แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมฝนหลวงและการบินเกษตร ปี พ.ศ. ๒๕๖๕

Information Technology Risk Management Plan

กรมฝนหลวงและการบินเกษตร

Department of Royal Rainmaking and Agricultural Aviation

คำนำ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของกรมฝนหลวงและการบินเกษตร ปีงบประมาณ พ.ศ. ๒๕๖๕ ถึง พ.ศ.๒๕๖๙ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทาง หรือมาตรการควบคุมเพื่อป้องกัน หรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น ศูนย์เทคโนโลยีสารสนเทศ หวังเป็นอย่างยิ่งว่า แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ กรมฝนหลวงและการบินเกษตร ฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของ กรมฝนหลวงและการบินเกษตร ต่อไป

ศูนย์เทคโนโลยีสารสนเทศ
กองวิจัยและพัฒนาเทคโนโลยีฝนหลวง
กรมฝนหลวงและการบินเกษตร
ธันวาคม ๒๕๖๔

สารบัญ

บทที่ ๑
บทนำ

๑. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดีโดยจะช่วยให้การบริหารงานและการตัดสินใจในการวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่กรมฝนหลวงและการบินเกษตร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในกรมฝนหลวงและการบินเกษตร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศภายใต้สภาวะการดำเนินงานของทุกหน่วยงานล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายของกรมฝนหลวงและการบินเกษตร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายของกรมฝนหลวงและการบินเกษตร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยงโดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๑. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของ กรมฝนหลวงและการบินเกษตร

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอน

๓. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลและระบบสารสนเทศหลัก เช่น เว็บไซต์กรมฝนหลวงและการบินเกษตร ระบบปฏิบัติการฝนหลวง ระบบบริหารจัดการสนับสนุนด้านการบินเกษตร ระบบสารสนเทศภูมิศาสตร์แม่ข่ายเชิงพื้นที่ (Geo-map) เป็นต้น

ระบบฐานข้อมูลและระบบสารสนเทศสนับสนุนการบริหารงานภายใน (Back Office) ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban) ระบบสารสนเทศทรัพยากรบุคคล (DPIS) ระบบสารสนเทศงานงบประมาณ พัสดุ การเงิน และบุคลากร เป็นต้น

ระบบบริหารจัดการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) โปรแกรมระบบตรวจสอบและเฝ้าระวังเครือข่าย (Network Monitoring) โปรแกรมป้องกันการบุกรุกเครือข่าย (IPS) เป็นต้น

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ (PC)

เครื่องคอมพิวเตอร์ชนิดพกพา (NB) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switch) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Access Point) เป็นต้น

๔. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง การกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้

รูปที่ ๑ แสดงกระบวนการบริหารความเสี่ยง

๔.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๑) การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๒) การใช้ Checklist

๓) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

๔) การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

๕) การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๔.๒ การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๔.๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน

เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้ง เกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก)

๔.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

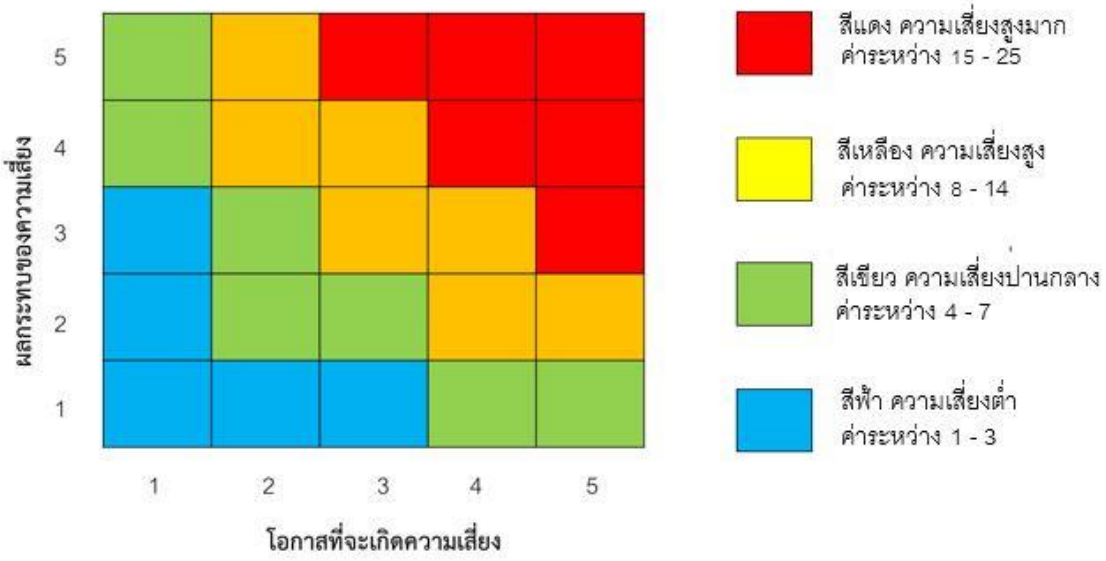
เกณฑ์การประเมิน เป็นการกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งใช้เกณฑ์ดังนี้

