แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ประจำปีงบประมาณ ๒๕๖๔-๒๕๖๗
(ฉบับทบทวนปี ๒๕๖๖)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

บทที่ ๑
บทนำ

๑. หลักการและเหตุผล

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

ด้วยภารกิจของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (สป.กษ.) จึงจำเป็นต้องจัดการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงาน หรือเป้าหมายขององค์กร การวิเคราะห์และระบุความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น การจัดลำดับความสำคัญของปัจจัยเสี่ยง การกำหนดแนวทางในการจัดการความเสี่ยง โดยคำนึงถึงความคุ้มค่าในการจัดการ ความเสี่ยงอย่างเหมาะสมและองค์กรยอมรับได้

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๑. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

๒. เพื่อเป็นแนวทางในการดำเนินงาน การกำกับดูแล การมอบหมาย การติดตามงานการตรวจประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ฉุกเฉิน

๓. เป้าหมาย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (สป.กษ.) มีแผนสำหรับดำเนินการเพื่อจัดการความเสี่ยง ดังนี้

๑. มีแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒. มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๓. มีแผนบริหารความต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔. ขอบเขตการดำเนินงาน

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการโดยคณะทำงานด้านการรักษาความปลอดภัยทางไซเบอร์ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ซึ่งจะมีการรวบรวมและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

๕. ประโยชน์ที่คาดว่าจะได้รับ

๑. มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบสารสนเทศ ระบบฐานข้อมูลและการจัดเก็บข้อมูล

๒. มีแนวทางในการดูแลบำรุงรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีเสถียรภาพและมีความพร้อมใช้งานอย่างต่อเนื่อง

บทที่ ๒
การบริหารความเสี่ยง

๑. กระบวนการบริหารความเสี่ยง

การบริหารความเสี่ยงตามแนวทางของ The Committee of Sponsoring Organizations of the Treadway Commission - Enterprise risk management (COSO-ERM) ซึ่งการบริหารความเสี่ยงตามแนวทางนี้ประกอบด้วยองค์ประกอบ ๘ ประการ ซึ่งสัมพันธ์กับการดำเนินการธุรกิจและกระบวนการบริหารงาน มีดังนี้

๑.๑. สภาพแวดล้อมภายในองค์กร (Internal Environment) สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญในการกำหนดกรอบการบริหารความเสี่ยงและเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงองค์กร ประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางปฏิบัติงานของบุคลากร กระบวนการทำงาน ระบบสารสนเทศ เป็นต้น โดยสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เป็นดังนี้

- ระบบฐานข้อมูลสารสนเทศ (Database & Software) เช่น เว็บไซต์กระทรวงเกษตรและสหกรณ์ และเว็บไซต์สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ฐานข้อมูลเว็บไซต์กระทรวงเกษตรและสหกรณ์และฐานข้อมูลเว็บไซต์สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เป็นต้น
- ระบบฐานข้อมูลสำหรับการบริหารงานภายใน (Back Office) ได้แก่ ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban) ฐานข้อมูลระบบสารสนเทศทรัพยากรบุคคล (DPIS) ฐานข้อมูลครุภัณฑ์คอมพิวเตอร์ (ICT Asset) เป็นต้น
- ระบบให้บริการเครือข่าย ได้แก่ ระบบเครือข่ายภายใน (LAN) ระบบเครือข่ายอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (WiFi) ระบบเครือข่ายมหาดไทย (Moi Net)
- อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบสารสนเทศ (Web Application Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer)เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น
- ระบบรักษาความปลอดภัย ได้แก่ โปรแกรมตรวจสอบและป้องกันไวรัส Firewall IPS (Instrution Prevention System) และ Web Application Firewall

๑.๒. การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม โดยทั่วไปวัตถุประสงค์และกลยุทธ์ควรได้รับการบันทึกเป็นลายลักษณ์อักษร และสามารถพิจารณาได้ในด้านต่างๆ ดังนี้

- วิสัยทัศน์ พันธกิจ เป้าหมาย วัตถุประสงค์ด้านยุทธศาสตร์
- ด้านปฏิบัติงาน เกี่ยวข้องกับประสิทธิภาพ ผลการปฏิบัติงาน
- ด้านการรายงาน เกี่ยวข้องกับการรายงานทั้งภายในและภายนอกองค์กร
- ด้านการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับการปฏิบัติตามกฎหมายและกฎระเบียบต่างๆ

๑.๓. การระบุความเสี่ยง (Risk Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งปัจจัยเสี่ยงที่เกิดจากปัจจัยภายในและปัจจัยภายนอกองค์กร และเมื่อเกิดขึ้นแล้วส่งผลให้องค์กรไม่บรรลุวัตถุประสงค์หรือเป้าหมาย เช่น นโยบายการบริหารงาน บุคลากร การปฏิบัติงานการเงิน ระบบสารสนเทศ ระเบียบข้อบังคับ เป็นต้น ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้นๆ และเพื่อให้ผู้บริหารพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้เป็นอย่างดี วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

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

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๑.๔. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงเป็นการวัดระดับความรุนแรงของความเสี่ยง เพื่อพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่โดยการประเมินจะประกอบด้วย ๒ มิติ คือ

- โอกาสที่จะเกิด (Likelihood) หมายถึง ความน่าจะเป็นที่จะเกิดเหตุการณ์ที่นำมาพิจารณาเกิดขึ้นมากน้อยเพียงใด ซึ่งจะมีการพิจารณาหาระดับของโอกาสที่จะเกิด ดังนี้

ระดับ	โอกาสที่จะเกิด	เชิงปริมาณ	เชิงคุณภาพ
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง ต่อปี	มีโอกาสเกิดในกรณียกเว้น
๒	น้อย	๒ ครั้งต่อปี	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
๓	ปานกลาง	๓ ครั้งต่อปี	มีโอกาสเกิดบางครั้ง
๔	สูง	๔ ครั้งต่อปี	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
๕	สูงมาก	มากกว่า ๔ ครั้งต่อปี	มีโอกาสเกิดเกือบทุกครั้ง

- ผลกระทบ (Impact) (ความรุนแรง) ที่เกิดจากเหตุการณ์ที่เกิดขึ้น หรือคาดคะเนว่าจะเกิดเหตุการณ์นั้น ๆ และเมื่อเกิดขึ้นแล้วจะเกิดผลกระทบ (ความรุนแรง) กับสิ่งต่าง ๆ และความเสียหายที่เกิดขึ้นในด้านการปฏิบัติงาน (Operational Risk) ด้านการเงิน (Financial Risk) ด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk) ด้านบุคลากร (People) แล้วให้พิจารณาความรุนแรงว่าอยู่ในระดับเท่าใด ดังตารางต่อไปนี้

ด้านการปฏิบัติงาน

ระดับ	ระดับผลกระทบ	รายละเอียด
๑	ต่ำมาก	ผลการดำเนินงานล่าช้าไม่เกิน ๑ สัปดาห์ / ระยะเวลาหยุดชะงักไม่เกิน ๓๐ นาที
๒	ต่ำ	ผลการดำเนินงานล่าช้าไม่เกิน ๒ สัปดาห์ / ระยะเวลาหยุดชะงักไม่เกิน ๑ ชั่วโมง
๓	ปานกลาง	ผลการดำเนินงานล่าช้า ๒ สัปดาห์ – ๑ เดือน / ระยะเวลาหยุดชะงัก ๑ ชั่วโมง – ๔ ชั่วโมง
๔	สูง	ผลการดำเนินงานล่าช้า ๑ เดือน – ๓ เดือน / ระยะเวลาหยุดชะงัก ๔ ชั่วโมง – ๑๒ ชั่วโมง
๕	สูงมาก	ผลการดำเนินงานล่าช้ามากกว่า ๓ เดือน / ระยะเวลาหยุดชะงักมากกว่า ๑๒ ชั่วโมง

ด้านการเงิน

ระดับ	ระดับผลกระทบ	รายละเอียด
๑	ต่ำมาก	เสียหายด้านการเงิน น้อยกว่า ๕ แสนบาท
๒	ต่ำ	เสียหายด้านการเงิน ๕ แสนบาท – ๑ ล้านบาท
๓	ปานกลาง	เสียหายด้านการเงิน ๑ ล้านบาท – ๕ ล้านบาท
๔	สูง	เสียหายด้านการเงิน ๕ ล้านบาท – ๑๐ ล้านบาท
๕	สูงมาก	เสียหายด้านการเงินมากกว่า ๑๐ ล้านบาท

ด้านภาพลักษณ์และชื่อเสียง

ระดับ	ระดับผลกระทบ	รายละเอียด
๑	ต่ำมาก	มีการเผยแพร่ข่าวที่รับรู้เฉพาะภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒	ต่ำ	มีการเผยแพร่ข่าวรับรู้เฉพาะภายในสำนักงานปลัดกระทรวงเกษตรและสหกรณ์
๓	ปานกลาง	มีการเผยแพร่ข่าวผ่านทางเอกสารตีพิมพ์ต่างๆ
๔	สูง	มีการเผยแพร่ข่าวผ่านทางสถานีโทรทัศน์
๕	สูงมาก	มีการเผยแพร่ข่าวผ่านทางสื่อสังคมออนไลน์

ด้านบุคลากร

ระดับ	ระดับผลกระทบ	รายละเอียด
๑	ต่ำมาก	ไม่ได้รับบาดเจ็บ
๒	ต่ำ	ได้รับบาดเจ็บเล็กน้อยในระดับปฐมพยาบาลเบื้องต้นได้
๓	ปานกลาง	ได้รับบาดเจ็บที่จำเป็นต้องได้รับการรักษาจากแพทย์
๔	สูง	ได้รับบาดเจ็บหรืออันตรายจนอาจทำให้สูญเสียอวัยวะหรือพิการ
๕	สูงมาก	ได้รับบาดเจ็บจนอาจถึงขั้นเสียชีวิต หรือทุพพลภาพถาวร

การพิจารณาความเสี่ยง หลังจากประเมินความเป็นไปได้ของโอกาสที่จะเกิด (Likelihood Score) และผลกระทบ (ความรุนแรง) (Impact Score) ของปัจจัยเสี่ยงต่าง ๆ โดยนำความเสี่ยงที่ระบุไว้แล้วทั้งหมดมาพิจารณาความเสี่ยง ดังนี้

คำนวณหาระดับความเสี่ยง โดยใช้ข้อมูลของโอกาสที่จะเกิด (Likelihood Score) และผลกระทบ (ความรุนแรง) (Impact Score) ดังนี้

ระดับความเสี่ยง = ระดับโอกาสที่จะเกิด x ระดับผลกระทบ

ตารางระดับและลำดับของความเสี่ยง (Degree of Risk)

