กรมป่าไม้

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ.2565

จัดทำโดย ศูนย์เทมคโนโลยีสารสนเทศและการสื่อสาร

สารบัญ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้
ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

บทนำ

หลักการและเหตุผล

ปัจจุบันกรมป่าไม้ได้นำเทคโนโลยีสารสนเทศมาใช้งาน เพื่อช่วยเพิ่มประสิทธิภาพการดำเนินงานภายในองค์กรให้ได้รับความสะดวก รวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากเหตุต่างๆ เช่น การถูกโจมตี ไวรัสคอมพิวเตอร์ บุคลากร ไฟฟ้าดับ เกิดอัคคีภัย เป็นต้น ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของกรมป่าไม้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ มีความมั่นคงปลอดภัย จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และทบทวนแผนบริหารความเสี่ยงให้เป็นปัจจุบันอยู่เสมอ

วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลสารสนเทศให้มีเสถียรภาพและพร้อมใช้งาน

๒. เพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

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 และการใช้ประโยชน์ทรัพยากรป่าไม้

๖. พัฒนาความสามารถเชิงรุกขององค์กร ทั้งระบบ กลไก ข้อมูลสารสนเทศ และปรับปรุงกฎระเบียบให้ทันสมัย ให้เหมาะกับภาวการณ์ปัจจุบัน

ภารกิจ

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

๑. ควบคุม กำกับ ดูแล ป้องกันการบุกรุก การทำลายป่า และการกระทำผิดในพื้นที่รับผิดชอบตามกฎหมายว่าด้วยการป่าไม้ กฎหมายว่าด้วยป่าสงวนแห่งชาติ กฎหมายว่าด้วยสวนป่า กฎหมายว่าด้วยเลื่อยโซ่ยนต์ กฎหมายว่าด้วยป่าชุมชน และกฎหมายอื่นที่เกี่ยวข้อง

๒. ศึกษา วิจัย วางแผน และประสานงานเกี่ยวกับการปลูกป่า เพื่อการฟื้นฟูสภาพป่าและระบบนิเวศ

๓. ส่งเสริมการปลูกป่า การจัดการป่าชุมชน และการปลูกสร้างสวนป่าเชิงเศรษฐกิจ ในลักษณะสวนป่าภาคเอกชนและสวนป่าในรูปแบบอื่นที่เกี่ยวข้อง ตลอดจนศึกษา วิเคราะห์ และประเมินสถานการณ์ป่าเศรษฐกิจของตลาดในประเทศและต่างประเทศ

๔. อนุรักษ์ คุ้มครอง ดูแลรักษา และจัดการให้มีการใช้ประโยชน์ที่ดินป่าไม้ และการอนุญาตที่เกี่ยวข้องกับการใช้ประโยชน์จากไม้ อุตสาหกรรมไม้ ที่ดินป่าไม้ และผลิตผลป่าไม้

๕. ศึกษา ค้นคว้า วิจัย และพัฒนาที่เกี่ยวข้องกับป่าไม้และผลิตผลป่าไม้ และที่เกี่ยวข้องกับไม้และผลิตภัณฑ์ไม้

๖. ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรมหรือตามที่กระทรวงหรือคณะรัฐมนตรีมอบหมาย

<u>แนวทางการพัฒนา</u>

๑. ป้องกันและปราบปรามการบุกรุกทำลายทรัพยากรป่าไม้

๒. ส่งเสริมการบริหารจัดการป่าชุมชน

๓. การบริหารจัดการที่ดินป่าไม้อย่างเป็นระบบ เป็นธรรมเพื่อให้ประชาชนอยู่ร่วมกับป่าอย่างสมดุลและอย่างยั่งยืน

๔. ส่งเสริมการฟื้นฟูป่าเสื่อมโทรมและเพิ่มพื้นที่ป่าเศรษฐกิจ

๕. ส่งเสริมและพัฒนาการเพิ่มพื้นที่สีเขียวในเขตเมืองและเขตชนบท

๖. การบริหารจัดการทรัพยากรป่าไม้

<u>อัตรากำลัง</u>

กรมป่าไม้ มีอัตรากำลังทั้งสิ้น ๑๑,๘๖๒ อัตรา แบ่งออกเป็น ๔ ประเภท ดังนี้

- ข้าราชการ	๑,๖๓๑	อัตรา
- ลูกจ้างประจำ	๙๔๑	อัตรา
- พนักงานราชการ	๖,๖๐๔	อัตรา
- พนักงานจ้างเหมา	๒,๒๓๓	อัตรา

หมายเหตุ ข้อมูล ณ วันที่ ๓๐ กันยายน ๒๕๖๔

<u>สถานภาพด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้</u>

กรมป่าไม้ มีระบบงานที่ใช้ในการปฏิบัติงาน มีรายละเอียดดังนี้

๑. ระบบข้อมูลสารสนเทศทรัพยากรบุคคลระดับกรม

๒. ระบบบุคลากร เงินเดือน และสวัสดิการ

๓. ระบบงานบุคคลของพนักงานราชการ

๔. ระบบสารบรรณอิเล็กทรอนิกส์ กรมป่าไม้

๕. ระบบติดตามการบุกรุกทำลายป่าและควบคุมไฟป่า

๖. ระบบเว็บไซต์กรมป่าไม้

๗. ระบบอีเมล์กรมป่าไม้

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

<u>สถานภาพด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร</u>

๑. อุปกรณ์ควบคุมอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Controller) จำนวน ๑ เครื่อง

๒. อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) จำนวน ๘๒ ตัว

๓. อุปกรณ์กระจายสัญญาณอาคาร (Core Switch BL) จำนวน ๒ ตัว

๔. อุปกรณ์กระจายสัญญาณ (Access Switch) จำนวน ๑๙ ตัว

๕. อุปกรณ์บันทึกภาพแบบไอพี (Network Video Recorder) จำนวน ๑ เครื่อง

๖. กล้องโทรทัศน์วงจรปิดแบบไอพี (IP Camera) จำนวน ๑๐ ตัว

๗. เครื่องสแกนลายนิ้วมือ (Finger Scan) จำนวน ๑ เครื่อง

๘. อุปกรณ์ป้องกันเครือข่าย (Firewall) จำนวน ๑ เครื่อง

๙. อุปกรณ์กระจายสัญญาณย่อย (Switch External) จำนวน ๑ ตัว

๑๐. อุปกรณ์ค้นหาเส้นทาง Router จำนวน ๒ ตัว

๑๑. อุปกรณ์ Info box อุปกรณ์แจกหมายเลข IP และ DNS จำนวน ๒ ตัว

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. เครื่องปรับอากาศควบคุมอุณหภูมิและความชื้น จำนวน ๒ เครื่อง