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

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**ระดับผลกระทบ**	**คำอธิบาย**
๕	สูงมาก	เกิดความสูญเสียต่อระบบสารสนเทศที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	เกิดความสูญเสียต่อระบบสารสนเทศที่สำคัญทั้งหมด และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

๔.๒.๓ การวิเคราะห์ความเสี่ยง

เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อกรมฝนหลวงและการบินเกษตร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปที่ ๒



รูปที่ ๒ แสดงแผนผังประเมินความเสี่ยง

๔.๒.๔ การจัดลำดับความเสี่ยง

เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อกรมฝนหลวงและการบินเกษตรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๔.๓ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

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

๔.๓.๑ ควบคุมเพื่อการป้องกัน (Preventive Control)

เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติการจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๔.๓.๒ การควบคุมเพื่อให้ตรวจพบ (Detective Control)

เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๔.๓.๓ การควบคุมโดยการชี้แนะ (Direction Control)

เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๔.๓.๔ การควบคุมเพื่อการแก้ไข (Corrective Control)

เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูงมาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

๒) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๔.๔ การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

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

๔.๔.๑ พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔.๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๔.๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔.๔.๔ ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๔.๕ การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๕. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กรมฝนหลวงและการบินเกษตรได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๕ ประเภท ดังนี้

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดขึ้นและส่งผลกระทบโดยตรงต่อระบบคอมพิวเตอร์ และห้องคอมพิวเตอร์ศูนย์แม่ข่ายกลาง เช่น ไฟไหม้ กระแสไฟฟ้าขัดข้อง รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)

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

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งกรมฝนหลวงและการบินเกษตร อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ อันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่กรมฝนหลวงและการบินเกษตร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูลดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัย

ของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศ

๖. การตอบสนองความเสี่ยง

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

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้นโดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่กรมฝนหลวงและการบินเกษตร ยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดหากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงานองค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๗. ปัจจัยเสี่ยง

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) แบ่งออกเป็น

๑.๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๓) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)

๑.๔) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า

๑.๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง

๒) ความเสี่ยงด้านบุคลากร (Human Risk) แบ่งออกเป็น

๒.๑) ความเสี่ยงจากผู้ดูแลระบบ

๒.๒) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย

๓) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk) แบ่งออกเป็น

๓.๑) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย

๓.๒) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์

๓.๓) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร

๓.๔) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน

๓.๕) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)

๓.๖) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)

๓.๗) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) แบ่งออกเป็น

๔.๑) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

๔.๒) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

๔.๓) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)

๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk) แบ่งออกเป็น

๕.๑) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน

๕.๒) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล

๕.๓) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

๘. การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๒. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบเทคโนโลยีสารสนเทศและฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๙. ระบบรักษาความปลอดภัยบนเครือข่าย

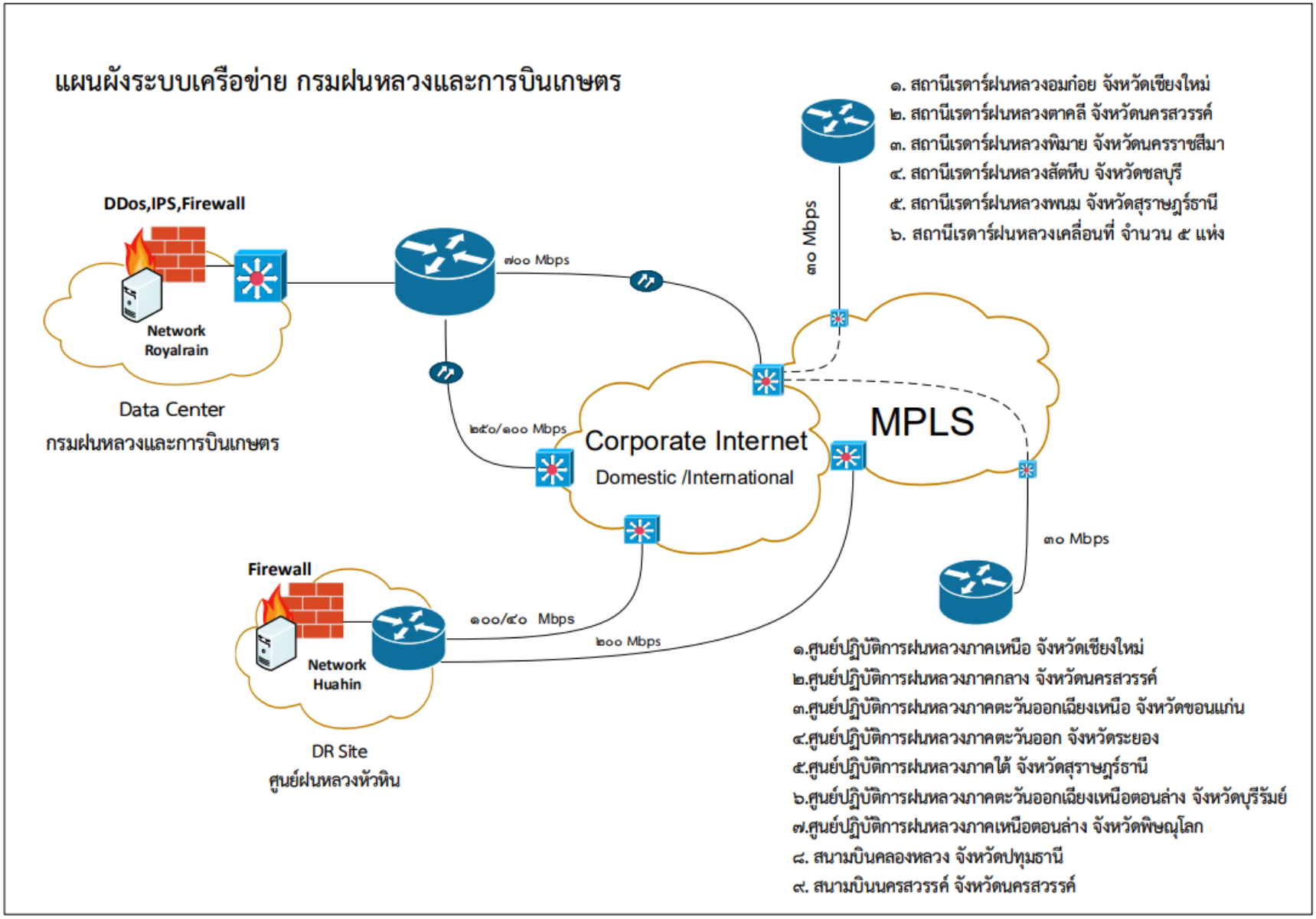
ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) ของกรมฝนหลวงและการบินเกษตรได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่าย กรมฝนหลวงและการบินเกษตร เป็นไปอย่างรวดเร็วและมีประสิทธิภาพตั้งอยู่ที่ภายในมหาวิทยาลัยเกษตรศาสตร์ เลขที่ ๕๐ ถนนพหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพฯ และศูนย์ฝนหลวงหัวหิน ตำบลหัวหิน อำเภอหัวหิน จังหวัดประจวบคีรีขันธ์

