



แผนบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ กรมป่าไม้

ปีงบประมาณ พ.ศ. 2569

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สารบัญ

<u>เรื่อง</u>	<u>หน้า</u>
<u>บทนำ</u>	
- หลักการและเหตุผล	๑
- วัตถุประสงค์	๑
<u>ข้อมูลพื้นฐานของหน่วยงาน</u>	
- วิสัยทัศน์	๒
- พันธกิจ	๒
- ภารกิจ	๒
- แนวทางการพัฒนา	๓
- อัตรากำลัง	๓
- สถานภาพด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้	๓
- สถานภาพด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้	๔
- สถานภาพด้านระบบเครือข่ายและการสื่อสาร กรมป่าไม้	๔
<u>กระบวนการบริหารความเสี่ยง</u>	
- คำนิยามความเสี่ยง	๕
- ความหมายของการบริหารความเสี่ยง	๕
- กระบวนการบริหารความเสี่ยง	๖
- บทบาท หน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยง	๑๐
<u>การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ</u>	
- ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๑
- การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๒
- ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๒
- ตารางวิเคราะห์แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๙	๑๔
- แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๙	๒๒
<u>การติดตามและรายงานผล</u>	
- การติดตามผลและรายงานผล	๒๘
- แบบฟอร์มรายงานผลการดำเนินงาน	๒๙
<u>ภาคผนวก</u>	
- คำสั่งแต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้	

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้

ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

บทนำ

หลักการและเหตุผล

กรมป่าไม้จำเป็นต้องจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ICT Risk Management Plan) เพื่อให้การดำเนินงานตามภารกิจหลักด้านป่าไม้เป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ เนื่องจากเทคโนโลยีสารสนเทศ เป็นปัจจัยสำคัญในการขับเคลื่อนองค์กรให้บรรลุเป้าหมาย แต่ก็มีความเสี่ยงหลากหลายรูปแบบ เช่น ภัยคุกคามทางไซเบอร์ ข้อมูลสูญหาย ระบบล่ม หรือการไม่ปฏิบัติตามกฎหมาย การบริหารความเสี่ยงจึงเป็นเครื่องมือสำคัญในการระบุ ประเมิน และจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบและเป็นรูปธรรม เพื่อลดผลกระทบ ความเสียหาย และความไม่แน่นอนที่อาจเกิดขึ้น อันจะนำไปสู่การป้องกัน รักษาความมั่นคงปลอดภัย และสร้างความเชื่อมั่นในการใช้เทคโนโลยีสารสนเทศของกรมป่าไม้ได้อย่างยั่งยืน

วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพและพร้อมใช้งาน
๒. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างต่อเนื่อง และมีประสิทธิภาพ
๓. เพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

ข้อมูลพื้นฐานของหน่วยงาน

วิสัยทัศน์

เป็นองค์กรที่มุ่งเน้นการรักษาป่าเดิม เพิ่มป่าใหม่ ใส่ใจประชาชน บนรากฐานนวัตกรรม และธรรมาภิบาล

พันธกิจ

๑. ป้องกันและรักษาป่าพื้นที่ป่าไม้ให้คงอยู่
๒. เพิ่มพื้นที่ป่าเศรษฐกิจ สนับสนุนการเพิ่มพื้นที่สีเขียว และฟื้นฟูพื้นที่ป่าไม้ให้อุดมสมบูรณ์
ตอบสนองความต้องการทั้งด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม
๓. บริหารจัดการทรัพยากรป่าไม้โดยการมีส่วนร่วม
๔. บริหารจัดการที่ดินป่าไม้อย่างเป็นระบบและเป็นธรรม เพื่อให้คนอยู่ร่วมกันกับป่าอย่างสมดุลและยั่งยืน
๕. วิจัยและพัฒนา เพื่อสร้างนวัตกรรม และถ่ายทอดเทคโนโลยีในการอนุรักษ์ และการใช้ประโยชน์
ทรัพยากรป่าไม้
๖. ส่งเสริมการจัดการพื้นที่ป่าไม้ เพื่อการนันทนาการ และการท่องเที่ยวเชิงนิเวศ บริหารจัดการ
โดยการมีส่วนร่วมของทุกภาคส่วน
๗. พัฒนาความสามารถเชิงรุกขององค์กร ทั้งระบบ กลไก ข้อมูลสารสนเทศ และปรับปรุงกฎระเบียบ
ให้ทันสมัย ให้เหมาะสมกับภาวะการณ์ปัจจุบัน

ภารกิจ

กรมป่าไม้มีภารกิจเกี่ยวกับการอนุรักษ์ สงวน คุ้มครอง ฟื้นฟู ดูแลรักษา ส่งเสริม ทำนุบำรุงป่า และการดำเนินการเกี่ยวกับการป่าไม้ การทำไม้ การเก็บหาของป่า การใช้ประโยชน์ที่ดินป่าไม้และการอื่น
เกี่ยวกับป่า และอุตสาหกรรมป่าไม้ ให้เป็นไปตามระเบียบและกฎหมายที่เกี่ยวข้อง ด้วยกลยุทธ์การเสริมสร้าง
ความร่วมมือของประชาชนเป็นหลัก เพื่อเพิ่มมูลค่าทางเศรษฐกิจของประเทศ และพัฒนาคุณภาพชีวิตของ
ประชาชน และมีภารกิจอื่นตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรมป่าไม้ โดยมีอำนาจหน้าที่ ดังนี้

๑. ควบคุม กำกับ ดูแล ป้องกันการบุกรุก การทำลายป่า และการกระทำความผิดในพื้นที่รับผิดชอบตาม
กฎหมายว่าด้วยการป่าไม้ กฎหมายว่าด้วยป่าสงวนแห่งชาติ กฎหมายว่าด้วยสวนป่า กฎหมายว่าด้วย
เลื่อยโซยนต์ กฎหมายว่าด้วยป่าชุมชน และกฎหมายอื่นที่เกี่ยวข้อง
๒. ศึกษา วิจัย วางแผน และประสานงานเกี่ยวกับการปลูกป่า เพื่อการฟื้นฟูสภาพป่าและระบบนิเวศ
๓. ส่งเสริมการปลูกป่า การจัดการป่าชุมชน และการปลูกสร้างสวนป่าเชิงเศรษฐกิจ ในลักษณะสวนป่า
ภาคเอกชนและสวนป่าในรูปแบบอื่นที่เกี่ยวข้อง ตลอดจนศึกษา วิเคราะห์ และประเมินสถานการณ์ป่า
เศรษฐกิจของตลาดในประเทศและต่างประเทศ
๔. อนุรักษ์ คุ้มครอง ดูแลรักษา และจัดการให้มีการใช้ประโยชน์ที่ดินป่าไม้ และการอนุญาตที่
เกี่ยวข้องกับการใช้ประโยชน์จากไม้ อุตสาหกรรมไม้ ที่ดินป่าไม้ และผลิตผลป่าไม้
๕. ศึกษา ค้นคว้า วิจัย และพัฒนาที่เกี่ยวข้องกับป่าไม้และผลิตผลป่าไม้ และที่เกี่ยวข้องกับไม้และ
ผลิตภัณฑ์ไม้
๖. ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรมหรือตามที่กระทรวงหรือ
คณะรัฐมนตรีมอบหมาย