๑๗. เครื่องกำเหนิดไฟฟ้า (Generator) จำนวน ๑ เครื่อง

๑๘. เครื่องควบคุมการสลับสัญญาณไฟฟ้า จำนวน ๑ เครื่อง

<u>สถานภาพด้านระบบเครือข่ายและการสื่อสาร กรมป่าไม้</u>

๑. ระบบเครือข่ายของกรมป่าไม้ ซึ่งมีการเชื่อมอินเตอร์เน็ตจำนวน ๒ คู่สาย เครือข่ายทรูความเร็ว ๕๐๐/๘๐ Mbps เครือข่าย CAT ความเร็ว ๕๐๐/๙๐ 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 รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

การวิเคราะห์ความเสี่ยง หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นต่อไปคือ 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 กระบวนการที่ใช้ในการระบุวิเคราะห์ความเสี่ยง 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 กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้

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

๑) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสียหายและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้าง ๗ องค์กร 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

<u>กระบวนการบริหารความเสี่ยง</u>

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) 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 ที่ได้กล่าวอ้างจากการกำหนดเป้าหมายการบริหารความเสี่ยง ข้างต้นมาพิจารณาระบุความเสี่ยง โดยมีรายละเอียดดังนี้

๑) นโยบายความมั่นคงปลอดภัย (Security policy)

- นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

- โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร
- โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานภายนอก

๓) การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

- หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร
- การจัดหมวดหมู่สารสนเทศ

๔) ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (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
- การสร้างความมันคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์
- การเฝ้าระวังทางด้านความมั่นคงปลอดภัย

๗) การควบคุมการเข้าถึง (Access control)

- ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้
- หน้าที่ความรับผิดชอบของผู้ใช้งาน

- การควบคุมการเข้าถึงเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ
- การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ
- การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

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

- ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ
- การประมวลสารสนเทศในแอปพลิเคชั่น
- 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/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
	ไม่เป็นสาระสำคัญ/น้อยมาก	1	1	2	3	4	5
Risk Assessment Matrix			1	2	3	4	5
			ต่ำมาก/น้อยมาก	ต่ำ/น้อย	ปานกลาง	สูง/บ่อย	สูงมาก/บ่อยมาก

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	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน	4
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลกรมป่าไม้	5

๔. การตอบสนองความเสี่ยง (Risk Response)

คือการกำหนดวิธีการจัดการความเสี่ยง เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์การจัดการความเสี่ยงอย่างใดอย่างหนึ่งผสมผสานกันดัง ต่อไปนี้

๑) การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง

๒) การลดการควบคุมความเสี่ยง (Risk Reduction) เป็นการปรับปรุงกระบวนการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่ยอมรับได้ เช่น การลดขนาดกิจกรรม

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

๔) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการกับความเสี่ยงที่มีอยู่ในระดับสูงมากและหน่วยงานไม่อาจยอมรับได้จึงต้องตัดสินใจ 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

- เดือนกันยายน – ตุลาคม พ.ศ. ๒๕๖๕ เฝ้าระวังและติดตามผลความเสี่ยง
- เดือนตุลาคม – พฤศจิกายน พ.ศ. ๒๕๖๕ จัดทำสรุปและรายงานผลการเฝ้าระวัง

<u>บทบาท หน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยง</u>

๑) บริหารระดับสูง ทำหน้าที่กำหนดนโยบายและแต่งตั้งคณะกรรมการหรือคณะทำงานในการกำกับดูแลให้มีการดำเนินการตามแผนบริหารความเสี่ยง

๒) คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ จัดทำวิธีปฏิบัติด้านเทคโนโลยีสารสนเทศ เพื่อบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้

๓) ผู้บริหารระดับสำนัก/กอง/ศูนย์ ดำเนินการบริหารความเสี่ยงในหน่วยงาน รวมทั้งติดตามประเมินผล

๔) บุคลากรในหน่วยงาน ดำเนินการตามแผนบริหารความเสี่ยงตามที่กำหนด อย่างถูกต้อง ครบถ้วน

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการศึกษาค้นคว้า ประกอบกับการตรวจสอบหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการและการควบคุมความเสี่ยงด้านสารสนเทศของกรมป่าไม้ 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 โดยอาจมีสาเหตุมาจากการที่หน่วยงานที่รับผิดชอบไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

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

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

ขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้าน และมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการปฏิบัติราชการ และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรอบรู้ และเชี่ยวชาญในงานที่รับผิดชอบ นอกจากความเสี่ยง ๔ ประเภทหลักตามที่กล่าวข้างต้น ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงหนึ่งที่ทำให้เกิดผลกระทบต่อระบบฐานข้อมูลกรมป่าไม้ เนื่องด้วยความเสี่ยงดังกล่าว อาจทำให้ระบบขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อภาพรวมของระบบฐานข้อมูลกรมป่าไม้ จึงจำเป็นต้องมีการจัดทำระบบบริหารจัดการความเสี่ยงและแผนแก้ไขปัญหาที่อาจเกิดขึ้นและแนวทางป้องกันต่อไป

<u>การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ</u>

คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ดำเนินการวิเคราะห์ความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยจากการดำเนินงานด้านเทคโนโลยีสารสนเทศ และวิเคราะห์ปัญหาหรือภัยคุกคามที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมป่าไม้ โดยปัญหาหรือภัยคุกคามนั้นสร้างผลกระทบสูงต่อการบรรลุความสำเร็จการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จากการสรุปปัญหาและภัยคุกคามทั้งหมดแล้วจะนำมาประเมินโอกาส (Likelihood) ที่อาจจะเกิดเหตุการณ์ความเสี่ยง พร้อมทั้งประเมินระดับความรุนแรงหรือมูลค่าความเสียหาย (Impact) จากความเสี่ยง โดยเลือกความเสี่ยงที่มีระดับสูงและสูงมาก มาจัดทำแผนบริหารความเสี่ยง

<u>ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้คือ</u>

๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติ สิ่งที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น วาตภัย น้ำท่วม ฟ้าผ่า 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 เป็นต้น

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

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

๖. ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากข้อมูล และฐานข้อมูลในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย 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), มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan), มีระบบรักษาความมั่นคงและปลอดภัย(Security) ของระบบฐานข้อมูล เช่น ระบบ Anti – Virus ระบบไฟฟ้าสำรองเป็นต้น, และมีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights) ในการเข้าถึงระบบสารสนเทศและเครือข่าย ซึ่งได้แสดงรายละเอียดการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

