจัดการแบบป้องกัน (Preventive Management Security Controls) ประกอบด้วยวิธีการดังนี้

- มอบหมายความรับผิดชอบด้านความปลอดภัย
- พัฒนาและดูแลแผนการรักษาความปลอดภัยระบบ
- มีการควบคุมด้านความปลอดภัยส่วนบุคคล รวมถึงการแบ่งหน้าที่และการเข้าใช้และยกเลิกการใช้งานบนเครื่องคอมพิวเตอร์
- จัดอบรมด้านเทคนิคเพื่อให้แน่ใจว่าผู้ใช้จะเข้าใจและตระหนักถึงกฎ กติกาที่เกี่ยวข้อง (User Awareness Training)

๒.๒ การควบคุมเชิงการจัดการแบบตรวจจับ (Detection management security Controls) ได้แก่

- ควบคุมระบบของแต่ละบุคคล
- คอยตรวจสอบการควบคุมความปลอดภัยเพื่อให้มั่นใจว่าการควบคุมนั้นมีประสิทธิภาพ
- ทำการตรวจสอบระบบอย่างเป็นประจำ
- ลงมือปฏิบัติการบริหารจัดการความเสี่ยงเพื่อนำไปสู่การประเมินและการบรรเทาความเสี่ยง

๒.๓ การควบคุมเชิงการจัดการด้านการกู้คืน (Recovery Management Security Controls) ประกอบด้วยวิธีการดังนี้

- มีการทดสอบและปรับปรุง ให้การสนับสนุนการควบคุมอย่างต่อเนื่อง และดูแลแผนการปฏิบัติงานอย่างต่อเนื่องเพื่อสร้างความมั่นใจว่าแผนงานสามารถนำมาใช้เมื่อเกิดเหตุฉุกเฉินกับหน่วยงานได้
- ติดตั้งระบบที่สามารถจัดเตรียม, รับรู้, รายงานผล และตอบสนองต่อเหตุการณ์ที่เกิดขึ้นและสามารถทำให้ระบบข้อมูลสารสนเทศกลับสู่สภาวะปกติได้

๓. การควบคุมความปลอดภัยเชิงกายภาพ (Physical Security Controls) เป็นการปฏิบัติเพื่อจัดการและลดความสูญเสียซึ่งเกิดจากความเสียหายทางด้านกายภาพ ซึ่งประกอบด้วยวิธีการดังนี้

- ๓.๑ การกำหนดพื้นที่หวงห้ามสำหรับการปฏิบัติงานหรือพื้นที่ติดตั้งอุปกรณ์ด้านสารสนเทศ
- ๓.๒ การกำหนดมาตรการสำหรับการเข้า - ออกเพื่อปฏิบัติงานในพื้นที่ปฏิบัติงานด้านสารสนเทศ
- ๓.๓ การควบคุมสินทรัพย์ทางด้านข้อมูลสารสนเทศ เพื่อป้องกันความเสียหายจากไฟไหม้และน้ำท่วม
- ๓.๔ การตรวจตราสินทรัพย์ทางด้านข้อมูลสารสนเทศ เช่น การใช้โทรทัศน์วงจรปิด, การติดตั้งระบบกันขโมย เป็นต้น
- ๓.๕ ดูแลระบบรักษาความปลอดภัยในสภาพแวดล้อม เช่น การใช้ตัวตรวจจับ เป็นต้น

## กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ขั้นที่ ๑ การระบุความเสี่ยงและผลกระทบที่มีผลกระทบต่อระบบข้อมูลสารสนเทศ

ขั้นที่ ๒ ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบซึ่งแต่ละความเสี่ยงก็จะมี ความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน

ขั้นที่ ๓ มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยง เพื่อให้สามารถบรรลุเป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของแต่ละหน่วยงานเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบและป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบที่วางไว้ โดยสามารถดำเนินการตามแผนได้

ขั้นที่ ๔ การประเมินแผนเพื่อทราบความเสี่ยงที่เหลืออยู่ ในขั้นตอนนี้เจ้าหน้าที่ผู้รับผิดชอบจะต้องมีการรวบรวมและรายงานข้อมูลของความเสี่ยงที่ยอมรับได้ และข้อมูลที่เกี่ยวข้องเพื่อนำเสนอให้ผู้บังคับบัญชาทราบและบันทึกไว้เป็นหลักฐาน

ขั้นที่ ๕ การติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยงตามแผนที่ดำเนินการไว้ในขั้นที่ ๓ มีการตรวจสอบการทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของระบบโดยมีหลักฐานประกอบ การปฏิบัติหน้าที่ตามระยะเวลาที่กำหนด

## การเฝ้าสังเกต (Monitoring)

กระบวนการเฝ้าสังเกตเป็นหลักประกันว่า หน่วยงานมีมาตรการต่างๆ ที่จำเป็นและเหมาะสมสำหรับ การบริหารความเสี่ยงต่าง ๆ และมาตรการเหล่านั้นมีผู้ปฏิบัติตามและบังเกิดผลจริง ดังนั้น กระบวนการเฝ้าสังเกตจึงพิจารณาว่า

- ได้มีการปฏิบัติตามมาตรการต่าง ๆ และบังเกิดผล
- กระบวนการที่กำหนดขึ้นมาสามารถปฏิบัติได้จริง
- มีการเรียนรู้เกิดขึ้นในหน่วยงานอันเป็นผลมาจากการบริหารความเสี่ยง

## แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสภาเกษตรกรแห่งชาติ

### ๑. หลักการและเหตุผล

การบริหารจัดการความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ ที่เป็นสินทรัพย์ของสำนักงานสภาเกษตรกรแห่งชาติ และยังรวมถึงการปกป้อง “ภารกิจ” ของสำนักงานสภาเกษตรกรแห่งชาติให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของสำนักงานสภาเกษตรกรแห่งชาติ ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของสำนักงานสภาเกษตรกรแห่งชาติ