แนวทางการพัฒนา

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

อัตรากำลัง

กรมป่าไม้ มีอัตรากำลังทั้งสิ้น ๘,๖๒๔ อัตรา แบ่งออกเป็น ๓ ประเภท ดังนี้

- ข้าราชการ	๑,๖๐๒	อัตรา
- ลูกจ้างประจำ	๓๓๐	อัตรา
- พนักงานราชการ	๖,๖๙๒	อัตรา

หมายเหตุ ข้อมูล ณ วันที่ ๑๗ พฤศจิกายน ๒๕๖๘

สถานภาพด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้

กรมป่าไม้ มีระบบงานที่ใช้ในการปฏิบัติงาน มีรายละเอียดดังนี้

๑. ระบบข้อมูลสารสนเทศทรัพยากรบุคคลระดับกรม
๒. ระบบบุคลากร เงินเดือน และสวัสดิการ
๓. ระบบรับรองไม้ และส่งออกไม้ และผลิตภัณฑ์จากไม้
๔. ระบบสารบรรณอิเล็กทรอนิกส์ กรมป่าไม้
๕. ระบบติดตามการบุกรุกทำลายป่า
๖. ระบบเว็บไซต์กรมป่าไม้
๗. ระบบอีเมลกรมป่าไม้
๘. ระบบ National Single Window (NSW)
๙. ระบบฐานข้อมูลความหลากหลายทางชีวภาพ
๑๐. ระบบสวนป่าออนไลน์
๑๑. ระบบแจกจ่ายกล้าไม้
๑๒. ระบบอนุญาตอุตสาหกรรมป่าไม้
๑๓. ระบบแผนงาน งบประมาณ และติดตามประเมินผล
๑๔. ระบบฐานข้อมูลเชิงแผนที่ของกรมป่าไม้
๑๕. ระบบเครือข่ายคอมพิวเตอร์เสมือน
๑๖. ระบบตรวจสอบและติดตามการทำงานของเครือข่าย (e-Monitoring)
๑๗. ระบบด่านป่าไม้
๑๘. ระบบขอตรวจพิสูจน์ไม้
๑๙. ระบบพิทักษ์ไพร
๒๐. ระบบบริหารจัดการข้อมูลการเบิกจ่ายเงิน
๒๑. ระบบรับเงินกลางอิเล็กทรอนิกส์
๒๒. ระบบบริหารงานทะเบียนครุภัณฑ์กรมป่าไม้

สถานภาพด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร

๑. อุปกรณ์ควบคุมอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Controller) จำนวน ๑ เครื่อง
๒. อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) จำนวน ๑๔๒ เครื่อง
๓. อุปกรณ์กระจายสัญญาณอาคาร (Core Switch BL) จำนวน ๔ เครื่อง
๔. อุปกรณ์กระจายสัญญาณ (Access Switch) จำนวน ๓๗ เครื่อง
๕. อุปกรณ์บันทึกภาพแบบไอพี (Network Video Recorder) จำนวน ๑ เครื่อง
๖. กล้องโทรทัศน์วงจรปิดแบบไอพี (IP Camera) จำนวน ๑๐ เครื่อง
๗. เครื่องสแกนลายนิ้วมือ (Finger Scan) จำนวน ๑ เครื่อง
๘. อุปกรณ์ป้องกันเครือข่าย (Firewall) จำนวน ๑ เครื่อง
๙. อุปกรณ์กระจายสัญญาณย่อย (Switch External) จำนวน ๑ เครื่อง
๑๐. อุปกรณ์ค้นหาเส้นทาง Router จำนวน ๒ เครื่อง
๑๑. อุปกรณ์ Info box อุปกรณ์แจกหมายเลข IP และ DNS จำนวน ๒ เครื่อง
๑๒. อุปกรณ์กระจายสัญญาณย่อย (DMZ Switch) จำนวน ๔ เครื่อง
๑๓. อุปกรณ์กระจายสัญญาณหลัก (Core Switch) จำนวน ๒ เครื่อง
๑๔. เครื่องสำรองไฟฟ้า ขนาด ๒๐ kVA จำนวน ๒ เครื่อง
๑๕. เครื่องสำรองไฟฟ้า ขนาด ๑๕ KVA จำนวน ๑ เครื่อง
๑๖. เครื่องสำรองไฟฟ้า ขนาด ๑ KVA จำนวน ๑๗ เครื่อง
๑๗. เครื่องปรับอากาศควบคุมอุณหภูมิและความชื้น จำนวน ๒ เครื่อง
๑๘. เครื่องกำเนิดไฟฟ้า (Generator) จำนวน ๑ เครื่อง
๑๙. เครื่องควบคุมการสลับสัญญาณไฟฟ้า (ATS) จำนวน ๑ เครื่อง
๒๐. เครื่องตรวจจับควันความไวสูง จำนวน ๑ เครื่อง
๒๑. เครื่องตรวจจับน้ำรั่วซึม จำนวน ๑ เครื่อง
๒๒. เครื่องเฝ้าดูและแจ้งเตือนอัตโนมัติ (SMS Server) จำนวน ๑ เครื่อง
๒๓. เครื่องวัดอุณหภูมิห้องปฏิบัติการคอมพิวเตอร์ (Data Center) จำนวน ๑ เครื่อง

สถานภาพด้านระบบเครือข่ายและการสื่อสาร กรมป่าไม้

๑. ระบบเครือข่ายของกรมป่าไม้ ซึ่งมีการเชื่อมต่ออินเทอร์เน็ตจำนวน ๓ คู่สาย เครือข่ายทูลความเร็ว ๙๐๐/๔๐๐ Mbps เครือข่าย UIH ความเร็ว ๘๐๐/๓๐๐ Mbps และเครือข่าย DG-Link ความเร็ว ๓๐๐/๓๐๐ Mbps

๒. การดำเนินการด้านการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายด้านความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย นั้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการปรับปรุงระบบเครือข่ายให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อให้ระบบคอมพิวเตอร์และเครือข่ายกรมป่าไม้ มีความมั่นคงปลอดภัยจากบุคคลผู้ไม่มีสิทธิในการเข้าถึงข้อมูล

กระบวนการบริหารความเสี่ยง

คำนิยามความเสี่ยง

ความเสี่ยง หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตาม วัตถุประสงค์และเป้าหมายที่กำหนด

การประเมินความเสี่ยง หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยง หรือการบริหารความเสี่ยง

การวิเคราะห์ความเสี่ยง หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นตอนต่อไปคือ การวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเพราะการวัดความเสี่ยงเป็นตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก 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 กระบวนการที่ใช้ในการบริหารจัดการให้อาสาที่จะเกิดความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้

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

๑) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสียหายและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างขององค์กร 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)

เพื่อเป็นกรอบการดำเนินงานในแต่ละระดับให้สามารถวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นได้อย่างครบถ้วน โดยจะยึดหลักการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Annex A) โดยมีหัวข้อดังต่อไปนี้

- ๑) นโยบายความมั่นคงปลอดภัย (Security policy)
- ๒) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)
- ๓) การบริหารจัดการทรัพย์สินขององค์กร (Asset management)
- ๔) ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (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 ที่ได้กล่าวอ้างจากการกำหนดเป้าหมายการบริหารความเสี่ยงข้างต้นมาพิจารณาระบุความเสี่ยง โดยมีรายละเอียดดังนี้

- ๑) นโยบายความมั่นคงปลอดภัย (Security policy)
 - นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ
- ๒) โครงสร้างทางด้านการมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)
 - โครงสร้างทางด้านการมั่นคงปลอดภัยภายในองค์กร
 - โครงสร้างทางด้านการมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานภายนอก
- 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
 - การบริหารจัดการทางด้านการมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร
 - การจัดการสื่อที่ใช้ในการบันทึกข้อมูล
 - การแลกเปลี่ยนสารสนเทศ
 - การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์
 - การเฝ้าระวังทางด้านการมั่นคงปลอดภัย
- 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 คูณ แนวนอน)