ตารางวิเคราะห์แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๕

ความเสี่ยง(ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม									
๑.๑ เกิดอัคคีภัย วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม แผ่นดินไหว วินาศภัย ก่อการร้าย	-การสูญหายและถูกทำลายของอุปกรณ์ -เกิดความเสียหายด้านโครงสร้างอาคาร -ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	-เสียงบประมาณในการจัดหาระบบทดแทน -ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน -เสียเวลาในการกู้ระบบ	๑	๕	๕	-จัดทำแผนรองรับสถานการณ์ฉุกเฉิน -ติดตั้งอุปกรณ์ดับเพลิง -จัดเก็บระบบและข้อมูลบน cloud ของหน่วยงานอื่น	-มีการจัดเก็บระบบและข้อมูลบน cloud แค่บางระบบ -ไม่ได้มีการดูแลอุปกรณ์ดับเพลิงอย่างต่อเนื่อง	ลด	-ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง -จัดทำแผนบริหารความต่อเนื่องด้าน IT -ซักซ้อมแผนรองรับสถานการณ์ฉุกเฉิน อย่างน้อยปีละครั้ง
๑.๒ กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	-แหล่งจ่ายไฟฟ้าหลักขัดข้อง -ตู้ควบคุมการจ่ายไฟฟ้าหลักของอาคารขัดข้อง	-ไม่สามารถใช้งานระบบได้ -ข้อมูลเสียหาย -ระบบปฏิบัติการ โปรแกรม หรือฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่	๒	๔	๘	-ติดตั้งอุปกรณ์สำรองไฟ (UPS) -ติดตั้งเครื่องผลิตไฟฟ้าสำรอง (Generator)	-เบื้องต้นสามารถแก้ไขปัญหาได้ในระดับหนึ่ง	ลด	-บำรุงรักษาการทำงาน UPS -บำรุงรักษาการทำงานของ Generator และบริเวณโดยรอบ
๑.๓ คอมพิวเตอร์ถูกโจรกรรม	-ขาดมาตรการระบบรักษาความปลอดภัย เช่น ระบบการเข้าเวรยาม กล้องวงจรปิด เป็นต้น	-เสียงบประมาณในการจัดหาคอมพิวเตอร์ทดแทน -ข้อมูลในเครื่องคอมพิวเตอร์สูญหาย	๑	๕	๕	-มียามประจำอาคาร -ติดตั้งกล้องวงจรปิด -มีการสแกนนิ้วมือก่อนเข้าห้อง Data Center	-การรักษาความปลอดภัยอาจยังไม่ครอบคลุม	ลด	-บำรุงรักษาและติดตั้งกล้องวงจรปิดให้ครอบคลุมและสามารถใช้งานได้อย่างต่อเนื่อง -มอบหมายเจ้าหน้าที่ตรวจสอบผู้มาติดต่อก่อนอนุญาตให้เข้าห้อง

ความเสี่ยง(ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๑.๔ ความเสี่ยงจากแมลงหรือสัตว์กัดแทะสายไฟฟ้าหรือสายสัญญาณ	-อาคารมีแหล่งอาศัยของหนูและแมลง -มีเศษอาหารในอาคาร ทำให้เป็นแหล่งอาหารของหนู	-เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน -ไม่สามารถใช้งานสารสนเทศและเครือข่ายได้	๑	๕	๕	-ทำท่อ/ราง/อื่นๆ ห่อหุ้มสาย	-เบื้องต้นสามารถป้องกันได้ระดับหนึ่ง	ลด	-ตรวจสอบและปรับปรุงสายไฟฟ้าและสายสัญญาณโดยห่อหุ้มวัสดุที่ป้องกันแมลงหรือสัตว์กัดแทะ -เตรียมความพร้อมของบุคลากรและอุปกรณ์ในการซ่อมบำรุงสายไฟฟ้าในห้อง Data Centerหรือสายสัญญาณของกรม -ประชาสัมพันธ์ให้รักษาความสะอาดในอาคาร
๑.๕ การแพร่ระบาดของโรคติดต่อ เช่น COVID-19	-เจ้าหน้าที่อาจติดโรคร้ายแรงทำให้ถูกกักตัว ไม่สามารถมาปฏิบัติงานได้ -ผู้ประกอบการไม่สามารถส่งมอบงานได้ตามกำหนดเวลา	-เจ้าหน้าที่ไม่สามารถมาปฏิบัติงานที่หน่วยงานได้ -หากอุปกรณ์เกิดความเสียหายไม่สามารถติดตั้งหรือแก้ไขได้ทันที ทำให้ระบบสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง	๑	๕	๕	-จัดหาเทคโนโลยีที่ช่วยให้เจ้าหน้าที่ปฏิบัติงานจากที่พัก -อบรมเจ้าหน้าที่เพื่อให้สามารถปฏิบัติงานแทนกันได้ -การแก้ไขปัญหาและควบคุมคอมพิวเตอร์จากระยะไกล	เบื้องต้นสามารถลดความเสี่ยงได้ในระดับหนึ่ง	ลด ยอมรับ	-จัดหาเทคโนโลยีที่ช่วยให้เจ้าหน้าที่ปฏิบัติงานจากที่พัก เช่น พื้นที่จัดเก็บข้อมูลระบบงานต่างๆ ฯลฯ -อบรมเจ้าหน้าที่เพื่อให้สามารถปฏิบัติงานแทนกันได้ -การแก้ไขปัญหาและควบคุมคอมพิวเตอร์จากระยะไกล

ความเสี่ยง(ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๒. ความเสี่ยงด้านบุคลากร									
๒.๑ บุคลากรสายงานคอมพิวเตอร์ขาดความรู้และทักษะในการปฏิบัติงาน	-เจ้าหน้าที่ปฏิบัติงานไม่ตรงตามสายงาน -มีการเปลี่ยนงานบ่อย	-เจ้าหน้าที่ไม่สามารถใช้งานระบบได้ -เจ้าหน้าที่ไม่สามารถแก้ไขปัญหาได้	๓	๔	๑๒	-มีการจัดอบรม เพื่อให้บุคลากรมีความรู้ความเข้าใจในระบบงานที่รับผิดชอบ	-เบื้องต้นสามารถลดความเสี่ยงได้ในระดับหนึ่ง	ลด	-จัดอบรมให้ความรู้ด้านคอมพิวเตอร์และเทคโนโลยีที่ทันสมัยให้แก่เจ้าหน้าที่อย่างสม่ำเสมอ -จัดทำคู่มือการปฏิบัติงานด้านคอมพิวเตอร์ -เพิ่มอัตรากำลังเจ้าหน้าที่และจัดทำ career path ให้แก่เจ้าหน้าที่ด้านคอมพิวเตอร์ -เพิ่มการจัดการความรู้ (KM) ในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการแก้ปัญหา
๒.๒ เจ้าหน้าที่ใช้คอมพิวเตอร์หรือเครือข่ายผิดวัตถุประสงค์	-ใช้งานในทางที่ผิด เช่น ดูหนัง เล่นการพนันและเล่นเกมส์ -ดาวน์โหลดโปรแกรมที่ไม่มีลิขสิทธิ์ -ดาวน์โหลดหนังออนไลน์	-ทำให้สูญเสีย Bandwidth ในเครือข่าย -อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก -อาจทำให้เครื่องติดไวรัส	๔	๓	๑๒	-มีการกำหนด policy ของ Firewall ให้เหมาะสม -ตรวจสอบและรายงานการใช้งานของผู้ใช้งานผิดวัตถุประสงค์ต่อผู้บังคับบัญชา	-เบื้องต้นสามารถลดความเสี่ยงได้ในระดับหนึ่ง	ลด	-กำหนด policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด port เท่าที่จำเป็น -ให้ความรู้แก่บุคลากรในเรื่องการใช้คอมพิวเตอร์และระบบเครือข่ายอย่างเหมาะสมและสม่ำเสมอ -ตรวจสอบและรายงานการใช้งานของผู้ใช้งานผิดวัตถุประสงค์ต่อผู้บังคับบัญชา