๑๐. ระบบคอมพิวเตอร์และเครือข่าย ของกรมฝนหลวงและการบินเกษตร

ระบบคอมพิวเตอร์และเครือข่าย ของกรมฝนหลวงและการบินเกษตรมีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์ และซอฟต์แวร์ทำงานร่วมกัน เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ของ FortiGate ๑๒๐๐D ซึ่งใช้ในการกรอง (Filter Package) ที่ผ่านเข้ามาภายในระบบ ของ กรมฝนหลวงและการบินเกษตรจากเครือข่ายภายนอก เช่น เครือข่ายอินเทอร์เน็ต เครือข่าย GIN นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของ DMZ ที่ดูแลเครื่องแม่ข่ายทั้งหมดของกรมฝนหลวงและการบินเกษตร รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของกรมฝนหลวงและการบินเกษตร มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของกรมฝนหลวงและการบินเกษตรในส่วนกลาง มีการแบ่ง Subnet เพื่อให้เป็นระบบกลุ่มบรอดคาสต์โดเมน (Broadcast Domain) เดียวกัน ประกอบกับกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความปลอดภัย สะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

ระบบเครือข่ายหลักของกรมฝนหลวงและการบินเกษตร (Core Network) ตั้งอยู่ที่ศูนย์เทคโนโลยีสารสนเทศ กองวิจัยและพัฒนาเทคโนโลยีฝนหลวง เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่าย ในความเร็วระดับ ๑,๐๐๐ Mbps และระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ต และ GIN เข้าด้วยกันซึ่งมี Core Switch ที่ออกแบบติดตั้งในลักษณะระบบเครือข่ายที่สามารถทดแทนกันได้ (Redundant Network) เพื่อแก้ปัญหาระบบเครือข่ายศูนย์กลางล่ม (Single Point of Failure) และแก้ปัญหาคอขวดในการเข้าถึงข้อมูล (Bottleneck) เพื่อรองรับภารกิจของกรมฝนหลวงและการบินเกษตร ซึ่งลักษณะงานต้องใช้อุปกรณ์เครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพสูงสามารถรองรับการเชื่อมต่อกับระบบเครือข่ายภายในและภายนอกแบบ ๒๔x๗ เพื่อใช้ระบบงานฐานข้อมูลที่สำคัญของกรมฝนหลวงและการบินเกษตร พร้อมทั้งเชื่อมโยงไปยังอุปกรณ์ Distributed Switch (L๓) และ Access Switch(L๒) ภายในอาคาร ซึ่งเป็นที่ตั้งของหน่วยงานในกรมฝนหลวงและการบินเกษตร

