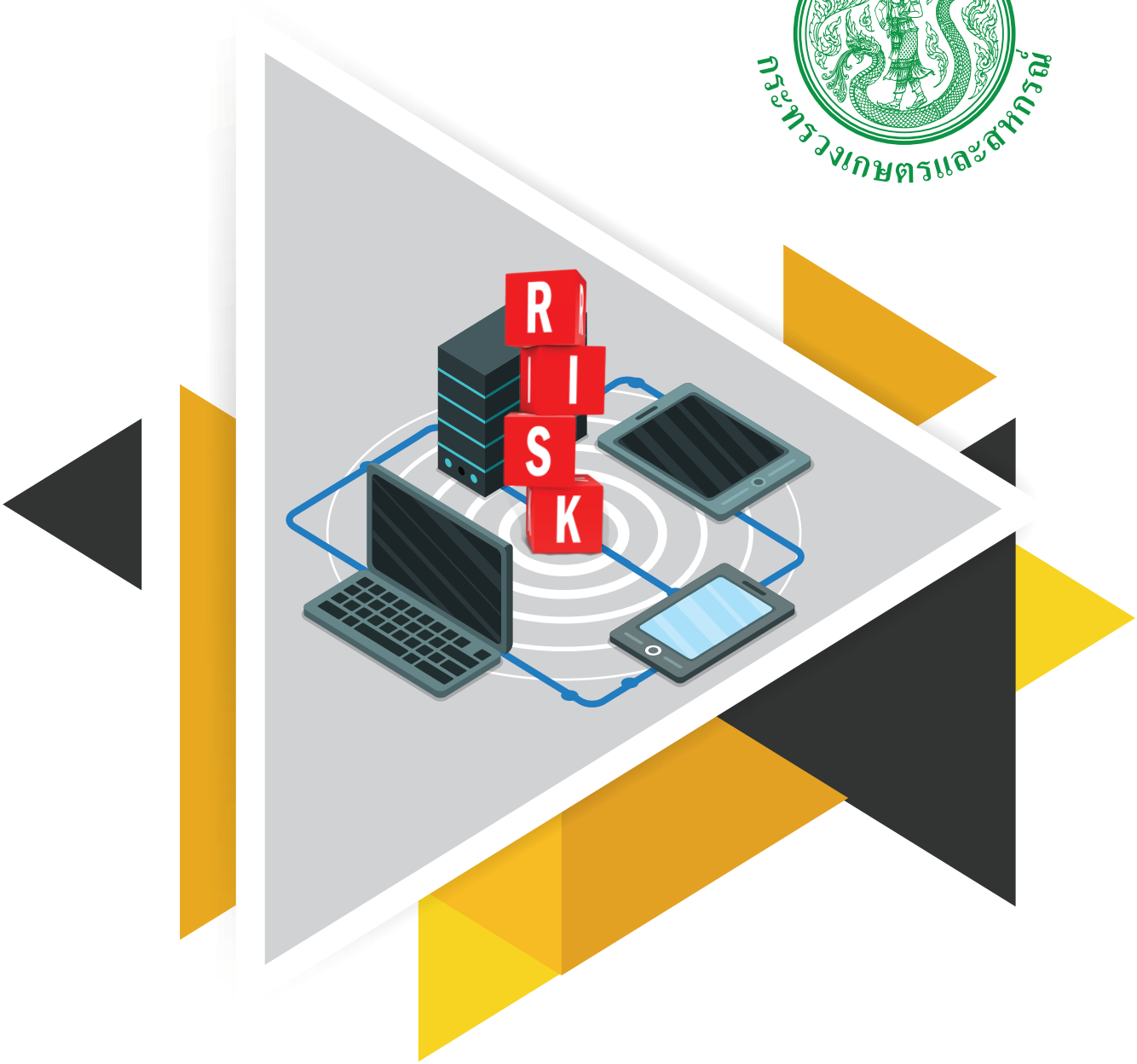


แผนบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

ประจำปีงบประมาณ ๒๕๖๑-๒๕๖๔

โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

คำนำ

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (สป.กษ.) ปี ๒๕๖๑-๒๕๖๔ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สป.กษ. ฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของ สป.กษ. ต่อไป

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเกษตรและสหณณ์
กรกฎาคม ๒๕๖๑

สารบัญ

หน้า

บทที่ ๑ ..... ๑

บทนำ ๑

๑. หลักการและเหตุผล ๑

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง ๑

๓. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ ๑

๔. กระบวนการบริหารความเสี่ยง ๒

๕. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ๖

๖. การตอบสนองความเสี่ยง ๗

๗. ปัจจัยเสี่ยง ๘

๘. การประเมินความเสียหาย ๘

๙. การติดตามและรายงานผล ๘

๑๐. ระบบรักษาความปลอดภัยบนเครือข่าย ๘

บทที่ ๒ ..... ๑๑

การวิเคราะห์การบริหารจัดการความเสี่ยง ๑๑

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง ๑๒

๒. กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ๑๓

๓. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ๑๔

๔. ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ๑๖

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ๒๒

บทที่ ๓ ..... ๒๖

สรุปและข้อเสนอแนะ ๒๖

๑. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ๒๖

๒. สรุป ๒๗

๓. ข้อเสนอแนะ ๒๘

สารบัญรูป

รูปที่ ๑ แสดงกระบวนการบริหารความเสี่ยง ๒

รูปที่ ๒ แสดงแผนผังประเมินความเสี่ยง ๔

รูปที่ ๓ แสดงโครงข่ายคอมพิวเตอร์สารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ๑๐