ผลกระทบ (ความรุนแรง)	สูงมาก/ หายหน้า	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 ๑ ครั้ง)	๑
น้อย	ไม่บ่อย (อาจเกิดขึ้นได้ทุกไตรมาส)	๒
ปานกลาง	ปานกลาง (อาจเกิดขึ้นได้ทุกเดือน)	๓
สูง	บ่อย (อาจเกิดขึ้นได้ทุกสัปดาห์)	๔
สูงมาก	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)	๕

หลักเกณฑ์การประเมินผลกระทบ (Impact) ที่จะเกิดความเสี่ยง

ผลกระทบ (ความรุนแรง)	ผลกระทบที่จะเกิดเหตุการณ์	ระดับคะแนน
น้อยมาก	เกิดเหตุไม่มีความสำคัญ	๑
น้อย	เกิดเหตุเล็กน้อยที่แก้ไขได้	๒
ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก	๓
สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบ ความปลอดภัยซึ่งส่งผลกระทบต่อความถูกต้องของ ข้อมูลบางส่วน	๔
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลกรมป่าไม้	๕

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 ขึ้นไป ให้นำมาดำเนินการจัดทำแผนบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ตามแบบฟอร์มที่กำหนด ประกอบด้วย ประเด็นความเสี่ยง กิจกรรม ตามแนวทางการจัดการความเสี่ยง เป้าหมาย/ผลสำเร็จของการดำเนินกิจกรรมตามแนวทางการจัดการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ระยะเวลาดำเนินการ ผู้รับผิดชอบ งบประมาณ

๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

จัดให้มีการสื่อสารข้อมูลที่ต้องการผ่านช่องทางการสื่อสารไปยังกลุ่มเป้าหมายที่กำหนด เพื่อให้บุคคลที่เกี่ยวข้องได้รับทราบการข้อมูลและนำไปสู่การปฏิบัติ

๗. การติดตามผลและเฝ้าระวังความเสี่ยง (Monitoring)

กำหนดให้มีการติดตามการประเมินผลการดำเนินงานตามระยะเวลาที่กำหนดไว้ดังนี้

- เดือนกรกฎาคม – กันยายน พ.ศ. ๒๕๖๔ เฝ้าระวังและติดตามผลความเสี่ยง
- เดือนตุลาคม – พฤศจิกายน พ.ศ. ๒๕๖๔ จัดทำสรุปและรายงานผลการเฝ้าระวัง

บทบาทหน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยง

๑) ผู้บริหารระดับสูงทำหน้าที่กำหนดนโยบายและแต่งตั้งคณะกรรมการหรือคณะทำงานในการกำกับดูแลให้มีการดำเนินการตามแผนบริหารความเสี่ยง

๒) คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ จัดทำวิธีปฏิบัติด้านเทคโนโลยีสารสนเทศ เพื่อบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้

๓) ผู้บริหารระดับสำนัก/กอง/ศูนย์ ดำเนินการบริหารความเสี่ยงในหน่วยงาน รวมทั้งติดตามประเมินผล

๔) บุคลากรในหน่วยงาน ดำเนินการตามแผนบริหารความเสี่ยงตามที่กำหนด อย่างถูกต้อง ครบถ้วน

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการศึกษาค้นคว้า ประกอบกับการตรวจสอบหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการ และการควบคุมความเสี่ยงด้านสารสนเทศของกรมป่าไม้ พิจารณาแล้วเห็นว่าความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับกรมป่าไม้สามารถ แบ่งออกเป็น ๔ ประเภทหลัก ดังนี้

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

๒. Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานที่ได้รับผิดชอบไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

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

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

ขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้าน และมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการปฏิบัติราชการ และการไม่ได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรอบรู้ และเชี่ยวชาญในงานที่ได้รับมอบ

นอกจากความเสี่ยง ๔ ประเภทหลักตามที่กล่าวข้างต้น ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นความเสี่ยงหนึ่งที่ทำให้เกิดผลกระทบต่อระบบฐานข้อมูลกรมป่าไม้ เนื่องด้วยความเสี่ยงดังกล่าว อาจทำให้ระบบขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อภาพรวมของระบบฐานข้อมูลกรมป่าไม้ จึงจำเป็นต้องมีการจัดทำระบบบริหารจัดการความเสี่ยงและแผนแก้ไขปัญหาที่อาจเกิดขึ้นและแนวทางป้องกันต่อไป

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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

ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้คือ

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

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

๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาด ช้องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายอุปกรณ์โดยไม่ได้รับอนุญาต การติดตั้งอุปกรณ์ในพื้นที่ที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ เป็นต้น

๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่าง ๆ ที่จัดทำและพัฒนาขึ้น 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 อันอาจจะก่อให้เกิดความเสียหาย 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. ๒๕๖๙

ความเสี่ยง(ภาวะ คุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม									
๑.๑ เกิดอัคคีภัย วาตภัย อุทกภัย ไฟป่า น้ำท่วม แผ่นดินไหว วินาศภัย ก่อการร้าย	-การสูญหายและถูกทำลาย ของอุปกรณ์ -เกิดความเสียหายด้าน โครงสร้างอาคาร -ความเสียหายของเครื่อง คอมพิวเตอร์และอุปกรณ์	-เสี่ยงประมาณในการจัดหา ระบบทดแทน -ไม่สามารถใช้งานระบบระหว่าง ที่มีการจัดหาระบบทดแทน -เสียเวลาในการกู้ระบบ	๑	๕	๕	-จัดทำแผนรองรับ สถานการณ์ฉุกเฉิน -จัดทำแผนบริหารความ ต่อเนื่องด้าน IT -ติดตั้งอุปกรณ์ดับเพลิง -จัดเก็บระบบและข้อมูล บน cloud ของ หน่วยงานอื่น -จัดทำป้ายแสดงขั้นตอน แนวทางปฏิบัติเมื่อเกิด กรณีฉุกเฉิน -มีระบบตรวจจับควัน ความไวสูง	-มีการจัดเก็บระบบ และข้อมูลบน cloud แค่บางระบบ -ไม่ได้มีการดูแล อุปกรณ์ดับเพลิง อย่างต่อเนื่อง -สารที่ใช้ในการดับไฟ เป็นสารที่ไม่ เหมาะสมกับการดับ ไฟในห้อง Data Center	ลด	-ตรวจสอบความพร้อมของ การใช้งานอุปกรณ์ดับเพลิง -ทบทวนแผนบริหารความ ต่อเนื่องด้าน IT -จัดทำและซักซ้อมแผน รองรับสถานการณ์ฉุกเฉิน -จัดทำร่างโครงการเพื่อ ขอรับงบประมาณในการ ปรับปรุงระบบดับเพลิง ใน ปีงบประมาณ พ.ศ. ๒๕๖๑
๑.๒ กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่ คงที่	-แหล่งจ่ายไฟฟ้าหลักขัดข้อง -ผู้ควบคุมการจ่ายไฟฟ้าหลัก ของอาคารขัดข้อง	-ไม่สามารถใช้งานระบบได้ -ข้อมูลเสียหาย -ระบบปฏิบัติการ โปรแกรม หรือ ฐานข้อมูลเสียหาย ต้องมีการ ติดตั้งใหม่ -อุปกรณ์คอมพิวเตอร์ เช่น เครื่อง แม่ข่ายเสียหาย	๓	๓	๙	-ติดตั้งเครื่องสำรอง ไฟฟ้า (UPS) -ติดตั้งเครื่องกำเนิด ไฟฟ้า (Generator)	-เบื้องต้นสามารถ ควบคุมความเสียหาย ได้ระดับหนึ่ง	ลด	-บำรุงรักษาการทำงาน เครื่องสำรองไฟฟ้า (UPS) -บำรุงรักษาการทำงานของ เครื่องกำเนิดไฟฟ้า (Generator) และบริเวณ โดยรอบ