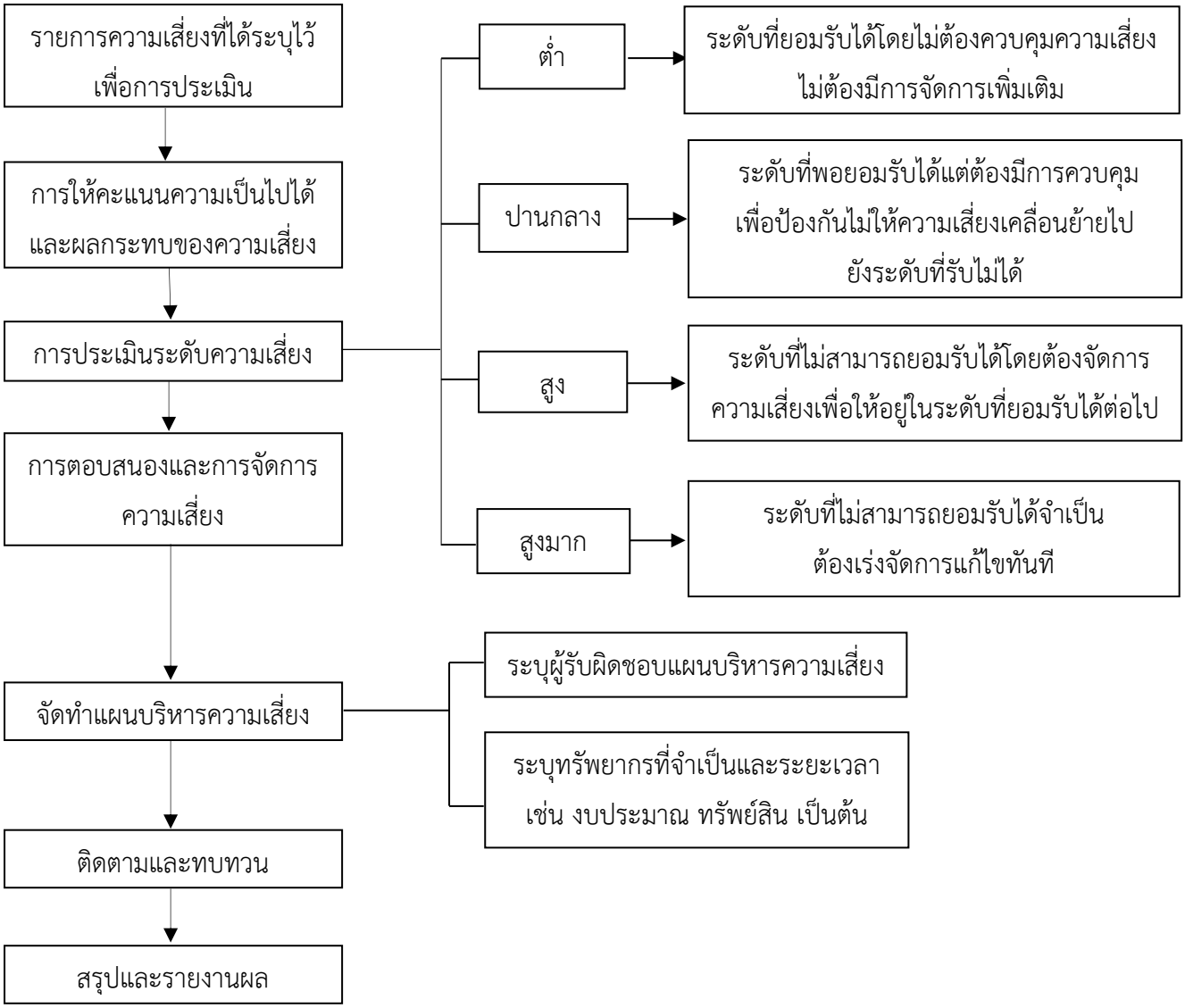
๑๑. แผนผังระบบและเครือข่าย ของกรมฝนหลวงและการบินเกษตร