สารบัญตาราง

ตารางที่ ๑ ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร.....๑๔

บทที่ ๑
บทนำ

๑. หลักการและเหตุผล

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

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๑. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

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)

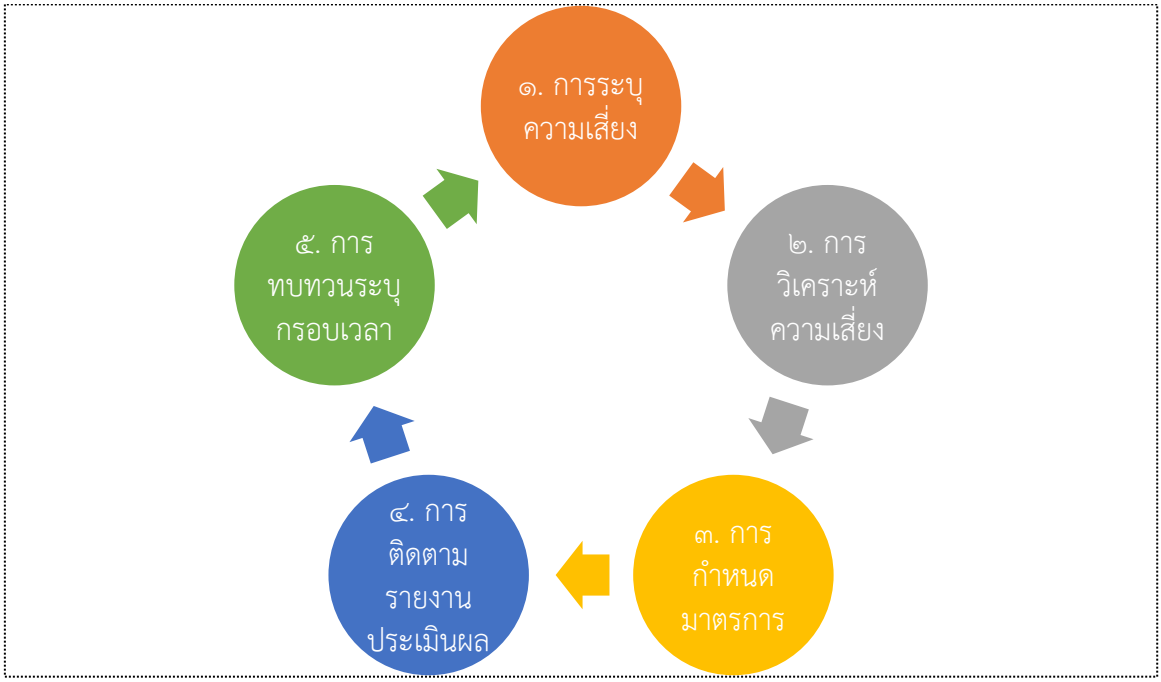
อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบสารสนเทศ (Web Application Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจาย

สัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

ระบบรักษาความปลอดภัย ได้แก่ โปรแกรมตรวจสอบและป้องกันไวรัส Firewall IPS (Instrution Prevention System) และ Web Application Firewall

๔. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้



รูปที่ ๑ แสดงกระบวนการบริหารความเสี่ยง

๑. การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๑.๑ การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๑.๒ การใช้ Checklist

๑.๓ การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

๑.๔ การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

๑.๕ การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๒. การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

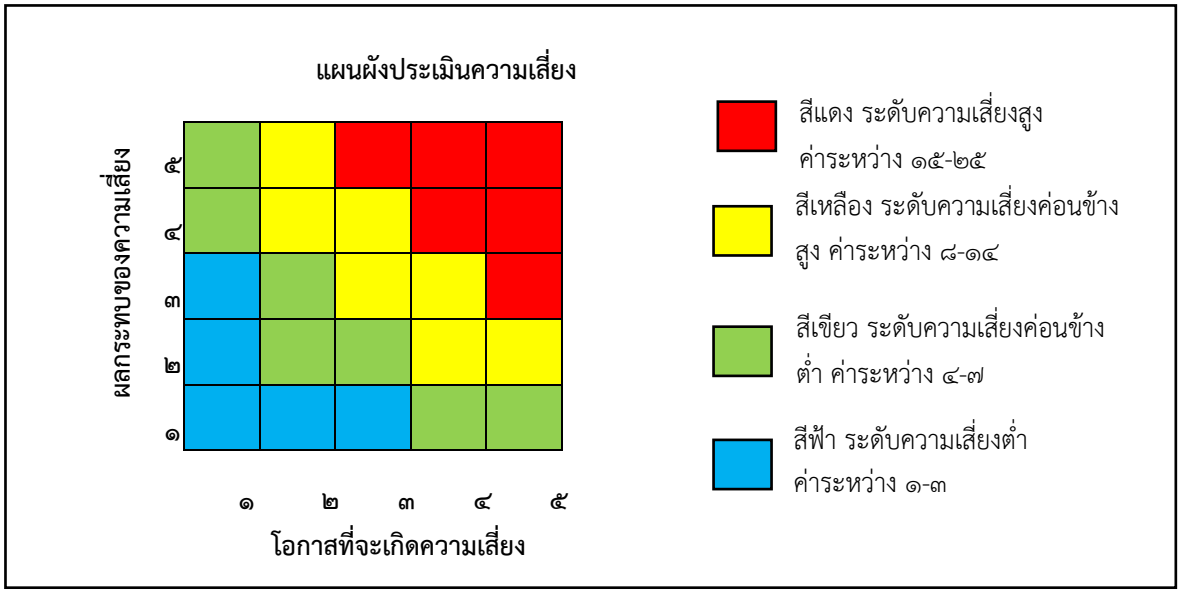
เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับ	การประเมิน
๑	น้อยมาก
๒	น้อย
๓	ปานกลาง
๔	สูง
๕	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