ความเสี่ยง(ภาวะ คุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๒. ความเสี่ยงด้านบุคลากร									
๒.๑ บุคลากรสายงาน คอมพิวเตอร์ขาดทักษะ และความรู้ที่ทันสมัยใน การปฏิบัติงานด้าน คอมพิวเตอร์และกฎหมาย ที่เกี่ยวข้อง	-เจ้าหน้าที่ปฏิบัติงานไม่ตรง ตามสายงาน -มีการเปลี่ยนงานบ่อย	-เจ้าหน้าที่ไม่สามารถใช้งาน ระบบได้ -เจ้าหน้าที่ไม่สามารถแก้ไขปัญหา ได้	๒	๓	๖	-จัดทำคู่มือการ ปฏิบัติงานด้าน คอมพิวเตอร์ -มีการจัดการความรู้ (KM) ในการทำงาน ด้านเทคโนโลยี สารสนเทศ เพื่อเป็น แนวทางในการแก้ปัญหา	-สามารถควบคุม ความเสี่ยงได้ในระดับ หนึ่ง	ลด	-จัดอบรมให้ความรู้ด้าน คอมพิวเตอร์ที่ทันสมัยและ กฎหมายที่เกี่ยวข้องให้แก่ เจ้าหน้าที่อย่างสม่ำเสมอ -ส่งเสริมให้เจ้าหน้าที่เข้า อบรมผ่าน e-Learning -ส่งเจ้าหน้าที่เข้ารับการ อบรมในหลักสูตรที่จำเป็น
๒.๒ เจ้าหน้าที่ใช้ คอมพิวเตอร์หรือ เครือข่ายผิดวัตถุประสงค์	-ใช้งานในทางที่ผิด เช่น ดูหนัง เล่นเกมพนัน เล่นเกมส์ เป็น ต้น -ดาวน์โหลดโปรแกรมที่ไม่มี ลิขสิทธิ์ -ดาวน์โหลดหนังออนไลน์	-ทำให้สูญเสีย Bandwidth ใน เครือข่าย -อาจถูกร่องเรียนหรือฟ้องร้อง จากบุคคลภายนอก -อาจทำให้เครื่องติดไวรัส	๒	๓	๖	-มีการกำหนด policy ของ Firewall ให้ เหมาะสม -ตรวจสอบและรายงาน การใช้งานของผู้ใช้งาน ผิดวัตถุประสงค์ต่อ ผู้บังคับบัญชา	-สามารถควบคุม ความเสี่ยงได้ในระดับ หนึ่ง	ลด	-กำหนด policy ของ Firewall ให้เหมาะสมอย่าง สม่ำเสมอ เปิด port เท่าที่ จำเป็น -ให้ความรู้แก่บุคลากรใน เรื่องการใช้คอมพิวเตอร์ และระบบเครือข่ายอย่าง เหมาะสมและสม่ำเสมอ -ตรวจสอบและรายงานการ ใช้งานของผู้ใช้งานผิด วัตถุประสงค์ต่อ ผู้บังคับบัญชา

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ									
๓.๑ การใช้งานระบบ วิดิทัศน์ทางไกล (Video Conference System) ไม่ชัดเจน	-สัญญาณเครือข่ายขัดข้อง -อุปกรณ์ Conference ของ หน่วยงานส่วนกลางที่ตั้งอยู่ใน ส่วนภูมิภาคบางหน่วยงานยังไม่ ทันสมัย	-ไม่สามารถเชื่อมต่อระบบได้ -ภาพไม่ชัดเจน -เสียงไม่ออก	๒	๓	๖	-จัดเจ้าหน้าที่ตรวจสอบ ติดตามการใช้งานระบบ Conference ให้แก่ หน่วยงานส่วนกลางที่ ตั้งอยู่ในส่วนภูมิภาค -ติดตั้งระบบเครือข่าย DG Link ให้แก่ หน่วยงานภูมิภาค	-สามารถลดความ เสี่ยงได้ในระดับหนึ่ง	ลด	-จัดเจ้าหน้าที่ตรวจสอบ ติดตามการใช้งานระบบ Conference ให้แก่ หน่วยงานส่วนกลางที่ตั้งอยู่ ในส่วนภูมิภาค
๓.๒ การติดไวรัส คอมพิวเตอร์หรือ Malware	-การต่อพ่วงกับอุปกรณ์ทาง คอมพิวเตอร์ที่ยังไม่ได้รับการ ตรวจสอบไวรัส (Scan Virus) -การดาวน์โหลดและติดตั้ง ซอฟต์แวร์ที่ไม่รู้แหล่งที่มา -การเข้าเว็บไซต์ที่มีความเสี่ยง และฝัง Spyware ไว้ เช่น เว็บไซต์ดาวน์โหลดโปรแกรม ฟรี, ภาพยนตร์ฟรี เป็นต้น -การเปิดอีเมลที่มีการแนบไฟล์ ที่ไม่รู้จักและไม่รู้แหล่งที่มา	-ไม่สามารถใช้คอมพิวเตอร์ได้ -ไม่สามารถใช้ระบบงานได้ -ข้อมูลสูญหาย -ทำให้มีปริมาณข้อมูลจราจร คอมพิวเตอร์ (Traffic) ที่เป็น อันตรายต่อระบบเครือข่ายและ สารสนเทศเป็นจำนวนมาก	๕	๕	๒๕	-ติดตั้งโปรแกรมป้องกัน ไวรัส (Anti-Virus) ให้ ผู้ใช้งานบางส่วน -ประกาศมาตรฐานการ รักษาความปลอดภัย ด้านเทคโนโลยี สารสนเทศของกรมป่า ไม้ -ให้ความรู้แก่ผู้ใช้งาน ให้ ตระหนักถึงภัยอันตราย ที่เกิดจากไวรัส -กำหนด Policy Firewall ให้ป้องกันการ เข้าใช้งานเว็บไซต์ที่เป็น อันตราย	-ผู้ใช้งานบางคนไม่ ให้ความร่วมมือ -เจ้าหน้าที่ดูแลไม่ ทั่วถึง -ไม่สามารถจัดหา โปรแกรมป้องกัน ไวรัสให้ครอบคลุม	ลด	-ให้ความรู้แก่ผู้ใช้งาน ให้ ตระหนักถึงภัยอันตรายที่ เกิดจากไวรัสอย่างต่อเนื่อง -อัปเดตข้อมูลไวรัสอย่าง สม่ำเสมอ -จัดการระบบสแกนไวรัสที่ ทันสมัยและมีลิขสิทธิ์มา ติดตั้งให้ครอบคลุมทุก เครื่องของผู้ใช้งาน -กำหนดสิทธิในการใช้งาน เครื่องคอมพิวเตอร์ของ ผู้ใช้งาน (Join Domain) -กำหนด Policy Firewall ให้ป้องกันการเข้าใช้งาน เว็บไซต์ที่เป็นอันตราย -ตรวจสอบและติดตามการ ติดไวรัสอย่างสม่ำเสมอ และแจ้งผู้ที่เกี่ยวข้องทราบ และดำเนินการแก้ไข