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ									
๓.๑ การใช้งานระบบ Web Conference	-สัญญาณเครือข่ายขัดข้อง -อุปกรณ์ Conference ของหน่วยงานส่วนกลางที่ตั้งอยู่ในส่วนภูมิภาคบางหน่วยงานยังไม่ทันสมัย -เจ้าหน้าที่ไม่มีความรู้และทักษะในการติดตั้งและใช้งานระบบ	-ไม่สามารถเชื่อมต่อระบบได้ -ภาพไม่ชัดเจน -เสียงไม่ออก	๓	๓	๙	-มีการจัดหาอุปกรณ์ Conference ของกรมป่าไม้ส่วนกลางและหน่วยงานส่วนกลางที่ตั้งอยู่ในส่วนภูมิภาคเพิ่มเติม -เพิ่มจำนวนผู้ใช้งานระบบให้มากขึ้นเป็น ๕๐๐ user	-สามารถลดความเสี่ยงได้ในระดับหนึ่ง	ลด	-อบรมการติดตั้งและใช้งานระบบ Conference อย่างสม่ำเสมอ -จัดหาอุปกรณ์ conference ที่ทันสมัยเพิ่มเติม -จัดหาอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายเพิ่มเติม
๓.๒ การติดไวรัสคอมพิวเตอร์หรือ Malware	-การต่อพ่วงกับอุปกรณ์ทางคอมพิวเตอร์ที่ยังไม่ได้รับการตรวจสอบไวรัส (Scan Virus) -การดาวน์โหลดและติดตั้งซอฟต์แวร์ที่ไม่รู้แหล่งที่มา -การเข้าเว็บไซต์ที่มีความเสี่ยงและฝัง Spyware ไว้ เช่น เว็บไซต์ดาวน์โหลดโปรแกรมฟรี, ภาพยนตร์ฟรี เป็นต้น -การเปิดอีเมล์ที่มีการแนบไฟล์ที่ไม่รู้จักและไม่รู้แหล่งที่มา	-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 -อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ และจัดหาระบบสแกนไวรัสที่ทันสมัยและมีลิขสิทธิ์มาติดตั้งให้ครอบคลุมทุกเครื่องของผู้ใช้งาน -กำหนดสิทธิในการใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้งาน

ความเสี่ยง(ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผลกระทบ (L)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์									
๔.๑ การพัฒนาระบบระบบสารสนเทศถูกเข้าถึงโดยไม่ได้รับอนุญาต	-การถูกโจรกรรมหรือเปลี่ยนแปลงข้อมูล -โปรแกรมเสียหาย -การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง -รูปแบบในการพัฒนาแตกต่างกัน ทำให้เปลี่ยนคนพัฒนาหรือรับงานต่อยาก -รหัสผ่านที่ใช้เข้าสู่ระบบสามารถคาดเดาได้ง่ายหรือไม่มีความปลอดภัย	-ทำให้กรมป่าไม้ขาดความน่าเชื่อถือ -อาจทำให้เกิดความเสียหาย หากเป็นข้อมูลที่เป็นความลับ -การใช้งานหรือพัฒนาโปรแกรมไม่ต่อเนื่อง	๓	๕	๑๕	-ให้ผู้เชี่ยวชาญตรวจสอบช่องโหว่ของแอพพลิเคชั่นตามมาตรฐานของ OWASP -มีการกำหนดชั้นการเข้าถึงของข้อมูล -มีการนำร่องกระบวนการควบคุมการเข้าถึงเครื่องแม่ข่ายของผู้พัฒนาระบบจากภายนอก	ลดความเสี่ยงได้ในระดับหนึ่ง	ลด	-จัดหาผู้เชี่ยวชาญตรวจสอบช่องโหว่ของแอพพลิเคชั่นอย่างต่อเนื่องเพื่อนำมาปรับปรุงระบบ -กำหนดมาตรฐานในการพัฒนาแอพพลิเคชั่น เพื่อให้ใช้เป็นรูปแบบเดียวกัน -กำหนดมาตรฐานความปลอดภัยในการพัฒนาแอพพลิเคชั่น เช่น มีการเข้ารหัส (encryption) ในฐานข้อมูลสำหรับปกปิดชื่อผู้ใช้และรหัสผ่าน -แจ้งเวียนแนวทางการตั้งค่ารหัสผ่านให้มีมาตรฐานความปลอดภัย -มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (logfile) เพื่อให้ระบุได้ว่าบัญชีผู้ใช้ใดถูกเข้าถึงโดยมิได้รับอนุญาต และแจ้งเตือนผู้ใช้ดังกล่าวให้เปลี่ยนไปใช้รหัสผ่านที่คาดเดาได้ยาก