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

๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปที่ ๒



รูปที่ ๒ แสดงแผนผังประเมินความเสี่ยง

๒.๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๓. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๓.๑ ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๓.๒ การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุม เพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓.๓ การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๓.๔ การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่

โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

๒) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๔. การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๔.๑ พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔.๔ ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยง ด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๕. การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๕. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๘ ประเภท ดังนี้

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

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

ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

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

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

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

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

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยง เนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

๖. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้(Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๗. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ได้แก่

๑. ปัจจัยภายนอก ได้แก่

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

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๑.๖ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๘. การประเมินความเสียหาย

๙.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๙.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๙. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

๑๐. ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบคอมพิวเตอร์และเครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่าย สำนักงานปลัดกระทรวงเกษตรและสหกรณ์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ตั้งอยู่ที่สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ถนนราชดำเนินนอก แขวงบ้านพานถม เขตพระนคร กรุงเทพฯ

ระบบคอมพิวเตอร์และเครือข่าย สำนักงานปลัดกระทรวงเกษตรและสหกรณ์มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์ และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ของ FortiGate ๖๒๐B ซึ่งใช้ในการกรอง (Filter Package) ที่ผ่านเข้ามาภายในระบบของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์จากเครือข่ายภายนอก เช่น เครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เครือข่ายอินเทอร์เน็ต เครือข่าย GIN[๑] นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของ DMZ[๒] ที่ดูแลเครื่องแม่ข่ายทั้งหมดของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่อง

คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ในส่วนกลาง มีการแบ่ง Subnet[๓] เพื่อให้เป็นระบบกลุ่มบรอดคาสต์โดเมน (Broadcast Domain) เดียวกัน ประกอบกับกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private[๔] เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

ระบบเครือข่ายหลักของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (Core Network) ตั้งอยู่ที่ห้องคอมพิวเตอร์แม่ข่ายกลาง (Server Room) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่ายภายในระดับกอง/สำนักงาน ในความเร็วระดับ ๑๐ Gbps และระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ต และ GIN เข้าด้วยกันซึ่งมี Core Switch ที่ออกแบบติดตั้งในลักษณะระบบเครือข่ายที่สามารถทดแทนกันได้ (Redundant Network) เพื่อแก้ปัญหาระบบเครือข่ายศูนย์กลางล่ม (Single Point of Failure) และแก้ปัญหาคอขวดในการเข้าถึงข้อมูล (Bottle neck) เพื่อรองรับภารกิจของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ซึ่งลักษณะงานต้องใช้อุปกรณ์เครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพสูงสามารถรองรับการเชื่อมต่อกับระบบเครือข่ายภายในและภายนอกแบบ ๒๔x๗ เพื่อใช้ระบบงานฐานข้อมูลที่สำคัญของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ พร้อมทั้งเชื่อมโยงไปยังอุปกรณ์ Distributed Switch (L๓) และ Access Switch (L๒) ไปยังอาคารต่างๆ ซึ่งเป็นที่ตั้งของหน่วยงานในสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