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๓.๓ ระบบงานสารสนเทศ ของกรมไม่สามารถ ให้บริการได้	-Harddisk เสียหาย -Raid Controller เสียหาย -Switch และ Router เสียหาย	-ไม่สามารถใช้ระบบงานได้อย่าง ต่อเนื่อง	๑	๕	๕	-จัดทำระบบสำรอง ข้อมูลและตรวจสอบ ระบบสำรองข้อมูลและ อุปกรณ์อย่างสม่ำเสมอ -มีระบบในการตรวจ ติดตามอุปกรณ์ที่ชำรุด เสียหาย	-เบื้องต้นสามารถ แก้ไขปัญหาได้ใน ระดับหนึ่ง	ลด	-จัดทำร่างโครงการพัฒนา ระบบสำรองข้อมูล ระยะไกล (DR Site) เพื่อ ของบประมาณใน ปีงบประมาณ พ.ศ. ๒๕๖๑ -จ้างบำรุงรักษาระบบ สำรองข้อมูลเครื่องแม่ข่าย
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์									
๔.๑ การพัฒนาระบบ สารสนเทศถูกเข้าถึงโดย ไม่ได้รับอนุญาต	-การถูกโจรกรรม (Hack) หรือ เปลี่ยนแปลงข้อมูล -โปรแกรมเสียหาย -การใช้ช่องโหว่ของโปรแกรม หรือช่อง Script ไว้เพื่อ วัตถุประสงค์แอบแฝง -รหัสผ่านที่ใช้เข้าสู่ระบบ สามารถคาดเดาได้ง่ายหรือ ไม่มีความปลอดภัย	-ทำให้กรมป่าไม้ขาดความ น่าเชื่อถือ -อาจทำให้เกิดความเสียหาย หาก เป็นข้อมูลที่เป็นความลับหรือ สำคัญ	๓	๕	๑๕	-มีการกำหนดชั้นการ เข้าถึงของข้อมูล -มีกระบวนการควบคุม การเข้าถึงเครื่องแม่ข่าย ระยะไกล (VPN) -กำหนดมาตรฐานความ ปลอดภัยในการพัฒนา แอปพลิเคชัน เช่น มีการ เข้ารหัส (encryption) ในฐานข้อมูลสำหรับ ปกปิดข้อมูลผู้ใช้และ รหัสผ่าน -มีการจัดเก็บข้อมูล จราจรคอมพิวเตอร์ (logfile) เพื่อให้ระบุได้ ว่าบัญชีผู้ใช้ใดถูกเข้าถึง โดยมิได้รับอนุญาต -มีการแจ้งเตือนให้ เปลี่ยนรหัสผ่าน และใช้ รหัสผ่านที่คาดเดาได้ ยาก	ลดความเสี่ยงได้ใน ระดับหนึ่ง	ลด	-ตรวจสอบหาช่องโหว่ของ แอปพลิเคชันอย่างต่อเนื่อง เพื่อนำมาปรับปรุงระบบ -แจ้งเวียนแนวทางการตั้ง ค่ารหัสผ่านให้มีมาตรฐาน ความปลอดภัย -มีการจัดเก็บข้อมูลจราจร คอมพิวเตอร์ (logfile) อย่างต่อเนื่อง เพื่อให้ระบุ ได้ว่าบัญชีผู้ใช้ใดถูกเข้าถึง โดยมิได้รับอนุญาต และ แจ้งเตือนผู้ใช้ดังกล่าวให้ เปลี่ยนไปใช้รหัสผ่านที่คาด เดาได้ยาก -พัฒนาระบบที่สามารถ ยืนยันตัวตนได้หลายปัจจัย (Multi Factor Authentication)

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๔.๒ การละเมิดลิขสิทธิ์โปรแกรม	-บุคลากรขาดการตระหนักถึงภัยที่มาจากการใช้โปรแกรมละเมิดลิขสิทธิ์ -ขาดงบประมาณในการจัดหาโปรแกรมที่มีลิขสิทธิ์ เนื่องจากมีราคาสูง เช่น Microsoft Office	-โดนฟ้องร้องจากเจ้าของลิขสิทธิ์ -ติดไวรัสจากโปรแกรมที่ละเมิดลิขสิทธิ์	๕	๕	๒๕	-รณรงค์ให้บุคลากรใช้งานโปรแกรมที่มีลิขสิทธิ์ -รณรงค์ให้บุคลากรใช้ซอฟต์แวร์ Open Source -จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เช่น โปรแกรมป้องกันไวรัส โปรแกรมสำนักงาน ระบบปฏิบัติการ -จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เช่น โปรแกรมป้องกันไวรัส โปรแกรมสำนักงาน ระบบปฏิบัติการ	-จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เช่น โปรแกรมป้องกันไวรัส โปรแกรมสำนักงาน ระบบปฏิบัติการ แต่ยังไม่ครอบคลุมทุกเครื่อง	ลด	-รวบรวม เผยแพร่ข้อมูล freeware บนเว็บไซต์ -จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เช่น โปรแกรมป้องกันไวรัส โปรแกรมสำนักงาน ระบบปฏิบัติการ
๕. ความเสี่ยงด้านระบบเครือข่าย									
๕.๑ ไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center	-การเสื่อมสภาพของอุปกรณ์ป้องกันการเกิดไฟไหม้ -การเสื่อมสภาพของอุปกรณ์ดับเพลิง	-เสี่ยงงบประมาณในการจัดหาใหม่ -ข้อมูลเสียหาย	๑	๕	๕	-มีการติดตั้งระบบดับเพลิง -มีการติดตั้งเครื่องตรวจจับควันความไวสูง (Smoke Detector)	-สามารถควบคุมความเสี่ยงได้ระดับหนึ่ง	ลด	-จัดทำร่างโครงการจัดหาระบบดับเพลิง เพื่อของบประมาณในปีงบประมาณ พ.ศ. ๒๕๗๑ -จัดทำร่างโครงการพัฒนาระบบสำรองข้อมูลระยะไกล (DR Site) เพื่อของบประมาณในปีงบประมาณ พ.ศ. ๒๕๗๑
๕.๒ ระบบไฟฟ้าห้อง Data Center ไม่เสถียร	-มีอุปกรณ์ใช้ไฟฟ้าในห้อง Data Center จำนวนมาก -ระบบไฟฟ้าเก่า เสื่อมสภาพ -อุปกรณ์สำรองไฟฟ้าเสื่อมสภาพ	-ไม่สามารถใช้ระบบงานได้ -อุปกรณ์เครือข่ายเสียหาย	๑	๕	๕	-จ้างบำรุงรักษาเครื่องสำรองไฟฟ้าสำหรับห้อง Data Center	-สามารถควบคุมความเสี่ยงในการเกิดระบบไฟฟ้าในห้อง Data Center ไม่เสถียรได้ในระดับหนึ่ง	ลด	-บำรุงรักษาเครื่องสำรองไฟฟ้าอย่างต่อเนื่อง -มีการตรวจสอบการใช้ไฟฟ้า ๓ เฟส เมื่อมีอุปกรณ์มาติดตั้งเพิ่มหรือถอดอุปกรณ์ออก