ผลกระทบ/ความรุนแรง

5	19	20	21	24	25
4	16	17	18	22	23
3	11	12	13	14	15
2	3	4	8	9	10
1	1	2	5	6	7
	1	2	3	4	5

โอกาสที่จะเกิด

จัดลำดับความเสี่ยง (Degree of Risk) ระดับความเสี่ยงที่เกิดจากความสัมพันธ์ระหว่างระดับความรุนแรงกับระดับโอกาสที่จะเกิด ซึ่งมีระดับของความเสี่ยงอยู่ที่ ๔ ระดับ โดยแต่ละระดับจะมีความหมายของความเสี่ยงและการปฏิบัติเพื่อใช้ในการบริหารความเสี่ยงต่อไป

ตารางแสดงการจัดลำดับความเสี่ยง (Degree of Risk) มี ๔ ระดับ คือ

ลำดับคะแนน	ระดับความเสี่ยง	แทนด้วยแถบสี	ความหมาย
๑๕-๒๕	สูงมาก		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที

ลำดับคะแนน	ระดับความเสี่ยง	แทนด้วยแถบสี	ความหมาย
๘-๑๔	สูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
๔-๗	ปานกลาง		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
๑-๓	ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยงไม่ต้องมีการจัดการเพิ่มเติม

๑.๕. การตอบสนองความเสี่ยง (Risk Response) เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้(Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

- **การหลีกเลี่ยง (Terminate)** เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้
- **การยอมรับ (Take)** เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง
- **การควบคุม (Treat)** เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น
- **การถ่ายโอน (Transfer)** การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือ

ในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๑.๖. กิจกรรมควบคุม (Control Activities) การกำหนดกิจกรรมและการปฏิบัติต่างๆ เพื่อช่วยลด หรือควบคุมความเสี่ยง เพื่อสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้อง และทำให้การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ป้องกันและลดระดับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน มีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

- **ควบคุมเพื่อการป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น
- **การควบคุมเพื่อให้ตรวจพบ (Detective Control)** เป็นวิธีการควบคุม เพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น
- **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์
- **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้
  ๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น
  ๒) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่
  ๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๑.๗. สารสนเทศและการสื่อสาร (Information and Communication) องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงต่อไปตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

๑.๘. การติดตามประเมินผล (Monitoring) การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมา

ผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงเมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

- พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่
- กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง
- ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๒. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ได้กำหนดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ออกได้เป็น ๘ ด้าน ประกอบด้วย

๒.๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

๒.๒. ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

๒.๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

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

๒.๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๒.๕. ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

๒.๖. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

๒.๗. ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

๒.๘. ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยง เนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

๓. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ได้แก่

๓.๑. ปัจจัยภายนอก ได้แก่

๑) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๒) การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓) การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

๔) ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

๕) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๖) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๗) ความไม่สงบเรียบร้อยทางการเมือง เช่น การชุมนุมประท้วง เหตุจลาจล เป็นต้น

๓.๒. ปัจจัยภายใน ได้แก่

๑) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

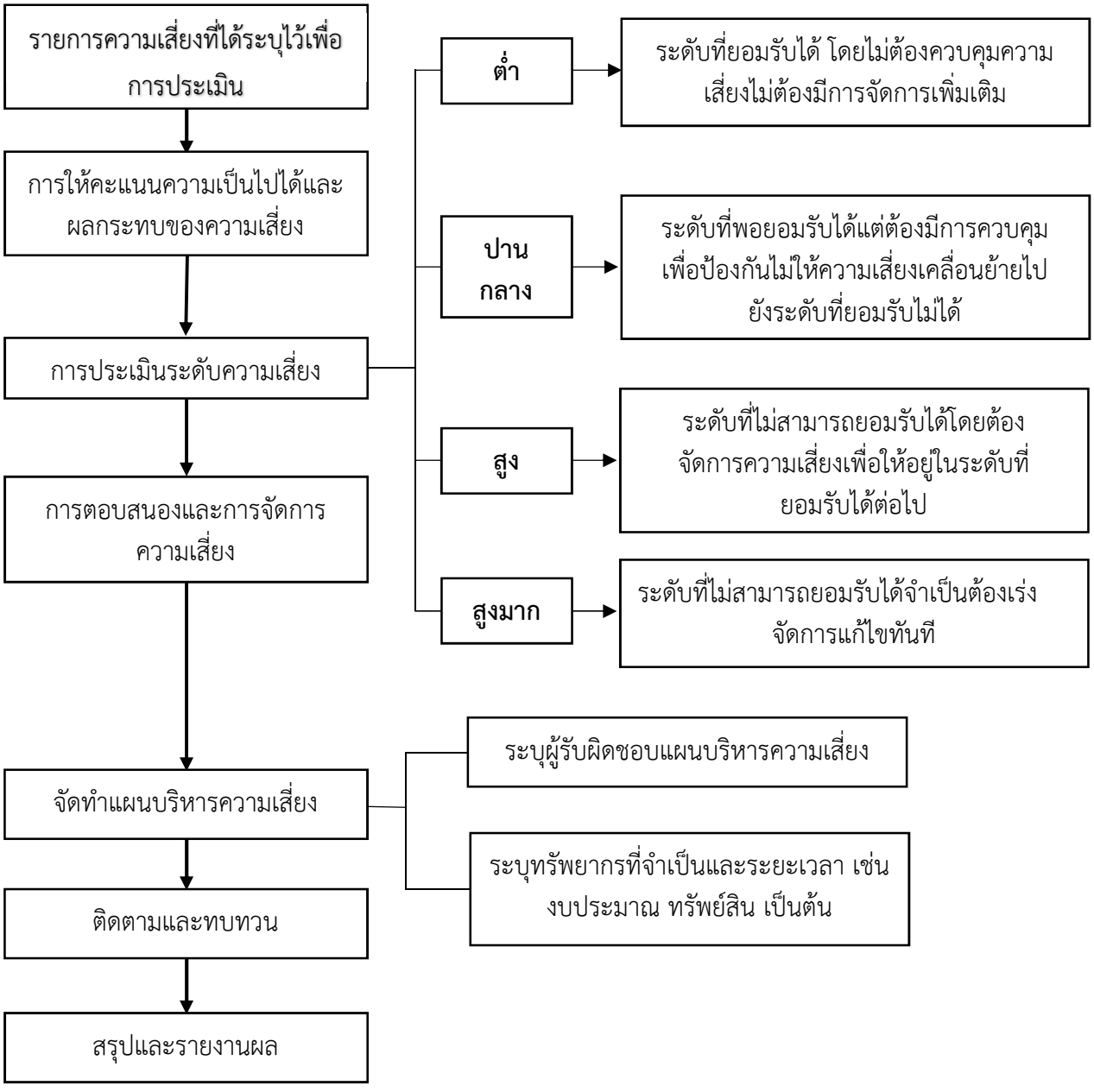
๒) การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

๓) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

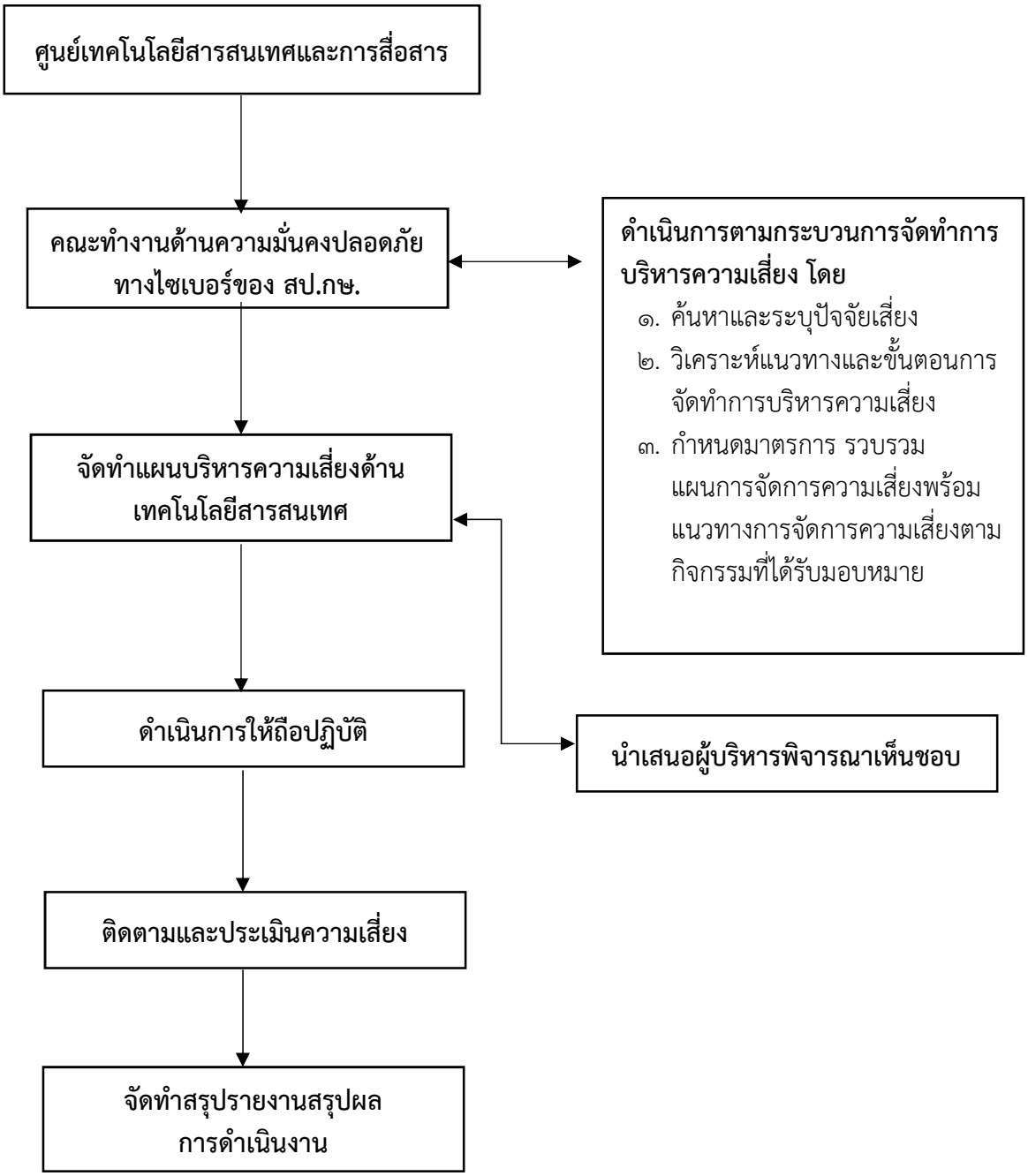
บทที่ ๓
การวิเคราะห์การบริหารจัดการความเสี่ยง