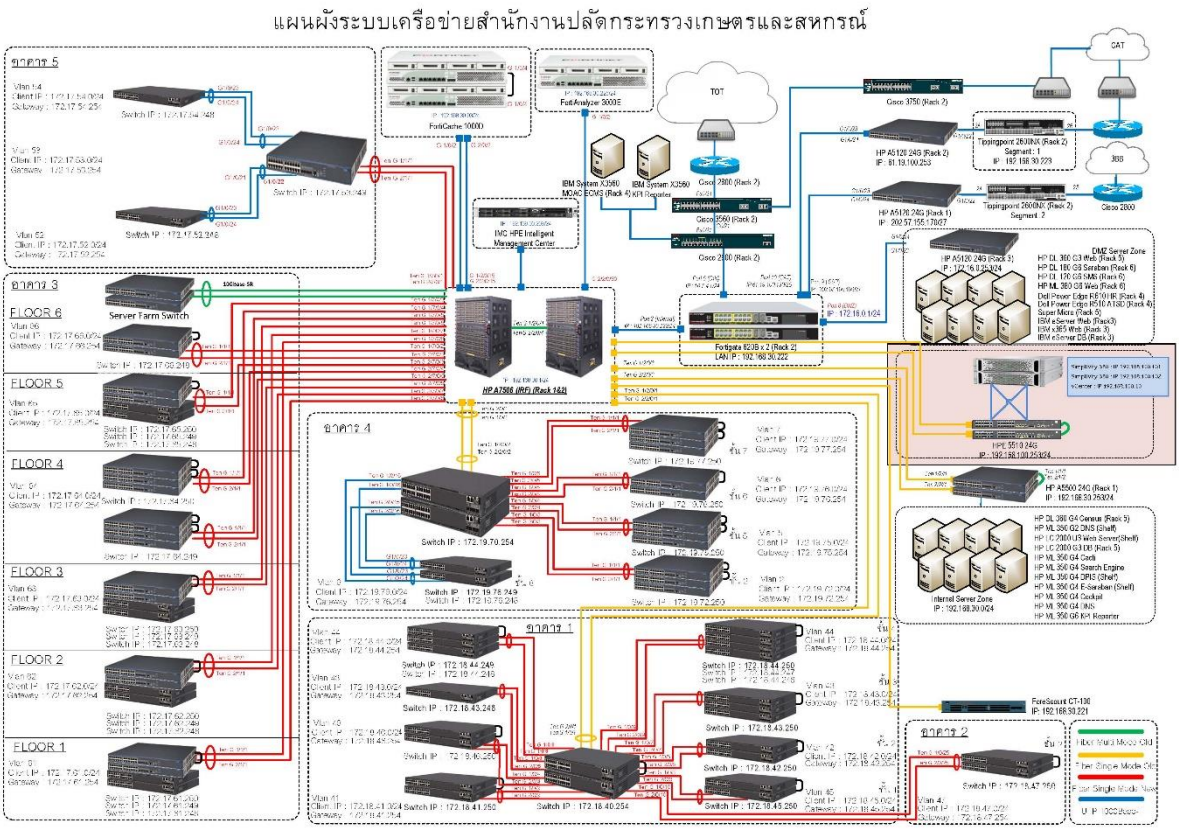
---

[๑] Government Information Network (Gin)

[๒] โซนเครื่องคอมพิวเตอร์แม่ข่าย (Demilitarized Zone)

๓ มีการแบ่งหมายเลข IP Address เป็นกลุ่มย่อย (Subnet Mask)

[๔] หมายเลขภายใน (Private IP Address)

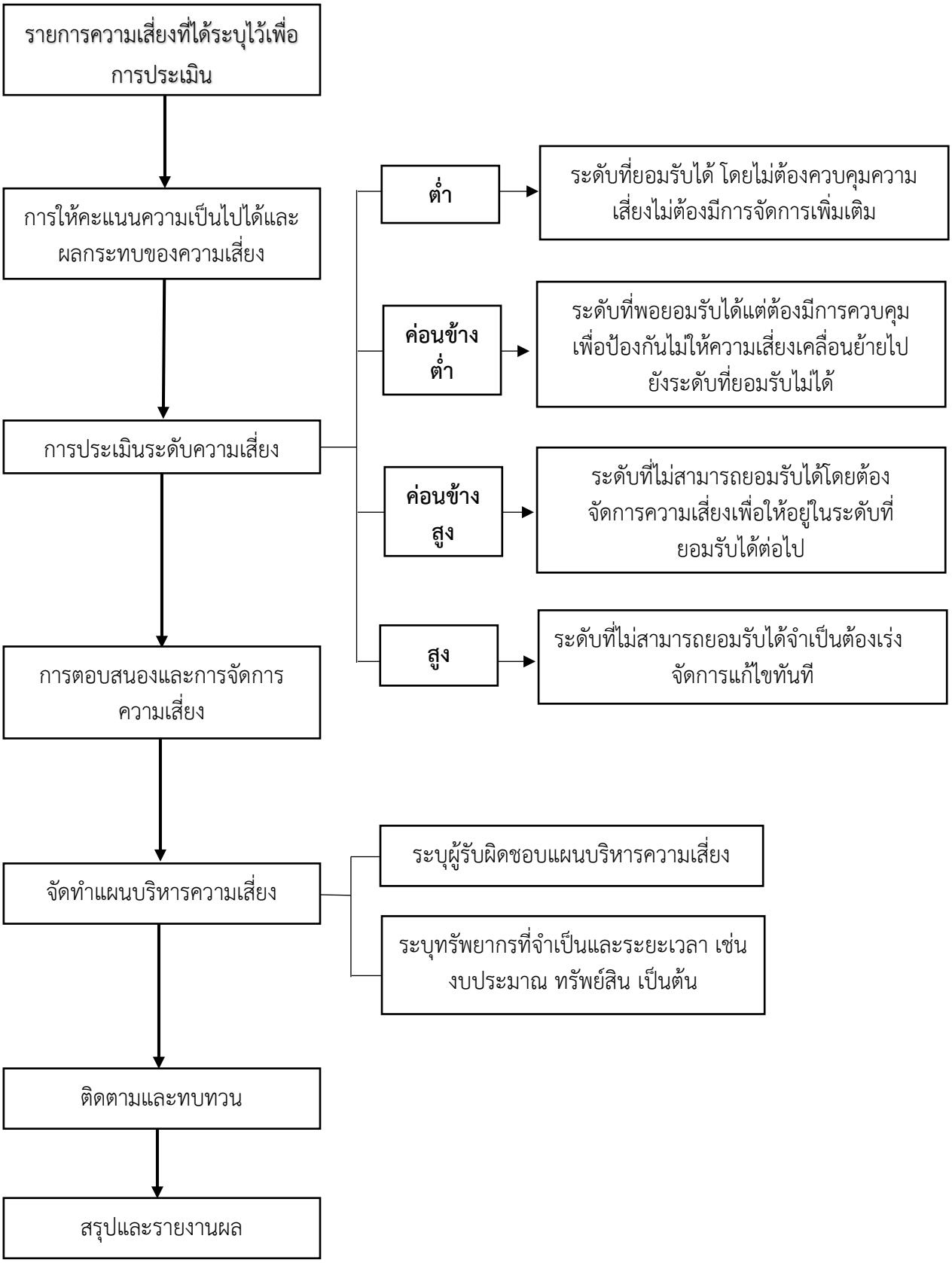


รูปที่ ๓ แสดงโครงข่ายคอมพิวเตอร์สารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

