กรมป่าไม้

# แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้

**พ.ศ. ๒๕๖๒**


**จัดทำโดย**

**ศูนย์สารสนเทศ**

**สำนักแผนงานและสารสนเทศ**

# สารบัญ

# บทนำ

**หลักการและเหตุผล**

ปัจจุบันกรมป่าไม้ได้พัฒนาระบบเครือข่าย ทั้งภายในและภายนอก เพื่อใช้ในการเชื่อมโยงข้อมูล และยังมีการพัฒนาระบบงานต่างๆ สำหรับใช้ในการบริหารจัดการ การปฏิบัติงาน และเผยแพร่ประชาสัมพันธ์ ดังนั้น เพื่อให้สามารถใช้งานเครือข่ายและระบบงานต่างๆ ได้อย่างต่อเนื่อง รวมถึงสามารถจัดการแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดสถานการณ์ฉุกเฉินได้ในระยะเวลาที่เหมาะสม จึงมีความจำเป็นต้องมีการป้องกันความเสี่ยงต่างๆ ที่อาจเกิดขึ้นได้ เพื่อลดความเสียหายที่อาจเกิดขึ้น ทำให้กรมป่าไม้สามารถดำเนินการไปได้อย่างต่อเนื่อง จึงได้มีการทบทวนและปรับปรุงเพื่อให้ได้แผนบริหารความเสี่ยงที่สามารถนำมาปฏิบัติได้จริงและสามารถลดความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

**วัตถุประสงค์**

๑. เพื่อให้กรมป่าไม้มีแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนทศและการสื่อสารที่สามารถรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนทศได้อย่างมีประสิทธิภาพและประสิทธิผล

๒. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๓. เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุด และลดโอกาสความเสียหายที่อาจเกิดขึ้น

๔. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมป่าไม้ ให้เจ้าหน้าที่ที่เกี่ยวข้องนำไปใช้ประโยชน์

๕. เพื่อให้ผู้ปฏิบัติงานตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นได้ และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้องให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และเข้าใจหลักกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมป่าไม้

๖. เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงแผนบริหารความเสี่ยงกับแผนงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

# ข้อมูลพื้นฐานของหน่วยงาน

**วิสัยทัศน์**

บริหารจัดการพื้นที่ป่าไม้อย่างมีส่วนร่วมและมุ่งสู่เป้าหมายป่าเศรษฐกิจ ร้อยละ ๑๕ ของพื้นที่ประเทศ ภายในปี พ.ศ. ๒๕๖๙

**พันธกิจ**

๑. ป้องกัน และรักษาพื้นที่ป่าไม้ให้คงอยู่

๒. บริหารจัดการที่ดินป่าไม้อย่างเป็นระบบและเป็นธรรม

๓. เพิ่มและฟื้นฟูพื้นที่ป่าไม้ในเชิงเศรษฐกิจ สังคม และสิ่งแวดล้อม

๔. บริหารจัดการทรัพยากรป่าไม้โดยการมีส่วนร่วม

๕. วิจัยและพัฒนาการป่าไม้ เพื่อการใช้ประโยชน์อย่างยั่งยืน

๖. เสริมสร้างขีดความสามารถเชิงรุกขององค์กร ระบบ กลไก และข้อมูลในการบริหารจัดการ รวมทั้ง การบังคับใช้กฎหมายให้มีประสิทธิภาพ

**ภารกิจ**

มีภารกิจเกี่ยวกับการอนุรักษ์ สงวน คุ้มครอง ฟื้นฟู ดูแลรักษา ส่งเสริม ทำนุ บำรุงป่า และการดำเนินการเกี่ยวกับการป่าไม้ การทำไม้ การเก็บหาของป่า การใช้ประโยชน์ ที่ดินป่าไม้ และการอื่นเกี่ยวกับป่าและอุตสาหกรรมป่าไม้ ให้เป็นไปตามระเบียบและกฎหมาย ที่เกี่ยวข้อง ด้วยกลยุทธ์การเสริมสร้างความร่วมมือของประชาชนเป็นหลัก เพื่อเพิ่มมูลค่าทางเศรษฐกิจของประเทศ และพัฒนาคุณภาพชีวิตของประชาชน และมีภารกิจอื่นตามที่กฎหมาย กำหนดให้เป็นอำนาจหน้าที่ของกรมป่าไม้ โดยมีอำนาจหน้าที่ ดังนี้

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

๒. ศึกษา วิจัย วางแผน และประสานงานเกี่ยวกับการปลูกป่าเพื่อการฟื้นฟูสภาพป่าและระบบนิเวศ

๓. ส่งเสริมการปลูกป่า การจัดการป่าชุมชน และการปลูกสร้างสวนป่าเชิงเศรษฐกิจ ในลักษณะสวนป่าภาคเอกชนและสวนป่าในรูปแบบอื่นที่เกี่ยวข้อง ตลอดจนศึกษาวิเคราะห์ และประเมินสถานการณ์ป่าเศรษฐกิจของตลาดในประเทศและต่างประเทศ

๔. อนุรักษ์ คุ้มครอง ดูแลรักษา และจัดการให้มีการใช้ประโยชน์ที่ดินป่าไม้ และการอนุญาตที่เกี่ยวกับการใช้ประโยชน์จากไม้ อุตสาหกรรมไม้ ที่ดินป่าไม้ และผลิตผลป่าไม้

๕. ศึกษา ค้นคว้า วิจัย และพัฒนาที่เกี่ยวข้องกับป่าไม้และผลิตผลป่าไม้ และที่เกี่ยวข้องกับไม้และผลิตภัณฑ์ไม้

๖. ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรมหรือ ตามที่กระทรวงหรือคณะรัฐมนตรีมอบหมาย

**<u>เป้าหมาย</u>**

ทรัพยากรธรรมชาติได้รับการจัดการอย่างสมดุลและยั่งยืน โดยให้มีพื้นที่ป่าไม้อย่างน้อย ๔๐% ของพื้นที่ประเทศภายใน ๒๐ ปี ในส่วนของกรมป่าไม้ แบ่งเป็น

๑) รักษาพื้นที่ป่าให้ได้ ๕๓.๔๐ ล้านไร่*

๒) บริหารจัดการพื้นที่ที่ไม่มีสภาพป่า**

๓) ฟื้นฟูป่าไม้ ปลูกป่า อื่นๆ ๑๔.๐๒ ล้านไร่

๔) ส่งเสริมปลูกไม้เศรษฐกิจ ๔.๖๘ ล้านไร่

* ปัจจุบันมีพื้นที่ป่าไม้ ๓๙.๗๔ ล้านไร่ ในอีก ๒๐ ปี จะมีพื้นที่ที่ต้องดูแลรักษาให้ได้ ๕๓.๕๐ ล้านไร่

** พื้นที่ผลการรังวัดตามมติ ครม. ๓๐ มิ.ย. ๔๑ (๒๕๔๕-๒๕๕๘) รวม ๕.๒๕ แสนราย ๕.๗๙ ล้านไร่ แยกเป็น

๑. ลุ่มน้ำชั้นที่ ๑,๒ จำนวน ๑.๔๔ แสนราย ๑.๔๗ ล้านไร่

๒. ลุ่มน้ำชั้นที่ ๓, ๔,๕ จำนวน ๓.๗๑ แสนราย ๓.๕๔ ล้านไร่

**<u>ประเด็นยุทธศาสตร์</u>**

ประเด็นยุทธศาสตร์ที่ ๑ ป้องกันรักษาพื้นที่ป่าที่เหลือให้คงอยู่และยั่งยืน

ประเด็นยุทธศาสตร์ที่ ๒ ฟื้นฟูป่าเสื่อมโทรมอย่างมีประสิทธิภาพ

ประเด็นยุทธศาสตร์ที่ ๓ ส่งเสริมธุรกิจป่าไม้และป่าเศรษฐกิจจากป่าปลูก และการส่งเสริมชุมชนในเมือง/ชุมชนชนบทเป็นพื้นที่สีเขียว

ประเด็นยุทธศาสตร์ที่ ๔ แก้ไขปัญหาราษฎรในพื้นที่ป่าไม้อย่างเป็นระบบและเป็นธรรม

ประเด็นยุทธศาสตร์ที่ ๕ สนับสนุนและส่งเสริมการวิจัยเพื่อพัฒนาการบริหารจัดการทรัพยากรป่าไม้

ประเด็นยุทธศาสตร์ที่ ๖ บูรณาการและส่งเสริมการมีส่วนร่วมทุกภาคส่วน

ประเด็นยุทธศาสตร์ที่ ๗ การพัฒนาระบบบริหารและจัดการองค์กร

**<u>อัตรากำลัง</u>**

กรมป่าไม้ มีอัตรากำลังทั้งสิ้น ๑๐,๗๕๔ อัตรา แบ่งออกเป็น ๓ ประเภท ดังนี้

| | | |
|---|---|---|
| - ข้าราชการ | ๑,๙๙๕ | อัตรา |
| - ลูกจ้างประจำ | ๑,๓๕๔ | อัตรา |
| - พนักงานราชการ | ๗,๔๐๕ | อัตรา |