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ได้ตระหนักถึงความสำคัญของข้อมูลและการทำงานของระบบเครือข่ายที่สนับสนุนการปฏิบัติงานของหน่วยงานที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. ๒๕๖๔-๒๕๖๗ โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๒. กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



๓. รายละเอียดของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)			
ความเสี่ยงจาก ไฟไหม้ ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร หรือการวางเพลิง - ภัยที่เกิดจากธรรมชาติ เช่น ฟ้าผ่า	เมื่อเกิดไฟไหม้อาคารสำนักงาน แผ่นดินไหว /อาคารทรุดตัว อาคารถล่ม ไม่สามารถย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ทัน ทำให้ได้รับความเสียหายทั้งหมด	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง และกระแสไฟฟ้าดับ	- แหล่งที่ให้บริการกระแสไฟฟ้าขัดข้อง - แรงดันไฟฟ้าขัดข้อง	เมื่อเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหายหรือ อาจทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปไม่สมบูรณ์ ส่งผลทำให้ข้อมูลบางส่วนเกิดการสูญหาย การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายบางประเภทไม่สามารถใช้งานได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
ความเสี่ยงจากระบบควบคุมอุณหภูมิ/ความชื้นในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ หยุดทำงาน	ควบคุมอุณหภูมิและความชื้นที่ไม่เหมาะสม	ระบบควบคุมอุณหภูมิ/ความชื้นหยุดทำงาน อาจเกิดความเสียหายขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
ความเสี่ยงจากไม่มีการควบคุมการ เข้า-ออก ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ (Server Room)	ไม่มีการควบคุม หรือบันทึกบุคลที่เข้า-ออก ห้อง Server Room	เมื่อไม่มีการควบคุมการ เข้า-ออก ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ อาจทำให้ผู้ไม่มีหน้าที่ รับผิดชอบ/มีอำนาจ เข้าไปทำลาย หรือขโมยข้อมูล หรืออุปกรณ์ จนทำให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยทางการเมือง	- การชุมนุมประท้วง - การจราจล/การก่อการร้าย - การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	เมื่อเกิดสถานการณ์ความรุนแรง หรือ ความไม่สงบเรียบร้อย อาจทำให้บุคลากรไม่สามารถเข้าปฏิบัติงานได้ตามปกติ	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
ความเสี่ยงด้านบุคลากร (Human Risk)			
การดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ	- ผู้บริหารไม่ให้ความสำคัญต่อความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร	- ระบบสารสนเทศที่พัฒนาไม่ได้ถูกนำไปใช้ให้เกิดประโยชน์กับหน่วยงาน และขาดการพัฒนาอย่างต่อเนื่อง	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ผู้รับผิดชอบที่ได้รับมอบหมายไม่ทำการติดตามตรวจสอบการใช้ระบบเทคโนโลยีสารสนเทศตามแผนที่กำหนด	- ไม่สามารถระบุตัวตนผู้ใช้งานได้เมื่อมีผู้ใช้งานกระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์และเครือข่าย - ไม่สามารถตรวจสอบการเข้าถึงการใช้งานระบบเทคโนโลยีสารสนเทศได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญความเชี่ยวชาญ ดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน อาจทำให้เสียเวลาในการแก้ไข ทำให้ต้องขยายเวลาทำงานและไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
	- บุคลากรด้านไอทีมีความรู้ความเข้าใจในงานด้านเทคโนโลยีสารสนเทศไม่เพียงพอ	- เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้ - อาจต้องเพิ่มค่าใช้จ่ายในการบำรุงรักษามากยิ่งขึ้น	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ผู้ใช้งาน (Users) ไม่มีความรู้ความชำนาญ และทักษะในการใช้งาน	- การใช้งานไม่เป็นไปตาม Work Flow ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขด้วยตัวเองในเบื้องต้นได้ งานติดขัด - เกิดความล่าช้าในการปฏิบัติงานและเพิ่มภาระให้แก่ผู้ดูแลระบบ - ไม่มีการใช้งานระบบ ทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบัน ขาดความน่าเชื่อถือ/ข้อมูลไม่ถูกนำไปใช้งาน	- ผู้ดูแลระบบ - หน่วยงาน
ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	ฐานข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศไม่เป็นปัจจุบันเนื่องจากผู้ใช้งานมีการลาออก โอน ย้าย สิ้นสุดการจ้างตลอดเวลา	- หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน/ข้อมูล/อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย - ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	อุปกรณ์ที่ใช้ไม่มีระบบรักษาความปลอดภัยที่ถูกต้องและเพียงพอ	อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงานและอาจมีการโจมตีทำให้ระบบไม่สามารถทำงานได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)			
ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	- ครุภัณฑ์ อุปกรณ์ ไม่ได้มาตรฐาน - การติดตั้งใช้งานไม่สมบูรณ์	- เกิดความเสียหายจากการจัดหาครุภัณฑ์ อุปกรณ์ที่ไม่ได้มาตรฐาน - การติดตั้งที่ไม่ได้มาตรฐาน	- ผู้ใช้งาน - ผู้ดูแลระบบ หน่วยงาน
ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	- เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง - เสียเวลาในการกู้ระบบ - เสียภาพลักษณ์ของสำนักงานฯ	- หน่วยงาน
ความเสี่ยงจากการบำรุงรักษา - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบเครือข่ายและอุปกรณ์ - คอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง	- ไม่มีการควบคุมบัญชีรายการ ปรับปรุงรายการอุปกรณ์เทคโนโลยี	- ครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีและเครือข่ายสื่อสารสูญหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ขาดแผนรองรับระบบฮาร์ดแวร์ภายในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	- ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้ เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ขาดการบริหารและจัดการสิทธิ์การใช้อุปกรณ์เทคโนโลยีสารสนเทศ	- ไม่สามารถระบุตัวตนผู้ใช้งาน / หาผู้กระทำความผิดไม่ได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ระบบเครือข่ายสื่อสารหลักไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	- เกิดความเสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote)	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
	- ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสาร	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน ● อนุมัติโครงการล่าช้า ● ไม่สามารถประกาศผลผู้ชนะการประกวดราคา ● สัญญาไม่ตรงตามร่างข้อกำหนด	- เกิดความล่าช้าไม่เป็นไปตามแผนปฏิบัติงานที่กำหนดทำให้ไม่สามารถทำงานได้ต่อเนื่อง - ไม่สามารถตรวจรับงานได้ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปี - มีผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	- หน่วยงาน
ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	การทำงานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ขัดข้อง	ระบบงานไม่สามารถใช้ได้ตามปกติ	- ผู้ดูแลระบบ - ผู้ใช้งาน
ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker Virus Malware ต่างๆเป็นต้น	การถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	- ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย - ระบบ/ข้อมูลอาจถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพ บน Web Site ของสำนักงานฯ	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
		- ถูกโจรกรรมข้อมูลที่เป็นความลับ	
ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	- ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่ายอินทราเน็ตได้ - ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	- เจ้าหน้าที่และผู้บริหารงานสำนักงานฯไม่สามารถใช้งานระบบอินเทอร์เน็ตสำหรับปฏิบัติงานได้ - บุคคลภายนอกไม่สามารถเข้าใช้งานข้อมูลสารสนเทศของหน่วยงานผ่านเครือข่าย	- ผู้ใช้งาน - ผู้ดูแลระบบ
ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้ หรือใช้ได้แต่ช้ามาก	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)			
การใช้งานของระบบโปรแกรมคอมพิวเตอร์ไม่มีความมั่นคงปลอดภัย	- ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System access control) และโปรแกรมประยุกต์ หรือแอปพลิเคชัน (เครื่องคอมพิวเตอร์แม่ข่าย)	- ไม่มีความมั่นคงปลอดภัยในการเข้าใช้งาน ขาดการควบคุมการเข้าถึง - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบ	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
	- ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Use of System Utilities) ของเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่าย	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware Trojan ที่แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ขาดการป้องกันหรือตรวจจับไวรัส	- เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบสารสนเทศและฐานข้อมูล	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- การรักษาความมั่นคงปลอดภัยจากผู้ปฏิบัติงานในระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือ ข้อมูลถูกทำลายเกิดความเสียหาย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายต่อระบบ - ระบบถูกโจมตีจนไม่สามารถให้บริการได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ไม่มีการกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบ (ที่พัฒนาไว้อย่างหลากหลาย) - ใช้งบประมาณสูงในการบำรุงรักษา (ไม่คุ้มค่า)	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- เกิดช่องโหว่ของซอฟต์แวร์	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตี	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ขาดการบำรุงรักษาโปรแกรม หรือ ระบบงานที่ครอบคลุม	- เกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้ - เกิดช่องโหว่จากการไม่มีการอัปเดตรุ่นใหม่ๆ อย่างสม่ำเสมอ ทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
ความเสี่ยงด้านระบบข้อมูล (Database Risk)			
โจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ ไม่มีอำนาจ เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ ไม่มีอำนาจ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	- การให้บริการระบบสารสนเทศหยุดให้บริการ ส่งผลต่อการให้บริการต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน
	- ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูล และระบบฐานข้อมูล	- เกิดความเสียหายแก่ระบบข้อมูล ระบบฐานข้อมูล ทำให้ใช้งานไม่ต่อเนื่อง - ไม่สามารถกู้คืนระบบข้อมูล/ฐานข้อมูลได้ เนื่องจากไม่มีแผนสำรองและกู้คืนข้อมูล	- ผู้ใช้งาน - ผู้ดูแลระบบ - หน่วยงาน

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
	- ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)	- ไม่มีแนวทางการป้องกันและการเตรียมการเมื่อเกิดสถานการณ์ฉุกเฉิน	
ระบบฐานข้อมูลไม่สามารถเชื่อมโยงบูรณาการ หรือออกรายงานได้	- การนำเข้าข้อมูลผิดพลาดทั้งจากการนำเข้าข้อมูล (Human Error) และจากความผิดพลาดของระบบฯ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - ผู้ใช้ประโยชน์จากฐานข้อมูล - หน่วยงาน - ผู้บริหาร
	- การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - ผู้ใช้ประโยชน์จากฐานข้อมูล - หน่วยงาน - ผู้บริหาร
	- ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบฐานข้อมูล	- ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - ผู้ใช้ประโยชน์จากฐานข้อมูล - หน่วยงาน - ผู้บริหาร
ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย	- ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้เสียหายต่อความเชื่อถือของ สป.กษ.	- ผู้ใช้งาน - ผู้ดูแลระบบ