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๔.๒ การละเมิดลิขสิทธิ์โปรแกรม	-บุคลากรขาดความรู้ความเข้าใจพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ -บุคลากรขาดการตระหนักถึงภัยที่มาจากการใช้โปรแกรมละเมิดลิขสิทธิ์ -ขาดงบประมาณในการจัดหาโปรแกรมที่มีลิขสิทธิ์ เนื่องมีราคาสูง เช่น Microsoft Office	โดนฟ้องร้องจากเจ้าของลิขสิทธิ์	๔	๕	๒๐	-มีการชี้แจงเป็นหนังสือเวียนให้กับบุคลากรภายในกรมป่าไม้ทราบเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐	-บุคลากรบางส่วน ยังไม่ตระหนักถึงภัยและความผิดที่เกิดจากการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ และยังคงมีการใช้งานโปรแกรมที่ไม่มีลิขสิทธิ์อยู่	ลด	-รณรงค์ให้บุคลากรใช้งานโปรแกรมที่มีลิขสิทธิ์ -รณรงค์ให้บุคลากรใช้ซอฟต์แวร์ Open Source -ให้ความรู้แก่บุคลากรถึงภัยและความผิดที่เกิดจากการใช้โปรแกรมละเมิดลิขสิทธิ์ -จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เช่น โปรแกรมสำนักงาน ระบบปฏิบัติการ
๔.๓ ระบบงานสารสนเทศไม่ตอบสนองความต้องการของผู้ใช้งาน	-ระบบงานบางระบบ ไม่สามารถตอบสนองการใช้งานของผู้ใช้งานปัจจุบันได้ -ความต้องการของผู้ใช้งานมีการเปลี่ยนแปลง	-ผู้ใช้งานไม่ใช้งานระบบ	๔	๕	๒๐	-ปรับปรุงแก้ไขระบบให้สามารถตอบสนองความต้องการใช้งานของผู้ใช้ให้เป็นปัจจุบันได้	-เบื้องต้นสามารถแก้ไขได้ในระดับหนึ่ง	ถ่ายโอน	-ประสานกับผู้ใช้งานพร้อมแจ้งผู้พัฒนาดำเนินการบำรุงรักษาและปรับปรุงระบบให้ครอบคลุมความต้องการของผู้ใช้งาน
๕. ความเสี่ยงด้านระบบเครือข่าย									
๕.๑ การเชื่อมโยงเครือข่ายล้มเหลว	-ผู้ให้บริการเครือข่ายให้บริการล่าช้า ไม่ดูแล -การเชื่อมโยงเครือข่ายล้มเหลว อันเกิดจากอุปกรณ์ชำรุด เช่น Router สาย Fiber Optic เป็นต้น	-ไม่สามารถใช้งานระบบเครือข่ายและระบบงานได้	๒	๕	๑๐	-จัดทำ Link สำรองในลักษณะ Load Balance	-เบื้องต้นสามารถแก้ปัญหาได้ในระดับหนึ่ง	ลด	-จ้างที่ปรึกษาวิเคราะห์และปรับปรุงระบบเครือข่ายคอมพิวเตอร์
๕.๒ ไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center	-การเสื่อมสภาพของอุปกรณ์ป้องกันการเกิดไฟไหม้ -การเสื่อมสภาพของอุปกรณ์ดับเพลิง	-เสียงบประมาณในการจัดหาใหม่ -ข้อมูลเสียหาย	๑	๕	๕	-ติดตั้งระบบดับเพลิง	-เบื้องต้นสามารถแก้ไขปัญหาได้ในระดับหนึ่ง -ระบบดับเพลิงเสื่อมประสิทธิภาพการใช้งาน	ลด	-ดำเนินการตามแผนพัฒนาไซต์สำรอง (DR-Site) -ติดตั้งอุปกรณ์ดับเพลิงใหม่

ความเสี่ยง (ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๕.๓ ระบบไฟฟ้าห้อง Data Center ไม่เสถียร	-ปริมาณการใช้ไฟฟ้ามาก -ระบบไฟฟ้าเก่า เสื่อมสภาพ	-ไม่สามารถใช้ระบบงานได้ -อุปกรณ์เครือข่ายเสียหาย	๒	๕	๑๐	-จัดหาเครื่องสำรองไฟฟ้าสำหรับห้อง Data Center	-เครื่องสำรองไฟฟ้าสำหรับห้อง Data Center สามารถสำรองไฟได้ระยะเวลาหนึ่ง	ลด	มอบหมายให้เจ้าหน้าที่ตรวจสอบระบบไฟฟ้าอย่างสม่ำเสมอ
๕.๔ เครื่องแม่ข่ายและอุปกรณ์เครือข่ายไม่สามารถให้บริการได้อย่างต่อเนื่อง	-เจ้าหน้าที่ขาดความรู้และทักษะในการแก้ไขปัญหาเฉพาะหน้า -เครื่องแม่ข่ายและอุปกรณ์ล้าสมัย -เครื่องแม่ข่ายและอุปกรณ์เครือข่ายชำรุด -มีจำนวนผู้ใช้งานปริมาณมาก ทำให้เครื่องแม่ข่ายและอุปกรณ์เครือข่าย ไม่สามารถรองรับได้	-ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง	๑	๕	๕	-จัดส่งเจ้าหน้าที่เข้ารับการอบรมเพื่อเพิ่มทักษะ -ติดตั้งอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายแบบ virtualization แล้ว - ทดแทนอุปกรณ์เครือข่ายแล้วบางส่วน	-มีการจัดอบรมแล้ว แต่ยังไม่เพียงพอ	ลด	-จ้างบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้พร้อมใช้งาน -จัดทำแผนการตรวจสอบความพร้อมใช้งานของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย
๕.๕ การโจมตี (Hack) ระบบเครือข่าย	-การโจมตีจากภายนอก -การโจมตีจากโปรแกรมต่าง ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน	-ไม่สามารถใช้งานระบบเครือข่ายได้ หรือใช้งานได้ แต่ช้า	๒	๕	๑๐	-สร้างมาตรการการเข้าใช้งานระบบเครือข่าย (Policy) -ดำเนินการเข้ารหัสใช้งานระบบสารสนเทศ		ลด	-บำรุงรักษาระบบป้องกันและเตือนภัย (Firewall) -มอบหมายเจ้าหน้าที่คอยตรวจสอบเป็นประจำ -ทำการสำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายอย่างสม่ำเสมอ -กำหนดรหัส (encryption) ระบบสารสนเทศ -จ้างที่ปรึกษาตรวจสอบหาช่องโหว่ของระบบเครือข่าย