หมายเหตุ ข้อมูล ณ วันที่ ๑๗ กันยายน ๒๕๖๑

**<u>สถานภาพด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้</u>**

กรมป่าไม้ มีระบบงานที่ใช้ในการปฏิบัติงาน มีรายละเอียดดังนี้

๑. ระบบบริหารจัดการป่าสงวนแห่งชาติ

๒. ระบบอนุญาตด้านอุตสาหกรรมป่าไม้

๓. ระบบบริหารจัดการเรื่องร้องเรียน

๔. ระบบบริหารจัดการสิทธิ์การใช้ที่ดินป่าไม้

๕. ระบบใช้ประโยชน์พื้นที่ป่า

๖. ระบบเชื่อมโยงข้อมูลกรมการปกครอง

๗. ระบบติดตามการบุกรุกทำลายป่าและควบคุมไฟป่า

๘. ระบบฐานข้อมูลเชิงแผนที่

๙. ระบบ RFD Single Window (NSW)
๑๐. ระบบสารบรรณอิเล็กทรอนิกส์
๑๑. ระบบเว็บไซต์กรมป่าไม้
๑๒. ระบบฐานข้อมูลเลื่อยโซ่ยนต์
๑๓. ระบบจัดการฐานความรู้ด้านความหลากหลายทางชีวภาพ
๑๔. ระบบจัดการฐานข้อมูลพรรณไม้ในสวนป่า
๑๕. ระบบจัดการฐานข้อมูลแมลงในสวนป่า
๑๖. ระบบภูมิศาสตร์สารสนเทศเพื่อการบริหาร (GIS)
๑๗. ระบบจองห้องประชุมกรมป่าไม้
๑๘. ระบบจัดตั้งป่าชุมชน

**<u>สถานภาพด้านระบบเครือข่ายและการสื่อสาร กรมป่าไม้</u>**

๑. ระบบเครือข่ายของกรมป่าไม้ ซึ่งมีการเชื่อมอินเตอร์เน็ตจำนวน ๒ คู่สาย เครือข่ายทรู ความเร็ว ๓๐๐/๔๐ Mb. เครือข่าย CAT ความเร็ว ๑๘๐/๔๐ Mb.

๒. การดำเนินการด้านการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย ด้านความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย นั้น ศูนย์สารสนเทศ ได้ดำเนินการปรับปรุงระบบเครือข่ายให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ เพื่อให้ระบบคอมพิวเตอร์และเครือข่ายกรมป่าไม้ มีความมั่นคงปลอดภัยจากบุคคลผู้ไม่มีสิทธิในการเข้าถึงข้อมูล

# กระบวนการบริหารความเสี่ยง

**คำนิยามความเสี่ยง**

**ความเสี่ยง** หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตาม วัตถุประสงค์และเป้าหมายที่กำหนด

**การประเมินความเสี่ยง** หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

**การวิเคราะห์ความเสี่ยง** หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นต่อไปคือ การวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเพราะการวัดความเสี่ยงเป็นตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิดหรือโอกาสที่จะเกิดความเสี่ยง

**การบริหารความเสี่ยง** เมื่อทราบความเสี่ยงที่มีนัยสำคัญและโอกาสที่จะเกิดความเสี่ยงแล้วควรวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยง และพิจารณาว่าจะยอมรับความเสี่ยงนั้นหรือจะกำหนดกิจกรรมการควบคุมต่าง ๆ เพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้

**ความหมายของการบริหารความเสี่ยง**

**๑. ความเสี่ยง (Risk)** คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจที่กำหนด

**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) เป็นวิธีการควบคุมที่กำหนดขึ้น เพื่อป้องกันไม่ให้เกิดความเสียหายและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร 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)**

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 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

<u>หลักเกณฑ์การวิเคราะห์ความเสี่ยง</u>

(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 |

<u>หลักเกณฑ์การประเมินโอกาส (Likelihood) ที่จะเกิดความเสี่ยง</u>

| ระดับโอกาส (ความเป็นไปได้) | ความถี่ที่จะเกิดเหตุการณ์ | ระดับคะแนน |
|---|---|---|
| น้อยมาก | นานๆครั้ง (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 ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล | 5 |

การประเมินระดับความเสี่ยง

**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 พ.ศ. ๒๕๖๑ – ตุลาคม พ.ศ. ๒๕๖๒ เฝ้าระวังและติดตามผลความเสี่ยง
- เดือนตุลาคม พ.ศ. ๒๕๖๑ – พฤศจิกายน พ.ศ. ๒๕๖๒ จัดทำสรุปและรายงานผลการเฝ้าระวัง

**<u>บทบาท หน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยง</u>**

๑) บริหารระดับสูง ทำหน้าที่กำหนดนโยบายและแต่งตั้งคณะกรรมการหรือคณะทำงานในการกำกับดูแลให้มีการดำเนินการตามแผนบริหารความเสี่ยง

๒) คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ จัดทำวิธีปฏิบัติด้านเทคโนโลยีสารสนเทศ เพื่อบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้

๓) ผู้บริหารระดับสำนัก/กอง/ศูนย์ ดำเนินการบริหารความเสี่ยงในหน่วยงาน รวมทั้งติดตามประเมินผลอย่างต่อเนื่อง

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** : เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานที่รับผิดชอบไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการปฏิบัติงาน โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการที่ไม่ได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้าน และมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การ

สนับสนุนการปฏิบัติราชการ และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรอบรู้ และเชี่ยวชาญในงานที่รับผิดชอบ

**<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

**๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์** หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่างๆ ที่ได้จัดทำและพัฒนาขึ้น รวมถึงโปรแกรมประยุกต์อื่น ๆ ที่ใช้ประกอบการใช้โปรแกรม และระบบงาน เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง, ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมี ช่องโหว่ทำให้มีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่งและการถูกผู้ไม่ประสงค์ดีทำลายระบบ (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

# ตารางวิเคราะห์แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๒

| ความเสี่ยง (ภาวะคุกคาม) | ปัจจัยเสี่ยง (จุดอ่อนของระบบ) | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุมที่ผ่านมา | ประเมินผลการควบคุม | วิธีการควบคุม | กิจกรรม | ผู้รับผิดชอบ | ระยะเวลาการดำเนินงาน | การตรวจสอบติดตาม/ประเมินผลกิจกรรม |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ๑.ไวรัสคอมพิวเตอร์ที่เครื่องผู้ใช้ | -การต่อพ่วงกับอุปกรณ์ทางคอมพิวเตอร์ที่ยังไม่ได้รับการตรวจสอบไวรัส (Scan Virus)<br>-การดาวน์โหลดและติดตั้งซอฟต์แวร์ที่ไม่รู้แหล่งที่มา<br>-การเข้าเว็บไซต์ที่มีความเสี่ยงและฝัง Spyware ไว้ เช่น เว็บไซต์ดาวน์โหลดโปรแกรมฟรี, ภาพยนตร์ฟรี เป็นต้น<br>-ระบบปฏิบัติการมีช่องโหว่ | ๕ | ๓ | ๑๕ | -มีมาตรการหรือข้อบังคับในการใช้อุปกรณ์ต่อพ่วงและเข้าเว็บไซต์ เช่น ก่อนใช้งานอุปกรณ์ต่อพ่วงต้องสแกนไวรัสทุกครั้ง ห้ามเข้าเว็บไซต์ที่มีความเสี่ยง เป็นต้น<br>-ขอความร่วมมือจากผู้ใช้งานไม่ลงโปรแกรมที่เสี่ยงต่อการติดไวรัส<br>-ติดตั้งโปรแกรมป้องกันไวรัส (Anti-Virus) ให้ผู้ใช้งาน | -ผู้ใช้งานไม่ให้ความร่วมมือ<br>-เจ้าหน้าที่ดูแลไม่ทั่วถึง<br>-จำนวนโปรแกรมป้องกันไวรัสไม่เพียงพอสำหรับผู้ใช้งาน | ลด | -ประกาศมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมป่าไม้<br>-ให้ความรู้แก่ผู้ใช้งาน ให้ตระหนักถึงภัยอันตรายที่เกิดจากไวรัส<br>-จัดหาโปรแกรมป้องกันไวรัสเพิ่มเติม | ศูนย์สารสนเทศ | ต.ค.๖๑-มี.ค.๖๒ | ๓ เดือน/ครั้ง |
| ๒.การเชื่อมโยงเครือข่ายล้มเหลว | -ผู้ให้บริการเครือข่ายให้บริการล่าช้า ไม่ดูแล<br>-การเชื่อมโยงเครือข่ายล้มเหลว | ๑ | ๕ | ๕ | -จัดทำ Link สำรองในลักษณะ Load Balance | -สามารถแก้ปัญหาได้ค่อนข้างดี | ลด | -เพิ่มเนื้อหาใน TOR ให้ครอบคลุมในเรื่องการให้บริการ การรับรองคุณภาพ เช่น การปรับในกรณีที่ผู้ให้บริการเครือข่ายตอบสนองล่าช้า | ศูนย์สารสนเทศ | ต.ค.๖๑ | ๓ เดือน/ครั้ง |
| ๓.ระบบไฟฟ้าห้อง Data Center ไม่เสถียร | -ปริมาณการใช้ไฟฟ้ามาก<br>-กระแสไฟฟ้าขัดข้อง ดับ แรงดันไฟฟ้าไม่คงที่ | ๒ | ๕ | ๑๐ | -จัดหาเครื่องสำรองไฟฟ้าสำหรับห้อง Data Center | -เครื่องสำรองไฟฟ้าสำหรับห้อง Data Center สามารถสำรองไฟได้ | ลด | -ตรวจสอบระบบไฟฟ้าอย่างสม่ำเสมอ | ศูนย์สารสนเทศ | ต.ค.๖๑-ก.ย.๖๒ | ๑ ครั้ง/เดือน |