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ที่ได้รับผลกระทบ
	เช่น Harddisk หรือ อุปกรณ์สำรองข้อมูลประเภทต่างๆ	- ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	- หน่วยงาน
ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล/ดำเนินการสำรองไม่ต่อเนื่อง/สำรองไม่ครบถ้วน	- ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน - ระบบเสียหายไม่สามารถใช้งานและบริการข้อมูลได้	- ผู้ใช้งาน - ผู้ดูแลระบบ
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)			
เป้าหมาย /ตัวชี้วัด ที่กำหนดตามคำรับรอง	- ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามคำรับรองได้	- การดำเนินงานไม่บรรลุเป้าหมาย และไม่มีผลสัมฤทธิ์ของงานตามตัวชี้วัดที่กำหนดในการจัดทำคำรับรอง	- สำนัก กอง ศูนย์
ความเสี่ยงด้านการเงิน (Financial Risk)			
งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	- โดนตัด/ปรับลดโครงการตามนโยบายการปรับลดเงินเป็นเปอร์เซ็นต์ ทำให้โครงการที่จำเป็นต้องดำเนินการ โดนตัด/ปรับลดไปด้วย	- ลดระยะเวลา ลดคุณภาพและประสิทธิภาพการให้บริการตามโครงการต่าง ๆ - ตัดโครงการที่จะดำเนินการออกไป มีผลกระทบต่อแผนงานที่กำหนด	- หน่วยงานซึ่งเป็นหน่วยรับงบประมาณ
ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)			
การจัดซื้อจัดจ้างในการบำรุงรักษาระบบไม่เป็นไปตามแผนปฏิบัติการ	ไม่สามารถดำเนินงานได้อย่างต่อเนื่องทันที	- ขาดช่วงในการบำรุงรักษาระบบต่างๆ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่าย	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน

๔. การประเมินความเสี่ยง (Risk Assessment) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

เป็นการวัดระดับความรุนแรงของความเสี่ยง เพื่อพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจะประกอบด้วย ๒ มิติ คือ

- โอกาสที่จะเกิด (Likelihood) หมายถึง ความน่าจะเป็นที่จะเกิดเหตุการณ์ที่นำมาพิจารณาเกิดขึ้นมากน้อยเพียงใด ซึ่งจะมีการพิจารณาหาระดับของโอกาสที่จะเกิด ดังนี้

ระดับ	โอกาสที่จะเกิด	เชิงปริมาณ	เชิงคุณภาพ
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง ต่อปี	มีโอกาสเกิดในกรณียกเว้น
๒	น้อย	๒ ครั้งต่อปี	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
๓	ปานกลาง	๓ ครั้งต่อปี	มีโอกาสเกิดบางครั้ง
๔	สูง	๔ ครั้งต่อปี	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
๕	สูงมาก	มากกว่า ๔ ครั้งต่อปี	มีโอกาสเกิดเกือบทุกครั้ง

- ผลกระทบ (Impact) (ความรุนแรง) ที่เกิดจากเหตุการณ์ที่เกิดขึ้น หรือคาดคะเนว่าจะเกิดเหตุการณ์นั้น ๆ และเมื่อเกิดขึ้นแล้วจะเกิดผลกระทบ (ความรุนแรง) กับสิ่งต่าง ๆ และความเสียหายที่เกิดขึ้นในด้านการปฏิบัติงาน (Operational Risk) ด้านการเงิน (Financial Risk) ด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk) ด้านบุคลากร (People) แล้วให้พิจารณาความรุนแรงว่าอยู่ในระดับเท่าใด ดังตารางต่อไปนี้

ความเสียหายจากผลกระทบ	ระดับความเสียหาย				
	ต่ำมาก (๑)	ต่ำ (๒)	ปานกลาง (๓)	สูง (๔)	สูงมาก
การปฏิบัติการ (Operation)	ผลการดำเนินงานล่าช้าไม่เกิน ๑ สัปดาห์ / ระยะเวลาหยุดชะงักไม่เกิน ๓๐ นาที	ผลการดำเนินงานล่าช้าไม่เกิน ๒ สัปดาห์ / ระยะเวลาหยุดชะงักไม่เกิน ๑ ชั่วโมง	ผลการดำเนินงานล่าช้า ๒ สัปดาห์ – ๑ เดือน / ระยะเวลาหยุดชะงัก ๑ ชั่วโมง – ๔ ชั่วโมง	ผลการดำเนินงานล่าช้า ๑ เดือน – ๓ เดือน / ระยะเวลาหยุดชะงัก ๔ ชั่วโมง – ๑๒ ชั่วโมง	ผลการดำเนินงานล่าช้ามากกว่า ๓ เดือน / ระยะเวลาหยุดชะงักมากกว่า ๑๒ ชั่วโมง
การเงิน (Finance)	เสียหายด้านการเงิน น้อยกว่า ๕ แสนบาท	เสียหายด้านการเงิน ๕ แสนบาท – ๑ ล้านบาท	เสียหายด้านการเงิน ๑ ล้านบาท – ๕ ล้านบาท	เสียหายด้านการเงิน ๕ ล้านบาท – ๑๐ ล้านบาท	เสียหายด้านการเงินมากกว่า ๑๐ ล้านบาท

ความเสียหายจากผลกระทบ	ระดับความเสียหาย				
	ต่ำมาก (๑)	ต่ำ (๒)	ปานกลาง (๓)	สูง (๔)	สูงมาก
ภาพลักษณ์และชื่อเสียง (Reputation)	กระทบชื่อเสียงและภาพพจน์องค์กรน้อย มีการเผยแพร่ข่าวที่รับรู้เฉพาะภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	กระทบชื่อเสียงและภาพพจน์องค์กรน้อย มีการเผยแพร่ข่าวรับรู้เฉพาะภายในสำนักงานปลัดกระทรวงเกษตรและสหกรณ์	กระทบชื่อเสียงและภาพพจน์องค์กรปานกลาง มีการเผยแพร่ข่าวผ่านทางเอกสารตีพิมพ์	กระทบชื่อเสียงและภาพพจน์องค์กรค่อนข้างมาก มีการเผยแพร่ข่าวผ่านทางสถานีโทรทัศน์	กระทบชื่อเสียงและภาพพจน์องค์กรสูงมาก มีการเผยแพร่ข่าวผ่านทางสื่อสังคมออนไลน์
บุคลากร (Employee)	ไม่ได้รับบาดเจ็บ	ได้รับบาดเจ็บเล็กน้อยในระดับปฐมพยาบาลเบื้องต้นได้	ได้รับบาดเจ็บที่จำเป็นต้องได้รับการรักษาจากแพทย์	ได้รับบาดเจ็บหรืออันตรายจนอาจทำให้สูญเสียอวัยวะหรือพิการ	ได้รับบาดเจ็บจนอาจถึงขั้นเสียชีวิต หรือทุพพลภาพถาวร

คำนวณหาระดับความเสี่ยง โดยใช้ข้อมูลของโอกาสที่จะเกิด (Likelihood Score) และผลกระทบ (ความรุนแรง) (Impact Score) ดังนี้

ระดับความเสี่ยง = ระดับโอกาสที่จะเกิด x ระดับผลกระทบ

ตารางระดับและลำดับของความเสี่ยง (Degree of Risk)

ผลกระทบ/ความรุนแรง

5	5x1=5 M	5x2=10 H	5x3=15 E	5x4=20 E	5x5=25 E
4	4x1=4 M	4x2=8 H	4x3=12 H	4x4=16 E	4x5=20 E
3	3x1=3 L	3x2=6 M	3x3=9 H	3x4=12 H	3x5=15 E
2	2x1=2 L	2x2=4 M	2x3=6 M	2x4=8 H	2x5=10 H
1	1x1=1 L	1x2=2 L	1x3=3 L	1x4=4 M	1x5=5 M
	1	2	3	4	5

โอกาสที่จะเกิด

จัดลำดับความเสี่ยง (Degree of Risk) ระดับความเสี่ยงที่เกิดจากความสัมพันธ์ระหว่างระดับความรุนแรงกับระดับโอกาสที่จะเกิด ซึ่งมีระดับของความเสี่ยงอยู่ที่ ๔ ระดับ โดยแต่ละระดับจะมีความหมายของความเสี่ยงและการปฏิบัติเพื่อใช้ในการบริหารความเสี่ยงต่อไป

ตารางแสดงการจัดลำดับความเสี่ยง (Degree of Risk) มี ๔ ระดับ คือ

ลำดับคะแนน	ระดับความเสี่ยง	แทนด้วยแถบสี	ความหมาย
๑๕-๒๕	สูงมาก		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
๘-๑๔	สูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
๔-๗	ปานกลาง		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
๑-๓	ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยงไม่ต้องมีการจัดการเพิ่มเติม

๕. ความเสี่ยงที่ค้นพบจากการดำเนินงานในปีที่ผ่านมา

ความเสี่ยงจากระบบควบคุมอุณหภูมิ/ความชื้นในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์หยุดทำงาน โดยในปีงบประมาณที่ผ่านมา พบว่า ระบบควบคุมอุณหภูมิห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ เกิดการชำรุดบ่อยครั้ง ทำให้อุณหภูมิของห้องเพิ่มขึ้น และต้องมีการเฝ้าระวังในช่วงเวลาดังกล่าว เพื่อไม่ให้ระบบคอมพิวเตอร์ และระบบเครือข่าย หยุดการทำงาน

ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง โดยในปีงบประมาณที่ผ่านมา ได้เกิดปัญหาการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต โดยมีการตัดสายนำสัญญาณ (สาย Fiber) ที่เชื่อมต่อเข้าสู่สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เพื่อดำเนินการนำสายสื่อสารลงใต้ดิน โดยการตัดสายนำสัญญาณ ไม่ได้มีการแจ้งล่วงหน้า จึงทำให้การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง ซึ่งเมื่อหน่วยงานได้ทราบถึงเหตุการณ์ดังกล่าว ได้รีบประสานงานไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ตให้รีบแก้ไข

๖. ผลการประเมินความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

กิจกรรม/ความเสี่ยง	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)				
ความเสี่ยงจาก ไฟไหม้ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	เมื่อเกิดไฟไหม้อาคารสำนักงาน แผ่นดินไหว /อาคารทรุดตัว อาคารถล่ม ไม่สามารถย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ ได้ทัน ทำให้ได้รับความเสียหายทั้งหมด	๑	๕	๕
ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง และกระแสไฟฟ้าดับ	เมื่อเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับ	๒	๕	๑๐

