



กรมป่าไม้

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. 2564



จัดทำโดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้

สารบัญ

<u>เรื่อง</u>	<u>หน้า</u>
<u>บทนำ</u>	
- หลักการและเหตุผล	๑
- วัตถุประสงค์	๑
- วิสัยทัศน์	๑
- พันธกิจ	๒
- ภารกิจ	๒
- แนวทางการพัฒนา	๓
- อัตรากำลัง	๓
- สถานภาพด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้	๓
- สถานภาพด้านระบบเครือข่ายและการสื่อสาร กรมป่าไม้	๔
<u>กระบวนการบริหารความเสี่ยง</u>	
- คำนิยามความเสี่ยง	๕
- ความหมายของการบริหารความเสี่ยง	๕
- กระบวนการบริหารความเสี่ยง	๖
- บทบาท หน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยง	๑๐
<u>การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ</u>	
- ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๑
- การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๒
- ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๓
- ตารางวิเคราะห์แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๔	๑๔
- แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๔	๒๒
<u>การติดตามและรายงานผล</u>	
- การติดตามผลและรายงานผล	๒๘
- แบบรายงานผลการดำเนินงาน	๒๙
<u>ภาคผนวก</u>	
- คำสั่งแต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้	

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้

ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

บทนำ

หลักการและเหตุผล

ปัจจุบันกรมป่าไม้ได้นำเทคโนโลยีสารสนเทศมาใช้งาน เพื่อช่วยเพิ่มประสิทธิภาพการดำเนินงานภายในองค์กรให้ได้รับความสะดวก รวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากเหตุต่างๆ เช่น การถูกโจมตี ไวรัสมัลแวร์ บุคลากร ไฟฟ้าดับ เกิดอัคคีภัย เป็นต้น ซึ่งอาจส่งผลกระทบต่อการทำงานของกรมป่าไม้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ มีความมั่นคงปลอดภัย จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และทบทวนแผนบริหารความเสี่ยงให้เป็นปัจจุบันอยู่เสมอ

วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลสารสนเทศให้มีเสถียรภาพและพร้อมใช้งาน
๒. เพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
๓. เพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

ข้อมูลพื้นฐานของหน่วยงาน

วิสัยทัศน์

เป็นหน่วยงานที่มุ่งมั่นรักษาป่า ส่งเสริมไม้มีค่า ป่าชุมชน คนอยู่กับป่า เพิ่มพื้นที่สีเขียว เพื่อความสุขของคนไทย

พันธกิจ

๑. ป้องกันและรักษาป่าพื้นที่ป่าไม้ให้คงอยู่
๒. เพิ่มพื้นที่ป่าเศรษฐกิจ สนับสนุนการเพิ่มพื้นที่สีเขียว และฟื้นฟูพื้นที่ป่าไม้ให้อุดมสมบูรณ์
ตอบสนองความต้องการทั้งด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม
๓. บริหารจัดการทรัพยากรป่าไม้โดยการมีส่วนร่วม
๔. บริหารจัดการที่ดินป่าไม้อย่างเป็นระบบและเป็นธรรม เพื่อให้คนอยู่ร่วมกันกับป่าอย่างสมดุลและยั่งยืน
๕. วิจัยและพัฒนา เพื่อสร้างนวัตกรรม และถ่ายทอดเทคโนโลยีในการอนุรักษ์ และการใช้ประโยชน์
ทรัพยากรป่าไม้
๖. พัฒนาความสามารถเชิงรุกขององค์กร ทั้งระบบ กลไก ข้อมูลสารสนเทศ และปรับปรุงกฎระเบียบ
ให้ทันสมัย ให้เหมาะสมกับสถานการณ์ปัจจุบัน

ภารกิจ

กรมป่าไม้มีภารกิจเกี่ยวกับการอนุรักษ์ สงวน คุ้มครอง ฟื้นฟู ดูแลรักษา ส่งเสริม ทำนุบำรุงป่า และการดำเนินการเกี่ยวกับการป่าไม้ การทำไม้ การเก็บหาของป่า การใช้ประโยชน์ที่ดินป่าไม้ และการอื่นเกี่ยวกับป่าและอุตสาหกรรมป่าไม้ ให้เป็นไปตามระเบียบและกฎหมายที่เกี่ยวข้อง ด้วยกลยุทธ์การเสริมสร้างความร่วมมือของประชาชนเป็นหลัก เพื่อเพิ่มมูลค่าทางเศรษฐกิจของประเทศ และพัฒนาคุณภาพชีวิตของประชาชน และมีภารกิจอื่นตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรมป่าไม้ โดยมีอำนาจหน้าที่ ดังนี้

๑. ควบคุม กำกับ ดูแล ป้องกันการบุกรุก การทำลายป่า และการกระทำผิดในพื้นที่รับผิดชอบตามกฎหมายว่าด้วยการป่าไม้ กฎหมายว่าด้วยป่าสงวนแห่งชาติ กฎหมายว่าด้วยสวนป่า กฎหมายว่าด้วยเสียประโยชน์ กฎหมายว่าด้วยป่าชุมชน และกฎหมายอื่นที่เกี่ยวข้อง
๒. ศึกษา วิจัย วางแผน และประสานงานเกี่ยวกับการปลูกป่า เพื่อการฟื้นฟูสภาพป่าและระบบนิเวศ
๓. ส่งเสริมการปลูกป่า การจัดการป่าชุมชน และการปลูกสร้างสวนป่าเชิงเศรษฐกิจ ในลักษณะสวนป่าภาคเอกชนและสวนป่าในรูปแบบอื่นที่เกี่ยวข้อง ตลอดจนศึกษา วิเคราะห์ และประเมินสถานการณ์ป่าเศรษฐกิจของตลาดในประเทศและต่างประเทศ
๔. อนุรักษ์ คุ้มครอง ดูแลรักษา และจัดการให้มีการใช้ประโยชน์ที่ดินป่าไม้ และการอนุญาตที่เกี่ยวข้องกับการใช้ประโยชน์จากไม้ อุตสาหกรรมไม้ ที่ดินป่าไม้ และผลิตภัณฑ์ป่าไม้
๕. ศึกษา ค้นคว้า วิจัย และพัฒนาที่เกี่ยวข้องกับป่าไม้และผลิตภัณฑ์ป่าไม้ และที่เกี่ยวข้องกับไม้และผลิตภัณฑ์ไม้
๖. ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรมหรือตามที่กระทรวงหรือคณะรัฐมนตรีมอบหมาย

แนวทางการพัฒนา

๑. ป้องกันและปราบปรามการบุกรุกทำลายทรัพยากรป่าไม้
๒. ส่งเสริมการบริหารจัดการป่าชุมชน
๓. การบริหารจัดการที่ดินป่าไม้อย่างเป็นระบบ เป็นธรรมเพื่อให้ประชาชนอยู่ร่วมกับป่าอย่างสมดุลและอย่างยั่งยืน
๔. ส่งเสริมการฟื้นฟูป่าเสื่อมโทรมและเพิ่มพื้นที่ป่าเศรษฐกิจ
๕. ส่งเสริมและพัฒนาการเพิ่มพื้นที่สีเขียวในเขตเมืองและเขตชนบท
๖. การบริหารจัดการทรัพยากรป่าไม้

อัตรากำลัง

กรมป่าไม้ มีอัตรากำลังทั้งสิ้น ๑๑,๘๖๒ อัตรา แบ่งออกเป็น ๔ ประเภท ดังนี้

- ข้าราชการ	๑,๙๒๗	อัตรา
- ลูกจ้างประจำ	๙๗๘	อัตรา
- พนักงานราชการ	๖,๗๒๔	อัตรา
- พนักงานจ้างเหมา	๒,๒๓๓	อัตรา

หมายเหตุ ปีงบประมาณ พ.ศ. ๒๕๖๔

สถานภาพด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้

กรมป่าไม้ มีระบบงานที่ใช้ในการปฏิบัติงาน มีรายละเอียดดังนี้

๑. ระบบข้อมูลสารสนเทศทรัพยากรบุคคลระดับกรม
๒. ระบบบุคลากร เงินเดือน และสวัสดิการ
๓. ระบบงานบุคคลของพนักงานราชการ
๔. ระบบสารบรรณอิเล็กทรอนิกส์ กรมป่าไม้
๕. ระบบติดตามการบุกรุกทำลายป่าและควบคุมไฟป่า
๖. ระบบเว็บไซต์กรมป่าไม้
๗. ระบบอีเมลกรมป่าไม้
๘. ระบบ National Single Window (NSW)
๙. ระบบจัดการฐานความรู้ด้านความหลากหลายทางชีวภาพ
๑๐. ระบบสวนป่า
๑๑. ระบบแจกจ่ายกล้าไม้
๑๒. ระบบอนุญาตด้านอุตสาหกรรมป่าไม้
๑๓. ระบบแผนงานและงบประมาณ กรมป่าไม้
๑๔. ระบบฐานข้อมูลเชิงแผนที่ของกรมป่าไม้
๑๕. ระบบเครือข่ายคอมพิวเตอร์เสมือน
๑๖. ระบบตรวจสอบและติดตามการทำงานของเครือข่าย (e-Monitoring)
๑๗. ระบบด่านป่าไม้
๑๘. ระบบขอตรวจพิสูจน์ไม้
๑๙. ระบบพิทักษ์ไพร
๒๐. Mobile Application Forest4thai