| ความเสี่ยง (ภาวะคุกคาม) | ปัจจัยเสี่ยง (จุดอ่อนของระบบ) | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุมที่ผ่านมา | ประเมินผลการควบคุม | วิธีการควบคุม | กิจกรรม | ผู้รับผิดชอบ | ระยะเวลาการดำเนินงาน | การตรวจสอบติดตาม/ประเมินผลกิจกรรม |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ๔.ละเมิดลิขสิทธิ์โปรแกรม | -บุคลากรขาดความรู้ความเข้าใจพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐<br>-บุคลากรขาดการตระหนักถึงภัยที่ได้จากการใช้โปรแกรมละเมิดลิขสิทธิ์<br>-ไม่มีโปรแกรมลิขสิทธ์ให้เจ้าหน้าที่ใช้งาน | ๕ | ๓ | ๑๕ | -มีการชี้แจงเป็นหนังสือเวียนให้กับบุคลากรภายในกรมป่าไม้ให้ทราบเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐<br>-มีการจัดประชุมเชิงปฏิบัติการเกี่ยวกับความปลอดภัยในระบบเทคโนโลยีสารสนเทศ | -บุคลากรยังไม่ตระหนักถึงภัยและความผิดที่เกิดจากการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ และยังคงมีการใช้งานโปรแกรมที่ไม่มีลิขสิทธิ์อยู่ | ลด | -รณรงค์ให้บุคลากรใช้งานโปรแกรมที่มีลิขสิทธิ์<br>-รณรงค์ให้บุคลากรใช้ซอฟต์แวร์ Open Source<br>-ให้ความรู้แก่บุคลากรถึงภัยและความผิดที่เกิดจากการใช้โปรแกรมละเมิดลิขสิทธิ์<br>-จัดหาโปรแกรมลิขสิทธ์ให้เจ้าหน้าที่ใช้งาน | -ศูนย์สารสนเทศ | ธ.ค.๖๑-มี.ค.๖๒ | ๓ เดือน/ครั้ง |
| ๕.บุคลากรกรมป่าไม้ ขาดความรู้และทักษะในการปฏิบัติงานด้านสารสนเทศ | -เจ้าหน้าที่ปฏิบัติงานไม่ตรงตามสายงาน<br>-มีการเปลี่ยนงานบ่อย<br>-หน่วยงานไม่ได้มีการจัดหลักสูตรในการอบรมด้านเทคโนโลยีสารสนเทศให้เพียงพอ | ๕ | ๓ | ๑๕ | -มีการจัดอบรมเพื่อให้บุคลากรมีความรู้ความเข้าในระบบงานที่รับผิดชอบ | -เบื้องต้นสามารถแก้ปัญหาได้ในระดับหนึ่ง | ลด | -จัดทำคู่มือการปฏิบัติงาน<br>-เพิ่มอัตรากำลังพนักงานราชการในตำแหน่งเจ้าหน้าที่ระบบงานคอมพิวเตอร์ให้หน่วยงานในส่วนภูมิภาค | -ศูนย์สารสนเทศ<br>-สำนักบริหารกลาง | มี.ค.-ก.ย.๖๒ | ๓ เดือน/ครั้ง |
| ๖.ข้อมูลสารสนเทศไม่ถูกต้องและเป็นปัจจุบัน | -ความไม่ถูกต้องของข้อมูลและข้อมูลไม่เป็นปัจจุบัน<br>-ไม่มีการกำหนดมาตรฐานในการบันทึกข้อมูล | ๕ | ๔ | ๒๐ | -ขอความร่วมมือเจ้าหน้าที่ให้ปรับปรุงข้อมูลให้เป็นปัจจุบัน<br>-จัดทำปฏิทินรายงานข้อมูลและการตรวจสอบข้อมูล | ยังไม่ได้รับความร่วมมือในการปรับปรุงข้อมูล | ลด | -จัดฝึกอบรมการใช้งานระบบอย่างสม่ำเสมอ<br>-กำหนดมาตรการในการตรวจสอบข้อมูล ก่อนนำขึ้นเผยแพร่บนเว็บไซต์<br>-กำกับ ติดตาม ให้นำเข้าข้อมูลให้เป็นปัจจุบัน<br>-มอบหมายให้เจ้าหน้าที่ปรับปรุงข้อมูลให้ครบถ้วนเป็นปัจจุบัน | -ศูนย์สารสนเทศ<br>-ฝ่ายสารสนเทศ สจป. | ต.ค.๖๑-ก.ย.๖๒ | ๓ เดือน/ครั้ง |

| ความเสี่ยง (ภาวะคุกคาม) | ปัจจัยเสี่ยง (จุดอ่อนของระบบ) | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุมที่ผ่านมา | ประเมินผลการควบคุม | วิธีการควบคุม | กิจกรรม | ผู้รับผิดชอบ | ระยะเวลาการดำเนินงาน | การตรวจสอบติดตาม/ประเมินผลกิจกรรม |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ๗.อุปกรณ์เครือข่ายไม่สามารถให้บริการได้ต่อเนื่อง | -เจ้าหน้าที่ขาดความรู้และทักษะในการแก้ไขปัญหา<br>-อุปกรณ์เครือข่ายชำรุด | ๑ | ๕ | ๕ | -จัดส่งเจ้าหน้าที่เข้ารับการอบรมเพื่อเพิ่มทักษะ<br>-จ้างบำรุงรักษาอุปกรณ์เครือข่าย | -มีการจัดอบรมแล้วแต่ยังไม่เพียงพอ<br>-ยังไม่สามารถควบคุมการใช้งานได้อย่างทั่วถึง | ลด | -ตรวจสอบความพร้อมใช้งานของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ | ศูนย์สารสนเทศ | ต.ค.๖๑-ก.ย.๖๒ | ๑ ครั้ง/เดือน |
| ๘.เครื่องแม่ข่ายไม่สามารถให้บริการได้ต่อเนื่อง | -โดนไวรัสโจมตี<br>-มีจำนวนผู้ใช้งานจำนวนมาก ไม่สามารถรองรับได้<br>-การโจมตี (Hack) ระบบ | ๒ | ๕ | ๑๐ | -ติดตั้งโปรแกรม Anti-Virus<br>-กำหนดมาตรการการเข้าใช้งานบางเว็บไซต์ เช่น ปิดการเข้าใช้งาน Facebook และ Youtube ในเวลางาน<br>-สร้างมาตรการการเข้าใช้งานระบบเครือข่าย(Policy)<br>-ดำเนินการเข้ารหัสใช้งานระบบสารสนเทศ<br>-มีการทดสอบการเจาะระบบเพื่อตรวจสอบช่องโหว่ | -เบื้องต้น สามารถแก้ไขปัญหาได้ในระดับหนึ่ง<br>-ยังไม่สามารถควบคุมการใช้งานได้อย่างทั่วถึง<br>-ยังมีการ Hack เกิดขึ้นอยู่ | ลด | -Update ซอฟต์แวร์ Anti-Virus ทุกเดือน<br>-จัดทำหนังสือแจ้งเตือนผู้ใช้งานที่ไม่เหมาะสม<br>จัดทำระบบสำรองข้อมูล<br>-กำหนดรหัส (encryption) ระบบสารสนเทศ<br>-จ้างที่ปรึกษาตรวจสอบหาช่องโหว่ของซอฟต์แวร์ | ศูนย์สารสนเทศ | ต.ค.๖๑-ก.ย.๖๒ | ๓ เดือน/ครั้ง |
| ๙.ระบบงานสารสนเทศของกรมไม่สามารถบริการได้ | -Harddisk เสียหาย<br>-Raid Controller เสียหาย<br>-Switch และ Router เสียหาย<br>-มีจำนวนผู้ใช้งานปริมาณมาก ไม่สามารถรับรองได้<br>ไม่มีคู่มือในการติดตั้งและปรับปรุงระบบ | ๑ | ๕ | ๕ | -จัดทำระบบสำรองข้อมูล | -เบื้องต้นสามารถแก้ไขปัญหาได้ในระดับหนึ่ง | ลด | -ตรวจสอบระบบสำรองข้อมูลและอุปกรณ์ทุกไตรมาส<br>-จัดทำไซต์สำรอง (DR-Site) | ศูนย์สารสนเทศ | ต.ค.๖๑-ก.ย.๖๒ | ๓ เดือน/ครั้ง |