กิจกรรม/ความเสี่ยง	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน
	ความเสียหายหรือ อาจทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปไม่สมบูรณ์ และอาจส่งผลทำให้ข้อมูลบางส่วนเกิดการสูญหาย การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายบางประเภทไม่สามารถใช้งานได้			
ความเสี่ยงจากระบบควบคุมอุณหภูมิ/ความชื้นในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ หยุดทำงาน	ระบบควบคุมอุณหภูมิ/ความชื้นหยุดทำงาน อาจเกิดความเสียหายขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	๓	๔	๑๒
ความเสี่ยงจากไม่มีการควบคุมการ เข้า-ออก ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	เมื่อไม่มีการควบคุมการ เข้า-ออก ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ อาจทำให้ผู้ไม่มีหน้าที่ รับผิดชอบ / มีอำนาจ เข้าไปทำลาย หรือขโมยข้อมูล หรืออุปกรณ์ จนทำให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ได้	๑	๓	๓
ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยทางการเมือง	เมื่อเกิดสถานการณ์ความรุนแรง หรือ ความไม่สงบเรียบร้อย อาจทำให้บุคลากรไม่สามารถเข้าปฏิบัติงานได้ตามปกติ	๑	๕	๕
ความเสี่ยงด้านบุคลากร (Human Risk)				
การดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ	- ระบบเทคโนโลยีสารสนเทศที่พัฒนา ไม่ได้ถูกนำไปใช้ให้เกิดประโยชน์กับหน่วยงาน และขาดการพัฒนาอย่างต่อเนื่อง	๑	๓	๓
	- ไม่สามารถระบุตัวตนผู้ใช้งานได้เมื่อมีผู้ใช้งานกระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์และเครือข่าย - ไม่สามารถตรวจสอบการเข้าถึงการใช้งานระบบเทคโนโลยีสารสนเทศได้	๑	๓	๓
	- มีข้อผิดพลาดและไม่เป็นไปตามแผน อาจทำให้เสียเวลาในการแก้ไข ทำให้ต้องขยายเวลาทำงานและไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	๑	๓	๓
	- เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้ - อาจต้องเพิ่มค่าใช้จ่ายในการบำรุงรักษามากยิ่งขึ้น	๑	๓	๓

กิจกรรม/ความเสี่ยง	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน
	- การใช้งานไม่เป็นไปตาม Work Flow ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขด้วยตัวเองในเบื้องต้นได้ งานติดขัด - เกิดความล่าช้าในการปฏิบัติงานและเพิ่มภาระให้แก่ผู้ดูแลระบบ - ไม่มีการใช้งานระบบ ทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบัน ขาดความน่าเชื่อถือ/ข้อมูลไม่ถูกนำไปใช้งาน	๑	๓	๓
ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	- หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน/ข้อมูล/อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย - ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ	๓	๔	๑๒
ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงานและอาจมีการโจมตีทำให้ระบบไม่สามารถทำงานได้	๕	๒	๑๐
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)				
ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	- เกิดความเสียหายจากการจัดหาครุภัณฑ์ อุปกรณ์ที่ไม่ได้มาตรฐาน - การติดตั้งที่ไม่ได้มาตรฐาน	๑	๓	๓
ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	- ทำให้ใช้ต้องใช้งบประมาณที่สูง ในการจัดหาเครื่องแม่ข่ายทดแทน - ต้องใช้เวลามากในการกู้ระบบ ทำให้เกิดผลกระทบต่อการปฏิบัติงานอื่น - ทำให้เกิดภาพลักษณ์ที่ไม่ดีต่อสำนักงานฯ	๑	๕	๕
ความเสี่ยงจากการบำรุงรักษา - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบเครือข่ายและอุปกรณ์ - คอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง	- ครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีและเครือข่ายสื่อสารสูญหาย	๑	๕	๕
	- ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้ เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	๑	๔	๔
	- ไม่สามารถระบุตัวตนผู้ใช้งาน / หาผู้กระทำความผิดไม่ได้	๑	๓	๓

กิจกรรม/ความเสี่ยง	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน
	- เกิดความเสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote)	๑	๓	๓
	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	๑	๔	๔
	- เกิดความล่าช้าไม่เป็นไปตามแผนปฏิบัติงานที่กำหนด ทำให้ไม่สามารถทำงานได้ต่อเนื่อง - ไม่สามารถตรวจรับงานได้ - ไม่สามารถเบิกจ่ายบงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปี - มีผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	๑	๓	๓
ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	ระบบงานไม่สามารถใช้ได้ตามปกติ	๓	๕	๑๕
ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker Virus Malware ต่างๆเป็นต้น	- ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย - ระบบ/ข้อมูลอาจถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพ บน Web Site ของสำนักงานฯ - ถูกโจรกรรมข้อมูลที่เป็นความลับ	๓	๔	๑๒
ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	- ไม่สามารถใช้งานระบบอินเทอร์เน็ตสำหรับปฏิบัติงานได้ - ไม่สามารถเข้าใช้งานข้อมูลสารสนเทศของหน่วยงานผ่านเครือข่าย	๓	๕	๑๕
ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้ หรือใช้ได้แต่ช้ามาก	๒	๓	๖
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)				
การใช้งานของระบบโปรแกรมคอมพิวเตอร์ไม่มีความมั่นคงปลอดภัย	- ไม่มีความมั่นคงปลอดภัยในการเข้าใช้งาน ขาดการควบคุมการเข้าใช้งานระบบ - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทาให้เกิดความเสียหายต่อระบบ	๑	๓	๓
	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา	๑	๓	๓

กิจกรรม/ความเสี่ยง	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน
	- เกิดภัยคุมคามจากไวรัส เช่น Malware Trojan ที่แฝงมากับโปรแกรมละเมิดลิขสิทธิ์			
	- เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบสารสนเทศและฐานข้อมูล	๑	๕	๕
	- อาจถูกลักลอบขโมยข้อมูล หรือ ข้อมูลถูกทำลาย เกิดความเสียหาย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายต่อระบบ - ระบบถูกโจมตีจนไม่สามารถให้บริการได้	๑	๕	๕
	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบ (ที่พัฒนาไว้อย่างหลากหลาย) - ใช้งบประมาณสูงในการบำรุงรักษา (ไม่คุ้มค่า)	๒	๓	๖
	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตี	๒	๓	๖
	- เกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้ - เกิดช่องโหว่จากการไม่มีการอัปเดตรุ่นใหม่ๆ อย่างสม่ำเสมอ ทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง	๑	๕	๕
การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	๓	๕	๑๕
ความเสี่ยงด้านระบบข้อมูล (Database Risk)				
โจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	๑	๔	๔
	- การให้บริการระบบสารสนเทศหยุดให้บริการส่งผลต่อการให้บริการต่อประชาชนและผู้ใช้บริการทั่วไป	๒	๓	๖

กิจกรรม/ความเสี่ยง	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน
	- ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข			
	- เกิดความเสียหายแก่ระบบข้อมูล ระบบฐานข้อมูล ทำให้ใช้งานไม่ต่อเนื่อง - ไม่สามารถกู้คืนระบบข้อมูล/ฐานข้อมูลได้ เนื่องจากไม่มีแผนสำรองและกู้คืนข้อมูล - ไม่มีแนวทางการป้องกันและการเตรียมการเมื่อเกิดสถานการณ์ฉุกเฉิน	๑	๕	๕
ระบบฐานข้อมูลไม่สามารถเชื่อมโยงบูรณาการ หรือออกรายงานได้	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้	๑	๓	๓
	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	๑	๓	๓
	- ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	๑	๓	๓
ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	- ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้เสียหายต่อความเชื่อถือของ สป.กษ. - ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	๒	๓	๖
ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	- ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน - ระบบเสียหายไม่สามารถใช้งานและบริการข้อมูลได้	๒	๕	๑๐
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)				
เป้าหมาย /ตัวชี้วัด ที่กำหนดตามคำรับรอง	- การดำเนินงานไม่บรรลุเป้าหมาย และไม่มีผลสัมฤทธิ์ของงานตามตัวชี้วัดที่กำหนดในการจัดทำคำรับรอง	๒	๔	๘
ความเสี่ยงด้านการเงิน (Financial Risk)				
งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	- ลดระยะเวลา ลดคุณภาพและประสิทธิภาพการให้บริการตามโครงการต่าง ๆ - ตัดโครงการที่จะดำเนินการออกไป มีผลกระทบต่อแผนงานที่กำหนด	๓	๓	๙

กิจกรรม/ความเสี่ยง	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน
ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)				
การจัดซื้อจัดจ้างในการบำรุงรักษาระบบไม่เป็นไปตามแผนปฏิบัติการ	- ขาดช่วงในการบำรุงรักษาระบบต่างๆ - ความเสียหายอาจเพิ่มมากจนเสียหายได้	๑	๓	๓

๗. การจัดการความเสี่ยง

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน	กลยุทธ์	แนวทางการควบคุม
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
ความเสี่ยงจาก ไฟไหม้ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร หรือการวางเพลิง - ภัยที่เกิดจากธรรมชาติ เช่น ฟ้าผ่า	เมื่อเกิดไฟไหม้อาคารสำนักงาน แผ่นดินไหว / อาคารทรุดตัว อาคารถล่ม ไม่สามารถย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ ได้ทันทำให้ได้รับความเสียหายทั้งหมด	๑	๕	๕	ควบคุมความเสี่ยง	- ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง/สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งาน และตรวจสอบระบบดับเพลิงอัตโนมัติ - สำรองข้อมูลระบบและฐานข้อมูล เก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Plan)
ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง และกระแสไฟฟ้าดับ	- แหล่งที่ให้บริการกระแสไฟฟ้าขัดข้อง - แรงดันไฟฟ้าขัดข้อง	เมื่อเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหายหรือ อาจทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปไม่สมบูรณ์ และอาจส่งผลทำให้ข้อมูลบางส่วนเกิดการสูญหาย การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายบางประเภทไม่สามารถใช้งานได้	๒	๕	๑๐	ควบคุมความเสี่ยง	ตรวจสอบระบบสำรองไฟฟ้า (UPS) /แบตเตอรี่สำรองไฟ
ความเสี่ยงจากระบบควบคุมอุณหภูมิ/ความชื้นในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ หยุดทำงาน	ควบคุมอุณหภูมิและความชื้นที่ไม่เหมาะสม	ระบบควบคุมอุณหภูมิ/ความชื้นหยุดทำงาน อาจเกิดความเสียหายขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	๓	๔	๑๒	ยอมรับความเสี่ยง	- ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศอย่างสม่ำเสมอ - ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น - เตรียมความพร้อม ซักซ้อมความเข้าใจกับช่างที่ให้บริการซ่อม เมื่อเกิดการชำรุดของระบบควบคุมอุณหภูมิ
ความเสี่ยงจากไม่มีการควบคุมการ เข้า-ออกห้องปฏิบัติการระบบ	ไม่มีการควบคุม หรือบันทึกบุคลที่เข้า-ออกห้อง Server Room	เมื่อไม่มีการควบคุมการ เข้า-ออกห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ อาจทำให้ผู้ไม่มีหน้าที่	๑	๓	๓	ควบคุมความเสี่ยง	- บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการ ในการเข้า-ออก ห้อง Server Room ทุกครั้ง