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผล กระทบ (I)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๕.๓ เครื่องแม่ข่ายและ อุปกรณ์เครือข่ายไม่ สามารถให้บริการได้อย่าง ต่อเนื่อง	-เจ้าหน้าที่ขาดความรู้และ ทักษะในการแก้ไขปัญหา เฉพาะหน้า -เครื่องแม่ข่ายและอุปกรณ์ ล้าสมัย -เครื่องแม่ข่ายและอุปกรณ์ เครือข่ายชำรุด	-ไม่สามารถใช้ระบบได้อย่าง ต่อเนื่อง	๑	๕	๕	-ติดตั้งอุปกรณ์เครื่อง คอมพิวเตอร์แม่ข่ายแบบ virtualization แล้ว - จัดหาอุปกรณ์ เครือข่ายทดแทนแล้ว บางส่วน -จัดทำแผนการ ตรวจสอบความพร้อมใช้ งานของเครื่องแม่ข่าย และอุปกรณ์เครือข่าย	-สามารถควบคุม ความเสี่ยงได้ในระดับ หนึ่ง	ลด	-จ้างบำรุงรักษาเครื่องแม่ ข่ายและอุปกรณ์เครือข่าย ให้พร้อมใช้งาน -จัดส่งเจ้าหน้าที่เข้ารับการ อบรมการใช้งานและดูแล เครื่องแม่ข่ายและอุปกรณ์ เครือข่ายอย่างต่อเนื่อง
๕.๔ การโจมตี (Hack) ระบบเครือข่าย	-การถูกโจมตีจากภายนอก -การถูกโจมตีจากโปรแกรมที่ ไม่มีความปลอดภัย ที่มีการ ติดตั้งที่เครื่องลูกข่าย โดย ผู้ใช้งานภายใน	-ไม่สามารถใช้งานระบบเครือข่าย ได้ หรือใช้งานได้ แต่ช้า	๕	๕	๒๕	-สร้างมาตรการการเข้า ใช้งานระบบเครือข่าย (Policy) -ดำเนินการเข้ารหัสใช้ งานระบบสารสนเทศ -บำรุงรักษาระบบ ป้องกันและเตือนภัย (Firewall) -ทำการสำรองข้อมูลการ ตั้งค่าอุปกรณ์เครือข่าย อย่างสม่ำเสมอ -จัดทำขั้นตอนการแก้ไข ปัญหาจากการถูกโจมตี ในเบื้องต้น -มอบหมายเจ้าหน้าที่ คอยตรวจสอบเป็น ประจำ	สามารถควบคุมความ เสี่ยงได้ในระดับหนึ่ง	ลด	-บำรุงรักษาระบบป้องกัน เครือข่ายอย่างต่อเนื่อง -ทำการสำรองข้อมูลการตั้ง ค่าอุปกรณ์เครือข่ายอย่าง สม่ำเสมอ -ตรวจสอบหาช่องโหว่ของ ระบบเครือข่าย -จัดทำ Policy เพื่อป้องกัน การโจมตี (DDos)

ความเสี่ยง(ภาวะ คุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผล กระทบ (L)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๖. ความเสี่ยงด้านข้อมูล									
๖.๑ข้อมูลและสารสนเทศ ไม่ถูกต้องและเป็นปัจจุบัน	-เจ้าหน้าที่ไม่ปรับปรุงข้อมูลให้ เป็นปัจจุบัน -ไม่มีการตรวจสอบความ ถูกต้องของข้อมูล	-ข้อมูลไม่ถูกต้อง และไม่เป็น ปัจจุบัน -ข้อมูลขาดความน่าเชื่อถือ	๕	๔	๒๐	-ขอความร่วมมือ เจ้าหน้าที่เจ้าของข้อมูล ทำการปรับปรุงข้อมูลให้ เป็นปัจจุบัน	มีการปรับปรุงข้อมูล แต่ยังไม่ครอบคลุม ทุกชุดข้อมูล	ลด	-ตรวจสอบข้อมูลในระบบ ให้ถูกต้องและเป็นปัจจุบัน -มีหนังสือขอความร่วมมือ เจ้าหน้าที่เจ้าของข้อมูลทำ การปรับปรุงข้อมูลให้เป็น ปัจจุบัน
๖.๒ การสำรองและกู้คืน ข้อมูลล้มเหลว	-กระบวนการสำรองข้อมูลเกิด ข้อผิดพลาด -ไม่มีการทดสอบการกู้คืน ข้อมูล -พื้นที่สำรองข้อมูลไม่เพียงพอ -มีการสำรองข้อมูลไม่ ครอบคลุมทุกระบบ	-ข้อมูลสูญหาย -เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือจัดทำขึ้นมาใหม่ -ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้ งาน	๒	๕	๑๐	-มีการสำรองข้อมูลบน เครื่องแม่ข่ายที่กรมป่า ไม้ -จ้างผู้เชี่ยวชาญ บำรุงรักษาระบบและ บริหารจัดการ การ สำรองข้อมูลอย่าง ต่อเนื่อง และมีการ ทดสอบการกู้คืนระบบ -จัดหาระบบสำรอง ข้อมูลที่มีประสิทธิภาพ	ควบคุมความเสี่ยงได้ ระดับหนึ่ง	ลด	-บำรุงรักษาระบบงานให้ ครอบคลุมทุกระบบงาน -จ้างบำรุงรักษาระบบ สำรองข้อมูลเครื่องแม่ข่าย อย่างต่อเนื่อง

ความเสี่ยง(ภาวะ คุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผล กระทบ (L)	ระดับ ความเสี่ยง	แนวทางการควบคุม ที่ผ่านมา	ประเมินผลการ ควบคุม	วิธีการ ควบคุม	กิจกรรม
๖.๓ การรั่วไหลของข้อมูล จากการเปลี่ยนมือผู้ใช้	-ไม่ได้ปรับปรุงสิทธิการใช้งาน ข้อมูลของเจ้าหน้าที่ให้เป็น ปัจจุบัน	-ข้อมูลความลับรั่วไหล ทำให้กรม เสียหาย ขาดความน่าเชื่อถือ	๒	๓	๖	-มีการตรวจสอบและ ยกเลิกสิทธิการใช้งาน ของผู้ใช้ ในส่วนที่ไม่มี สิทธิใช้งานแล้ว ในบาง ระบบงาน -มีการจัดทำข้อมูล ประวัติการใช้งานระบบ (Log File)	ยังไม่ครอบคลุมทุก ระบบงาน	ลด	-มีการจัดทำข้อมูลประวัติ การใช้งานระบบ (Log File) อย่างต่อเนื่อง -แจ้งเวียนหน่วยงานให้ ตรวจสอบผู้ใช้งานระบบที่ หน่วยงานรับผิดชอบให้เป็น ปัจจุบัน
๖.๔ การจัดเก็บ ประมวลผล และเปิดเผย ข้อมูลส่วนบุคคลไม่เป็นไป ตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	-ไม่จัดเก็บข้อมูล ประมวลผล และเปิดเผยข้อมูลตาม พระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. ๒๕๖๒ -เจ้าหน้าที่นำข้อมูลส่วนบุคคล ที่ได้รับการยกเว้น โดยไม่ต้อง ขอความยินยอมตาม พระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. ๒๕๖๒ ไปใช้ โดยมิชอบ	มีความผิดทางกฎหมาย โดน ฟ้องร้อง เรียกค่าเสียหาย	๒	๔	๘	-จัดทำคำขอความ ยินยอมให้จัดเก็บประวัติ ใช้งานเว็บไซต์ (cookie) -จัดทำคำขอยินยอมให้ จัดเก็บและประมวล ข้อมูลส่วนบุคคลที่ระบบ สารสนเทศที่เกี่ยวข้อง -ให้ความรู้แก่เจ้าหน้าที่ ถึงความผิดในการนำ ข้อมูลส่วนบุคคลไปใช้ โดยมิชอบ -เปิดช่องทางให้เจ้าของ ข้อมูลเข้ามายื่นขอใช้ สิทธิข้อมูลส่วนบุคคล -เปิดช่องทางให้เจ้าของ ข้อมูลแจ้งเหตุการละเมิด ข้อมูลส่วนบุคคล	สามารถลดความ เสี่ยงได้	ลด	-จัดทำข้อตกลงระหว่าง กรมป่าไม้กับผู้ประมวลผล ข้อมูลที่เป็นบุคคลภายนอก เพื่อควบคุมการดำเนินงาน ตามหน้าที่ของผู้ประมวลผล ข้อมูลส่วนบุคคลให้เป็นไป ตามกฎหมาย -บันทึกกิจกรรมการจัดเก็บ ข้อมูล (ROPA) -ประชาสัมพันธ์ให้เจ้าหน้าที่ เข้ารับการอบรมเกี่ยวกับ พระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๙