สถานการณ์ด้านระบบเครือข่ายและการสื่อสาร กรมป่าไม้

๑. ระบบเครือข่ายของกรมป่าไม้ ซึ่งมีการเชื่อมต่ออินเทอร์เน็ตจำนวน ๒ คู่สาย เครือข่ายทูลความเร็ว ๔๐๐/๘๐ Mbps เครือข่าย CAT ความเร็ว ๔๐๐/๘๐ Mbps

๒. การดำเนินการด้านการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย ด้านความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย นั้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการปรับปรุงระบบเครือข่ายให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้ระบบคอมพิวเตอร์และเครือข่ายกรมป่าไม้ มีความมั่นคงปลอดภัยจากบุคคลผู้ไม่มีสิทธิในการเข้าถึงข้อมูล

กระบวนการบริหารความเสี่ยง

คำนิยามความเสี่ยง

ความเสี่ยง หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตาม วัตถุประสงค์และเป้าหมายที่กำหนด

การประเมินความเสี่ยง หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

การวิเคราะห์ความเสี่ยง หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นตอนต่อไปคือ การวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเพราะการวัดความเสี่ยงเป็นตัวเลขว่าเมื่อผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิดหรือ โอกาสที่จะเกิดความเสี่ยง

การบริหารความเสี่ยง เมื่อทราบความเสี่ยงที่มีนัยสำคัญและโอกาสที่จะเกิดความเสี่ยง แล้วควรวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยง และพิจารณาว่าจะยอมรับความเสี่ยงนั้นหรือจะกำหนดกิจกรรมการควบคุมต่างๆ เพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้

ความหมายของการบริหารความเสี่ยง

๑. ความเสี่ยง (Risk) คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจที่กำหนด

๒. ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

๓. กระบวนการบริหารความเสี่ยง (Risk Management Process) เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยงโดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกระบวนการดังกล่าวนี้จะสำเร็จได้ ต้องมีการสื่อสารให้คนในองค์กรมีความรู้ ความเข้าใจในเรื่องการบริหารความเสี่ยงในทิศทางเดียวกัน

๔. การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการที่ใช้ในการระบุวิเคราะห์ ความเสี่ยง และจัดลำดับความเสี่ยง โดยประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

- โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดความเสี่ยง
- ผลกระทบ (Impact) หมายถึง ขนาดของความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง

๕. ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งเป็น ๔ ระดับ คือ ระดับสูงมาก ระดับสูง ระดับปานกลาง และระดับต่ำ

๖. การบริหารความเสี่ยง/การจัดการความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้อุปสรรคที่จะเกิดความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้

๗. การควบคุม (Control) หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ

๑) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสียหายและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้าง ๗ องค์การ การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงเอกสาร ข้อมูล ทรัพย์สิน

๒) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การสอบทาน การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง

๓) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดี

๔) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต เช่น การจัดเตรียมเครื่องมือดับเพลิงเพื่อช่วยลดความรุนแรงของความเสียหายให้น้อยลงหากเกิดไฟไหม้

กระบวนการบริหารความเสี่ยง

กรมป่าไม้กำหนดให้ดำเนินการจัดทำแผนบริหารความเสี่ยงตามกระบวนการบริหารความเสี่ยงมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) ๗ ขั้นตอน ดังนี้

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เพื่อเป็นกรอบการดำเนินงานในแต่ละระดับให้สามารถวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นได้อย่างครบถ้วนและเป็นไปในทิศทางเดียวกันกับแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้ (พ.ศ. ๒๕๕๔ – ๒๕๕๗) โดยจะยึดหลักการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Annex A) โดยมีหัวข้อดังต่อไปนี้

- ๑) นโยบายความมั่นคงปลอดภัย (Security policy)
- ๒) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)
- ๓) การบริหารจัดการทรัพย์สินขององค์กร (Asset management)
- ๔) ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร (Human resources security)
- ๕) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)
- ๖) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)
- ๗) การควบคุมการเข้าถึง (Access control)
- ๘) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)
- ๙) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (information security incident management)
- ๑๐) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)
- ๑๑) การปฏิบัติตามข้อกำหนด (Compliance)

๒. การระบุความเสี่ยง (Event Identification)

เป็นการระบุรายการความเสี่ยง ที่อาจเกิดขึ้นได้ทุกกรณี และสามารถเป็นต้นเหตุของการเกิดความเสียหาย ความล้มเหลว รวมถึงการลดโอกาสที่จะบรรลุความสำเร็จตามเป้าหมายของการปฏิบัติงาน หรือกิจกรรม โดยการระบุความเสี่ยงจะนำกิจกรรมที่อยู่ภายใต้มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ ที่ได้กล่าวอ้างจากการกำหนดเป้าหมายการบริหารความเสี่ยง ข้างต้นมาพิจารณาระบุความเสี่ยง โดยมีรายละเอียดดังนี้

๑) นโยบายความมั่นคงปลอดภัย (Security policy)

- นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

- โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร
- โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานภายนอก

๓) การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

- หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร
- การจัดหมวดหมู่สารสนเทศ

๔) ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร (Human resources security)

- การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน
- การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน
- การสิ้นสุดหรือการเปลี่ยนการจ้างงาน

๕) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

- บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย
- ความมั่นคงปลอดภัยของอุปกรณ์

๖) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

- การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน
- การบริหารจัดการการให้บริการของหน่วยงานภายนอก
- การวางแผนและตรวจรับทรัพยากรสารสนเทศ
- การป้องกันโปรแกรมที่ไม่ประสงค์ดี
- การสำรองข้อมูล
- การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร
- การจัดการสื่อที่ใช้ในการบันทึกข้อมูล
- การแลกเปลี่ยนสารสนเทศ
- การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์
- การเฝ้าระวังทางด้านความมั่นคงปลอดภัย

๗) การควบคุมการเข้าถึง (Access control)

- ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้
- หน้าที่ความรับผิดชอบของผู้ใช้งาน

- การควบคุมการเข้าถึงเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ
- การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ
- การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

๘) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

- ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ
- การประมวลสารสนเทศในแอปพลิเคชัน
- มาตรฐานการเข้ารหัสข้อมูล
- การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ
- การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน
- การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

๙) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (information security incident management)

- การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย
- การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๑๐) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

- หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

๑๑) การปฏิบัติตามข้อกำหนด (Compliance)

- การปฏิบัติตามข้อกำหนดทางกฎหมาย
- การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค
- การตรวจประเมินระบบสารสนเทศ

๓. การประเมินความเสี่ยง (Risk Assessment)

เป็นการประเมินความเสี่ยงที่นำกิจกรรมจากกิจกรรมที่ได้ทำการระบุความเสี่ยง มาประเมินตามเกณฑ์ เพื่อให้ทราบโอกาสและผลกระทบที่อาจเกิดขึ้นกับองค์กร โดยได้กำหนดการประเมินประกอบด้วยเกณฑ์การให้ความรุนแรงของผลกระทบ (x) และโอกาสที่จะเกิดความเสียหาย (Y) รายละเอียดตามตารางการประเมินความเสี่ยง ดังนี้

หลักเกณฑ์การวิเคราะห์ความเสี่ยง

(ตัวเลขที่แสดงในตารางเกิดจากผลคูณของ แนวตั้ง คุณ แนวนอน)

ผลกระทบ (ความรุนแรง)	สูงมาก/ หายนะ	5	5	10	15	20	25
	สูง/วิกฤต	4	4	8	12	16	20
	ปานกลาง	3	3	6	9	12	15
	ต่ำ/น้อย	2	2	4	6	8	10
	ไม่เป็น สาระสำคัญ/ น้อยมาก	1	1	2	3	4	5
Risk Assessment Matrix			1	2	3	4	5
		ต่ำ มาก/ น้อย มาก	ต่ำ/ น้อย	ปาน กลาง	สูง/ บ่อย	สูง มาก/ บ่อย มาก	

หลักเกณฑ์การประเมินโอกาส (Likelihood) ที่จะเกิดความเสี่ยง

ระดับโอกาส (ความเป็นไปได้)	ความถี่ที่จะเกิดเหตุการณ์	ระดับคะแนน
น้อยมาก	นานๆ ครั้ง (อาจเกิดขึ้นได้ปีละ 1 ครั้ง)	1
น้อย	ไม่บ่อย (อาจเกิดขึ้นได้ทุกไตรมาส)	2
ปานกลาง	ปานกลาง (อาจเกิดขึ้นได้ทุกเดือน)	3
สูง	บ่อย (อาจเกิดขึ้นได้ทุกสัปดาห์)	4
สูงมาก	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)	5