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะแนน	กลยุทธ์	แนวทางการควบคุม
คอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์		รับผิดชอบ / มีอำนาจ เข้าไปทำลาย หรือขโมยข้อมูล หรืออุปกรณ์ จนทำให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ได้					- มีระบบประตูไฟฟ้า/ระบบสแกนลายนิ้วมือเข้าออกทุกครั้ง - มีระบบกล้องโทรทัศน์วงจรปิดในการดูแลห้อง
ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยทางการเมือง	- การชุมนุมประท้วง - การจราจล/การก่อการร้าย - การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	เมื่อเกิดสถานการณ์ความรุนแรง หรือ ความไม่สงบเรียบร้อย อาจทำให้บุคลากรไม่สามารถเข้าปฏิบัติงานได้ตามปกติ	๑	๕	๕	ควบคุมความเสี่ยง	- จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan) - จัดทำระบบการสำรองข้อมูลและสารสนเทศ - จัดทำแผน/ใช้แผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของ สป.กษ.
ความเสี่ยงด้านบุคลากร (Human Risk)							
การดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ	- ผู้บริหารไม่ให้ความสำคัญต่อความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร	- ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่พัฒนาไม่ได้ถูกนำไปใช้ให้เกิดประโยชน์กับหน่วยงาน และขาดการพัฒนาอย่างต่อเนื่อง	๑	๓	๓	ควบคุมความเสี่ยง	- มีแนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ - มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร - มีแนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ - รายงายผู้บริหารอย่างสม่ำเสมอ เพื่อรับทราบและความสำคัญในการจัดการความเสี่ยงเนื่องจากจำเป็นต้องทำ ไม่ทำไม่ได้
	- ผู้รับผิดชอบที่ได้รับมอบหมายไม่ทำการติดตามตรวจสอบการใช้ระบบเทคโนโลยีสารสนเทศตามแผนที่กำหนด	- ไม่สามารถระบุตัวผู้ใช้งานได้เมื่อมีผู้ใช้งานกระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์และเครือข่าย - ไม่สามารถตรวจสอบการเข้าถึงการใช้งานระบบเทคโนโลยีสารสนเทศได้	๑	๓	๓	ควบคุมความเสี่ยง	- ปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.กษ. การขอใช้งานบัญชีผู้ใช้งาน การจัดเก็บ Log) - ปฏิบัติตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูล

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะแนน	กลยุทธ์	แนวทางการควบคุม
							จราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔ - รายงานผลการติดตามตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศ
	- การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญความเชี่ยวชาญ ดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน อาจทำให้เสียเวลาในการแก้ไข ทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	๑	๓	๓	ควบคุมความเสี่ยง	- มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน - มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจนและควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้ - มีการติดตามเพื่อป้องกันการผิดพลาดและให้เกิดการแก้ไขปัญหาได้ทันที โดยมีการประชุมทุก ๆ สัปดาห์
	- บุคลากรด้านไอทีมีความรู้ความเข้าใจในงานด้านเทคโนโลยีสารสนเทศไม่เพียงพอ	- เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้ - อาจต้องเพิ่มค่าใช้จ่ายในการบำรุงรักษามากยิ่งขึ้น	๑	๓	๓	ควบคุมความเสี่ยง	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้าง บุคลากรภายนอก(Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน - มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงในตำแหน่งที่ว่าง
	- ผู้ใช้งาน (Users) ไม่มีความรู้ความชำนาญและทักษะในการใช้งาน	- การใช้งานไม่เป็นไปตาม Work Flow ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขด้วยตัวเองในเบื้องต้นได้ งานติดขัด - เกิดความล่าช้าในการปฏิบัติงานและเพิ่มภาระให้แก่ผู้ดูแลระบบ	๑	๓	๓	ควบคุมความเสี่ยง	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีระบบ Call Center สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุง หรือตามความต้องการของ User

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน	กลยุทธ์	แนวทางการควบคุม
		- ไม่มีการใช้งานระบบ ทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบัน ขาดความน่าเชื่อถือ/ข้อมูลไม่ถูกนำไปใช้งาน					
ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	สิทธิ์ฐานข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศไม่เป็นปัจจุบันเนื่องจากผู้ใช้งานมีการลาออก โอน ย้าย สิ้นสุดการจ้างตลอดเวลา	- หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน/ข้อมูล/อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย - ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ	๓	๔	๑๒	ควบคุมความเสี่ยง	หน่วยงานในสังกัด สป.กษ. ต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออก โอน ย้าย หรือสิ้นสุดการจ้างให้หน่วยงานทำหนังสือแจ้งให้กับ ศทส. /หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน
ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	อุปกรณ์ที่ใช้ไม่มีระบบรักษาความปลอดภัยที่ถูกต้องและเพียงพอ	อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงานและอาจมีการโจมตีทำให้ระบบไม่สามารถทำงานได้	๕	๒	๑๐	ควบคุมความเสี่ยง	- อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน - กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)							
ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	- ครุภัณฑ์ อุปกรณ์ไม่ได้มาตรฐาน - การติดตั้งใช้งานไม่สมบูรณ์	- เกิดความเสียหายจากการจัดหาครุภัณฑ์อุปกรณ์ที่ไม่ได้มาตรฐาน - การติดตั้งที่ไม่ได้มาตรฐาน	๑	๓	๓	ควบคุมความเสี่ยง	กำหนดให้การจัดหาและใช้งานคอมพิวเตอร์เป็นไปตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	- เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง - เสียเวลาในการกู้ระบบ - เสียภาพลักษณ์ของสำนักงานฯ	๑	๕	๕	ควบคุมความเสี่ยง	- ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะแนน	กลยุทธ์	แนวทางการควบคุม
							- จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน - ควบคุมการเข้าออกและขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคารตลอดเวลา - ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่
ความเสี่ยงจากการบำรุงรักษา - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบเครือข่ายและอุปกรณ์ - คอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง	- ไม่มีการควบคุมบัญชีรายการ ปรับปรุงรายการอุปกรณ์เทคโนโลยี	- ครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีและเครือข่ายสื่อสารสูญหาย	๑	๕	๕	ควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์ของ ศทส.
	- ขาดแผนรองรับระบบฮาร์ดแวร์ภายในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	- ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	๑	๔	๔	ควบคุมความเสี่ยง	- มีแผนการบำรุงรักษา ตรวจสอบ และซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุกเดือน - จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ - ทดสอบการโจมตีตามแผนที่กำหนดจริง
	- ขาดการบริหารและจัดการสิทธิ์การใช้อุปกรณ์เทคโนโลยีสารสนเทศ	- ไม่สามารถระบุตัวตนผู้ใช้งาน / หาผู้กระทำความผิดไม่ได้	๑	๓	๓	ควบคุมความเสี่ยง	มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน	กลยุทธ์	แนวทางการควบคุม
	- ระบบเครือข่ายสื่อสารหลักไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	- เกิดความเสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote)	๑	๓	๓	ควบคุมความเสี่ยง	- ระบุข้อกำหนด/ข้อตกลง ระดับการให้บริการที่ชัดเจนกับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนทุกครั้งที่ขัดข้องเพื่อให้แก้ปัญหาได้ทันที
	- ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสาร	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	๑	๔	๔	ควบคุมความเสี่ยง	- ทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ โดยมีระบบพิสูจน์และยืนยันตัวบุคคล - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา - มีการปรับเพิ่มประสิทธิภาพการบริหารจัดการทุก ๆ ปี
	- กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน ● อนุมัติโครงการล่าช้า ● ไม่สามารถประกาศผลผู้ชนะการประกวดราคา ● สัญญาไม่ตรงตามร่างข้อกำหนด	- เกิดความล่าช้าไม่เป็นไปตามแผนปฏิบัติงานที่กำหนด ทำให้ไม่สามารถทำงานได้ต่อเนื่อง - ไม่สามารถตรวจรับงานได้ - ไม่สามารถเบิกจ่ายบงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปี - มีผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	๑	๓	๓	ควบคุมความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการ ให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการอย่างจริงจัง กรณีผู้บริหารอนุมัติโครงการล่าช้า ต้องขอวาระชี้แจงเหตุผลความจำเป็นและจัดลำดับความสำคัญ/ความเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะแนน	กลยุทธ์	แนวทางการควบคุม
ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	การทำงานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ขัดข้อง	ระบบงานไม่สามารถใช้ได้ตามปกติ	๓	๕	๑๕	ถ่ายโอนความเสี่ยง	- ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล - จัดหา DR-Site - จัดจ้างผู้ดูแลระบบ (Outsource)
ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker ไวรัส Malware ต่างๆเป็นต้น	การถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	- ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย - ระบบ/ข้อมูลอาจจะถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพ บนเว็บไซต์ของสำนักงานฯ - ถูกโจรกรรมข้อมูลที่เป็นความลับ	๓	๔	๑๒	ควบคุมความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้งระบบป้องกัน และเตือนภัย Spam,Virus, Malware, Trojan - ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการสม่ำเสมอ - จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ/เฝ้าระวัง
ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	- ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่ายอินทราเน็ตได้ - ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	- เจ้าหน้าที่และผู้บริหารงานสำนักงานฯไม่สามารถใช้งานระบบอินเทอร์เน็ตสำหรับปฏิบัติงานได้ - บุคคลภายนอกไม่สามารถเข้าใช้งานข้อมูลสารสนเทศของหน่วยงานผ่านเครือข่าย	๓	๕	๑๕	ควบคุมความเสี่ยง	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการเครือข่ายอินเทอร์เน็ต - ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ - เตรียมความพร้อมกับบริษัทผู้ให้บริการระบบเครือข่ายอินเทอร์เน็ต กรณีการโดนตัดสายสัญญาณ
ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้ หรือใช้ได้แต่ช้ามาก	๒	๓	๖	ควบคุมความเสี่ยง	- กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ - การควบคุมด้วยระบบ Desktop Management