| ความเสี่ยง (ภาวะคุกคาม) | ปัจจัยเสี่ยง (จุดอ่อนของระบบ) | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุมที่ผ่านมา | ประเมินผลการควบคุม | วิธีการควบคุม | กิจกรรม | ผู้รับผิดชอบ | ระยะเวลาการดำเนินงาน | การตรวจสอบติดตาม/ประเมินผลกิจกรรม |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ๑๐.ไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center | -การเสื่อมสภาพของอุปกรณ์ป้องกันการเกิดไฟไหม้<br>-การเสื่อมสภาพของอุปกรณ์ดับไฟ | ๑ | ๕ | ๕ | -ติดตั้งระบบดับเพลิง | -เบื้องต้นสามารถแก้ไขปัญหาได้ในระดับหนึ่ง | ลด | -ตรวจสอบข้อมูลอุปกรณ์ดับเพลิงให้สม่ำเสมอ<br>-จัดทำไซต์สำรอง (DR-Site) | ศูนย์สารสนเทศ | ต.ค.๖๑-ก.ย.๖๒ | ๑ เดือน/ครั้ง |
| ๑๑.ภัยธรรมชาติ | -ภัยธรรมชาติทุกด้าน | ๑ | ๕ | ๕ | ไม่มี | ไม่มี | ลด | -จัดทำไซต์สำรอง (DR-Site) ให้ครบทุกระบบงาน | ศูนย์สารสนเทศ | ม.ค.-มิ.ย.๖๒ | ๑ ครั้ง/ปี |
| ๑๒.สถานการณ์การเมือง | -ไม่สามารถเข้าปฏิบัติงานที่หน่วยงานได้ | ๑ | ๕ | ๕ | ไม่มี | ไม่มี | ลด | -ทบทวนแผนรองรับสถานการณ์ฉุกเฉินและซักซ้อมตามแผน | ศูนย์สารสนเทศ | ส.ค.-ก.ย.๖๒ | ๑ ครั้ง/ปี |
| ๑๓.อุปกรณ์ it ถูกโจรกรรม | -ขาดมาตรการระบบรักษาความปลอดภัย เช่น ระบบการเข้าเวรยาม เป็นต้น | ๑ | ๕ | ๕ | -มียามประจำอาคาร<br>-ติดตั้งกล้องวงจรปิด | -การรักษาความปลอดภัยอาจยังไม่ครอบคลุม | ลด | -ตรวจสอบกล้องวงจรปิดให้สามารถใช้งานได้ | ทุกหน่วยงาน | ต.ค.๖๑-ก.ย.๖๒ | ๓ เดือน/ครั้ง |

# แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมป่าไม้ ประจำปีงบประมาณ พ.ศ. ๒๕๖๒

| ความเสี่ยง | กิจกรรม | ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๒ | | | | | | | | | | | | การตรวจสอบ/ติดตาม | ผู้รับผิดชอบ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ๒๕๖๑ | | | ๒๕๖๒ | | | | | | | | | | |
| | | 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.ไวรัสคอมพิวเตอร์ที่เครื่องผู้ใช้ | -ประกาศมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ | ← | — | → | | | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -ให้ความรู้แก่ผู้ใช้งาน ให้ตระหนักถึงภัยอันตรายที่เกิดจากไวรัส | | | ← | — | → | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จัดหาโปรแกรมป้องกันไวรัสเพิ่มเติม | | | | ← | — | → | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| ๒.การเชื่อมโยงเครือข่ายล้มเหลว | -เพิ่มเนื้อหาใน TOR ให้ครอบคลุมในเรื่องการให้บริการการรับรองคุณภาพ เช่น การปรับ ในกรณีที่ผู้ให้บริการเครือข่ายตอบสนองล่าช้า | ← | → | | | | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| ๓.ระบบไฟฟ้าห้อง Data Center ไม่เสถียร | -ตรวจสอบระบบไฟฟ้าอย่างสม่ำเสมอ | ← | — | — | — | — | — | — | — | — | — | — | → | ๑ ครั้ง/เดือน | ศูนย์สารสนเทศ |
| ๔.ละเมิดลิขสิทธิ์โปรแกรม | -รณรงค์ให้บุคลากรใช้งานโปรแกรมที่มีลิขสิทธิ์ | | | ← | — | → | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -รณรงค์ให้บุคลากรใช้ซอฟต์แวร์ Open Source | | | ← | — | → | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -ให้ความรู้แก่บุคลากรถึงภัยและความผิดที่เกิดจากการใช้โปรแกรมละเมิดลิขสิทธิ์ | | | ← | — | → | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จัดหาโปรแกรมลิขสิทธิ์ให้เจ้าหน้าที่ใช้งาน | | | | ← | — | → | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| ๕.บุคลากรกรมป่าไม้ ขาดความรู้และทักษะในการปฏิบัติงานด้านสารสนเทศ | -จัดทำคู่มือการปฏิบัติงาน | | | | | | ← | — | → | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -เพิ่มอัตรากำลังพนักงานราชการในตำแหน่งเจ้าหน้าที่ระบบงานคอมพิวเตอร์ให้หน่วยงานในส่วนภูมิภาค | | | | | | | ← | — | — | — | — | → | ๓ เดือน/ครั้ง | สำนักบริหารกลาง |

| ความเสี่ยง | กิจกรรม | ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๒ | | | | | | | | | | | | การตรวจสอบ/ติดตาม | ผู้รับผิดชอบ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ๒๕๖๑ | | | ๒๕๖๒ | | | | | | | | | | |
| | | 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.ข้อมูลสารสนเทศไม่ถูกต้องและเป็นปัจจุบัน | -จัดฝึกอบรมการใช้งานระบบอย่างสม่ำเสมอ | | | | ← | | → | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -กำหนดมาตรการในการตรวจสอบข้อมูล ก่อนนำขึ้นเผยแพร่บนเว็บไซต์ | | | | ← | → | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -กำกับ ติดตาม ให้นำเข้าข้อมูลให้เป็นปัจจุบัน | | | ← | | | | | | | | | → | ๓ เดือน/ครั้ง | ฝ่ายสารสนเทศ สจป. |
| | -มอบหมายให้เจ้าหน้าที่ปรับปรุงข้อมูลให้ครบถ้วนเป็นปัจจุบัน | ← | → | | | | | | | | | | | ๓ เดือน/ครั้ง | ฝ่ายสารสนเทศ สจป. |
| **๗..อุปกรณ์เครือข่ายไม่สามารถให้บริการได้ต่อเนื่อง** | -ตรวจสอบความพร้อมใช้งานของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ | ← | | | | | | | | | | | → | ๑ ครั้ง/เดือน | ศูนย์สารสนเทศ |
| ๘.เครื่องแม่ข่ายไม่สามารถให้บริการได้ต่อเนื่อง | -Update ซอฟต์แวร์ Anti-Virus ทุกเดือน | ← | | | | | | | | | | | → | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จัดทำหนังสือแจ้งเตือนผู้ใช้งานที่ไม่เหมาะสม | ← | | | | | | | | | | | → | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จัดทำระบบสำรองข้อมูล | | | | ← | | | → | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -กำหนดรหัส (encryption) ระบบสารสนเทศ | ← | | | → | | | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จ้างที่ปรึกษาตรวจสอบหาช่องโหว่ของซอฟต์แวร์ | | | | ← | | → | | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| ๙.ระบบงานสารสนเทศของกรมไม่สามารถบริการได้ | -ตรวจสอบระบบสำรองข้อมูลและอุปกรณ์ทุกไตรมาส | | | ↔ | | | ↔ | | | ↔ | | | ↔ | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จัดทำไซต์สำรอง (DR-Site) | | | | ← | | | → | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| ๑๐.ไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center | -ตรวจสอบข้อมูล อุปกรณ์ดับเพลิงให้สม่ำเสมอ | ← | | | | | | | | | | | → | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จัดทำไซต์สำรอง (DR-Site) | | | | ← | | | → | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |

| ความเสี่ยง | กิจกรรม | ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๒ | | | | | | | | | | | | การตรวจสอบ/ติดตาม | ผู้รับผิดชอบ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ๒๕๖๑ | | | ๒๕๖๒ | | | | | | | | | | |
| | | ต.ค. | พ.ย. | ธ.ค. | ม.ค. | ก.พ. | มี.ค. | เม.ย. | พ.ค. | มิ.ย. | ก.ค. | ส.ค. | ก.ย. | | |
| ๑๑.ภัยธรรมชาติ | -จัดทำไซต์สำรอง (DR-Site) ให้ครบทุกระบบงาน | | | | ← | — | — | → | | | | | | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| | -จัดทำแผนรองรับสถานการณ์ฉุกเฉินและซักซ้อมตามแผน | | | | | | | | | | | | ↔ | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| **๑๒.สถานการณ์การเมือง** | -จัดทำแผนรองรับสถานการณ์ฉุกเฉินและซักซ้อมตามแผน | | | | | | | | | | | | ↔ | ๓ เดือน/ครั้ง | ศูนย์สารสนเทศ |
| **๑๓.อุปกรณ์ it ถูกโจรกรรม** | -ตรวจสอบกล้องวงจรปิดให้สามารถใช้งานได้ | | | ↔ | | | ↔ | | | ↔ | | | ↔ | ๓ เดือน/ครั้ง | ทุกหน่วยงาน |

๑๑

พิจารณาเห็นชอบดำเนินการ

ลงชื่อ.....