ความเสี่ยง(ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผลกระทบ (L)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๕.๖ ระบบงานสารสนเทศของกรมไม่สามารถให้บริการได้	-Harddisk เสียหาย -Raid Controller เสียหาย -Switch และ Router เสียหาย	-ไม่สามารถใช้ระบบงานได้อย่างต่อเนื่อง	๑	๕	๕	-จัดทำระบบสำรองข้อมูล	-เบื้องต้นสามารถแก้ไขปัญหาได้ในระดับหนึ่ง	ลด	-ตรวจสอบระบบสำรองข้อมูลและอุปกรณ์อย่างสม่ำเสมอ
๖. ความเสี่ยงด้านข้อมูล									
๖.๑ข้อมูลและสารสนเทศไม่ถูกต้องและเป็นปัจจุบัน	-เจ้าหน้าที่ไม่ปรับปรุงข้อมูลให้เป็นปัจจุบัน -ไม่มีการตรวจสอบความถูกต้องของข้อมูล	-ข้อมูลไม่ถูกต้อง และไม่เป็นปัจจุบัน	๕	๔	๒๐	-ขอความร่วมมือเจ้าหน้าที่ให้ปรับปรุงข้อมูลให้เป็นปัจจุบัน -จัดฝึกอบรมการใช้งานระบบสารสนเทศอย่างสม่ำเสมอ	ยังไม่ได้รับความร่วมมือในการปรับปรุงข้อมูล	ลด	-ออกคำสั่งให้เจ้าหน้าที่ปรับปรุงข้อมูลให้ครบถ้วนเป็นปัจจุบัน -ประชุมเจ้าหน้าที่เพื่อจัดทำบัญชีข้อมูล (Data catalog) ของกรมป่าไม้ -จัดทำบัญชีข้อมูล (Data catalog) ของกรมป่าไม้ -ติดตามการทบทวนข้อมูลให้ถูกต้องและเป็นปัจจุบัน
๖.๒ การสำรองและกู้คืนข้อมูลล้มเหลว	-กระบวนการสำรองข้อมูลเกิดข้อผิดพลาด -ไม่มีการทดสอบการกู้คืนข้อมูล	-ข้อมูลสูญหาย -เสียค่าใช้จ่ายในการกู้คืนข้อมูลหรือจัดทำขึ้นมาใหม่ -ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งาน	๓	๕	๑๕	-มีการสำรองข้อมูลบนเครื่องแม่ข่ายที่กรมป่าไม้ -จ้างผู้เชี่ยวชาญบำรุงรักษาระบบและบริหารจัดการ การสำรองข้อมูลอย่างต่อเนื่อง และมีการทดสอบการกู้คืนระบบ	ลดความเสี่ยงได้ระดับหนึ่ง ยังไม่มีการทดสอบครอบคลุมทุกระบบ	ลด	-จัดหาระบบสำรองข้อมูลที่มีประสิทธิภาพ -บูรณาการแบบรวมศูนย์ (จัดเก็บข้อมูลในฐานข้อมูลเดียวกัน)
๖.๓ การรั่วไหลจากการเปลี่ยนมือผู้ใช้	-ไม่ปรับปรุงสิทธิการใช้งานข้อมูลของเจ้าหน้าที่ให้เป็นปัจจุบัน	-ข้อมูลความลับรั่วไหล ทำให้กรมเสียหาย ขาดความน่าเชื่อถือ	๒	๓	๖	มีการตรวจสอบและยกเลิกสิทธิการใช้งานของผู้ใช้ ในส่วนที่ไม่มีสิทธิใช้งานแล้ว ในบางระบบงาน	ยังไม่ครอบคลุมทุกระบบงาน	ลด	-จัดทำคู่มือในการขอสิทธิใช้งาน การตรวจสอบสิทธิและการยกเลิกสิทธิการใช้งาน

ความเสี่ยง(ภาวะคุกคาม)	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบที่เกี่ยวข้อง	โอกาส (I)	ผลกระทบ (L)	ระดับความเสี่ยง	แนวทางการควบคุมที่ผ่านมา	ประเมินผลการควบคุม	วิธีการควบคุม	กิจกรรม
๖.๔ การประมวลผลและเปิดเผยข้อมูลส่วนบุคคลไม่เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	ไม่ได้มีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล	โดนฟ้องร้อง เรียกค่าเสียหาย	๔	๔	๑๖			ลด	-จัดทำคำขอความยินยอมให้จัดเก็บประวัติใช้งานเว็บไซต์ (cookie) -จัดทำคำขอยินยอมให้จัดเก็บและประมวลข้อมูลส่วนบุคคลที่ระบบสารสนเทศที่เกี่ยวข้อง