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน	กลยุทธ์	แนวทางการควบคุม
	เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ						
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
การใช้งานของระบบโปรแกรมคอมพิวเตอร์ไม่มีความมั่นคงปลอดภัย	- ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System access control) และโปรแกรมระยุกต์หรือแอปพลิเคชัน (เครื่องคอมพิวเตอร์แม่ข่าย)	- ไม่มีความมั่นคงปลอดภัยในการเข้าใช้งาน ขาดการควบคุมการเข้าใช้งานระบบ - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบ	๑	๓	๓	ควบคุมความเสี่ยง	- มีการกำหนดสิทธิ์ในการเข้าถึงเพื่อทำการจำกัดและควบคุมการเข้าถึง - ใช้งานโปรแกรมเพื่อป้องกันการละเมิด โดยการตรวจสอบสิทธิ์ - มีการทบทวนสิทธิ์เป็นประจำ โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ ทุก ๑๒ เดือน - ปฏิบัติตามข้อปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร สป.กษ. อย่างเคร่งครัด
	- ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Use of System Utilities) ของเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่าย	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware Trojan ที่แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	๑	๓	๓	ควบคุมความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบาย หรือระเบียบด้านสารสนเทศอย่างจริงจัง - จัดทำ และส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะแนน	กลยุทธ์	แนวทางการควบคุม
	- ขาดการป้องกันหรือตรวจจับไวรัส	- เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบสารสนเทศและฐานข้อมูล	๑	๕	๕	ควบคุมความเสี่ยง	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - ปรับปรุงโปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ
	- การรักษาความมั่นคงปลอดภัยจากผู้ปฏิบัติงานในระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือ ข้อมูลถูกทำลายเกิดความเสียหาย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายต่อระบบ - ถูกโจมตีระบบจนไม่สามารถให้บริการได้	๑	๕	๕	ควบคุมความเสี่ยง	มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง
	- ไม่มีการกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบ (ที่พัฒนาไว้อย่างหลากหลาย) - ใช้งบประมาณสูงในการบำรุงรักษา (ไม่คุ้มค่า)	๒	๓	๖	ควบคุมความเสี่ยง	- จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ - ระบุมาตรฐานการพัฒนาซอฟต์แวร์ และคุณสมบัติผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR - ควบคุม ติดตามทุกขั้นตอนการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐาน และTOR
	- เกิดช่องโหว่ของซอฟต์แวร์	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตี	๒	๓	๖	ควบคุมความเสี่ยง	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง
	- ขาดการบำรุงรักษาโปรแกรม หรือระบบงานที่ครอบคลุม	- เกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้ - เกิดช่องโหว่จากการไม่มีการอัปเดตรุ่นใหม่ๆ อย่างสม่าเสมอ ทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง	๑	๕	๕	ควบคุมความเสี่ยง	ทำแผนการบำรุงรักษาโปรแกรม และระบบงานอย่างต่อเนื่อง เพื่อปิดช่องโหว่จากการอัพเดตรุ่นใหม่ๆ อย่างสม่ำเสมอ ทำให้สามารถใช้ระบบได้อย่างต่อเนื่องและใช้ในเวลาที่ต้องการได้

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน	กลยุทธ์	แนวทางการควบคุม
การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	๓	๕	๑๕	ควบคุมความเสี่ยง	- การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น - สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย
ความเสี่ยงด้านระบบข้อมูล (Database Risk)							
โจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ ไม่มีอำนาจเจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	๑	๔	๔	ควบคุมความเสี่ยง	มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall
	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ ไม่มีอำนาจเจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	- การให้บริการระบบสารสนเทศหยุดให้บริการ ส่งผลต่อการให้บริการต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	๒	๓	๖	ควบคุมความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์ปรับปรุง - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก ๖ เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายในหรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะแนน	กลยุทธ์	แนวทางการควบคุม
							- จัดทำการสำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมอ อย่างน้อยอาทิตย์ละ ๑ ครั้ง
	- ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูล และระบบฐานข้อมูล - ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)	- เกิดความเสียหายแก่ระบบข้อมูล ระบบฐานข้อมูล ทำให้ใช้งานไม่ต่อเนื่อง - ไม่สามารถกู้คืนระบบข้อมูล/ฐานข้อมูลได้ เนื่องจากไม่มีแผนสำรองและกู้คืนข้อมูล - ไม่มีแนวทางการป้องกันและการเตรียมการเมื่อเกิดสถานการณ์ฉุกเฉิน	๑	๕	๕	จัดการความเสี่ยง	- จัดทำการสำรองข้อมูลแบบอัตโนมัติโดยจัดเก็บข้อมูลทั้งระบบแบบ Full Backup บน Storage สัปดาห์ละ ๑ ครั้ง - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติโดยจัดเก็บใน Hard Disk เป็นประจำทุกเดือน - มีการทดสอบการกู้คืนข้อมูลของทุกระบบงานอย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการเตรียมความพร้อมหากเกิดสถานการณ์ฉุกเฉิน - มีการควบคุมกำกับการสำรองข้อมูลให้เป็นไปตามแผน พร้อมทั้งการตรวจสอบความสมบูรณ์ในการสำรองข้อมูลทุกครั้ง
ระบบฐานข้อมูลไม่สามารถเชื่อมโยงบูรณาการ หรือออกรายงานได้	- การนำเข้าข้อมูลผิดพลาด ทั้งจากการนำเข้าข้อมูล (Human Error) และจากความผิดพลาดของระบบฯ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้	๑	๓	๓	ควบคุมความเสี่ยง	มีการตรวจสอบทุกครั้งเมื่อนำข้อมูลเข้าเสร็จเรียบร้อย
	- การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	๑	๓	๓	ควบคุมความเสี่ยง	ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ
	- ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบฐานข้อมูล	- ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	๑	๓	๓	ควบคุมความเสี่ยง	- มีการติดตามการนำมาตรฐานข้อมูลกลาง สป.กษ. ไปใช้อย่างสม่ำเสมอ - มีการดำเนินงานทบทวน/ปรับปรุง และเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลาง สป.กษ. ที่

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะแนน	กลยุทธ์	แนวทางการควบคุม
							ครอบคลุมภารกิจของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ และสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี - มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ ได้แก่ ระบบบริหารสำนักงาน (Back Office)
ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือ อุปกรณ์สำรองข้อมูลประเภทต่างๆ	- ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้เสียหายต่อความเชื่อถือของ สป.กษ. - ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	๒	๓	๖	ยอมรับความเสี่ยง	มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Harddisk อุปกรณ์สำรองข้อมูลประเภทต่างๆ ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้ก่อนจำหน่าย
ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล/ดำเนินการสำรองไม่ต่อเนื่อง	- ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน - ระบบเสียหายไม่สามารถใช้งานและบริการข้อมูลได้	๒	๕	๑๐	ควบคุมความเสี่ยง	- หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ - มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) - จัดหา DR-Site
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)							
เป้าหมาย /ตัวชี้วัด ที่กำหนดตามคำรับรอง	- ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามคำรับรองได้	- การดำเนินงานไม่บรรลุเป้าหมาย และไม่มีผลสัมฤทธิ์ของงานตามตัวชี้วัดที่กำหนดในการจัดทำคำรับรอง	๒	๔	๘	จัดการความเสี่ยง	- บรรจุโครงการแผนปฏิบัติการให้ผู้บริหารเห็นชอบแผน - กำหนดกรอบเวลาให้ชัดเจนและอยู่ในกรอบเวลาที่สามารถดำเนินการได้ - กำหนดกลุ่มเป้าหมายที่ชัดเจน - หน่วยงานวิเคราะห์งบประมาณต้องมีการดำเนินการตัดปรับลดโดยการมีการจัดทำความ

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง/ความเสียหายที่อาจจะเกิดขึ้น	โอกาส	ผลกระทบ	คะนน	กลยุทธ์	แนวทางการควบคุม
							เสี่ยงและการให้น้ำหนักของความสำคัญของโครงการที่ใช้หมวดเงินประเภทเดียวกัน
ความเสี่ยงด้านการเงิน (Financial Risk)							
งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	- โดนตัด/ปรับลดโครงการ ตามนโยบายการปรับลดเงินเป็นเปอร์เซ็นต์ ทำให้โครงการที่จำเป็นต้องดำเนินการโดนตัด/ปรับลดไปด้วย	- ลดระยะเวลา ลดคุณภาพและประสิทธิภาพการให้บริการตามโครงการต่าง ๆ - ตัดโครงการที่จะดำเนินการออกไป มีผลกระทบต่อแผนงานที่กำหนด	๓	๓	๙	จัดการความเสี่ยง	- ปรับลดโครงการตามลำดับความสำคัญ และลดปริมาณหน่วยบริการ - ปรับแผนการดำเนินงาน ตามแผนการใช้จ่ายงบประมาณตามงวดงานที่ได้รับ
ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)							
การจัดซื้อจัดจ้างในการบำรุงรักษาระบบไม่เป็นไปตามแผนปฏิบัติการ	ไม่สามารถดำเนินงานได้อย่างต่อเนื่องทันที	- ขาดช่วงในการบำรุงรักษาระบบต่างๆ - ความเสียหายอาจเพิ่มมากจนเสียหายได้	๑	๓	๓	ควบคุมความเสี่ยง	จัดทำแผนปฏิบัติการและดำเนินการ ให้เป็นไปตามแผนที่กำหนด

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้รับผิดชอบหลัก ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ กระทรวงเกษตรและสหกรณ์

ระยะเวลา ตุลาคม ๒๕๖๓ – กันยายน ๒๕๖๗

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๔			๒๕๖๕			๒๕๖๖			๒๕๖๗			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
ความเสี่ยงจาก ไฟไหม้ห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	๑. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูลเป็นประจำ ๒. จัดหา Dr-Site	ทุกวัน ปี ๒๕๖๗	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง และกระแสไฟฟ้าดับ	๑. ตรวจสอบการทำงานระบบสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ ๒. วางแผนการจัดหาและติดตั้ง UPS และเครื่องกำเนิดไฟฟ้า (Electrical Generator)	ทุกวัน ปี ๒๕๖๗	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
ความเสี่ยงจากระบบควบคุมอุณหภูมิ/ความชื้นในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์หยุดทำงาน	๑. ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ ๒. วางแผนจัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ใน	ทุกวัน ปี ๒๕๖๗	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๔			๒๕๖๕			๒๕๖๖			๒๕๖๗			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
	สภาวะที่เหมาะสมและสามารถทำงานสลับกันได้														
ความเสี่ยงจากไม่มีการควบคุมการ เข้า-ออกห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์	๑. ใช้งานระบบประตูไฟฟ้า/ระบบสแกนลายนิ้วมือเข้าออกทุกครั้ง ๒. ใช้งานระบบกล้องโทรทัศน์วงจรปิดในการช่วยดูแลห้อง	ทุกวัน ทุกวัน	←	←	→	←	←	→	←	←	→	←	←	→	ศทส.
ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยทางการเมือง	จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan) และซักซ้อมทำความเข้าใจเป็นประจำ	๑ ครั้ง/ปี			← →			← →			← →			← →	ศทส./หน่วยงานในสังกัด สป.กษ./ผู้ใช้งาน
การดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ	๑. อบรม สร้างความรู้ความเข้าใจการใช้งานที่ถูกวิธี ๒. กำหนด Policy ของอุปกรณ์รักษาความปลอดภัยของหน่วยงานให้มีความปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอ และการเปิด Port เท่าที่จำเป็น ๓. กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	๑ ครั้ง/ปี			← →			← →			← →			← →	ศทส./หน่วยงานในสังกัด สป.กษ./ผู้ใช้งาน
ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับ	ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	๑ ครั้ง/ปี			← →			← →			← →			← →	ศทส.