หลักเกณฑ์การประเมินผลกระทบ (Impact) ที่จะเกิดความเสี่ยง

ผลกระทบ (ความรุนแรง)	ผลกระทบที่จะเกิดเหตุการณ์	ระดับคะแนน
น้อยมาก	เกิดเหตุไม่มีความสำคัญ	1
น้อย	เกิดเหตุเล็กน้อยที่แก้ไขได้	2
ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก	3
สูง	เกิดปัญหาเกี่ยวกับระบบ IT ที่สำคัญ และระบบ ความปลอดภัยซึ่งส่งผลกระทบต่อความถูกต้องของ ข้อมูลบางส่วน	4
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลกรมป่าไม้	5

การประเมินระดับความเสี่ยง

๔. การตอบสนองความเสี่ยง (Risk Response)

คือการกำหนดวิธีการจัดการความเสี่ยง เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์การจัดการความเสี่ยงอย่างใดอย่างหนึ่งผสมผสานกันดังต่อไปนี้

๑) การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง

๒) การลดการควบคุมความเสี่ยง (Risk Reduction) เป็นการปรับปรุงกระบวนการทำงาน หรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่ยอมรับได้ เช่น การลดขนาดกิจกรรม

๓) การกระจายความเสี่ยงหรือถ่ายโอนความเสี่ยง (Risk Sharing/Risk Transfer) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งเบาความรับผิดชอบ เช่น การใช้บริการจากภายนอก (Out Source)

๔) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการกับความเสี่ยงที่มีอยู่ในระดับสูงมาก และหน่วยงานไม่อาจยอมรับได้จึงต้องตัดสินใจ หยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรม/โครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง

๕. กิจกรรมการบริหารความเสี่ยง (Control Activities)

โดยการกำหนดปัจจัยเสี่ยงที่มีคะแนนประเมินความเสี่ยงที่ระดับสูงตั้งแต่ ๕ - ๒๕ ขึ้นไปให้นำมาดำเนินการจัดทำแผนบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ตามแบบฟอร์มที่กำหนดประกอบด้วย ประเด็นความเสี่ยง กิจกรรม ตามแนวทางการจัดการความเสี่ยง เป้าหมาย/ผลสำเร็จของการดำเนินกิจกรรมตามแนวทางการจัดการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ระยะเวลาดำเนินการ ผู้รับผิดชอบ งบประมาณ

๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

จัดให้มีการสื่อสารข้อมูลที่ต้องการผ่านช่องทางการสื่อสารไปยังกลุ่มเป้าหมายที่กำหนด เพื่อให้บุคคลที่เกี่ยวข้องได้รับทราบการข้อมูลและนำไปสู่การปฏิบัติ

๗. การติดตามผลและเฝ้าระวังความเสี่ยง (Monitoring)

กำหนดให้มีการติดตามการประเมินผลการดำเนินงานตามระยะเวลาที่กำหนดไว้ดังนี้

- เดือนกันยายน - ตุลาคม พ.ศ. ๒๕๖๔ เฝ้าระวังและติดตามผลความเสี่ยง
- เดือนตุลาคม - พฤศจิกายน พ.ศ. ๒๕๖๔ จัดทำสรุปและรายงานผลการเฝ้าระวัง

บทบาทหน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยง

๑) บริหารระดับสูง ทำหน้าที่กำหนดนโยบายและแต่งตั้งคณะกรรมการหรือคณะทำงานในการกำกับดูแลให้มีการดำเนินการตามแผนบริหารความเสี่ยง

๒) คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ จัดทำวิธีปฏิบัติด้านเทคโนโลยีสารสนเทศ เพื่อบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้

๓) ผู้บริหารระดับสำนัก/กอง/ศูนย์ ดำเนินการบริหารความเสี่ยงในหน่วยงาน รวมทั้งติดตามประเมินผลอย่างต่อเนื่อง

๔) บุคลากรในหน่วยงาน ดำเนินการตามแผนบริหารความเสี่ยงตามที่กำหนด อย่างถูกต้อง ครบถ้วน

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการศึกษาค้นคว้า ประกอบกับการตรวจสอบหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการ และการควบคุมความเสี่ยงด้านสารสนเทศของกรมป่าไม้ พิจารณาแล้วเห็นว่าความเสี่ยงด้านสารสนเทศที่เกี่ยวข้องกับกรมป่าไม้สามารถ แบ่งออกเป็น ๔ ประเภทหลัก ดังนี้

๑. Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานที่รับผิดชอบไม่ได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปใช้ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน กรมไม่ได้มีการกำหนดรหัสผ่าน(password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การไม่ได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

๒. Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานที่รับผิดชอบ ไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบ และรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

๓. Availability Risk : เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการซึ่งอาจทำให้การปฏิบัติงานหรือการให้บริการด้านต่าง ๆ อาจหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการที่ไม่ได้มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์ และป้องกันความเสียหายอย่างเพียงพอ และยังรวมถึงการที่ไม่ได้ทำการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ ถ้าหากไม่ได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์เสียหายได้

๔. Infrastructure Risk : เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานที่รับผิดชอบไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่โดยรวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการปฏิบัติงาน โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบย้อนและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการที่ไม่ได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรือเกิดจากการไม่มีแผนงานและ

ขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้าน และมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการปฏิบัติราชการ และการไม่ได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรอบรู้ และเชี่ยวชาญในงานที่รับผิดชอบ นอกจากนี้ความเสี่ยง ๔ ประเภทหลักตามที่กล่าวข้างต้น ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงหนึ่งที่ทำให้เกิดผลกระทบต่อระบบฐานข้อมูลกรมป่าไม้ เนื่องด้วยความเสี่ยงดังกล่าว อาจทำให้ระบบขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อภาพรวมของระบบฐานข้อมูลกรมป่าไม้ จึงจำเป็นต้องมีการจัดทำระบบบริหารจัดการความเสี่ยงและแผนแก้ไข ปัญหาที่อาจเกิดขึ้นและแนวทางป้องกันต่อไป

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ดำเนินการวิเคราะห์ ความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยจากการดำเนินงานด้านเทคโนโลยีสารสนเทศ และวิเคราะห์ปัญหาหรือ ภัยคุกคามที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมป่าไม้ โดยปัญหาหรือภัยคุกคามนั้น สร้างผลกระทบต่อการบรรลุความสำเร็จการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จากการสรุปปัญหาและภัยคุกคามทั้งหมดแล้วจะนำมาประเมินโอกาส (Likelihood) ที่อาจจะเกิดเหตุการณ์ความเสี่ยง พร้อมทั้งประเมินระดับความรุนแรงหรือมูลค่าความเสียหาย (Impact) จากความเสี่ยง โดยเลือกความเสี่ยงที่มีระดับสูงและสูงมาก มาจัดทำแผนบริหารความเสี่ยง

ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้คือ

๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติ สิ่งที่มีมนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น วัตถุภัย น้ำท่วม ไฟฟ้า เพลิงไหม้ กระแสไฟฟ้าขัดข้อง การเข้า – ออก ห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงโดยไม่ได้รับอนุญาต เป็นต้น

๒. ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรทั้งภายในและภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงการวางแผน การมอบหมายหน้าที่ การปฏิบัติงาน การตรวจสอบ และสิทธิของบุคลากร/คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งานการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายอุปกรณ์โดยไม่ได้รับอนุญาต การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์

๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่างๆ ที่ได้จัดทำและพัฒนาขึ้น รวมถึงโปรแกรมประยุกต์อื่นๆ ที่ใช้ประกอบการใช้งาน เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีช่องโหว่ทำให้มีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่งและการถูกผู้ไม่ประสงค์ดีทำลายระบบ (Hacker) การพัฒนาระบบสารสนเทศที่ไม่มีการกำหนดสิทธิ์การเข้าถึงระบบ เป็นต้น

๕. ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่าง ๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กร ทั้งเครือข่ายอินทราเน็ต (Intranet) และเครือข่ายอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากภายในระบบเครือข่ายเอง ได้แก่ ความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย เป็นต้น และความเสี่ยงจากภัยภายนอกได้แก่ การบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่าง ๆ

๖. ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากข้อมูล และฐานข้อมูลในระบบสารสนเทศ อันอาจก่อให้เกิดความเสียหาย ได้แก่ การทำลายข้อมูล การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต การโจรกรรมข้อมูลที่สำคัญ เป็นต้น ความเสี่ยงเหล่านี้ล้วนมีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ซึ่งความเสี่ยงทั้ง ๖ เรื่อง ได้แก่

- ๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม
- ๒) ความเสี่ยงด้านบุคลากร
- ๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ
- ๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์
- ๕) ความเสี่ยงด้านระบบเครือข่าย
- ๖) ความเสี่ยงด้านข้อมูล