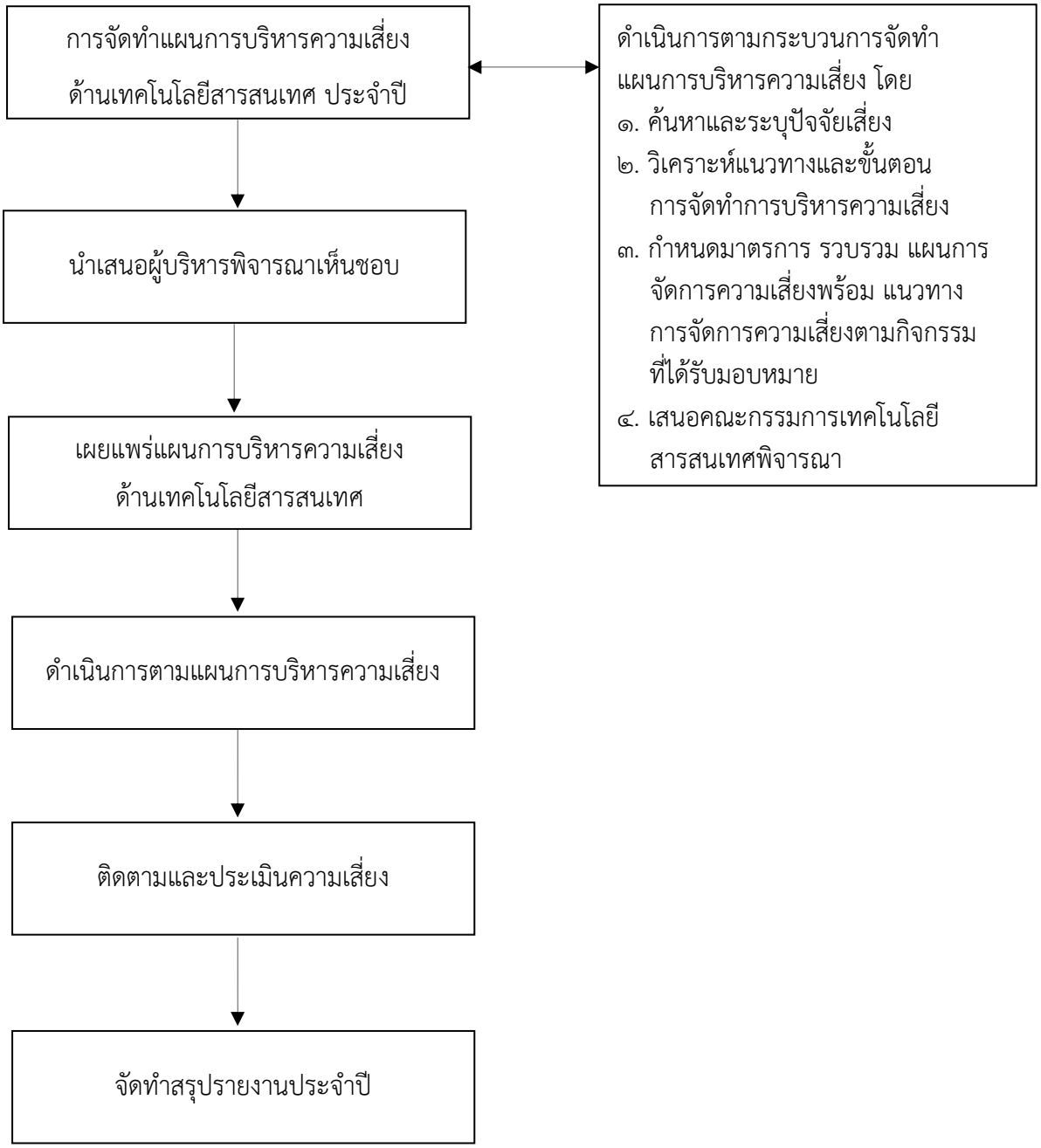
บทที่ ๒
การวิเคราะห์และการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กรมฝนหลวงและการบินเกษตร ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงแต่ละด้าน จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕ โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม การวิเคราะห์ปัจจัยเสี่ยง และกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังต่อไปนี้

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๒. กระบวนการจัดทำแผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



๓. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

จากการวิเคราะห์ความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศของกรมฝนหลวงและการบินเกษตร สามารถสรุปความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization) จำแนกได้ ๕ ด้าน ดังนี้

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) แบ่งออกเป็น

๑.๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๓) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)

๑.๔) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า

๑.๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง

๒) ความเสี่ยงด้านบุคลากร (Human Risk) แบ่งออกเป็น

๒.๑) ความเสี่ยงจากผู้ดูแลระบบ

๒.๒) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย

๓) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk) แบ่งออกเป็น

๓.๑) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย

๓.๒) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์

๓.๓) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร

๓.๔) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน

๓.๕) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)

๓.๖) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)

๓.๗) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) แบ่งออกเป็น

๔.๑) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

๔.๒) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

๔.๓) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)

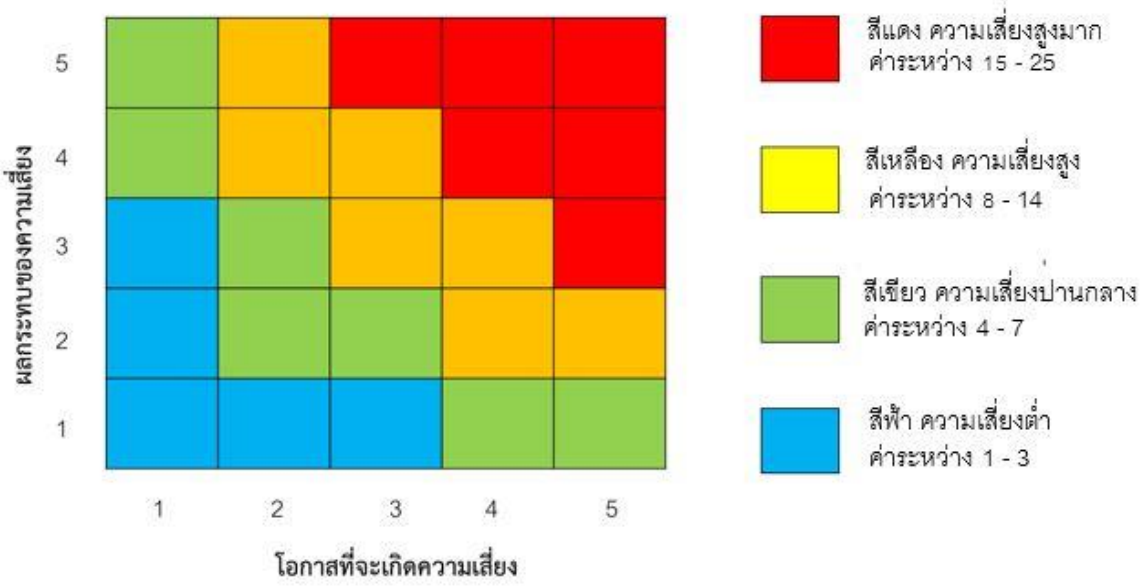
๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk) แบ่งออกเป็น