ଭାବେ

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๙												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.	
๒. ความเสี่ยงด้านบุคลากร														
๒.๑ บุคลากรสายงานคอมพิวเตอร์ขาดทักษะและความรู้ที่ทันสมัยในการปฏิบัติงานด้านคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง	จัดอบรมให้ความรู้ด้านคอมพิวเตอร์ที่ทันสมัยและกฎหมายที่เกี่ยวข้องให้แก่เจ้าหน้าที่อย่างสม่ำเสมอ	←												ทุกส่วน ศทส.
	ส่งเสริมให้เจ้าหน้าที่เข้าอบรมผ่าน e-Learning	←												ทุกส่วน ศทส.
	ส่งเจ้าหน้าที่เข้ารับการอบรมในหลักสูตรที่จำเป็น	←												ทุกส่วน ศทส.
๒.๒ เจ้าหน้าที่ใช้คอมพิวเตอร์หรือเครือข่ายผิดวัตถุประสงค์	กำหนด policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด port เท่าที่จำเป็น	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ให้ความรู้แก่บุคลากรในเรื่องการใช้คอมพิวเตอร์และระบบเครือข่ายอย่างเหมาะสมและสม่ำเสมอ	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ตรวจสอบและรายงานการใช้งานของผู้ใช้งานผิดวัตถุประสงค์ต่อผู้บังคับบัญชา				↔				↔				↔	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๙												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. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ														
๓.๑ การใช้งานระบบวีดิทัศน์ทางไกล (Video Conference System) ไม่ชัดเจน	จัดเจ้าหน้าที่ตรวจสอบติดตามการใช้งานระบบ Conference ให้แก่หน่วยงานส่วนกลางที่ตั้งอยู่ในส่วนภูมิภาค					←								ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๓.๒ การติดไวรัสคอมพิวเตอร์หรือ Malware	ให้ความรู้แก่ผู้ใช้งาน ให้ตระหนักถึงภัยอันตรายที่เกิดจากไวรัสอย่างต่อเนื่อง	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดหาระบบสแกนไวรัสที่ทันสมัยและมีลิขสิทธิ์ มาติดตั้งให้ครอบคลุมทุกเครื่องของผู้ใช้งาน					←	→							-ส่วนอำนวยการ ศทส. -ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	กำหนดสิทธิในการใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้งาน (Join Domain)						←							ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	กำหนด Policy Firewall ให้ป้องกันการเข้าใช้งานเว็บไซต์ที่เป็นอันตราย	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ตรวจสอบและติดตามการติดไวรัสอย่างสม่ำเสมอและแจ้งผู้ที่เกี่ยวข้องทราบและดำเนินการแก้ไข	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๓.๓ ระบบงานสารสนเทศของกรมไม่สามารถให้บริการได้	จัดทำร่างโครงการพัฒนาระบบสำรองข้อมูลระยะไกล (DR Site) เพื่อของบประมาณ ในปีงบประมาณ พ.ศ. ๒๕๗๑										←	→		ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	จ้างบำรุงรักษาระบบสำรองข้อมูลเครื่องแม่ข่ายอย่างต่อเนื่อง	←												ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๙												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.	
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์														
๔.๑ การพัฒนาระบบสารสนเทศถูกเข้าถึงโดยไม่ได้รับอนุญาต	ตรวจสอบหาช่องโหว่ของแอปพลิเคชันอย่างต่อเนื่อง เพื่อนำมาปรับปรุงระบบ													ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	แจ้งเวียนแนวทางการตั้งค่ารหัสผ่านให้มีมาตรฐานความปลอดภัย													ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (logfile)อย่างต่อเนื่อง เพื่อให้ระบุได้ว่าบัญชีผู้ใช้ใดถูกเข้าถึงโดยมิได้รับอนุญาต และแจ้งเตือนผู้ใช้งานดังกล่าวให้เปลี่ยนไปใช้รหัสผ่านที่คาดเดาได้ยาก													ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	พัฒนาระบบที่สามารถยืนยันตัวตนได้หลายปัจจัย (Multi Factor Authentication)													ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
๔.๒ การละเมิดลิขสิทธิ์โปรแกรม	รวบรวม เผยแพร่ข้อมูล freeware บนเว็บไซต์													ทุกส่วนของ ศทส.
	จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เช่น โปรแกรมป้องกันไวรัส โปรแกรมสำนักงาน ระบบปฏิบัติการ													-ส่วนอำนวยการ ศทส. -ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕. ความเสี่ยงด้านระบบเครือข่าย														
๕.๑ ไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center	จัดทำร่างโครงการจัดหาระบบดับเพลิง เพื่อของบประมาณ ในปีงบประมาณ พ.ศ. ๒๕๖๑													ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดทำร่างโครงการพัฒนาระบบสำรองข้อมูลระยะไกล (DR Site) เพื่อของบประมาณ ในปีงบประมาณ พ.ศ. ๒๕๖๑													ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
๕.๒ ระบบไฟฟ้าห้อง Data Center ไม่เสถียร	บำรุงรักษาเครื่องสำรองไฟฟ้าอย่างต่อเนื่อง													ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	มีการตรวจสอบการใช้งานไฟฟ้า ๓ เฟส เมื่อมีอุปกรณ์มาติดตั้งเพิ่มหรือถอดอุปกรณ์ออก													ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๙												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.	
๕.๓ เครื่องแม่ข่ายและอุปกรณ์เครือข่ายไม่สามารถให้บริการได้อย่างต่อเนื่อง	จ้างบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้พร้อมใช้งาน	←												-ส่วนระบบคอมพิวเตอร์และเครือข่าย -ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	จัดส่งเจ้าหน้าที่เข้ารับการอบรมการใช้งานและการดูแลรักษาเครื่องแม่ข่ายและอุปกรณ์เครือข่ายอย่างต่อเนื่อง	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๔ การโจมตี (Hack) ระบบเครือข่าย	บำรุงรักษาระบบป้องกันเครือข่ายอย่างต่อเนื่อง	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ทำการสำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ตรวจสอบหาช่องโหว่ของระบบเครือข่าย	←												ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดทำ Policy เพื่อป้องกันการโจมตี (DDos)				←									ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๖. ความเสี่ยงด้านข้อมูล														
๖.๑ ข้อมูลและสารสนเทศไม่ถูกต้องและเป็นปัจจุบัน	ตรวจสอบข้อมูลในระบบให้ถูกต้องและเป็นปัจจุบัน	←												ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	มีหนังสือขอความร่วมมือเจ้าหน้าที่เจ้าของข้อมูลทำการปรับปรุงข้อมูลให้เป็นปัจจุบัน				←									ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.