กรมป่าไม้ ได้กำหนดแผนการบริหารจัดการความเสี่ยง โดยอ้างอิงหลักการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Annex A) ทั้ง ๑๑ ประเด็น ได้แก่ นโยบายความมั่นคงปลอดภัย (Security policy), โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security), การบริหารจัดการทรัพย์สินขององค์กร (Asset management), ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (Human resources security), การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security), การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management), การควบคุมการเข้าถึง (Access control), การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance), การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (information security incident management), การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management), การปฏิบัติตามข้อกำหนด (Compliance) โดยดำเนินการวิเคราะห์ประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ เพื่อให้มีการบริหารความเสี่ยง เพื่อกำจัดป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ และการสำรองและการกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery), มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan), มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti - Virus ระบบไฟฟ้าสำรอง เป็นต้น, และมีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights) ในการเข้าถึงระบบสารสนเทศและเครือข่าย ซึ่งได้แสดงรายละเอียดการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

ตารางวิเคราะห์แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๔

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม									
๑.๑ เกิดอัคคีภัย วาตภัย อุทกภัย ไฟฟ้า น้ำท่วม แผ่นดินไหว วินาศภัย ก่อการร้าย	-การสูญหายและถูกทำลายของอุปกรณ์ -เกิดความเสียหายด้านโครงสร้างอาคาร -ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	-เสี่ยงประมาณในการจัดหาระบบทดแทน -ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน -เสียเวลาในการกู้ระบบ	๑	๕	๕	-จัดทำแผนรองรับสถานการณ์ฉุกเฉิน -ติดตั้งอุปกรณ์ดับเพลิง -จัดเก็บระบบและข้อมูลบน cloud ของหน่วยงานอื่น	-มีการจัดเก็บระบบและข้อมูลบน cloud แคบวงระบบ -ไม่ได้มีการดูแลอุปกรณ์ดับเพลิงอย่างต่อเนื่อง	ลด	-จัดทำแผนพัฒนาไซต์สำรอง (DR-Site) -ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง -จัดทำแผนบริหารความต่อเนื่องด้าน IT
๑.๒ กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	-แหล่งจ่ายไฟฟ้าหลักขัดข้อง -ตู้ควบคุมการจ่ายไฟฟ้าหลักของอาคารขัดข้อง	-ไม่สามารถใช้งานระบบได้ -ข้อมูลเสียหาย -ระบบปฏิบัติการ โปรแกรม หรือฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่	๒	๔	๘	-ติดตั้งอุปกรณ์สำรองไฟ (UPS) -ติดตั้งเครื่องผลิตไฟฟ้าสำรอง (Generator)	-เบื้องต้นสามารถแก้ไขปัญหได้ในระดับหนึ่ง	ลด	-บำรุงรักษาการทำงาน UPS -บำรุงรักษาการทำงานของ Generator
๑.๓ คอมพิวเตอร์ถูกโจรกรรม	-ขาดมาตรการระบบรักษาความปลอดภัย เช่น ระบบการเข้าเวรยาม กล้องวงจรปิด เป็นต้น	-เสี่ยงประมาณในการจัดหาคอมพิวเตอร์ทดแทน -ข้อมูลในเครื่องคอมพิวเตอร์สูญหาย	๑	๕	๕	-มียามประจำอาคาร -ติดตั้งกล้องวงจรปิด	-การรักษาความปลอดภัยอาจยังไม่ครอบคลุม	ลด	-บำรุงรักษาและติดตั้งกล้องวงจรปิดให้ครอบคลุมและสามารถใช้งานได้อย่างต่อเนื่อง
๑.๔ ความเสี่ยงจากแมลงหรือสัตว์กัดแทะสายไฟฟ้าหรือสายสัญญาณ	-อาคารมีแหล่งอาศัยของหนูและแมลง -มีเศษอาหารในอาคาร ทำให้เป็นแหล่งอาหารของหนู	-เสี่ยงประมาณในการซ่อมแซมหรือจัดหาทดแทน -ไม่สามารถใช้งานสารสนเทศและเครือข่ายได้	๑	๕	๕	-ทำท่อ/ราง/อื่นๆ ห่อหุ้มสาย	-เบื้องต้นสามารถป้องกันได้ระดับหนึ่ง	ลด	-ตรวจสอบและปรับปรุงสายไฟฟ้าและสายสัญญาณโดยห่อหุ้มวัสดุที่ป้องกันแมลงหรือสัตว์กัดแทะ -จ้างกำจัดหนูและแมลง -รณรงค์รักษาความสะอาดในอาคาร
๑.๕ เกิดเหตุสถานการณ์ทางการเมือง	-ถูกปิดทางเข้าสำนักงาน -ถูกตัดสาธารณูปโภค	-ไม่สามารถเข้าปฏิบัติงานที่หน่วยงานได้ -หากระบบมีปัญหา ไม่สามารถแก้ไขได้	๑	๔	๔	-จัดทำไซต์สำรอง (DR-Site) ที่หน่วยงานอื่น -จัดทำแผนรองรับสถานการณ์ฉุกเฉิน	-การจัดเก็บระบบและข้อมูลบน cloud แคบวงระบบ	ลด	-จัดทำแผนพัฒนาไซต์สำรอง (DR-Site) -จัดทำแผนบริหารความต่อเนื่องด้าน IT

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๑.๖ การแพร่ระบาดของโรคติดต่อ เช่น COVID-19	-เจ้าหน้าที่อาจติดโรคร้ายแรง ทำให้ถูกกักตัว ไม่สามารถมาปฏิบัติงานได้ -ผู้ประกอบการไม่สามารถส่งมอบงานได้ตามกำหนดเวลา	-เจ้าหน้าที่ไม่สามารถมาปฏิบัติงานที่หน่วยงานได้ -อุปกรณ์ที่เสียหายไม่สามารถติดตั้งหรือแก้ไขได้ทันที ทำให้ระบบสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง	๑	๕	๕			ลด ยอมรับ	-จัดหาเทคโนโลยีที่ช่วยให้เจ้าหน้าที่ปฏิบัติงานจากที่พัก -อบรมเจ้าหน้าที่เพื่อให้สามารถปฏิบัติงานแทนกันได้
๒. ความเสี่ยงด้านบุคลากร									
๒.๑ บุคลากรด้านคอมพิวเตอร์ขาดความรู้ และทักษะในการปฏิบัติงาน	-เจ้าหน้าที่ปฏิบัติงานไม่ตรงตามสายงาน -มีการเปลี่ยนงานบ่อย	-เจ้าหน้าที่ไม่สามารถใช้งานระบบได้ -เจ้าหน้าที่ไม่สามารถแก้ไขปัญหาได้	๓	๔	๑๒	-มีการจัดอบรม เพื่อให้บุคลากรมีความรู้ความเข้าใจในระบบงานที่รับผิดชอบ	-เบื้องต้นสามารถลดความเสี่ยงได้ในระดับหนึ่ง	ลด	-จัดอบรมให้ความรู้ด้านคอมพิวเตอร์และเทคโนโลยีที่ทันสมัยให้แก่เจ้าหน้าที่อย่างสม่ำเสมอ -จัดทำคู่มือการปฏิบัติงานด้านคอมพิวเตอร์ -เพิ่มอัตรากำลังเจ้าหน้าที่และจัดทำ career path ให้แก่เจ้าหน้าที่ด้านคอมพิวเตอร์ -เพิ่มการจัดการความรู้ (KM) ในการปฏิบัติงานด้าน IT เพื่อเป็นแนวทางในการแก้ปัญหา

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๒.๒ เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	-ใช้งานในทางที่ผิด เช่น ดูหนัง เล่นการพนัน และเล่นเกมส์ -ดาวน์โหลดโปรแกรมที่ไม่มีลิขสิทธิ์ -ดาวน์โหลดหนังออนไลน์	-ทำให้สูญเสีย Bandwidth ในเครือข่าย -อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก -อาจทำให้เครื่องติดไวรัส	๔	๓	๑๒	-มีการกำหนด policy ของ Firewall ให้เหมาะสม	-เบื้องต้นสามารถลดความเสี่ยงได้ในระดับหนึ่ง	ลด	-กำหนด policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด port เท่าที่จำเป็น -ให้ความรู้แก่บุคลากรในเรื่องการใช้คอมพิวเตอร์และระบบเครือข่ายอย่างเหมาะสมและสม่ำเสมอ -ตรวจสอบและรายงานการใช้งานของผู้ใช้งานผิดวัตถุประสงค์ต่อผู้บังคับบัญชา
๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ									
๓.๑ เครื่องคอมพิวเตอร์และอุปกรณ์ IT ขาดและล้าสมัย	-ขาดงบประมาณในการจัดหาอุปกรณ์ที่ทันสมัยให้เพียงพอต่อการใช้งานของหน่วยงาน -ระเบียบในการจัดซื้อจัดจ้าง -การจัดหาต้องผ่านความเห็นชอบจากคณะกรรมการ ICT ของกรมป่าไม้หรือกระทรวงฯ	-ไม่สามารถใช้ระบบงานได้ -ข้อมูลที่จัดเก็บไว้เสียหาย	๕	๓	๑๕	-มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ให้หน่วยงานในกรมป่าไม้อย่างต่อเนื่อง	-เครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับการจัดสรรยังไม่เพียงพอ	ลด	-สำรวจความต้องการเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ -จัดประชุมคณะกรรมการ ICT อย่างสม่ำเสมอ -สำรวจข้อมูลไว้อีกที่หนึ่ง เช่น บน cloud เพื่อป้องกันการสูญหายของข้อมูล