(.....)

ตำแหน่ง.....

# ภาคผนวก

สำเนา

คำสั่งกรมป่าไม้

ที่ ๒๕๘๕ /๒๕๖๑

เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

---

เพื่อเป็นการเตรียมความพร้อมและลดความเสี่ยงจากสถานการณ์ฉุกเฉินต่างๆ เช่น ภัยคุกคาม ไวรัส ไฟดับ ไฟไหม้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ จึงแต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้และแผนรองรับภาวะฉุกเฉิน ประกอบด้วย

| | | |
|---|---|---|
| ๑. ผู้อำนวยการสำนักแผนงานและสารสนเทศ | | ที่ปรึกษาคณะทำงาน |
| ๒. ผู้อำนวยการศูนย์สารสนเทศ | สำนักแผนงานและสารสนเทศ | หัวหน้าคณะทำงาน |
| ๓. นายสุกันฑ์ พึ่งกุล | นักวิชาการป่าไม้ชำนาญการ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๔. นางสาวณัฏฐิณี ปิ่นเนียม | นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๕. ว่าที่ร้อยตรีนพดล เกษจันทร์ | เจ้าพนักงานพัสดุชำนาญงาน สำนักบริหารกลาง | คณะทำงาน |
| ๖. นายไกรวุฒิ ศิริอ่อน | นักวิชาการป่าไม้ปฏิบัติการ สำนักจัดการที่ดินป่าไม้ | คณะทำงาน |
| ๗. นายพิทยา หาดชุม | นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๘. นายทนงศักดิ์ มนตรี | นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๙. นายประพันธ์พงษ์ คงศรีรอด | นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๑๐. นายวีร์ ศรีทิพโพธิ์ | นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักแผนงานและสารสนเทศ | คณะทำงาน |

/๑๑.นายธนวรรธน์...

| | | |
|---|---|---|
| ๑๑. นายธนวรรธน์ พงษ์เกิด | นักวิเคราะห์นโยบายและแผนชำนาญการ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๑๒. นางสาวกนกวรรณ ศิริสุขไพบูลย์ | เจ้าหน้าที่ระบบงานคอมพิวเตอร์ สำนักส่งเสริมการปลูกป่า | คณะทำงาน |
| ๑๓. นายชาลิสา นิลกำแหง | เจ้าหน้าที่เครื่องคอมพิวเตอร์ สำนักป้องกันรักษาป่าและควบคุมไฟป่า | คณะทำงาน |
| ๑๔. นายสุรเชษฐ์ เศรณีวิจัยกิจการ | เจ้าหน้าที่วิเคราะห์นโยบายและแผน สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๑๕. นายดำรงศักดิ์ ธนีบุญ | เจ้าหน้าที่ระบบงานคอมพิวเตอร์ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๑๖. นายวิบูลย์ชัย ปาสองห้อง | เจ้าหน้าที่บริหารงานทั่วไป สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๑๗. นายจักรพงษ์ ดรแก้วริมขวา | เจ้าหน้าที่เครื่องคอมพิวเตอร์ สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๑๘. นายณภัทร์ ดลเสถียร | เจ้าหน้าที่บริหารงานทั่วไป สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๑๙. นายสมชาย เขียวตี๋ | เจ้าหน้าที่บันทึกข้อมูล สำนักแผนงานและสารสนเทศ | คณะทำงาน |
| ๒๐. นางสาวสพินนา อ่อนเพ็ง | นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักแผนงานและสารสนเทศ | คณะทำงาน และเลขานุการ |
| ๒๑. นางสาวณัฐพร นาเกลือ | นักวิชาการป่าไม้ สำนักแผนงานและสารสนเทศ | คณะทำงาน และผู้ช่วยเลขานุการ |

<u>อำนาจหน้าที่</u>

ให้คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ มีอำนาจหน้าที่ ดังต่อไปนี้

๑) ทบทวนและวิเคราะห์ให้ความคิดเห็นในการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้และแผนรองรับภาวะฉุกเฉิน

๒) เสนอแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้และแผนรองรับภาวะฉุกเฉินต่อผู้บริหารเพื่อให้ความเห็นชอบ

/๓) แจ้งเวียน...

๓) แจ้งเวียน เผยแพร่ แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้ให้แก่บุคลากรกรมป่าไม้และแผนรองรับภาวะฉุกเฉินได้รับทราบ และแจ้งผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้

๔) สรุปรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมป่าไม้และแผนรองรับภาวะฉุกเฉิน

๕) ประสานและปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๒ สิงหาคม พ.ศ. ๒๕๖๑

(ลงนาม) จเรศักดิ์ นันตะวงษ์

(นายจเรศักดิ์ นันตะวงษ์)

รองอธิบดี ปฏิบัติราชการแทน

อธิบดีกรมป่าไม้

สำเนาถูกต้อง

(นางสาวสพินนา อ่อนเพ็ง)

นักวิชาการคอมพิวเตอร์ชำนาญการ


# แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

จัดทำโดย
ศูนย์สารสนเทศ
สำนักแผนงานและสารสนเทศ

# สารบัญ

# แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบสารสนเทศ

**๑. บทนำ**

ปัจจุบันกรมป่าไม้ได้พัฒนาระบบเครือข่าย ทั้งภายในและภายนอก เพื่อใช้ในการเชื่อมโยงข้อมูล และยังมีการพัฒนาระบบงานต่างๆ สำหรับใช้ในการบริหารจัดการ การปฏิบัติงาน และเผยแพร่ประชาสัมพันธ์ ดังนั้น เพื่อให้สามารถใช้งานเครือข่ายและระบบงานต่างๆ ได้อย่างต่อเนื่อง ทั้งนี้อาจจะเกิดความเสียหายจากการถูกโจมตีจากไวรัสคอมพิวเตอร์ ปัญหาไฟฟ้า อัคคีภัย วาตภัย บุคลากร หรือปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศ เพื่อป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้น รวมถึงสามารถจัดการแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดสถานการณ์ฉุกเฉินได้ในระยะเวลาที่เหมาะสม จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ เพื่อทำให้กรมป่าไม้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ

**๒. วัตถุประสงค์**

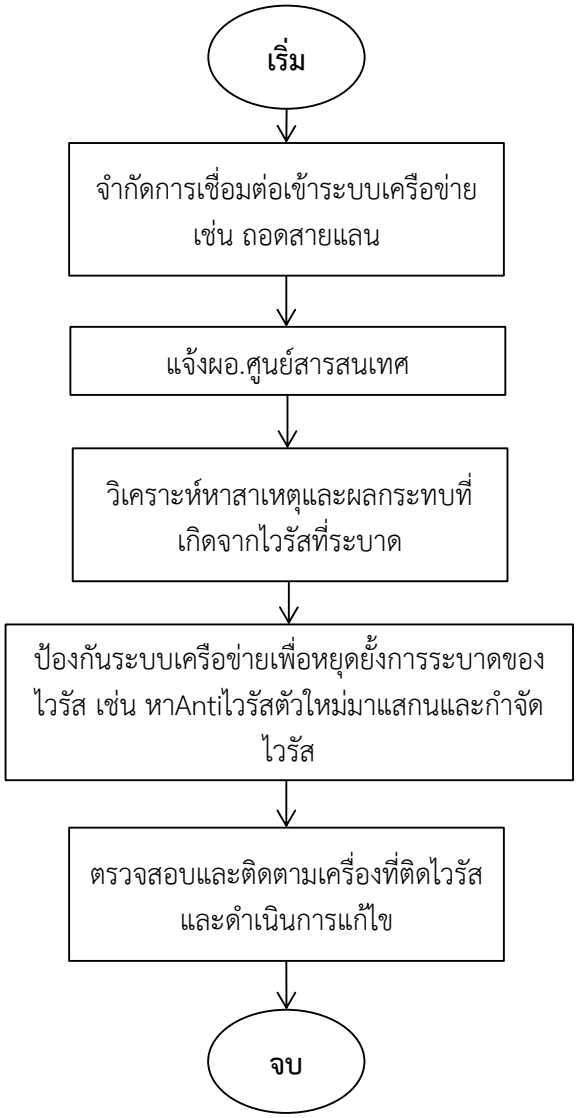
๑. เพื่อให้กรมป่าไม้มีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศที่สามารถรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนทศได้อย่างมีประสิทธิภาพและประสิทธิผล