๕.๑) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน

๕.๒) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล

๕.๓) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่กรมฝนหลวงและการบินเกษตรเผชิญอยู่ ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้



ตารางแสดงประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศตามค่าคะแนนความเสี่ยง

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ
๑.	**ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม**				
๑.๑	ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑	๕	๕	ปานกลาง
๑.๒	ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๓	๔	๔	ปานกลาง
๑.๓	ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	๓	๔	๑๒	สูง
๑.๔	ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า	๑	๓	๓	ต่ำ
๑.๕	ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์ เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง	๑	๓	๓	ต่ำ
๒.	**ความเสี่ยงด้านบุคลากร**				
๒.๑	ความเสี่ยงจากผู้ดูแลระบบ	๑	๓	๓	ต่ำ
๒.๒	ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย	๓	๓	๙	สูง

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ
๓.	**ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย**				
๓.๑	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๕	๔	๒๐	สูงมาก
๓.๒	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	๓	๒	๖	ปานกลาง
๓.๓	ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	๓	๔	๑๒	สูง
๓.๔	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน	๑	๓	๓	ต่ำ
๓.๕	ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)	๑	๓	๓	ต่ำ
๓.๖	ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	๑	๓	๓	ต่ำ
๓.๗	ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)	๑	๓	๓	ต่ำ
๔.	**ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์**				
๔.๑	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑	๓	๓	ต่ำ
๔.๒	ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑	๓	๓	ต่ำ
๔.๓	ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	๓	๔	๑๒	สูง
๕.	**ความเสี่ยงด้านระบบฐานข้อมูล**				
๕.๑	ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	๑	๓	๓	ต่ำ
๕.๒	ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล	๑	๓	๓	ต่ำ
๕.๓	ความเสี่ยงจากการโจรกรรมระบบฐานข้อมูล	๑	๓	๓	ต่ำ

จากการวิเคราะห์ความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศของกรมฝนหลวงและการบินเกษตร สามารถสรุปความเสี่ยงออกเป็น ๔ ระดับ เรียงตามลำดับค่าความเสี่ยง ดังนี้

๑) ความเสี่ยงระดับสูงมาก แบ่งออกเป็น

๑.๑) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย

๒) ความเสี่ยงระดับสูง แบ่งออกเป็น

๒.๑) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)

๒.๒) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย

๒.๓) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร

๒.๔) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)

๓) ความเสี่ยงระดับปานกลาง แบ่งออกเป็น

๓.๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๓.๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๓.๓) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์

๔) ความเสี่ยงระดับต่ำ แบ่งออกเป็น

๔.๑) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า

๔.๒) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง

๔.๓) ความเสี่ยงจากผู้ดูแลระบบ

๔.๔) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน

๔.๕) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)

๔.๖) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)

๔.๗) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)

๔.๘) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

๔.๙) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

๔.๑๐) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน

๔.๑๑) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล

๔.๑๒) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

๔. ผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและแนวทางการควบคุมที่มีอยู่