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๓.๒ การใช้งานระบบ Web Conference	-สัญญาณเครือข่ายขัดข้อง -ไม่ได้จองใช้งานระบบ GIN Conference -ระบบ zoom สามารถใช้งานได้ ๑ ห้อง จำนวน user ไม่เกิน ๑๐๐ -อุปกรณ์ Conference ไม่ทันสมัย -เจ้าหน้าที่ไม่มีความรู้และทักษะในการติดตั้งและใช้งานระบบ	-ห้องประชุม conference ไม่เพียงพอในการใช้งาน -ไม่สามารถเชื่อมต่อระบบได้ -ภาพไม่ชัดเจน -เสียงไม่ออก	๕	๕	๒๕	-มีการจัดหาอุปกรณ์ Conference ของกรม ป่าไม้ส่วนกลางและหน่วยงานในภูมิภาค	-สามารถใช้งานได้	ลด	-มอบหมายเจ้าหน้าที่รับผิดชอบในการจองใช้งานระบบ GIN Conference -อบรมการติดตั้งและใช้งานระบบ Conference อย่างสม่ำเสมอ -จัดหาอุปกรณ์ conference ที่ทันสมัยทดแทน
๓.๓ การติดไวรัส คอมพิวเตอร์หรือ Malware	-การต่อพ่วงกับอุปกรณ์ทางคอมพิวเตอร์ที่ยังไม่ได้รับการตรวจสอบไวรัส (Scan Virus) -การดาวน์โหลดและติดตั้งซอฟต์แวร์ที่ไม่รู้แหล่งที่มา -การเข้าเว็บไซต์ที่มีความเสี่ยงและฝัง Spyware ไว้ เช่น เว็บไซต์ดาวน์โหลดโปรแกรมฟรี, ภาพยนตร์ฟรี เป็นต้น -การเปิดอีเมลที่มีการแนบไฟล์ที่ไม่รู้จักและไม่รู้แหล่งที่มา	-ไม่สามารถใช้คอมพิวเตอร์ได้ -ไม่สามารถใช้ระบบงานได้ -ข้อมูลสูญหาย -ทำให้มีปริมาณข้อมูลจราจรคอมพิวเตอร์ (Traffic) ที่เป็นอันตรายต่อระบบเครือข่ายและสารสนเทศเป็นจำนวนมาก	๕	๕	๒๕	-ติดตั้งโปรแกรมป้องกันไวรัส (Anti-Virus) ให้ผู้ใช้งานบางส่วน -ขอความร่วมมือจากผู้ใช้งานไม่เข้าเว็บไซต์ที่มีความเสี่ยง และไม่ดาวน์โหลดซอฟต์แวร์ที่ไม่รู้แหล่งที่มา -มีมาตรการหรือข้อบังคับในการใช้อุปกรณ์ต่อพ่วงและเข้าเว็บไซต์ เช่น ก่อนใช้งานอุปกรณ์ต่อพ่วงต้องสแกนไวรัสทุกครั้ง ห้ามเข้าเว็บไซต์ที่มีความเสี่ยง เป็นต้น	-ผู้ใช้งานบางคนไม่ให้ความร่วมมือ -เจ้าหน้าที่ดูแลไม่ทั่วถึง	ลด	-ประกาศมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ -ให้ความรู้แก่ผู้ใช้งาน ให้ตระหนักถึงภัยอันตรายที่เกิดจากไวรัส -อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ และจัดหาระบบสแกนไวรัสที่ทันสมัยและมีลิขสิทธิ์มาติดตั้งให้ครอบคลุมทุกเครื่องของผู้ใช้งาน -กำหนดสิทธิในการใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้งาน

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผล กระทบ (L)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์									
๔.๑ การพัฒนาระบบ ระบบสารสนเทศมีช่อง โหว่	-การถูกโจรกรรมหรือ เปลี่ยนแปลงข้อมูล -โปรแกรมเสียหาย -การใช้ช่องโหว่ของโปรแกรม หรือช่อง Script ไว้เพื่อ วัตถุประสงค์แอบแฝง -รูปแบบในการพัฒนาแตกต่าง กัน ทำให้เปลี่ยนคนพัฒนา หรือรับงานต่อยาก	-ทำให้กรมป่าไม้ขาดความ น่าเชื่อถือ -อาจทำให้เกิดความเสียหาย หาก เป็นข้อมูลที่มีชั้นความลับ -การใช้งานหรือพัฒนาโปรแกรม ไม่ต่อเนื่อง	๓	๕	๑๕	-ให้ผู้เชี่ยวชาญ ตรวจสอบช่องโหว่ของ แอปพลิเคชัน ตาม มาตรฐานของ OWASP -มีการกำหนดชั้นการ เข้าถึงของข้อมูล		ลด	-จัดหาผู้เชี่ยวชาญ ตรวจสอบช่องโหว่ของ แอปพลิเคชันอย่างต่อเนื่อง เพื่อนำมาปรับปรุงระบบ -กำหนดมาตรฐานในการ พัฒนาแอปพลิเคชัน เพื่อให้ ใช้เป็นรูปแบบเดียวกัน -กำหนดมาตรฐานความ ปลอดภัยในการพัฒนา แอปพลิเคชัน เช่น มีการ เข้ารหัส (encryption) ใน ฐานข้อมูลสำหรับปกปิดชื่อ ผู้ใช้และรหัสผ่าน
๔.๒ การละเมิดลิขสิทธิ์ โปรแกรม	-บุคลากรขาดความรู้ความ เข้าใจพระราชบัญญัติว่าด้วย การกระทำผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ.๒๕๕๐ และ พระราชบัญญัติข้อมูลข่าวสาร ของทางราชการ พ.ศ. ๒๕๔๐ -บุคลากรขาดการตระหนักถึง ภัยที่มาจากการใช้โปรแกรม ละเมิดลิขสิทธิ์ -ขาดงบประมาณในการจัดหา โปรแกรมที่มีลิขสิทธิ์	โดนฟ้องร้องจากเจ้าของลิขสิทธิ์	๔	๕	๒๐	-มีการชี้แจงเป็น หนังสือเวียนให้กับ บุคลากรภายในกรมป่า ไม้ทราบเกี่ยวกับ พระราชบัญญัติว่าด้วย การกระทำผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พระราชบัญญัติข้อมูล ข่าวสารของทางราชการ พ.ศ.๒๕๔๐	-บุคลากรบางส่วน ยัง ไม่ตระหนักถึงภัยและ ความผิดที่เกิดจาก การใช้โปรแกรมที่ไม่ มีลิขสิทธิ์ และยังคงมี การใช้งานโปรแกรม ที่ไม่มีลิขสิทธิ์อยู่	ลด	-รณรงค์ให้บุคลากรใช้งาน โปรแกรมที่มีลิขสิทธิ์ -รณรงค์ให้บุคลากรใช้ ซอฟต์แวร์ Open Source -ให้ความรู้แก่บุคลากรถึงภัย และความผิดที่เกิดจากการ ใช้โปรแกรมละเมิดลิขสิทธิ์ -จัดหาโปรแกรมที่มีลิขสิทธิ์ ถูกต้อง เช่น โปรแกรม สำนักงาน ระบบปฏิบัติการ
๔.๓ ระบบงานสารสนเทศ ไม่ตอบสนองความ ต้องการของผู้ใช้งาน	-ระบบงานบางระบบ ไม่ สามารถตอบสนองการใช้งาน ของผู้ใช้งานปัจจุบันได้	-ผู้ใช้งานไม่ใช้งานระบบ -ระบบไม่สามารถใช้งานได้	๔	๕	๒๐	-ปรับปรุงแก้ไขระบบให้ สามารถตอบสนองการ ใช้งานของผู้ใช้ได้	-เบื้องต้นสามารถ แก้ไขได้ในระดับหนึ่ง	ถ่ายโอน	-ปรับปรุงระบบตามความ ต้องการของผู้ใช้งาน