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๕

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๕												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	ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	←	—	—	—	—	—	—	—	—	—	—	→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดทำแผนบริหารความต่อเนื่องด้าน IT								←	—	—	—	→	ส่วนบริหารเทคโนโลยีสารสนเทศและการสื่อสาร ศทส.
	ซักซ้อมแผนรองรับสถานการณ์ฉุกเฉิน อย่างน้อยปีละครั้ง								←	—	—	—	→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๑.๒ กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	บำรุงรักษาการทำงาน UPS	←	—	—	—	—	—	—	—	—	—	—	→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	บำรุงรักษาการทำงานของ Generator	←	—	—	—	—	—	—	—	—	—	—	→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๑.๓ คอมพิวเตอร์ถูกโจรกรรม	บำรุงรักษาและติดตั้งกล้องวงจรปิดให้ครอบคลุมและสามารถใช้งานได้อย่างต่อเนื่อง	←	—	—	—	—	—	—	—	—	—	—	→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ประชาสัมพันธ์การระมัดระวังการถูกโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์อย่างต่อเนื่อง	←	—	—	—	—	—	—	—	—	—	—	→	ส่วนอำนวยการ ศทส.
๑.๔ ความเสี่ยงจากแมลงหรือสัตว์กัดแทะสายไฟฟ้าในห้อง Data Center หรือสายสัญญาณของกรมป่าไม้	ตรวจสอบและปรับปรุงสายไฟฟ้าและสายสัญญาณ โดยห่อหุ้มวัสดุที่ป้องกันแมลงหรือสัตว์กัดแทะ	←	—	—	—	—	—	—	—	—	—	—	→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	เตรียมความพร้อมของบุคลากรและอุปกรณ์ในการซ่อมบำรุงสายไฟฟ้าในห้อง Data Center หรือสายสัญญาณของกรม	←	—	—	—	—	—	—	—	—	—	—	→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ประชาสัมพันธ์ให้รักษาความสะอาดในอาคาร								←	—	→			ส่วนอำนวยการ ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๕												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.	
๑.๕ การแพร่ระบาดของโรคติดต่อ เช่น COVID-19	จัดหาเทคโนโลยีที่ช่วยให้เจ้าหน้าที่ปฏิบัติงานจากที่พัก เช่น พื้นที่จัดเก็บข้อมูล ระบบงานต่างๆ ฯลฯ	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
	มอบหมายเจ้าหน้าที่เพื่อให้สามารถปฏิบัติงานแทนกันได้	←	—	—	—	—	—	—	—	—	—	—	→	ทุกหน่วยงาน
	การแก้ไขปัญหาและควบคุมคอมพิวเตอร์จากระยะไกล	←	—	—	—	—	—	—	—	—	—	—	→	ศทส
๒. ความเสี่ยงด้านบุคลากร														
๒.๑ บุคลากรสายงานคอมพิวเตอร์ขาดความรู้และทักษะในการปฏิบัติงาน	จัดอบรมให้ความรู้ด้านคอมพิวเตอร์และเทคโนโลยีที่ทันสมัยให้แก่บุคลากรอย่างสม่ำเสมอ	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
	จัดทำคู่มือการปฏิบัติงานด้านคอมพิวเตอร์						←	—	→					ศทส.
	เพิ่มอัตรากำลังบุคลากรและจัดทำ career path ให้แก่บุคลากรด้านคอมพิวเตอร์										←	—	→	ส่วนการเจ้าหน้าที่ สบก.
	เพิ่มการจัดการความรู้ (KM) ในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการแก้ปัญหา										←	—	→	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. ๒๕๖๕												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 การใช้งานระบบ Web Conference	อบรมการติดตั้งและทบทวนการใช้งานระบบ Conference อย่างสม่ำเสมอ								↔					ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดหาอุปกรณ์ conference ที่ทันสมัยเพิ่มเติม							↔	↔					ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดหาอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายเพิ่มเติม											↔	↔	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๓.๒ การติดไวรัสคอมพิวเตอร์หรือ Malware	ประกาศมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมป่าไม้									↔	↔			ส่วนบริหารเทคโนโลยีสารสนเทศและการสื่อสาร ศทส.
	ให้ความรู้แก่ผู้ใช้งาน ให้ตระหนักถึงภัยอันตรายที่เกิดจากไวรัส							↔						ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ และจัดหาระบบสแกนไวรัสที่ทันสมัยและมีลิขสิทธิ์มาติดตั้งให้ครอบคลุมทุกเครื่องของผู้ใช้งาน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	กำหนดสิทธิในการใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้งาน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์														
๔.๑ การพัฒนาระบบสารสนเทศถูกเข้าถึงโดยไม่ได้รับอนุญาต	จัดหาผู้เชี่ยวชาญตรวจสอบช่องโหว่ของแอพพลิเคชั่นอย่างต่อเนื่อง เพื่อนำมาปรับปรุงระบบ								↔	↔				ส่วนระบบสารสนเทศฯ ศทส.
	กำหนดมาตรฐานในการพัฒนาแอพพลิเคชั่นเพื่อให้ใช้เป็นรูปแบบเดียวกัน								↔	↔				ส่วนระบบสารสนเทศฯ ศทส.
	กำหนดมาตรฐานความปลอดภัยในการพัฒนาแอพพลิเคชั่น เช่น มีการเข้ารหัส (encryption) ในฐานข้อมูลสำหรับปกปิดชื่อผู้ใช้และรหัสผ่าน								↔	↔				ส่วนระบบสารสนเทศฯ ศทส.
	แจ้งเวียนแนวทางการตั้งค่ารหัสผ่านให้มีมาตรฐานความปลอดภัย								↔	↔				ส่วนระบบสารสนเทศฯ ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๕												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.	
	มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (logfile)เพื่อให้ระบุได้ว่าบัญชีผู้ใช้ใดถูกเข้าถึงโดยมิได้รับอนุญาต และแจ้งเตือนผู้ใช้ดังกล่าวให้เปลี่ยนไปใช้รหัสผ่านที่คาดเดาได้ยาก	←											→	ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
๔.๒ การละเมิดลิขสิทธิ์โปรแกรม	รณรงค์ให้บุคลากรใช้งานโปรแกรมที่มีลิขสิทธิ์								←	→				ศทส.
	รณรงค์ให้บุคลากรใช้ซอฟต์แวร์ Open Source								←	→				ศทส.
	ให้ความรู้แก่บุคลากรถึงภัยและความผิดที่เกิดจากการใช้โปรแกรมละเมิดลิขสิทธิ์							←	→					ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง เพื่อรองรับการปฏิบัติงาน เช่น โปรแกรมสำนักงาน ระบบปฏิบัติการ	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๔.๓ ระบบงานสารสนเทศไม่ตอบสนองความต้องการของผู้ใช้งาน	ประสานงานกับผู้ใช้งานพร้อมแจ้งผู้พัฒนาดำเนินการบำรุงรักษาและปรับปรุงระบบให้ครอบคลุมความต้องการของผู้ใช้งาน	←											→	ส่วนระบบสารสนเทศฯ ศทส.
๕. ความเสี่ยงด้านระบบเครือข่าย														
๕.๑ การเชื่อมโยงเครือข่ายล้มเหลว	จ้างที่ปรึกษาวิเคราะห์และปรับปรุงระบบเครือข่ายคอมพิวเตอร์									←	→			ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๒ ไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center	ดำเนินการตามแผนพัฒนาไซต์สำรอง (DR-Site)				←								→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ติดตั้งอุปกรณ์ดับเพลิงใหม่	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๓ ระบบไฟฟ้าห้อง Data Center ไม่เสถียร	มอบหมายให้เจ้าหน้าที่ตรวจสอบระบบไฟฟ้าอย่างสม่ำเสมอ	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๔ เครื่องแม่ข่ายและอุปกรณ์เครือข่ายไม่สามารถให้บริการได้อย่างมีประสิทธิภาพและต่อเนื่อง	จ้างบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้พร้อมใช้งาน	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๕												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.	
	จัดทำแผนการตรวจสอบความพร้อมใช้งานของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย							←	→					ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๕ การโจมตี (Hack) ระบบเครือข่าย	บำรุงรักษาระบบป้องกันและเตือนภัย (Firewall)	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	มอบหมายเจ้าหน้าที่คอยตรวจสอบเป็นประจำ	←											→	ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	ทำการสำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	←											→	-ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
	กำหนดรหัส (encryption) ระบบสารสนเทศ					←	→							ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	จ้างที่ปรึกษาตรวจสอบหาช่องโหว่ของระบบเครือข่าย								←	→				ส่วนระบบคอมพิวเตอร์และเครือข่าย ศทส.
๕.๖ ระบบงานสารสนเทศของกรมป่าไม้ไม่สามารถให้บริการได้	ตรวจสอบระบบสำรองข้อมูลและอุปกรณ์อย่างสม่ำเสมอ			↔			↔			↔			↔	ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
๖. ความเสี่ยงด้านข้อมูล														
๖.๑ข้อมูลและสารสนเทศไม่ถูกต้องและเป็นปัจจุบัน	ออกคำสั่งให้เจ้าหน้าที่ปรับปรุงข้อมูลให้ครบถ้วนเป็นปัจจุบัน	←											→	ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	ประชุมเจ้าหน้าที่เพื่อจัดทำบัญชีข้อมูล (Data catalog) ของกรมป่าไม้				←	→								ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	จัดทำบัญชีข้อมูล (Data catalog) ของกรมป่าไม้	←											→	ทุกหน่วยงาน
	ติดตามการทบทวนข้อมูลให้ถูกต้องและเป็นปัจจุบัน									←			→	ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
๖.๒ การสำรองและกู้คืนข้อมูลล้มเหลว	จัดหาระบบสำรองข้อมูลที่มีประสิทธิภาพ								←				→	-ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส. -ส่วนอำนวยการ ศทส.
	บูรณาการแบบรวมศูนย์ (จัดเก็บข้อมูลในฐานข้อมูลเดียวกัน)								←				→	ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๕												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.	
๖.๓ การรั่วไหลจากการเปลี่ยนมือผู้ใช้	จัดทำคู่มือในการขอสิทธิใช้งาน การตรวจสอบสิทธิ และการยกเลิกสิทธิการใช้งาน								←	→				ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
๖.๔ การประมวลผลและเปิดเผยข้อมูลส่วนบุคคลไม่เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	จัดทำคำขอความยินยอมให้จัดเก็บประวัติใช้งานเว็บไซต์ (cookie)	←	→											ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.
	จัดทำคำขอยินยอมให้จัดเก็บและประมวลข้อมูลส่วนบุคคลที่ระบบสารสนเทศที่เกี่ยวข้อง	←	→											ส่วนระบบสารสนเทศและภูมิสารสนเทศ ศทส.