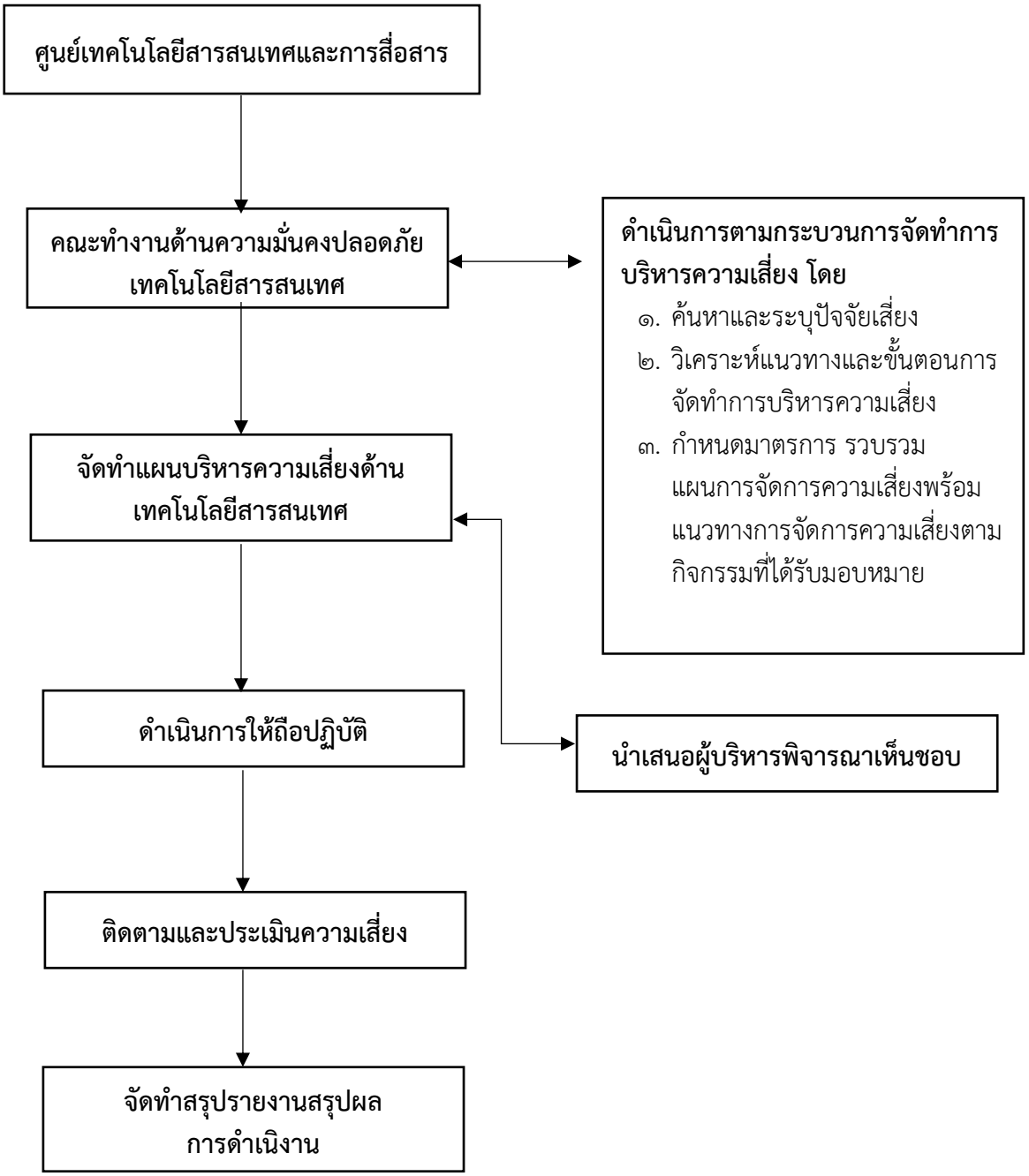
บทที่ ๒
การวิเคราะห์การบริหารจัดการความเสี่ยง

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ได้ตระหนักถึงความสำคัญของข้อมูลและการทำงานของระบบเครือข่ายที่สนับสนุนการปฏิบัติงานของหน่วยงานที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. ๒๕๕๙-๒๕๖๓ ให้สอดคล้องกับแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ สป.กษ. (IT๔) กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศและทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง

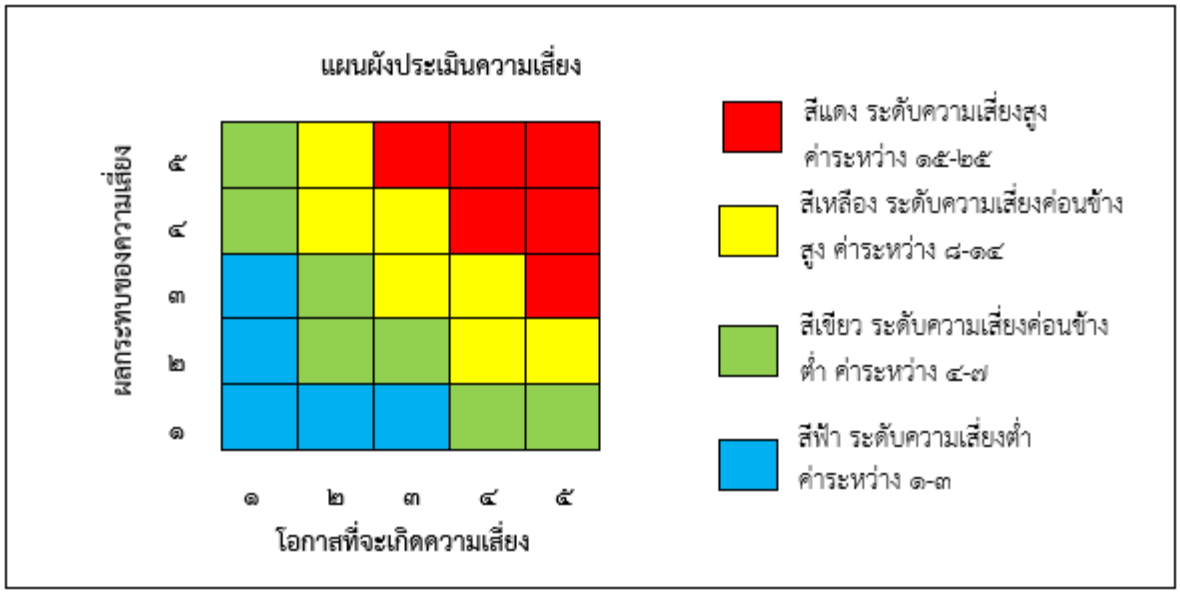


๒. กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



๓. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้



ตารางที่ ๑ ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑	ความชื้น อุณหภูมิห้องคอมพิวเตอร์แม่ข่ายกลาง	๔	๔	๑๖
๒	ระบบกระแสไฟฟ้าขัดข้อง	๔	๔	๑๖
๓	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย	๓	๕	๑๕
๔	การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	๔	๔	๑๖
๕	การนำอุปกรณ์เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่าย	๕	๓	๑๕
๖	ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	๔	๔	๑๖
๗	การบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์	๓	๔	๑๒
๘	การสูญหายของข้อมูล	๒	๕	๑๐
๙	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๒	๕	๑๐
๑๐	การเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	๑	๕	๕
๑๑	สถานการณ์ความสงบเรียบร้อยในบ้านเมือง	๑	๕	๕

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑๒	แมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/ สายสัญญาณ	๑	๔	๔
๑๓	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	๑	๕	๕
๑๔	การถูกโจมตีระบบจากเครือข่ายภายใน	๒	๓	๖
๑๕	ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	๒	๓	๖
๑๖	การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	๑	๔	๔

๔. ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ระดับความเสี่ยงสูง							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑. ความเสี่ยงจากความชื้น อุณหภูมิ ห้องคอมพิวเตอร์แม่ข่ายไม่มีระบบปรับอากาศที่ได้มาตรฐาน สามารถควบคุมอุณหภูมิความชื้นได้	ระบบปรับอากาศที่ไม่ได้มาตรฐานสำหรับห้องคอมพิวเตอร์แม่ข่าย	การทำงานของเครื่องอายุและอุปกรณ์สั้นลง	สูง ๔x๔=๑๖	๑. ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ ๒. วางแผนจัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	การยอมรับ (Take)	ศทส.
	๑. ความเสี่ยงไม่สามารถใช้งานเครื่องแม่ข่าย และระบบเครือข่ายได้กรณีเกิดไฟฟ้าขัดข้อง ๒. ความเสี่ยงต่อการCrash ของเครื่องแม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม	๑. ระบบกระแสไฟฟ้าขัดข้อง ๒. UPS มีอายุการใช้งานมาก ไม่มีระบบการสำรองไฟ/ไม่มีระบบการแจ้งเตือนที่รวดเร็ว	๑. ระบบไม่สามารถทำงานได้ ๒. ข้อมูล/อุปกรณ์เสียหาย ๓. ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายเสียหาย ต้องมีการติดตั้งใหม่	สูง ๔x๔=๑๖	๑. ตรวจสอบการทำงานระบบสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ ๒. วางแผนการจัดหาและติดตั้ง UPS และ เครื่องกำเนิดไฟฟ้า (Electrical Generator)	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๑. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	-การทำงานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ขัดข้อง	๑. ระบบงานไม่สามารถใช้ได้ตามปกติ ๒. ข้อมูลเสียหาย	สูง ๓x๕=๑๕	๑. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒. จัดหา Dr-Site ๓. จัดจ้างผู้ดูแลระบบ (Out Source)	การถ่ายโอน (Transfer)	ศทส.