สำนักงานสภาเกษตรกรแห่งชาติจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องสำนักงานสภาเกษตรกรแห่งชาติจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยงและเพื่อความสามารถในการดำเนินภารกิจของสำนักงานสภาเกษตรกรแห่งชาติให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือสำนักงานสภาเกษตรกรแห่งชาติเพียงเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ตามพระราชกฤษฎีกา ว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้สำนักงานสภาเกษตรกรแห่งชาติบรรลุเป้าประสงค์และภารกิจที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานของสำนักงานสภาเกษตรกรแห่งชาติ ที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่า

### ๒. วัตถุประสงค์

๑. เพื่อให้การจัดการภายในสำนักงานสภาเกษตรกรแห่งชาติ มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

๒. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาติ

๓. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๕. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบต่อการทำงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

### ๓. ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของสำนักงานสภาเกษตรกรแห่งชาติ

### ๔. การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของสำนักงานสภาเกษตรกรแห่งชาติสามารถแยกประเภทความเสี่ยงได้เป็น ๔ ประเภท ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์อาจถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงจากผู้ใช้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญใน การเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของสำนักงานสภาเกษตรกรแห่งชาติ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม ชุมชนประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการทำงานด้านสารสนเทศ



## ๕. ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตาราง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับผลกระทบ
๑. ความเสี่ยง ในการเข้าถึง ข้อมูลของ บุคคลอื่น	RIT๐๑	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังใน การเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้ รหัสผ่านของตนเองเข้าใช้ ระบบหรือใช้งานแทน	-การอำพรางหรือ สวมรอยผู้ใช้ -การเข้าถึงข้อมูล/ เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
๒. ความเสี่ยง จากการนำเอา อุปกรณ์อื่นที่ ไม่ได้รับอนุญาต มาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังใน การใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มา เชื่อมต่อกับระบบเครือข่าย สำนักงานสภาเกษตรกร แห่งชาติ โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ ถูกต้อง ทำให้เครื่อง คอมพิวเตอร์อื่นในระบบ เครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ ตั้งค่าการ รักษาความปลอดภัย ทำให้ เครื่องคอมพิวเตอร์ของบุคคล ภายนอกอื่น ๆ ที่รับสัญญาณ ได้เชื่อมต่อเข้ากับระบบ เครือข่ายของสำนักงานสภา เกษตรกรแห่งชาติ ทำให้เกิด ช่องโหว่กับระบบรักษาความ ปลอดภัยของสำนักงานสภา เกษตรกรแห่งชาติ	-การนำอุปกรณ์อื่น มาเชื่อมต่อเข้าระบบ -ความล้มเหลวทาง เทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย

## ๖. การประมาณความเสี่ยง แสดงดังตาราง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๕	๔	๒๐
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายสำนักงาน สภาเกษตรกรแห่งชาติ โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่น ๆ ที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงาน สภาเกษตรกรแห่งชาติ ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสำนักงาน สภาเกษตรกรแห่งชาติ	๕	๓	๑๕
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดัน ไฟฟ้าที่ไม่คงที่หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๕	๒	๑๐

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๔. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๔	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติด <b>Malware</b>	๒	๔	๘
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๕	๔	๒๐
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับความกระทบ	๑	๑	๑
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๕	๔	๒๐
๘. ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๑	๕	๕
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๑	๒	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิคหรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	๓	๔	๑๒
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๑	๕	๕

### ๗. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting) แสดงดังตาราง

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๒๐
๒	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๒๐
๓	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๒๐
๔	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายสำนักงานสภาเกษตรกรแห่งชาติ โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานสภาเกษตรกรแห่งชาติ	๑๕
๕	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	๑๒

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๖	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๑๐
๗	RIT๐๔ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	๘
๘	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม น้ำท่วม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๕
๙	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากผูปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๕
๑๐	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อยจนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๒
๑๑	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๑

#### ๘. การจัดการความเสี่ยง แสดงดังตาราง

ระดับความเสี่ยงคงเหลือที่ยอมรับได้  $\leq ๘$

สำนักงานสภาเกษตรกรแห่งชาติกำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการ ความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพิงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	กองสื่อสารและสารสนเทศ	-
๒	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้	กองการเจ้าหน้าที่	-
๓	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำโครงการเพื่อขอรับการสนับสนุน	กองยุทธศาสตร์	-
๔	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๑๕	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดฝึกอบรมเพื่อสร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง	กองสื่อสารและสารสนเทศ	-

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
				- ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย		
๕	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- หาทางป้องกันสัตว์กัดแทะอุปกรณ์ - จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราวเพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ	กองกลาง	-
๖	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๑๐	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาเครื่องกำเนิดไฟฟ้าและเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่	กองสื่อสารและสารสนเทศ	-
๗	RIT๐๔ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	๘	- ยอมรับความเสี่ยง	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	กองสื่อสารและสารสนเทศ	-



ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๘	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	๕	- ยอมรับความเสี่ยง	- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	กองสื่อสารและสารสนเทศ	-
๙	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๕	- ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - กำหนดพื้นที่หวงห้ามในการเข้าถึงพื้นที่ปฏิบัติงาน - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง	กองกลาง	-
๑๐	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๒	- ยอมรับความเสี่ยง	- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	กองสื่อสารและสารสนเทศ	-
๑๑	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	๑	- ยอมรับความเสี่ยง		-	-