การติดตามผลและรายงานผล

การติดตามผล

เป็นการติดตามผลหลังจากที่ได้ดำเนินการตามแผนการบริหารจัดการความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารจัดการความเสี่ยงนั้นมีประสิทธิภาพ รวมทั้งสาเหตุของความเสี่ยงที่มีผลต่อความสำเร็จ ความรุนแรงของผลกระทบ วิธีการจัดการความเสี่ยง รวมถึงแนวทางการจัดการความเสี่ยง มีความเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป และรับทราบปัญหาอุปสรรคที่เกิดขึ้นจากการดำเนินการตามกิจกรรมที่กำหนดไว้ในแผนบริหารความเสี่ยง รวมทั้งข้อเสนอแนะ เพื่อนำไปใช้ประกอบการพิจารณาทบทวนและกำหนดแผนบริหารความเสี่ยงของกรมป่าไม้ในปีงบประมาณถัดไป

การรายงานผล

เป็นการรายงานผลการวิเคราะห์และจัดการความเสี่ยงว่า กิจกรรมที่ใช้ในการจัดการความเสี่ยงใดที่มีประสิทธิภาพ ควรดำเนินการต่อเนื่อง วิธีการจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามดังกล่าวมาจัดทำรายงาน โดยให้หน่วยงานที่รับผิดชอบตามกิจกรรม ดำเนินการจัดทำแบบรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๕ และส่งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ภายในวันที่ ๓๐ กันยายน ๒๕๖๕ จากนั้นให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการวิเคราะห์ผลจากแบบรายงานดังกล่าว จัดทำรายงานผล เสนอต่ออธิบดีกรมป่าไม้เพื่อรับทราบและใช้เป็นเครื่องมือหรือข้อมูลประกอบการบริหารราชการกรมป่าไม้ต่อไป

แบบฟอร์มรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๕

ความเสี่ยง.....

ผู้รับผิดชอบ.....

วันที่รายงาน.....

ความเสี่ยง	กิจกรรม	ผลลัพธ์ของกิจกรรม	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรคและแนวทางการแก้ไข

๓๐

ภาคผนวก

ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ กรมป่าไม้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐๒๕๖๑๔๒๙๒ ต่อ ๕๗๕๔

ที่ ทส ๑๖๑๒.๑/ ๑๑๗๗ **วันที่** ๒๔ มกราคม ๒๕๖๕

เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

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

กรมป่าไม้ ขอส่งสำเนาคำสั่งกรมป่าไม้ ที่ ๒๗๒ /๒๕๖๕ ลงวันที่ ๒๔ มกราคม พ.ศ. ๒๕๖๕ เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ มาเพื่อโปรดทราบ สำหรับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้แจ้งผู้มีรายชื่อตามคำสั่งทราบและถือปฏิบัติ

(นายพฤกษ์ โสโน)
ผู้อำนวยการสำนักส่งเสริมการปลูกป่า รักษาราชการแทน
รองอธิบดีกรมป่าไม้ ปฏิบัติราชการแทน
อธิบดีกรมป่าไม้

คำสั่งกรมป่าไม้

ที่ ๒๗๒ /๒๕๖๕

เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

ตามคำสั่งกรมป่าไม้ ที่ ๓๙๗๑/๒๕๖๓ ลงวันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๖๓ เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ เพื่อเป็นการเตรียมความพร้อม และลดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น ซึ่งจะส่งผลกระทบและก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ นั้น

กรมป่าไม้พิจารณาแล้ว เพื่อให้การจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ เป็นไปอย่างมีประสิทธิภาพ และบรรลุตามวัตถุประสงค์ จึงอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และแก้ไขเพิ่มเติม และระเบียบสำนักนายกรัฐมนตรีว่าด้วยพนักงานราชการ พ.ศ. ๒๕๔๗ ให้ยกเลิกคำสั่งกรมป่าไม้ ที่ ๓๙๗๑/๒๕๖๓ ลงวันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๖๓ และแต่งตั้งคณะทำงานเพื่อดำเนินการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ โดยมีองค์ประกอบและอำนาจหน้าที่ ดังนี้

๑. องค์ประกอบ

๑.๑ นายอภิรักษ์ ทหรานนท์	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	หัวหน้าคณะทำงาน
๑.๒ นางสาวณัฏฐิณี ปิ่นเนียม	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๓ นายทนงศักดิ์ มนตรี	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๔ นายประพันธ์พงษ์ คงศรีรอด	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๕ นายวีร์ ศรีทิพโพธิ์	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑.๖ นางสาวนรนันท์ อภิชนาพงศ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๑.๗ นายดำรงศักดิ์ ธนีบุญ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๑.๘ นายกิตติทัศน์ สุริยา	นักวิชาการคอมพิวเตอร์	คณะทำงาน
๑.๙ นางสาวปรียานุช กิจสิทธิโชค	นักจัดการงานทั่วไป	คณะทำงาน
๑.๑๐ นายณภัทร์ ดลเสถียร	นักจัดการงานทั่วไป	คณะทำงาน
๑.๑๑ นายถณธร เพลินมาลัย	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน
๑.๑๒ นายภาคิน กรณ์ธนกฤติ	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน
๑.๑๓ ว่าที่ ร.ต.หญิงพรพิมล แก่นโท	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน

/๑.๑๔ นางสาวสายธาร ...

๑.๑๔ นางสาวสายธาร สุดจริตธรรมจริยางกูร	เจ้าพนักงานคอมพิวเตอร์	คณะทำงาน
๑.๑๕ นายวีระพล บุประเสริฐ	เจ้าหน้าที่ธุรการ	คณะทำงาน
๑.๑๖ นางสาวสพินนา อ่อนเพ็ง	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงานและเลขานุการ
๑.๑๗ นายวิบูลย์ชัย ปาสองห้อง	นักจัดการงานทั่วไป	คณะทำงานและผู้ช่วยเลขานุการ

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 ๒๔ มกราคม พ.ศ. ๒๕๖๕

(ลงนาม) พฤกษ์ โสโน

(นายพฤกษ์ โสโน)
ผู้อำนวยการสำนักส่งเสริมการปลูกป่า รักษาราชการแทน
รองอธิบดีกรมป่าไม้ ปฏิบัติราชการแทน
อธิบดีกรมป่าไม้

สำเนาถูกต้อง

(นายวิบูลย์ชัย ปาสองห้อง)
นักจัดการงานทั่วไป
๒๐ ม.ค. ๒๕๖๕