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
	๒. ความเสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล						
ความเสี่ยงด้านบุคลากร (Human Risk)	๑. ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	-สิทธิ์ฐานข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศไม่เป็นปัจจุบัน เนื่องจากผู้ใช้งานมีการลาออก โอน ย้าย สิ้นสุดการจ้างตลอดเวลา	๑.หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน/ข้อมูล/อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย ๒.ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ	สูง ๔x๔=๑๖	หน่วยงานในสังกัด สป.กษ. ต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออก โอน ย้าย หรือสิ้นสุดการจ้างให้หน่วยงานทำหนังสือแจ้งให้กับ ศทส. /หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	การควบคุม (Treat)	หน่วยงานในสังกัด สป.กษ./หน่วยงาน หน่วยงานผู้ดูแล/เจ้าของระบบ/ศทส.
	๒. ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	อุปกรณ์ที่ใช้ไม่มีระบบรักษาความปลอดภัยที่ถูกต้องและเพียงพอ	๑. อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงานและอาจมีการโจมตีทำให้ระบบไม่สามารถทำงานได้	สูง ๕x๓=๑๕	๑.อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน ๒.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม (Treat)	ศทส./หน่วยงานในสังกัด สป.กษ./ผู้ใช้งาน
	๓. ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	๑.เจ้าหน้าที่หรือบุคลากรของ หน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้ง	๑. ระบบเสียหายหยุดชะงักการทำงาน ๒.สูญเสีย Bandwidth	สูง ๔x๔=๑๖	๑. อบรม สร้างความรู้ความเข้าใจการใช้งานที่ถูกวิธี ๒.กำหนด Policy ของอุปกรณ์รักษาความปลอดภัยของหน่วยงานให้มีความ	การควบคุม (Treat)	ศทส./

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
		ด้าน Hardware และ Software อย่างปลอดภัย ๒. การใช้ทรัพยากรของหน่วยงานทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	ในเครือข่ายทำให้ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี ๓. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก		ปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอ และการเปิด Port เท่าที่จำเป็น ๒.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด		
ความเสี่ยงค่อนข้างสูง							
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๑. ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker ไวรัส Malware ต่างๆเป็นต้น	การถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	๑. อาจทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ๒. ระบบ/ข้อมูลอาจจะถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพ บน Web Site ของสำนักงานฯ ๓. อาจถูกโจรกรรมข้อมูลที่เป็นความลับ	ค่อนข้างสูง ๓x๔=๑๒	๑. ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ ๒. ติดตั้งระบบป้องกัน และเตือนภัย Spam,Virus, Malware, Trojan ๓.ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ ๔. ติดตั้ง patch ของระบบปฏิบัติการสม่ำเสมอ ๕. จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ/เฝ้าระวัง	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	๑. ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล/ดำเนินการสำรองไม่ต่อเนื่อง	๑. ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน	ค่อนข้างสูง ๒x๕=๑๐	๑. หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ	การควบคุม (Treat)	ศทส./หน่วยงานเจ้าของระบบ

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
			๒. ระบบเสียหายไม่สามารถใช้งานและบริการข้อมูลได้		๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)		
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	๑. การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๑. หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	ค่อนข้างสูง ๒x๕=๑๐	๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒.สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ยอมรับ (Accept)	ศทส./หน่วยงานในสังกัด สป.กษ.
ความเสี่ยงต่ำ							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม จนไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลให้ระบบหลักไม่สามารถงานได้ คอมพิวเตอร์และเครือข่ายและข้อมูลสูญหาย	-ไฟไหม้ ไฟฟ้าลัดวงจร การวางเพลิง -ภัยธรรมชาติ	๑. เสียงบประมาณในการจัดหาระบบทดแทน ๒. ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทนได้	ต่ำ ๑x๕=๕	๑. จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Plan) ๒. วางแผนจัดหาและติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง ๓. จัดหา Dr-Site ๔. สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	การควบคุม (Treat)	ศทส.
	๒.ความเสี่ยงจากสถานการณ์ความสงบเรียบร้อยในบ้านเมือง	-การชุมนุมประท้วง -การจลาจล/ก่อการร้าย -การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	ต่ำ ๑x๕=๕	๑. จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Plan) ๒. จัดทำศูนย์สำรอง (Backup Site)	การควบคุม (Treat)	ศทส.

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
	๓. ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/ สายสัญญาณ	เสี่ยงต่อการอุปกรณ์/ระบบไม่สามารถใช้งานได้ปกติ	๑. เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน ๒. ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ต่ำ ๑x๔=๔	๑. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack ๒. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๑. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	๑. ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่ายอินทราเน็ตได้ ๒. ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	๑. เจ้าหน้าที่และผู้บริหารงานสำนักงานฯ ไม่สามารถใช้งานระบบอินเทอร์เน็ตสำหรับปฏิบัติงานได้ ๒. บุคคลภายนอกไม่สามารถเข้าใช้งานข้อมูลสารสนเทศของหน่วยงานผ่านเครือข่าย	ต่ำ ๑x๕=๕	๑.ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ใหบริการเครือข่ายอินเทอร์เน็ต ๒.ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	การควบคุม (Treat)	ศทส.
	๒. ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้หรือใช้ได้แต่ช้ามาก	ต่ำ ๒x๓=๖	๑. กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ๒. การควบคุมด้วยระบบ Desktop Management	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	๑. ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือ	๑. ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้	ต่ำ ๒x๓=๖	๑. มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk อุปกรณ์สำรองข้อมูลประเภทต่างๆ	การยอมรับ (Take)	ศทส. / หน่วยงานในสังกัด สป.กษ.

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
		อุปกรณ์สำรองข้อมูลประเภทต่างๆ	เสียหายต่อความเชื่อถือของ สป.กษ. ๒. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้		ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้ ๒.ก่อนจำหน่าย		
	๒. ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	๑. เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง ๒. เสียเวลาในการกู้ระบบ ๓. เสียภาพลักษณ์ของสำนักงานฯ	ต่ำ ๑x๔=๔	๑. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย ๒. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน ๓. ควบคุมการเข้าออกและขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคารตลอดเวลา ๓. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	การควบคุม (Treat)	ศทส./หน่วยงานในสังกัด สป.กษ.