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑. ระบบคอมพิวเตอร์และระบบเครือข่ายถูกทำลาย ๒. ระบบสารสนเทศและระบบฐานข้อมูลถูกทำลาย	๑	๕	๕	๑. ตรวจสอบระบบดับเพลิงแบบอัตโนมัติตามมาตรฐานเดือนละ ๑ ครั้ง ๒. ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก ๓ เดือน	การควบคุม (Treat)	ศทส.
๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑. ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้ ๒. ไม่สามารถระบบสารสนเทศและระบบฐานข้อมูลได้ ๓. ระบบปฏิบัติการ และระบฐานข้อมูลเกิดความเสียหายจากเครื่องไม่ได้ถูกทำการปิดอย่างเหมาะสม	๑	๔	๔	๑. ตรวจสอบระบบสำรองไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่ายกลาง สัปดาห์ละ ๑ ครั้ง ๒. ตรวจสอบเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน (Electrical Generator) สัปดาห์ละ ๑ ครั้ง	การถ่ายโอน (Transfer)	ศทส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	เกิดความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย	๓	๔	๑๒	ตรวจสอบเครื่องปรับอากาศที่ควบคุมอุณหภูมิ และความชื้น วันละ ๑ ครั้ง	การถ่ายโอน (Transfer)	ศทส.
๔) ความเสี่ยงจากแมลง สัตว์กัดแทะอุปกรณ์เครือข่ายและระบบไฟฟ้า	๑. ไม่สามารถใช้งานระบบเครือข่ายได้ ๒. ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง	๑	๓	๓	ตรวจสอบอุปกรณ์เครือข่ายและระบบไฟฟ้า เดือนละ ๑ ครั้ง	การยอมรับ (Take)	ศทส.
๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง	๑. อุปกรณ์ และข้อมูลที่มีความสำคัญสูญหาย ๒. เสียภาพลักษณ์ของหน่วยงาน	๑	๓	๓	๑. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า - ออกห้องคอมพิวเตอร์แม่ข่าย ๒. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้ง ๓. ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก ๓ เดือน	การยอมรับ (Take)	ศทส. ฝ่ายอาคารสถานที่และยานพาหนะ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๒. ความเสี่ยงด้านบุคลากร (Human Risk)							
๖) ความเสี่ยงจากผู้ดูแลระบบ	ข้อมูลที่อยู่ในชั้นความลับ รั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือของหน่วยงาน	๑	๓	๓	๑. การทำ Authentication การเข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ) ๒. การจัดระดับการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล	การยอมรับ (Take)	ศทส.
๗) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย	๑. สูญเสีย Bandwidth ในระบบเครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้น เนื่องจากการใช้งานนอกเหนือจากงานราชการ ๒. เครื่องคอมพิวเตอร์ เสียหายและเสื่อมอายุการใช้งานเร็วกว่าปกติ	๓	๓	๙	๑. กำหนด Policy ของ Firewall ให้เหมาะสมต่อการใช้งาน ๒. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่างๆ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งาน และรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา ๓. ตรวจสอบและแนะนำผู้ใช้งานให้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง อย่างเหมาะสม	การควบคุม (Treat)	ศทส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
๘) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๑. เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล ๒. ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	๕	๔	๒๐	๑. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลัก ทุกวัน ๒. สำรองระบบและข้อมูล (Backup) ทุกวัน ๓. ทดสอบการกู้คืนระบบแม่ข่ายหลัก เดือนละ ๑ ครั้ง	การควบคุม (Treat)	ศทส.
๙) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	๑. โปรแกรมหรือข้อมูลถูกทำลาย ๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ ๓. การถูกขโมยข้อมูลที่สำคัญ	๓	๒	๖	๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ ๒. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งคัด	การควบคุม (Treat)	ศทส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๐) ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	๑.ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้ ๒. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ๓. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของหน่วยงาน ๔. ถูกโจรกรรมข้อมูลที่เป็นความลับ ๕. ไม่สามารถเข้าใช้ระบบสารสนเทศได้	๓	๔	๑๒	๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ ๒. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่าย ทุกวัน ๓. มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่างๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายอินทราเน็ต ของกรมฝนหลวงและการบินเกษตร	การควบคุม (Treat)	ศทส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๑) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ต ภายในและภายนอกสถานที่ทำงาน	๑. ระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตไม่สามารถใช้งานได้ ๒. ไม่สามารถเข้าใช้งานระบบสารสนเทศ ผ่านเครือข่ายอินทราเน็ตและอินเทอร์เน็ตได้	๑	๓	๓	๑. ตรวจสอบระบบเครือข่ายสื่อสารหลักทุกวัน ๒. ควบคุมการเข้าใช้เครือข่ายอินทราเน็ต และอินเทอร์เน็ต โดยใช้ระบบยืนยันตน (Authentication)	การยอมรับ (Take)	ศทส.
๑๒) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)	๑. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ ๒. ลดความน่าเชื่อถือของหน่วยงาน	๑	๓	๓	๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ ๒. ปรับปรุง Firewall และการ Monitoring ระบบเครือข่าย เป็นประจำทุกปี	การยอมรับ (Take)	ศทส.
๑๓) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องไม่สามารถเข้าร่วมประชุมได้	๑	๓	๓	ตรวจสอบการเชื่อมต่ออุปกรณ์ การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนใช้งาน	การยอมรับ (Take)	ศทส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๔) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)	๑. ระบบโทรศัพท์ (IP Phone) ขัดข้อง ทำให้เจ้าหน้าที่ในหน่วยงานไม่สามรถใช้งานระบบโทรศัพท์ติดต่อประสานงานทั้งภายใน/ภายนอก ได้อย่างต่อเนื่อง	๑	๓	๓	ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) อย่างสม่ำเสมอ	การยอมรับ (Take)	ศทส.
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
๑๕) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑. การถูกฟ้องร้อง และเสื่อมเสียชื่อเสียง และ ความน่าเชื่อถือของหน่วยงาน ๒. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ ๓. หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	๑	๓	๓	๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งาน Open Source	การยอมรับ (Take)	ศทส.
๑๖) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศและระบบฐานข้อมูล ๒. ลดความน่าเชื่อถือต่อหน่วยงาน	๑	๓	๓	๑. อัพเดทเครื่องมือและโปรแกรมที่ใช้พัฒนาอย่างสม่ำเสมอ ๒. ตรวจสอบช่องโหว่ และดำเนินการแก้ไขทุก ๓ เดือน	การยอมรับ (Take)	ศทส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๗) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	๑. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ผิดพลาดได้อย่างทันท่วงที ๒. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว เนื่องจากโปรแกรมหมดลิขสิทธิ์ และขาดการปรับปรุง (Update) โปรแกรม	๓	๔	๑๒	๑. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการออกแบบการพัฒนาระบบ และชุดคำสั่ง (Source Code) ฉบับสมสมบูรณ์ ทั้งในกรณีพัฒนาเสร็จสิ้น และเมื่อมีการปรับปรุงแก้ไข ๒. มีกระบวนการทบทวนชุดคำสั่ง (Code Review) เพิ่มเติม ในกระบวนการส่งมอบงาน ๓. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ ๔. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลให้มีความทันสมัย และใช้งานได้อย่างต่อเนื่อง	การควบคุม (Treat)	ศทส. หรือกลุ่ม/กองที่มีการจัดจ้างผู้รับจ้างภายนอก