[illegible]

การติดตามผลและรายงานผล

การติดตามผล

เป็นการติดตามผลหลังจากที่ได้ดำเนินการตามแผนการบริหารจัดการความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารจัดการความเสี่ยงนั้นมีประสิทธิภาพ รวมทั้งสาเหตุของความเสี่ยงที่มีผลต่อความสำเร็จ ความรุนแรงของผลกระทบ วิธีการจัดการความเสี่ยง รวมถึงแนวทางการจัดการความเสี่ยง มีความเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป และรับทราบปัญหาอุปสรรคที่เกิดขึ้นจากการดำเนินการตามกิจกรรมที่กำหนดไว้ในแผนบริหารความเสี่ยง รวมทั้งข้อเสนอแนะ เพื่อนำไปใช้ประกอบการพิจารณาทบทวนและกำหนดแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ในปีงบประมาณถัดไป

การรายงานผล

เป็นการรายงานผลการวิเคราะห์และจัดการความเสี่ยงว่า กิจกรรมที่ใช้ในการจัดการความเสี่ยงใดที่มีประสิทธิภาพ ควรดำเนินการต่อเนื่อง วิธีการจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามดังกล่าวมาจัดทำรายงาน โดยให้หน่วยงานที่รับผิดชอบตามกิจกรรม ดำเนินการจัดทำแบบรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๙ และส่งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ภายในวันที่ ๑๕ ตุลาคม ๒๕๖๙ จากนั้นให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการวิเคราะห์ผลจากแบบรายงานดังกล่าว จัดทำรายงานผล เสนอต่ออธิบดีกรมป่าไม้เพื่อรับทราบและใช้เป็นเครื่องมือหรือข้อมูลประกอบการบริหารราชการกรมป่าไม้ต่อไป

แบบฟอร์มรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๙

หน่วยงาน.....

๙๑

ความเสี่ยง	กิจกรรม	ผลลัพธ์ของกิจกรรม	ระยะเวลาดำเนินการ	% ความ คืบหน้า	ปัญหาอุปสรรคและ แนวทางการแก้ไข

หมายเหตุ : ผลลัพธ์ของกิจกรรม หมายถึง ผลการดำเนินงานที่ได้ดำเนินการตามกิจกรรม เช่น จัดอบรมให้ความรู้เกี่ยวกับระบบเทคโนโลยีสารสนเทศ จำนวน ๓ ครั้ง

ผู้รายงาน.....
(.....)

วันที่รายงาน.....

ภาคผนวก



ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ กรมป่าไม้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐ ๒๕๖๑ ๔๒๙๒-๓ ต่อ ๕๗๕๔

ที่ ทส.๑๖๑๒.๑/ว ๑ ๘ ๓ ๘ ๙ วันที่ ๑๕ ตุลาคม ๒๕๖๘

เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

เรียน รองอธิบดีกรมป่าไม้ทุกท่าน
ผู้ตรวจราชการกรมป่าไม้ทุกท่าน
ผู้อำนวยการสำนักทุกสำนัก
ผู้อำนวยการกองการอนุญาต
ผู้อำนวยการสำนักจัดการทรัพยากรป่าไม้ ที่ ๑ - ๑๓
ผู้อำนวยการสำนักจัดการทรัพยากรป่าไม้สาขาทุกสาขา
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ผู้อำนวยการกลุ่มนิติการ
ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร
ผู้อำนวยการกลุ่มตรวจสอบภายใน
ผู้อำนวยการกลุ่มงานจริยธรรม

กรมป่าไม้ ขอส่งสำเนาคำสั่งกรมป่าไม้ ที่ ๓๗๕๖ /๒๕๖๘ ลงวันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๘ เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ มาเพื่อโปรดทราบ สำหรับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้แจ้งผู้มีรายชื่อตามคำสั่งทราบและถือปฏิบัติ

(นายพงศ์พลชัย ศรียา)

รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมป่าไม้

สำเนา



คำสั่งกรมป่าไม้

ที่ ๓๗๕๖ /๒๕๖๘

เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้
ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

ด้วยปัจจุบันกรมป่าไม้ได้นำเทคโนโลยีสารสนเทศมาใช้งาน เพื่อช่วยเพิ่มประสิทธิภาพการดำเนินงานภายในองค์กรให้ได้รับความสะดวก รวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหาย จากเหตุต่างๆ เช่น การถูกโจมตี ไวรัสมัลแวร์ บุคลากร ไฟฟ้าดับ เกิดอัคคีภัย เป็นต้น ซึ่งอาจจะส่งผลกระทบต่อการทำงานของกรมป่าไม้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมป่าไม้มีความมั่นคง ปลอดภัย และลดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น และเพื่อป้องกันการเกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของกรมป่าไม้

กรมป่าไม้พิจารณาแล้ว เพื่อให้การจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ เป็นไปอย่างมีประสิทธิภาพ และบรรลุตามวัตถุประสงค์ จึงอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และแก้ไขเพิ่มเติม และระเบียบสำนักนายกรัฐมนตรีว่าด้วยพนักงานราชการ พ.ศ. ๒๕๔๗ ให้ยกเลิกคำสั่งกรมป่าไม้ ที่ ๔๖๔๒/๒๕๖๗ ลงวันที่ ธันวาคม พ.ศ. ๒๕๖๗ และแต่งตั้งคณะทำงานเพื่อดำเนินการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ โดยมีองค์ประกอบและอำนาจหน้าที่ ดังนี้

๑. องค์ประกอบ

๑.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	หัวหน้าคณะทำงาน
๑.๒ ผู้อำนวยการส่วนบริหารเทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงาน
๑.๓ ผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย	คณะทำงาน
๑.๔ ผู้อำนวยการส่วนระบบสารสนเทศและภูมิสารสนเทศ	คณะทำงาน
๑.๕ นายดำรงศักดิ์ ธนินบุญ นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๖ นางสาวกนกพรรณ สงเคราะห์ราษฎร์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๑.๗ นายพชร วรรณสุข นักวิชาการป่าไม้ปฏิบัติการ	คณะทำงาน
๑.๘ นายกิตติทัศน์ สุริยา นักวิชาการคอมพิวเตอร์	คณะทำงาน
๑.๙ นางสาวปริญญช กิจสิทธิ์โชค นักจัดการงานทั่วไป	คณะทำงาน
๑.๑๐ นายณภัทร ดลเสถียร นักจัดการงานทั่วไป	คณะทำงาน
๑.๑๑ นายณธร เพลินมัลย์ เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน
๑.๑๒ นายภาคิน กรณ์ธนฤติ เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน

/๑.๑๓ ผู้อำนวยการ...

๑.๑๓ ผู้อำนวยการส่วนอำนวยการ		คณะทำงาน และเลขานุการ
๑.๑๔ นายวิบูลย์ชัย ปาสองห้อง	นักจัดการงานทั่วไป	คณะทำงาน และผู้ช่วยเลขานุการ
๑.๑๕ ว่าที่ ร.ต.หญิง นฤทัย พอกพูน	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน และผู้ช่วยเลขานุการ
๑.๑๖ นางสาวมนัญญา ลงสุวรรณ	เจ้าพนักงานธุรการ	คณะทำงาน และผู้ช่วยเลขานุการ
๑.๑๗ นางสาวธัญชนก ชฎามหากุล	เจ้าหน้าที่ธุรการ	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 ๑๕ ตุลาคม พ.ศ. ๒๕๖๘

(ลงนาม) พงศ์พยัคฆ์ ศรียา
(นายพงศ์พยัคฆ์ ศรียา)
รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมป่าไม้

สำเนาถูกต้อง



(นายวิบูลย์ชัย ปาสองห้อง)
นักจัดการงานทั่วไป
๙ ตุลาคม ๒๕๖๘