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผล กระทบ (L)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๕. ความเสี่ยงด้านระบบเครือข่าย									
๕.๑ การเชื่อมโยง เครือข่ายล้มเหลว	-ผู้ให้บริการเครือข่ายให้บริการ ล่าช้า ไม่ดูแล -การเชื่อมโยงเครือข่าย ล้มเหลว	-ไม่สามารถใช้งานระบบเครือข่าย และระบบงานได้	๕	๕	๒๕	-จัดทำ Link สำรองใน ลักษณะ Load Balance	-เบื้องต้นสามารถ แก้ปัญหาได้ในระดับ หนึ่ง	ลด	-จัดทำ TOR ให้ชัดเจนใน เรื่องการให้บริการ เช่น การกำหนดค่าปรับ ในกรณี ที่ผู้ให้บริการเครือข่ายไม่ สามารถดำเนินการตาม TOR ได้ -จ้างที่ปรึกษาวิเคราะห์และ ปรับปรุงระบบเครือข่าย คอมพิวเตอร์
๕.๒ ไฟไหม้เครื่องแม่ข่าย หรือภายในห้อง Data Center	-การเสื่อมสภาพของอุปกรณ์ ป้องกันการเกิดไฟไหม้ -การเสื่อมสภาพของอุปกรณ์ ดับเพลิง	-เสี่ยงประมาณในการจัดหาใหม่ -ข้อมูลเสียหาย	๑	๕	๕	-จัดทำไซต์สำรอง (DR- Site) -ติดตั้งระบบดับเพลิง	-เบื้องต้นสามารถ แก้ไขปัญหได้ใน ระดับหนึ่ง	ลด	-จัดทำแผนพัฒนาไซต์ สำรอง (DR-Site) -ตรวจสอบ บำรุงรักษา อุปกรณ์ป้องกันไฟไหม้ และ อุปกรณ์ดับเพลิง ให้อยู่ใน สภาพพร้อมใช้งาน
๕.๓ ระบบไฟฟ้าห้อง Data Center ไม่เสถียร	-ปริมาณการใช้ไฟฟ้ามาก -ระบบไฟฟ้าเก่า เสื่อมสภาพ	-ไม่สามารถใช้ระบบงานได้ -อุปกรณ์เครือข่ายเสียหาย	๒	๕	๑๐	-จัดหาเครื่องสำรอง ไฟฟ้าสำหรับห้อง Data Center	-เครื่องสำรองไฟฟ้า สำหรับห้อง Data Center สามารถ สำรองไฟได้ ระยะเวลาหนึ่ง	ลด	-ตรวจสอบระบบไฟฟ้าอย่าง สม่ำเสมอ -จัดทำแผนพัฒนาระบบ ติดตามและเฝ้าระวังระบบ ไฟฟ้าในห้อง Data Center

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผล กระทบ (L)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๕.๔ เครื่องแม่ข่ายและ อุปกรณ์เครือข่ายไม่ สามารถให้บริการได้อย่าง ต่อเนื่อง	-เจ้าหน้าที่ขาดความรู้และ ทักษะในการแก้ไขปัญหา -เครื่องแม่ข่ายและอุปกรณ์ ล้าสมัย -เครื่องแม่ข่ายและอุปกรณ์ เครือข่ายชำรุด -มีจำนวนผู้ใช้งานปริมาณมาก ทำให้เครื่องแม่ข่ายและ อุปกรณ์เครือข่าย ไม่สามารถ รองรับได้	-ไม่สามารถใช้ระบบได้อย่าง ต่อเนื่อง	๓	๕	๑๕	-จัดส่งเจ้าหน้าที่เข้ารับ การอบรมเพื่อเพิ่มทักษะ -กำหนดมาตรการการ เข้าใช้งานบางเว็บไซต์ เช่น ปิดการเข้าใช้งาน Facebook และ You tube ในเวลางาน -ติดตั้งอุปกรณ์เครื่อง คอมพิวเตอร์แม่ข่าย แบบ virtualization แล้ว - ทดแทนอุปกรณ์ เครือข่ายแล้วบางส่วน	-มีการจัดอบรมแล้ว แต่ยังไม่เพียงพอ -ยังไม่สามารถ ควบคุมการใช้งานได้ อย่างทั่วถึง	ลด	-จัดหาผู้เชี่ยวชาญด้าน ระบบเครือข่ายมาให้ความรู้ และเพิ่มทักษะในการแก้ไข ปัญหาเครื่องแม่ข่ายและ อุปกรณ์เครือข่ายให้แก่ เจ้าหน้าที่ -จ้างบำรุงรักษาเครื่องแม่ ข่ายและอุปกรณ์เครือข่าย ให้พร้อมใช้งาน -จัดทำแผนการตรวจสอบ ความพร้อมใช้งานของ เครื่องแม่ข่ายและอุปกรณ์ เครือข่าย -จัดทำหนังสือแจ้งเตือน ผู้ใช้งานเครือข่ายที่ไม่ เหมาะสม
๕.๕ การโจมตี (Hack) ระบบเครือข่าย	-การโจมตีจากภายนอก -การโจมตีจากโปรแกรมต่าง ที่ มีการติดตั้งที่เครื่องลูกข่าย โดยผู้ใช้งานภายใน	-ไม่สามารถใช้งานระบบเครือข่าย ได้ หรือใช้งานได้ แต่ช้า	๑	๕	๕	-สร้างมาตรการการเข้า ใช้งานระบบเครือข่าย (Policy) -ดำเนินการเข้ารหัสใช้ งานระบบสารสนเทศ	-ยังมีการ Hack เกิด ขึ้นอยู่	ลด	-ติดตั้งระบบป้องกันและ เตือนภัย -มอบหมายเจ้าหน้าที่คอย ตรวจสอบเป็นประจำ -จัดทำระบบสำรองข้อมูล -กำหนดรหัส (encryption) ระบบสารสนเทศ -จ้างที่ปรึกษาตรวจสอบหา ช่องโหว่ของระบบเครือข่าย

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผล กระทบ (L)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๕.๖ ระบบงานสารสนเทศ ของกรมไม่สามารถ ให้บริการได้	-Hard disk เสียหาย -Raid Controller เสียหาย -Switch และ Router เสียหาย	-ไม่สามารถใช้ระบบงานได้อย่าง ต่อเนื่อง	๑	๕	๕	-จัดทำไซด์สำรอง (DR- Site) -จัดทำระบบสำรอง ข้อมูล	-เบื้องต้นสามารถ แก้ไขปัญหาได้ใน ระดับหนึ่ง	ลด	-ตรวจสอบระบบสำรอง ข้อมูลและอุปกรณ์ อย่างสม่ำเสมอ -ปรับปรุงเครื่อง คอมพิวเตอร์แม่ข่าย ฐานข้อมูล (Data base) เป็นแบบ Cluster
๖. ความเสี่ยงด้านข้อมูล									
๖.๑ ข้อมูลและสารสนเทศ ไม่ถูกต้องและเป็นปัจจุบัน	-เจ้าหน้าที่ไม่ปรับปรุงข้อมูลให้ เป็นปัจจุบัน -ไม่มีการตรวจสอบความ ถูกต้องของข้อมูล	-ข้อมูลไม่ถูกต้อง และไม่เป็น ปัจจุบัน	๕	๔	๒๐	-ขอความร่วมมือ เจ้าหน้าที่ให้ปรับปรุง ข้อมูลให้เป็นปัจจุบัน -จัดทำปฏิทินรายงาน ข้อมูลและการตรวจสอบ ข้อมูล	ยังไม่ได้รับความ ร่วมมือในการ ปรับปรุงข้อมูล	ลด	-จัดฝึกอบรมการใช้งาน ระบบสารสนเทศอย่าง สม่ำเสมอ -กำหนดมาตรการในการ ตรวจสอบข้อมูล ก่อนนำขึ้น เผยแพร่บนเว็บไซต์ -มอบหมายให้เจ้าหน้าที่ ปรับปรุงข้อมูลให้ครบถ้วน เป็นปัจจุบัน
๖.๒ การสำรองข้อมูลไม่มี ประสิทธิภาพ	-ไม่มีการสำรองข้อมูลตามเวลา ที่กำหนด -ไม่มีการทดสอบการกู้คืน ข้อมูล	-ข้อมูลสูญหาย -เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือจัดทำขึ้นมาใหม่ -ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้ งาน	๓	๕	๑๕	-มีการสำรองข้อมูลบน เครื่องแม่ข่ายที่กรมป่า ไม้	ลดความเสี่ยงได้ ระดับหนึ่ง	ลด	-จ้างผู้เชี่ยวชาญบำรุงรักษา ระบบและบริหารจัดการ การสำรองข้อมูลอย่าง ต่อเนื่อง -ทดสอบการนำข้อมูล กลับคืนสู่ระบบ -จัดหาระบบสำรองข้อมูลที่มี ประสิทธิภาพ
๖.๓ การรั่วไหลจากการ เปลี่ยนมือผู้ใช้	-ไม่ปรับปรุงสิทธิการใช้งาน ข้อมูลของเจ้าหน้าที่ให้เป็น ปัจจุบัน	-ข้อมูลความลับรั่วไหล ทำให้กรม เสียหาย ขาดความน่าเชื่อถือ	๒	๓	๖	-มีการกำหนดสิทธิการ ใช้งานระบบของผู้ใช้	ไม่มีการตรวจสอบ และยกเลิกสิทธิการ ใช้งานของผู้ใช้ ที่ไม่มี สิทธิใช้งานแล้ว	ลด	-จัดทำแนวทางในการ ตรวจสอบสิทธิการใช้งาน และยกเลิกสิทธิการใช้งาน ของผู้ใช้ข้อมูล