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์
กระทรวงเกษตรและสหกรณ์

ผู้รับผิดชอบหลัก
หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ระยะเวลา ตุลาคม ๒๕๖๐ - ตุลาคม ๒๕๖๔

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๑			๒๕๖๒			๒๕๖๓			๒๕๖๔			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	
๑. ความเสี่ยงจากความชื้น อุณหภูมิ ห้องคอมพิวเตอร์แม่ข่ายกลางไม่มีระบบปรับอากาศที่ได้มาตรฐาน สามารถควบคุมอุณหภูมิความชื้นได้	๑. ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ ๒. วางแผนจัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	- ทุกวัน ปีงบประมาณ ๒๕๖๓	←	—	→				←	→					ศทส.
๒.ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้อง	๑. ตรวจสอบการทำงานระบบสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ ๒. วางแผนการจัดหาและติดตั้ง UPS และเครื่องกำเนิดไฟฟ้า (Electrical Generator)	- ทุกวัน ปีงบประมาณ ๒๕๖๒	←	—	→	←	→							→	ศทส.

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๑			๒๕๖๒			๒๕๖๓			๒๕๖๔			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	
๓. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย	๑. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒. จัดหา Dr-Site ๓. จัดจ้างผู้ดูแลระบบ (Out Source)	- ทุกวัน ปีงบประมาณ ๒๕๖๓													ศทส.
๔.ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	หน่วยงานในสังกัด สป.กษ. ต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออก โอน ย้าย หรือสิ้นสุดการจ้างให้หน่วยงานทำหนังสือแจ้งให้กับ ศทส. /หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	ทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งาน												หน่วยงานในสังกัด สป.กษ./หน่วยงานผู้ดูแลระบบ/ศทส.
๕. ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart Phone,Tablet,PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	๑.อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน ๒.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	๑ ครั้ง/ปี													ศทส./หน่วยงานในสังกัด สป.กษ./ผู้ใช้งาน

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๑			๒๕๖๒			๒๕๖๓			๒๕๖๔			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	
๖.ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	๑. อบรม สร้างความรู้ความเข้าใจการใช้งานที่ถูกวิธี ๒.กำหนด Policy ของอุปกรณ์รักษาความปลอดภัยของหน่วยงานให้มีความปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอ และการเปิด Port เท่าที่จำเป็น ๓.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	๑ ครั้ง/ปี ๑ ครั้ง/เดือน			→			→			→			→	ศทส./หน่วยงานในสังกัด สป.กษ./ผู้ใช้งาน
๗. 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	๒ ครั้ง/ปี ความเหมาะสม ๑ ครั้ง/ปี	→	→	→	→	→	→	→	→	→	→	→	→	ศทส.
๘.ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	๑. หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	ทุกวัน/ตามความเหมาะสม ๑ ครั้ง/ปี	→	→	→	→	→	→	→	→	→	→	→	→	ศทส./หน่วยงานเจ้าของระบบ

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๑			๒๕๖๒			๒๕๖๓			๒๕๖๔			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	
๙.การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒.สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	๑ ครั้ง/ปี	←											→	ศทส./หน่วยงานในสังกัด สป.กษ.

บทที่ ๓
สรุปและข้อเสนอแนะ

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

๑. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีระดับสูง ได้ข้อสรุป ดังนี้

๑. ความเสี่ยงจากความชื้น อุณหภูมิ มีแนวทางปฏิบัติดังนี้

๑.๑ ตรวจสอบการทำงาน/อุณหภูมิ เครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ

๑.๒ วางแผนจัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้

๒. ความเสี่ยงระบบกระแสไฟฟ้าขัดข้อง มีแนวทางปฏิบัติดังนี้

๒.๑ ตรวจสอบการทำงานระบบสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ

๒.๒ วางแผนการจัดหาและติดตั้งระบบสำรองไฟฟ้าและเครื่องกำเนิดไฟฟ้า (Electrical Generator)

๓. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย มีแนวทางปฏิบัติดังนี้

๓.๑ ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล

๓.๒ จัดหา Dr-Site

๓.๓ จัดจ้างผู้ดูแลระบบ (Out Source)

๔. ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย มีแนวทางปฏิบัติดังนี้

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

๕. ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart Phone ,Tablet ,PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงาน มีแนวทางปฏิบัติดังนี้

๕.๑ อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน

๕.๒ กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

๖. ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย มีแนวทางปฏิบัติดังนี้

๖.๑ อบรม สร้างความรู้ความเข้าใจการใช้งานที่ถูกวิธี

๖.๒ กำหนด Policy ของอุปกรณ์รักษาความปลอดภัยของหน่วยงานให้มีความปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอ และการเปิด Port เท่าที่จำเป็น

๖.๓ กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

๗. ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ มีแนวทางปฏิบัติดังนี้

๗.๑ ติดตั้งโปรแกรมป้องกันไวรัส Malware, Trojan, และ update อย่างสม่ำเสมอ

๗.๒ ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ

๗.๓ อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของหน่วยงาน

๘. ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง มีแนวทางปฏิบัติดังนี้

๘.๑ หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ

๘.๒ มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)

๙. การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย มีแนวทางปฏิบัติดังนี้

๙.๑ การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น

๙.๒ สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย

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

๓.๓.๑ พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

๓.๓.๒ พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

๓.๓.๓ กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

๓.๒ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