๒. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๓. เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุด และลดโอกาสความเสียหายที่อาจเกิดขึ้น

๔. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | **๓.๑ สถานการณ์ที่เกิดจากความขัดข้องทางเทคนิค** | **แก้ไขครั้งที่ : ๐๐** |
| | **ขั้นตอนการปฏิบัติ :** ๓.๑.๑ กรณีการป้องกันไวรัสล้มเหลว | **หน้าที่ : ๒** |




**ผู้รับผิดชอบ**

**ทนงศักดิ์ กิตติทัศน์ ปรียานุช**

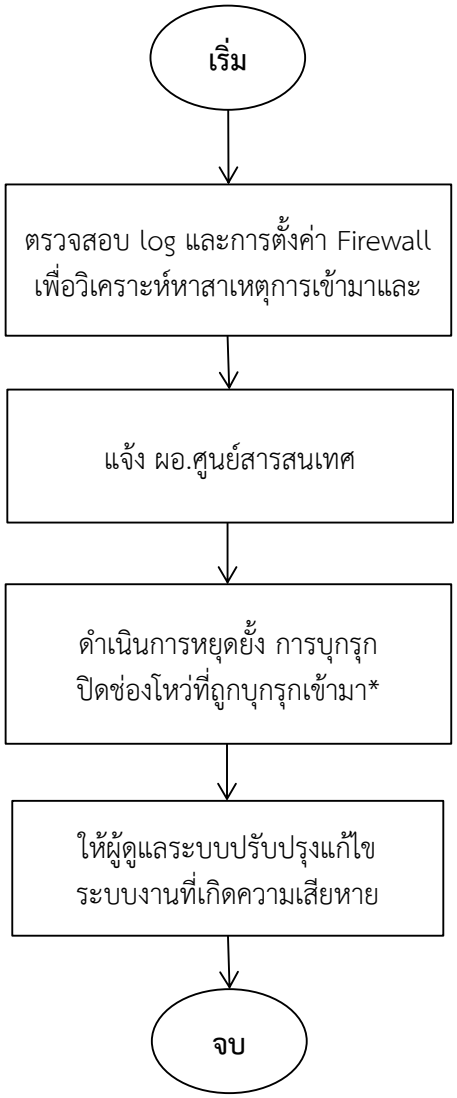
**ทนงศักดิ์**

**ทนงศักดิ์ บริษัท เบย์ คอมพิวติ้ง จำกัด**

**ทนงศักดิ์ กิตติทัศน์ ปรียานุช**

**กิตติทัศน์ ปรียานุช ณภัทร**

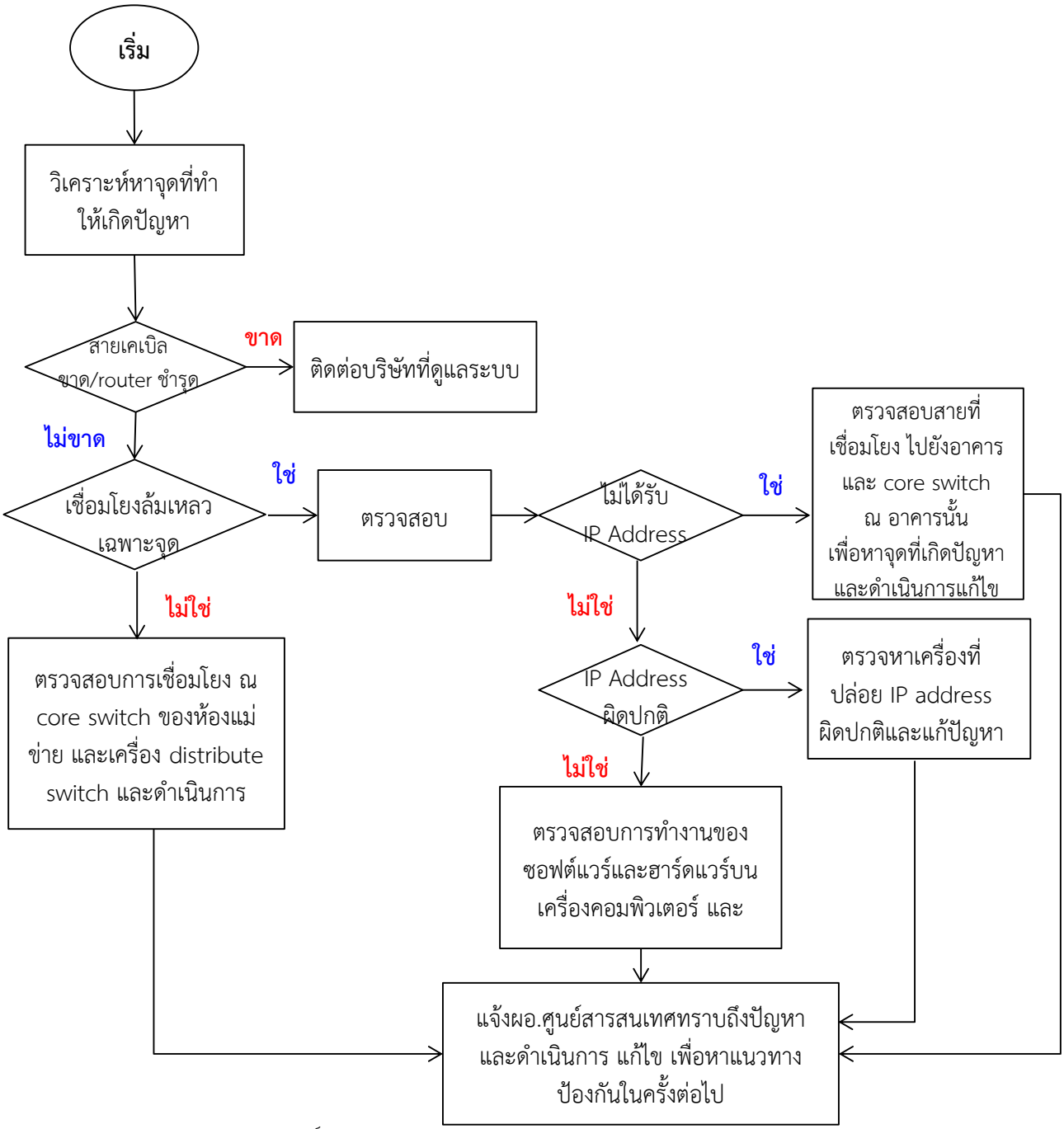
| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | **๓.๑ สถานการณ์ที่เกิดจากความขัดข้องทางเทคนิค** | **แก้ไขครั้งที่ : ๐๐** |
| | **ขั้นตอนการปฏิบัติ :** ๓.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว | **หน้าที่ : ๓** |




| ผู้รับผิดชอบ |
|---|
| ประพันธ์พงษ์ ทนงศักดิ์ |
| ทนงศักดิ์ |
| ณัฏฐิณี นรนันท์ ดำรงศักดิ์ |
| สพินนา วีร์ ดำรงศักดิ์ |