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๔

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๔												ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม														
๑.๑ เกิดอัคคีภัย วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม แผ่นดินไหว วินาศภัย ก่อการร้าย	จัดทำแผนพัฒนาไซต์สำรอง (DR-Site)				←									ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
	ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ ดับเพลิง			↔			↔			↔			↔	ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
	จัดทำแผนบริหารความต่อเนื่องด้าน IT				↔	↔								ส่วนบริหารเทคโนโลยีฯ ศทส.
๑.๒ กระแสไฟฟ้าขัดข้อง ไฟฟ้า ดับ แรงดันไฟฟ้าไม่คงที่	บำรุงรักษาการทำงาน UPS	←												ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
	บำรุงรักษาการทำงานของ Generator	←												ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
๑.๓ คอมพิวเตอร์ถูกโจรกรรม	บำรุงรักษาและติดตั้งกล้องวงจรปิดให้ครอบคลุม และสามารถใช้งานได้อย่างต่อเนื่อง										↔	↔		-ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส. -ส่วนพัสดุ สบก.
๑.๔ ความเสี่ยงจากแมลงหรือ สัตว์กัดแทะสายไฟฟ้า หรือ สายสัญญาณ	ตรวจสอบและปรับปรุงสายไฟฟ้าและ สายสัญญาณ โดยห่อหุ้มวัสดุที่ป้องกันแมลงหรือ สัตว์กัดแทะ							↔	↔	↔				-ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส. -ส่วนพัสดุ สบก.
	จ้างกำจัดหนูและแมลง							↔	↔	↔				ส่วนพัสดุ สบก.
	รณรงค์รักษาความสะอาดในอาคาร	←												-ทุกหน่วยงาน
๑.๕ เกิดเหตุสถานการณ์ทาง การเมือง	จัดทำแผนพัฒนาไซต์สำรอง (DR-Site)				←									ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
	จัดทำแผนบริหารความต่อเนื่องด้าน IT					↔	↔							ส่วนบริหารเทคโนโลยีฯ ศทส.

[illegible]

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๔												ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๓.๒ การใช้งานระบบ Web Conference	มอบหมายเจ้าหน้าที่รับผิดชอบในการจองใช้งานระบบ GIN Conference				↔									ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	อบรมการติดตั้งและใช้งานระบบ Conference อย่างสม่ำเสมอ							↔						ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดหาอุปกรณ์ conference ที่ทันสมัยทดแทน											↔		ทุกหน่วยงาน
๓.๓ การติดไวรัสคอมพิวเตอร์หรือ Malware	ประกาศมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมป่าไม้									↔				ส่วนบริหารเทคโนโลยีฯ ศทส.
	ให้ความรู้แก่ผู้ใช้งาน ให้ตระหนักถึงภัยอันตรายที่เกิดจากไวรัส						↔							ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ และจัดการระบบสแกนไวรัสที่ทันสมัยและมีลิขสิทธิ์มาติดตั้งให้ครอบคลุมทุกเครื่องของผู้ใช้งาน	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	กำหนดสิทธิในการใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้งาน					↔								ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์														
๔.๑ การพัฒนาระบบสารสนเทศมีช่องโหว่	จัดหาผู้เชี่ยวชาญตรวจสอบช่องโหว่ของแอปพลิเคชันอย่างต่อเนื่อง เพื่อนำมาปรับปรุงระบบ						↔							ส่วนระบบสารสนเทศฯ ศทส.
	กำหนดมาตรฐานในการพัฒนาแอปพลิเคชัน เพื่อให้ใช้เป็นรูปแบบเดียวกัน						↔							ส่วนระบบสารสนเทศฯ ศทส.
	กำหนดมาตรฐานความปลอดภัยในการพัฒนาแอปพลิเคชัน เช่น มีการเข้ารหัส (encryption) ในฐานข้อมูลสำหรับปกปิดข้อมูลผู้ใช้และรหัสผ่าน						↔							ส่วนระบบสารสนเทศฯ ศทส.
๔.๒ การละเมิดลิขสิทธิ์โปรแกรม	รณรงค์ให้บุคลากรใช้งานโปรแกรมที่มีลิขสิทธิ์					↔								ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	รณรงค์ให้บุคลากรใช้ซอฟต์แวร์ Open Source					↔								ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๔												ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
	ให้ความรู้แก่บุคลากรถึงภัยและความผิดที่เกิดจากการใช้โปรแกรมละเมิดลิขสิทธิ์					←→								ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เพื่อรองรับการปฏิบัติงาน เช่น โปรแกรมสำนักงาน ระบบปฏิบัติการ					←→								ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๔.๓ ระบบงานสารสนเทศไม่ตอบสนองความต้องการของผู้ใช้งาน	ปรับปรุงระบบให้เป็นไปตามความต้องการของผู้ใช้งาน	←											→	ส่วนระบบสารสนเทศฯ ศทส.
๕. ความเสี่ยงด้านระบบเครือข่าย														
๕.๑ การเชื่อมโยงเครือข่ายล้มเหลว	จัดทำ TOR ให้ชัดเจนในเรื่องการให้บริการ เช่น การกำหนดค่าปรับ ในกรณีที่ผู้ให้บริการเครือข่ายไม่สามารถดำเนินการตาม TOR ได้	↔												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จ้างที่ปรึกษาวิเคราะห์และปรับปรุงระบบเครือข่ายคอมพิวเตอร์								←→					-ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส. -ส่วนอำนวยการ ศทส.
๕.๒ ไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center	จัดทำแผนพัฒนาไซต์สำรอง (DR-Site)				←								→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันไฟไหม้และอุปกรณ์ดับเพลิงให้อยู่ในสภาพพร้อมใช้งาน	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๓ ระบบไฟฟ้าห้อง Data Center ไม่เสถียร	ตรวจสอบระบบไฟฟ้าอย่างสม่ำเสมอ	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดทำแผนพัฒนาระบบติดตามและเฝ้าระวังระบบไฟฟ้าในห้อง Data Center											←→		ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๔ เครื่องแม่ข่ายและอุปกรณ์เครือข่ายไม่สามารถให้บริการได้อย่างมีประสิทธิภาพและต่อเนื่อง	จัดหาผู้เชี่ยวชาญด้านระบบเครือข่ายมาให้ความรู้และเพิ่มทักษะในการแก้ไขปัญหาเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้แก่เจ้าหน้าที่								←→					ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จ้างบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้พร้อมใช้งาน	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๔												ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
	จัดทำแผนการตรวจสอบความพร้อมใช้งานของ เครื่องแม่ข่ายและอุปกรณ์เครือข่าย				↔									-ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส. -ส่วนบริหารเทคโนโลยี สารสนเทศและการสื่อสาร ศทส.
	จัดทำหนังสือแจ้งเตือนผู้ใช้งานเครือข่ายที่ไม่ เหมาะสม			↔			↔			↔			↔	ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
๕.๕ การโจมตี (Hack) ระบบ เครือข่าย	ติดตั้งระบบป้องกันและเตือนภัย										↔			ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
	มอบหมายเจ้าหน้าที่คอยตรวจสอบเป็นประจำ	←											→	ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
	จัดหาระบบสำรองข้อมูล					↔								ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
	กำหนดรหัส (encryption) ระบบสารสนเทศ					↔								ส่วนระบบสารสนเทศฯ ศทส.
	จ้างที่ปรึกษาตรวจสอบหาช่องโหว่ของระบบ เครือข่าย								↔					ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
๕.๖ ระบบงานสารสนเทศของ กรมป่าไม้ไม่สามารถให้บริการได้	ตรวจสอบระบบสำรองข้อมูลและอุปกรณ์ อย่างสม่ำเสมอ			↔			↔			↔			↔	ส่วนระบบสารสนเทศฯ ศทส.
	ปรับปรุงเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล (Data base) เป็นแบบ Cluster						↔							ส่วนระบบคอมพิวเตอร์และ เครือข่าย ศทส.
๖. ความเสี่ยงด้านข้อมูล														
๖.๑ ข้อมูลและสารสนเทศไม่ ถูกต้องและเป็นปัจจุบัน	จัดฝึกอบรมการใช้งานระบบสารสนเทศอย่าง สม่ำเสมอ	←											→	ส่วนระบบสารสนเทศฯ ศทส.
	กำหนดมาตรการในการตรวจสอบข้อมูล ก่อนนำ ขึ้นเผยแพร่บนเว็บไซต์				↔									ส่วนระบบสารสนเทศฯ ศทส.
	มอบหมายให้เจ้าหน้าที่ปรับปรุงข้อมูลให้ ครบถ้วนเป็นปัจจุบัน	←											→	ทุกหน่วยงาน

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๔												ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๖.๒ การสำรองข้อมูลไม่มีประสิทธิภาพ	จ้างผู้เชี่ยวชาญบำรุงรักษาระบบและบริหารจัดการการสำรองข้อมูลอย่างต่อเนื่อง	←												-ส่วนระบบสารสนเทศฯ ศทส. -ส่วนอำนวยการ ศทส.
	ทดสอบการนำข้อมูลกลับคืนสู่ระบบ			↔			↔			↔			↔	ส่วนระบบสารสนเทศฯ ศทส.
	จัดหาระบบสำรองข้อมูลที่มีประสิทธิภาพ			↔			↔			↔			↔	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๖.๓ การรั่วไหลจากการเปลี่ยนมือผู้ใช้	จัดทำแนวทางในการตรวจสอบสิทธิการใช้งานและยกเลิกสิทธิการใช้งานของผู้ใช้ข้อมูล					↔	↔							ส่วนระบบสารสนเทศฯ ศทส.