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๔			๒๕๖๕			๒๕๖๖			๒๕๖๗			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
อนุญาตไปใช้ในทางที่ผิดกฎหมาย															
ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	๑. อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน ๒. กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	๑ ครั้ง/ปี ทุกวัน			→			→			→			→	ศทส./หน่วยงานเจ้าของระบบ
ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	กำหนดให้การจัดหาและใช้งานคอมพิวเตอร์เป็นไปตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	๒ ครั้ง/ปี	→		→	→		→	→		→	→		→	ศทส./หน่วยงานในสังกัด สป.กษ.
ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	๑. ใช้งานระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย ๒. ควบคุมการเข้าออกและขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคารตลอดเวลา	ทุกวัน ทุกวัน													ศทส.
ความเสี่ยงจากการบำรุงรักษา - เครื่องคอมพิวเตอร์แม่ข่าย	๑. มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ	ทุกเดือน													ศทส.

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๔			๒๕๖๕			๒๕๖๖			๒๕๖๗			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
- ระบบเครือข่ายและอุปกรณ์ - คอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง	๒. มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุกเดือน ๓. จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ ๔. ทดสอบการโจมตีตามแผนที่กำหนดจริง														
ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	๑. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒. จัดหา Dr-Site	ทุกวัน	←											→	ศทส.
ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker ไวรัส Malware ต่างๆเป็นต้น	๑. ติดตั้งโปรแกรมป้องกันไวรัส Malware, Trojan และ update patch อย่างสม่ำเสมอ ๒. ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ ๓. อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน	ทุกวัน ๑ ครั้ง/ปี ๑ ครั้ง/ปี	←											→	ศทส./หน่วยงานในสังกัด สป.กษ.

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๔			๒๕๖๕			๒๕๖๖			๒๕๖๗			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	๑. ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ใหบริการเครือข่ายอินเทอร์เน็ต ๒. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	ทุกวัน	←											→	ศทส.
ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	๑. กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ๒. การควบคุมด้วยระบบ Desktop Management	ทุกวัน	←											→	ศทส.
การใช้งานของระบบโปรแกรมคอมพิวเตอร์ไม่มีความมั่นคงปลอดภัย	๑. มีการกำหนดสิทธิ์ในการเข้าถึงเพื่อทำการจำกัดและควบคุมการเข้าถึง ๒. มีการทบทวนสิทธิ์เป็นประจำ โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข	ทุกวัน	←											→	ศทส.
การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒. สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ทุกวัน	←											→	ศทส.
โจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	ติอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall	ทุกวัน	←											→	ศทส.

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๔			๒๕๖๕			๒๕๖๖			๒๕๖๗			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
ระบบฐานข้อมูลไม่สามารถเชื่อมโยงบูรณาการ หรือออกรายงานได้	มีการตรวจสอบทุกครั้งเมื่อนำข้อมูลเข้าเสร็จเรียบร้อย	ทุกวัน	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk อุปกรณ์สำรองข้อมูลประเภทต่างๆ ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้ก่อนจำหน่าย	ทุกวัน	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	๑. หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	ทุกสัปดาห์ ๒ ครั้ง/ปี	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
เป้าหมาย /ตัวชี้วัด ที่กำหนดตามคำรับรอง	๑. บรรจุโครงการแผนปฏิบัติการให้ผู้บริหารเห็นชอบแผน ๒. กำหนดกรอบเวลาให้ชัดเจนและอยู่ในกรอบเวลาที่สามารถดำเนินการได้ ๓. กำหนดกลุ่มเป้าหมายที่ชัดเจน ๔. หน่วยงานวิเคราะห์งบประมาณต้องมีการดำเนินการตัดปรับลดโดยการมีการจัดทำความเสี่ยงและการให้น้ำหนักของความสำคัญของ	ทุกปี	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๔			๒๕๖๕			๒๕๖๖			๒๕๖๗			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
	โครงการที่ใช้หมวดเงินประเภทเดียวกัน														
งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	ปรับปรุงโครงการให้สอดคล้องกับงบประมาณที่ได้รับ	ทุกปี	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
การจัดซื้อจัดจ้างในการบำรุงรักษาระบบไม่เป็นไปตามแผนปฏิบัติการ	กำหนดกรอบระยะเวลาและวิธีปฏิบัติให้สามารถดำเนินการได้ไม่เร่งด่วนจนเกินไป	ทุกปี	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.

บทที่ ๔
สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อมีการปรับเปลี่ยนโดยใช้เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญเป็นกลไกในการขับเคลื่อน การดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการความเสี่ยงในองค์กร นั่นเอง

จึงมีการทบทวนแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ แนวทางการดำเนินงานเพื่อลดความเสี่ยงที่เกิดขึ้น เพื่อให้ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้

๑. ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

จากการประเมินความเสี่ยง และจัดระดับความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ พบว่า ยังมีกิจกรรมที่ยังมีความเสี่ยงที่อยู่ใน**ระดับสูงมาก และสูง** อยู่ถึง ๙ กิจกรรม ด้วยกัน ซึ่งได้กำหนดแนวทางในการควบคุมเรียบร้อยแล้ว ดังนี้

๑.๑ ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ (ระดับสูงมาก) ซึ่งปัจจัยเสี่ยงอาจเกิดขึ้นได้จากการทำงานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ขัดข้อง และได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- ตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และสำรองฐานข้อมูล เป็นประจำ และสม่ำเสมอ
- จัดหา Dr-Site เพื่อรองรับกรณีแม่ข่ายหลักที่ใช้งานเกิดความเสียหาย
- จัดจ้างผู้ดูแลระบบ (Out Source) เพื่อช่วยดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย

๑.๒ ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง (ระดับสูงมาก) ส่งผลให้ไม่สามารถใช้งานระบบอินเทอร์เน็ต และไม่สามารถเข้าใช้งานระบบสารสนเทศของหน่วยงานผ่านระบบเครือข่ายได้ โดยได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการเครือข่ายอินเทอร์เน็ต
- ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ
- เตรียมความพร้อมกับบริษัทผู้ให้บริการระบบเครือข่ายอินเทอร์เน็ต กรณีการโดนตัดสายสัญญาณ

๑.๓ การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย (ระดับสูงมาก) ซึ่งอาจทำให้หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ และได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น
- สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย

๑.๔ ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker Virus Malware ต่างๆเป็นต้น (ระดับสูง) มีโอกาสทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย, ระบบ/ข้อมูลอาจจะถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพ บน Web Site ของสำนักงานฯ, ถูกโจรกรรมข้อมูลที่เป็นความลับ ซึ่งปัจจัยเสี่ยงอาจเกิดขึ้นได้จากการถูกโจมตีระบบผ่านระบบเครือข่ายอินเตอร์เน็ตจากผู้ไม่ประสงค์ดี โดยได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ
- ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ
- ติดตั้งระบบป้องกัน และเตือนภัย Spam,Virus, Malware, Trojan
- ติดตั้ง patch ของระบบปฏิบัติการสม่ำเสมอ
- จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ/เฝ้าระวัง

๑.๕ ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย (ระดับสูง) มีโอกาสทำให้ หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน/ข้อมูล/อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย หรือข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ ซึ่งปัจจัยเสี่ยงอาจเกิดขึ้นได้เนื่องจากไม่ได้ปรับปรุงฐานข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบันเนื่องจากมีบุคลากรลาออก โอน ย้าย โดยได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- หน่วยงานในสังกัด สป.กษ. ต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออก โอน ย้าย หรือสิ้นสุดการจ้างให้หน่วยงานทำหนังสือแจ้งให้กับ ศทส. /หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน

๑.๖ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง และกระแสไฟฟ้าดับ (ระดับสูง) โดยเมื่อเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ อาจทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย หรือ อาจทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปไม่สมบูรณ์ และอาจส่งผลทำให้ข้อมูลบางส่วนเกิดการสูญหาย การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายบางประเภทไม่สามารถใช้งานได้ ซึ่งปัจจัยเสี่ยงอาจเกิดขึ้นได้เนื่องจากแหล่งที่ให้บริการกระแสไฟฟ้าขัดข้อง หรือแรงดันไฟฟ้าขัดข้อง โดยได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- ให้มีการใช้งานระบบสำรองไฟฟ้า (UPS)
- ตรวจสอบระบบสำรองไฟฟ้า (UPS) /แบตเตอรี่สำรองไฟ เป็นประจำ

๑.๗ ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน (ระดับสูง) ซึ่งอาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงานและอาจมีการโจมตีทำให้ระบบไม่สามารถทำงานได้ ซึ่งปัจจัยเสี่ยงอาจเกิดขึ้นได้เนื่องจากอุปกรณ์ที่นำมาใช้ไม่มีระบบรักษาความปลอดภัยที่ถูกต้องและเพียงพอ โดยได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน
- กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

๑.๘ ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง (ระดับสูง) ซึ่งอาจทำให้ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน ระบบเสียหายไม่สามารถใช้งานและบริการข้อมูลได้ โดยอาจเกิดจากระบบสารสนเทศที่ไม่มีการสำรองข้อมูล/ดำเนินการสำรองไม่ต่อเนื่อง โดยได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ
- มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)

๑.๙ ความเสี่ยงจากระบบควบคุมอุณหภูมิ/ความชื้นในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ หยุดทำงาน (ระดับสูง) อาจเกิดความเสียหายขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ โดยได้มีการกำหนดแนวทางควบคุมไว้แล้ว ดังนี้

- ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศอย่างสม่ำเสมอ
- ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น
- เตรียมความพร้อม ซักซ้อมความเข้าใจกับช่างที่ให้บริการซ่อม เมื่อเกิดการชำรุดของระบบควบคุมอุณหภูมิ

๒. สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการจัดทำโดยมีวัตถุประสงค์

๒.๑ เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

๒.๒ เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๒.๓ ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓. ข้อเสนอแนะ

๓.๑ การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

๓.๑.๑ พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

๓.๑.๒ พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

๓.๑.๓ กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

๓.๒ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการ

ติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