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๕. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)							
๑๘) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	๑. ระบบฐานข้อมูลไม่สามารถนำไปใช้สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ ๒. ลดความน่าเชื่อถือของหน่วยงาน	๑	๓	๓	๑. จัดทำรายการข้อมูลและความถี่ในการปรับปรุง ๒. กำหนดมาตราการแนวทางการปรับปรุง และช่องทางการเข้าถึงข้อมูลเพื่อให้ผู้ดูแลข้อมูลถือปฏิบัติ	การยอมรับ (Take)	ศทส.
๑๙) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล	๑.เกิดการสูญหายของข้อมูล และกระทบต่อการทำงานตามปกติ ๒.ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้สนับสนุนการปฏิบัติงานได้	๑	๓	๓	๑. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุกสัปดาห์	การยอมรับ (Take)	ศทส.
๒๐) ความเสี่ยงจากการโจรกรรมระบบฐานข้อมูล	๑.ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ ๒. ข้อมูลที่สำคัญสูญหายและถูกทำลาย	๑	๓	๓	๑. ตรวจสอบระบบป้องกันการบุกรุกและระบบตรวจสอบและเฝ้าระวังเครือข่าย เป็นประจำทุกวัน ๒. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกและระบบเฝ้าระวังเครือข่าย เป็นประจำทุกวัน	การยอมรับ (Take)	ศทส.

แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. ๒๕๖๕

กรมฝนหลวงและการบินเกษตร
กระทรวงเกษตรและสหกรณ์

ผู้รับผิดชอบหลัก
หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศ
ระยะเวลาการดำเนินการ ตุลาคม ๒๕๕๔ – กันยายน ๒๕๖๕

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมฝนหลวงและการบินเกษตรบรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง	แผนปฏิบัติ	ระยะเวลา	เดือน											
			ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	ตรวจสอบระบบดับเพลิงแบบอัตโนมัติตามมาตรฐาน	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
	ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site)	ทุก ๓ เดือน	/			/			/			/		
๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	ตรวจสอบระบบสำรองไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่ายกลาง	สัปดาห์ละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
	ตรวจสอบเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน (Electrical Generator)	สัปดาห์ละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/

ประเภทความเสี่ยง	แผนปฏิบัติ	ระยะเวลา	เดือน											
			ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
๓) ความเสี่ยงจากอุณหภูมิและความชื้นของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	ตรวจสอบเครื่องปรับอากาศที่ควบคุมอุณหภูมิและความชื้น	ทุกวัน	/	/	/	/	/	/	/	/	/	/	/	/
๔) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย	กำหนด Policy ของ Firewall ให้เหมาะสมต่อการใช้งาน	ทุก ๓ เดือน	/			/			/			/		
	บันทึกการใช้งาน และรายงานการใช้งานของผู้ใช้ในทางที่ผิดต่อผู้บังคับบัญชา	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
	ตรวจสอบและแนะนำผู้ใช้งานให้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างเหมาะสม	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/

ประเภทความเสี่ยง	แผนปฏิบัติ	ระยะเวลา	เดือน											
			ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
๕) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลัก	ทุกวัน	/	/	/	/	/	/	/	/	/	/	/	/
	สำรองระบบและข้อมูล (Backup)	ทุกวัน	/	/	/	/	/	/	/	/	/	/	/	/
	ทดสอบการกู้คืนระบบแม่ข่ายหลัก	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
๖) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
	ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งคัด	ทุกวัน	/	/	/	/	/	/	/	/	/	/	/	/
๗) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่าย	ทุกวัน	/	/	/	/	/	/	/	/	/	/	/	/

ประเภทความเสี่ยง	แผนปฏิบัติ	ระยะเวลา	เดือน											
			ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
๘) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการออกแบบการพัฒนาระบบ และชุดคำสั่ง (Source Code) ฉบับสมสมบูรณ์ ทั้งในกรณีพัฒนาเสร็จสิ้นและเมื่อมีการปรับปรุงแก้ไข	กรณีมีการปรับปรุงชุดคำสั่ง												
	มีกระบวนการทบทวนชุดคำสั่ง (Code Review) เพิ่มเติม ในกระบวนการส่งมอบงาน	กรณีมีการปรับปรุงชุดคำสั่ง												
	มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่	กรณีมีการปรับปรุงชุดคำสั่ง												
	จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลให้มีความทันสมัย และใช้งานได้อย่างต่อเนื่อง	ทุกปี					/			/	/			

บทที่ ๓
การติดตามและรายงานผล

การติดตามและรายงานผล มีการดำเนินงานดังต่อไปนี้

๑. ติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยศูนย์เทคโนโลยีสารสนเทศ ระหว่างปฏิบัติงาน เพื่อให้เป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที โดยทำการติดตามและประเมินผลรายไตรมาส

๒. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการเทคโนโลยีสารสนเทศ กรมฝนหลวงและการบินเกษตร ทุก ๖ เดือน และ ๑๒ เดือน เพื่อให้มั่นใจว่าการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศมีคุณภาพ และมีความเหมาะสม

๓. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (DCIO) ทุก ๖ เดือน และ ๑๒ เดือน เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และวิเคราะห์ถึงปัญหาที่เกิดขึ้นเพื่อเสนอแนวทางแก้ไขอย่างถูกต้องมีประสิทธิภาพ