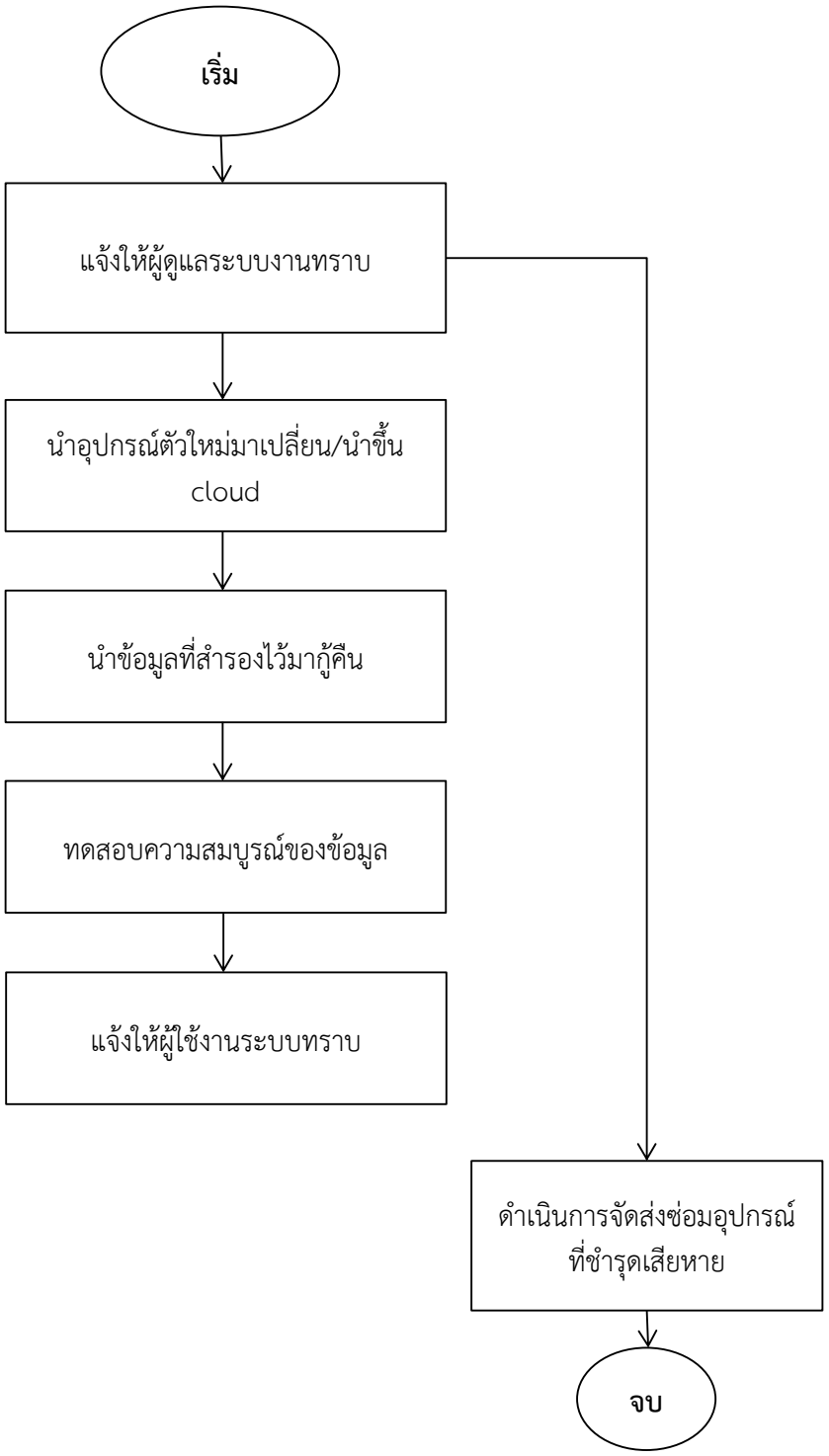
หมายเหตุ : *ดำเนินการได้โดยอัพเดท patch

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | **๓.๑ สถานการณ์ที่เกิดจากความขัดข้องทางเทคนิค** | **แก้ไขครั้งที่ : ๐๐** |
| | **ขั้นตอนการปฏิบัติ :** ๓.๑.๓ กรณีการเชื่อมโยงล้มเหลว | **หน้าที่ : ๔** |




ผู้รับผิดชอบ ประพันธ์พงษ์ ทนงศักดิ์ ณภัทร กิตติทัศน์

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | **๓.๑ สถานการณ์ที่เกิดจากความขัดข้องทางเทคนิค** | **แก้ไขครั้งที่ : ๐๐** |
| | **ขั้นตอนการปฏิบัติ :** ๓.๑.๔ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย | **หน้าที่ : ๕** |




**ผู้รับผิดชอบ**

**กิตติทัศน์ ปรียานุช ณภัทร**

**ทนงศักดิ์ ประพันธ์พงษ์ วีร์**

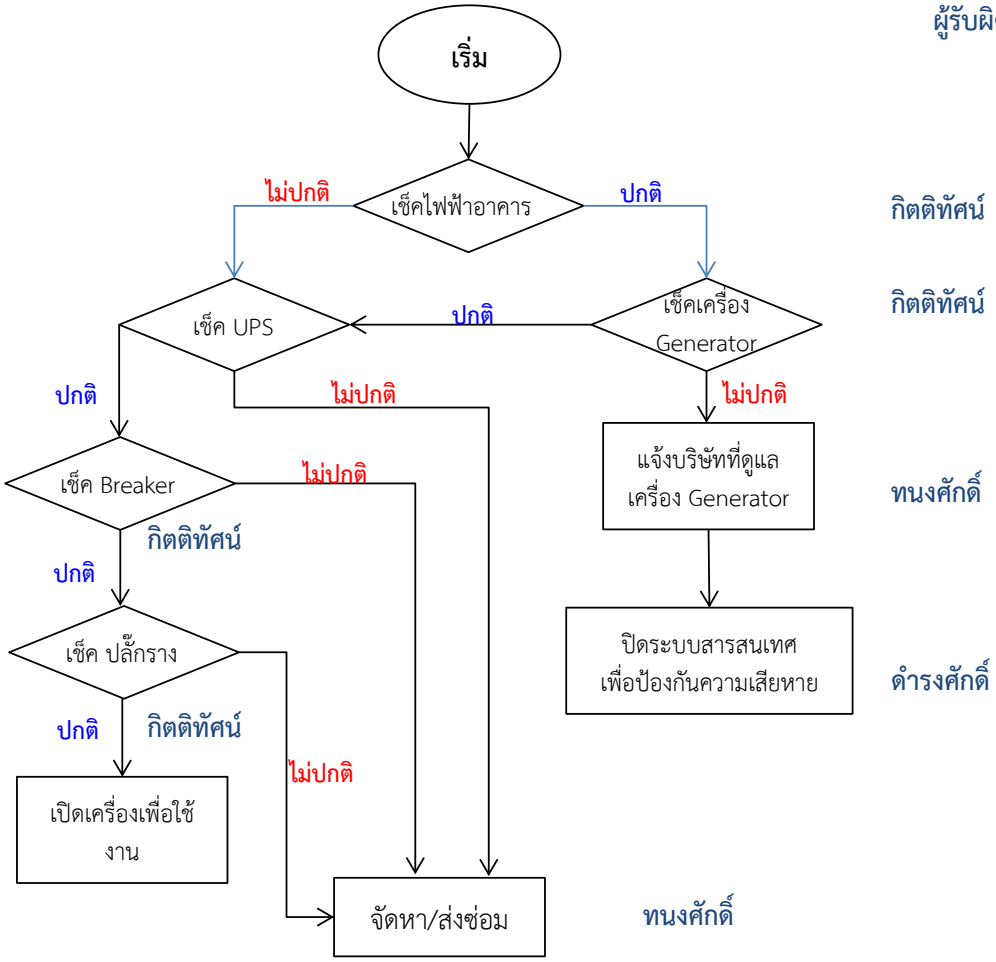
**สพินนา วีร์ ดำรงศักดิ์**

**สพินนา วีร์ ดำรงศักดิ์**

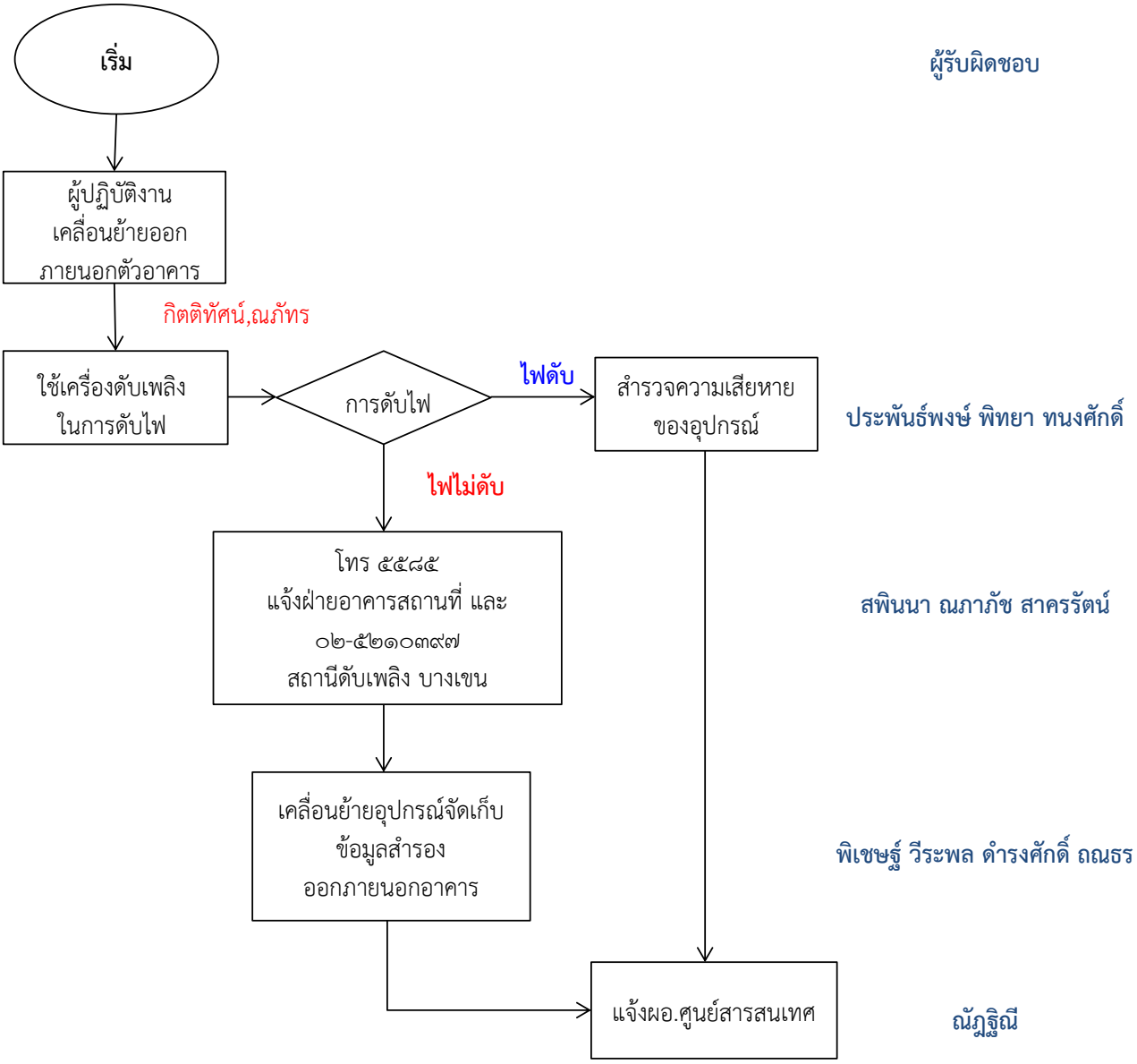
**สพินนา ดำรงศักดิ์**

**ทนงศักดิ์**

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | ๓.๑ สถานการณ์ที่เกิดจากความขัดข้องทางเทคนิค | แก้ไขครั้งที่ : ๐๐ |
| | ขั้นตอนการปฏิบัติ : ๓.๑.๕ กรณีไฟฟ้าขัดข้อง | หน้าที่ : ๖ |