พิจารณาเห็นชอบดำเนินการ

ลงชื่อ.....
(.....)
ตำแหน่ง.....

การติดตามผลและรายงานผล

การติดตามผล

เป็นการติดตามผลหลังจากที่ได้ดำเนินการตามแผนการบริหารจัดการความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารจัดการความเสี่ยงนั้นมีประสิทธิภาพ รวมทั้งสาเหตุของความเสี่ยงที่มีผลต่อความสำเร็จ ความรุนแรงของผลกระทบ วิธีการจัดการความเสี่ยง รวมถึงแนวทางการจัดการความเสี่ยง มีความเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป และรับทราบปัญหาอุปสรรคที่เกิดขึ้นจากการดำเนินการตามกิจกรรมที่กำหนดไว้ในแผนบริหารความเสี่ยง รวมทั้งข้อเสนอแนะ เพื่อนำไปใช้ประกอบการพิจารณาทบทวนและกำหนดแผนบริหารความเสี่ยงของกรมป่าไม้ในปีงบประมาณถัดไป

การรายงานผล

เป็นการรายงานผลการวิเคราะห์และจัดการความเสี่ยงว่า กิจกรรมที่ใช้ในการจัดการความเสี่ยงใดที่มีประสิทธิภาพ ควรดำเนินการต่อเนื่อง วิธีการจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามดังกล่าวมาจัดทำรายงาน โดยให้หน่วยงานที่รับผิดชอบตามกิจกรรม ดำเนินการจัดทำแบบรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๔ และส่งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ภายในวันที่ ๓๐ กันยายน ๒๕๖๔ จากนั้นให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการวิเคราะห์ผลจากแบบรายงานดังกล่าว จัดทำรายงานผล เสนอต่ออธิบดีกรมป่าไม้เพื่อรับทราบและใช้เป็นเครื่องมือหรือข้อมูลประกอบการบริหารราชการกรมป่าไม้ต่อไป

รายงานผลการดำเนินงานตามบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๔

ความเสี่ยง.....
ผู้รับผิดชอบ.....
วันที่รายงาน.....

ความเสี่ยง	กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความ คืบหน้า	ปัญหาอุปสรรคและ แนวทางการแก้ไข

ภาคผนวก



บันทึกข้อความ

ส่วนราชการ กรมป่าไม้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐๒๕๖๑๔๒๙๒ ต่อ ๕๗๕๔

ที่ ทส ๑๖๑๒.๑/ ๒๒๗๒๐

วันที่ ๑๓ พฤศจิกายน ๒๕๖๓

เรื่อง แต่งตั้งคณะกรรมการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

เรียน รองอธิบดีกรมป่าไม้ทุกท่าน

ผู้ตรวจราชการกรมป่าไม้ทุกท่าน

ผู้อำนวยการสำนักทุกสำนัก

ผู้อำนวยการสำนักจัดการทรัพยากรป่าไม้ ที่ ๑ - ๑๓

ผู้อำนวยการสำนักจัดการทรัพยากรป่าไม้สาขาทุกสาขา

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร

หัวหน้ากลุ่มตรวจสอบภายใน

หัวหน้ากลุ่มคุ้มครองจริยธรรมกรมป่าไม้

กรมป่าไม้ ขอส่งสำเนาคำสั่งกรมป่าไม้ ที่ ๓๙๗๑ /๒๕๖๓ ลงวันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๖๓ เรื่อง แต่งตั้งคณะกรรมการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ มาเพื่อโปรดทราบ สำหรับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้แจ้งผู้มีรายชื่อตามคำสั่งทราบ และถือปฏิบัติ

(นายอดิสร นุชดำรงค์)
อธิบดีกรมป่าไม้

สำเนา

คำสั่งกรมป่าไม้

ที่ ๓๙ ๗๑ /๒๕๖๓

เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

ตามคำสั่งกรมป่าไม้ ที่ ๓๐๐๙/๒๕๖๓ ลงวันที่ ๑ กันยายน พ.ศ. ๒๕๖๓ เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ เพื่อเป็นการเตรียมความพร้อม และลดความเสี่ยงจากสถานการณ์ฉุกเฉินต่าง ๆ เช่น ภัยคุกคาม ไวรัส ไฟดับ ไฟไหม้ ที่อาจจะเกิดขึ้น ซึ่งจะส่งผลกระทบและก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ นั้น

กรมป่าไม้พิจารณาแล้ว เพื่อให้การจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ เป็นไปอย่างมีประสิทธิภาพ และบรรลุตามวัตถุประสงค์ จึงอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และแก้ไขเพิ่มเติม และระเบียบสำนักนายกรัฐมนตรีว่าด้วยพนักงานราชการ พ.ศ. ๒๕๔๗ จึงให้ยกเลิกคำสั่งกรมป่าไม้ ที่ ๓๐๐๙/๒๕๖๓ ลงวันที่ ๑ กันยายน พ.ศ. ๒๕๖๓ และแต่งตั้งคณะทำงานเพื่อดำเนินการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ โดยมีองค์ประกอบและอำนาจหน้าที่ ดังนี้

๑. องค์ประกอบ

๑.๑ นายอภิรักษ์ ทหรานนท์	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	หัวหน้าคณะทำงาน
๑.๒ นางสาวณัฐฉิณี ปิ่นเนียม	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๓ นายทองศักดิ์ มนต์รี	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๔ นายประพันธ์พงษ์ คงศรีรอด	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๕ นายวีร์ ศรีทิพโพธิ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๑.๖ นางสาวนรนนท์ อภิขนาพงศ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๑.๗ นางสาวปรียานุช กิจสิทธิโชค	นักจัดการงานทั่วไป	คณะทำงาน
๑.๘ นายณภัทร์ ดลเสถียร	นักจัดการงานทั่วไป	คณะทำงาน
๑.๙ นางสาวจิราภรณ์ เพิ่มศิริวานิชย์	นักจัดการงานทั่วไป	คณะทำงาน
๑.๑๐ นายกิตติทัศน์ สุริยา	นักวิชาการคอมพิวเตอร์	คณะทำงาน
๑.๑๑ นายถนอมธรร เพ็ลนิมลัย	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน
๑.๑๒ นายภาคิน กรณ์ธนฤต	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน
๑.๑๓ ว่าที่ ร.ต.หญิงพรพิมล แก่นโท	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน
๑.๑๔ นางสาวชนันเนตร ภูแผ่นนา	เจ้าพนักงานธุรการ	คณะทำงาน

/๑.๑๕ นายวีระพล...

๑.๑๕ นายวีระพล บุประเสริฐ	เจ้าหน้าที่ธุรการ	คณะทำงาน
๑.๑๖ นางสาวจุฬารัตน์ นัยฉิม	เจ้าหน้าที่ธุรการ	คณะทำงาน
๑.๑๗ นางสาวสพินนา อ่อนเพ็ง	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน และเลขานุการ
๑.๑๘ นายวิบูลย์ชัย ปาสองห้อง	นักจัดการงานทั่วไป	คณะทำงาน และผู้ช่วยเลขานุการ

๒. อำนาจหน้าที่

ให้คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ มีอำนาจหน้าที่ดังต่อไปนี้

๒.๑ ทบทวน และวิเคราะห์ให้ความคิดเห็นในการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

๒.๒ เสนอแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ต่อผู้บริหารเพื่อให้ความเห็นชอบ

๒.๓ แจ้งเวียน เผยแพร่ แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ให้แก่บุคลากรกรมป่าไม้ทราบ และแจ้งผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

๒.๔ สรุปรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ เสนอต่อผู้บริหารทราบ

๒.๕ ประสาน และปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๖๓

(ลงนาม) อติสร นุชดำรงค์
(นายอติสร นุชดำรงค์)
อธิบดีกรมป่าไม้

สำเนาถูกต้อง

- ๐๖ -

(นางสาวสพินนา อ่อนเพ็ง)
นักวิชาการคอมพิวเตอร์ชำนาญการ