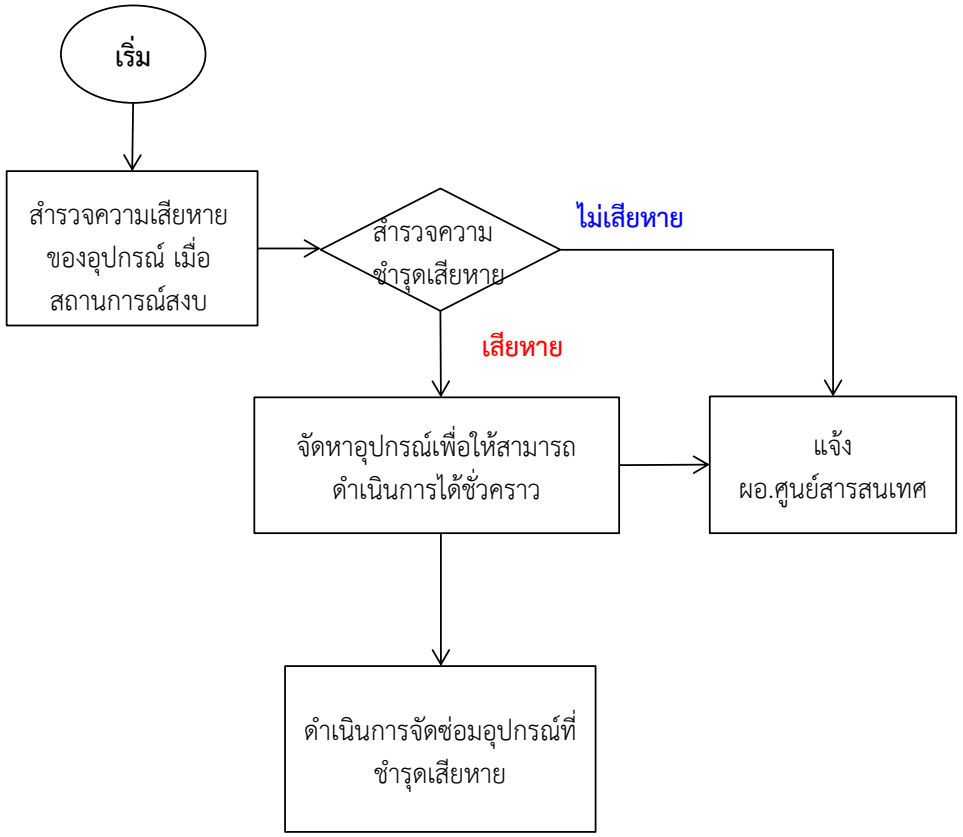


| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | ๓.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ | แก้ไขครั้งที่ : ๐๐ |
| | ขั้นตอนการปฏิบัติ : ๓.๒.๑ กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่) | หน้าที่ : ๗ |




กรณี ใช้ออกซิเจนเหลวในการดับไฟ ห้ามเจ้าหน้าที่อยู่ในห้อง data center เด็ดขาด

| กรมป่าไม้ | แผนรองรับสถานการณ์ฉุกเฉิน | |
|---|---|---|
| | ๓.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ | แก้ไขครั้งที่ : ๐๐ |
| | **ขั้นตอนการปฏิบัติ :** ๓.๒.๑ กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่) | หน้าที่ : ๘ |



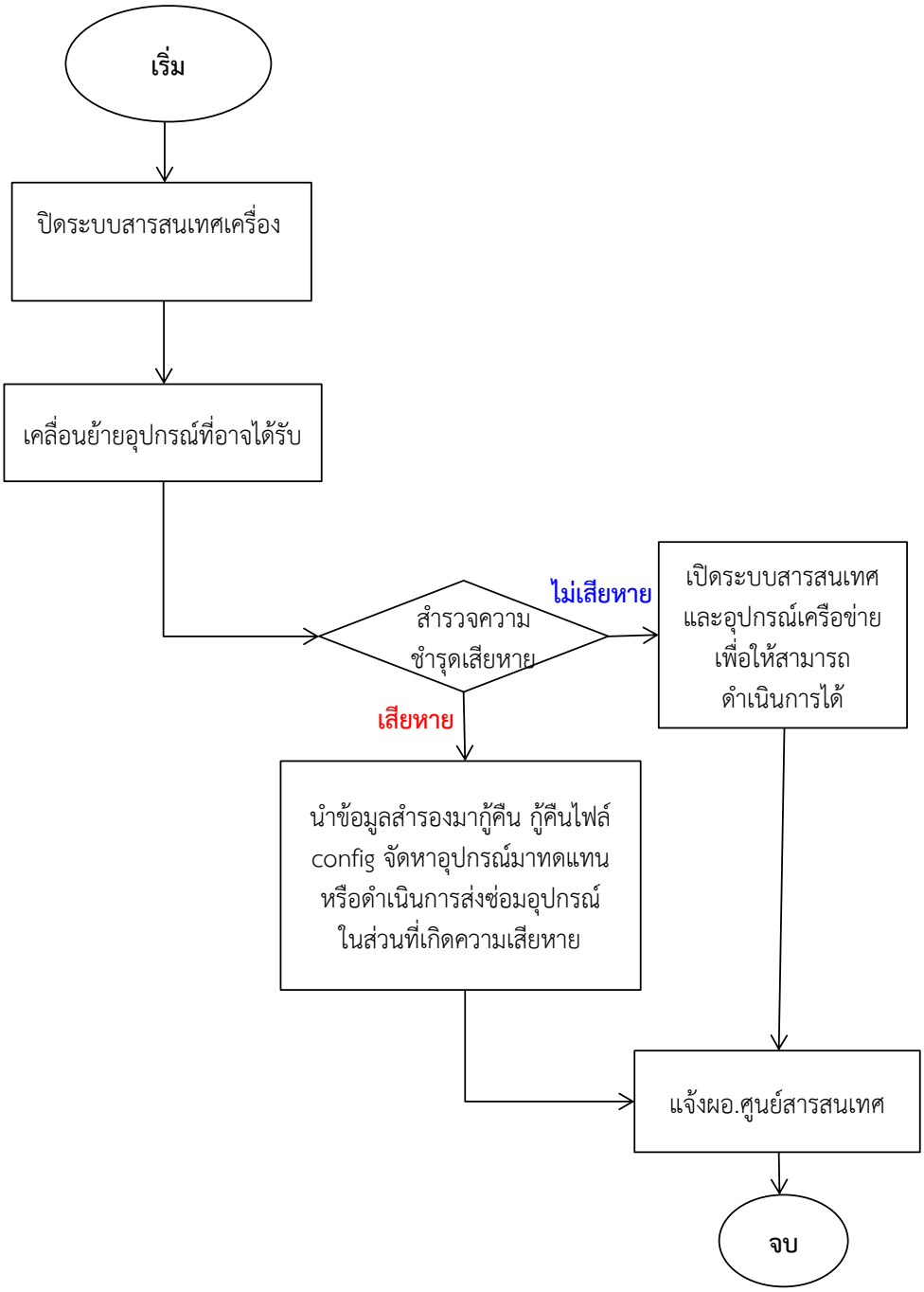

**ผู้รับผิดชอบ**

**ประพันธ์พงษ์ พิทยา ทนงศักดิ์**

**ประพันธ์พงษ์ พิทยา ทนงศักดิ์**

**ประพันธ์พงษ์ พิทยา ทนงศักดิ์**

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | ๓.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ | แก้ไขครั้งที่ : ๐๐ |
| | ขั้นตอนการปฏิบัติ : ๓.๒.๒ กรณีน้ำท่วม | หน้าที่ : ๙ |




ผู้รับผิดชอบ

ดำรงศักดิ์ วีร์ ทนงศักดิ์

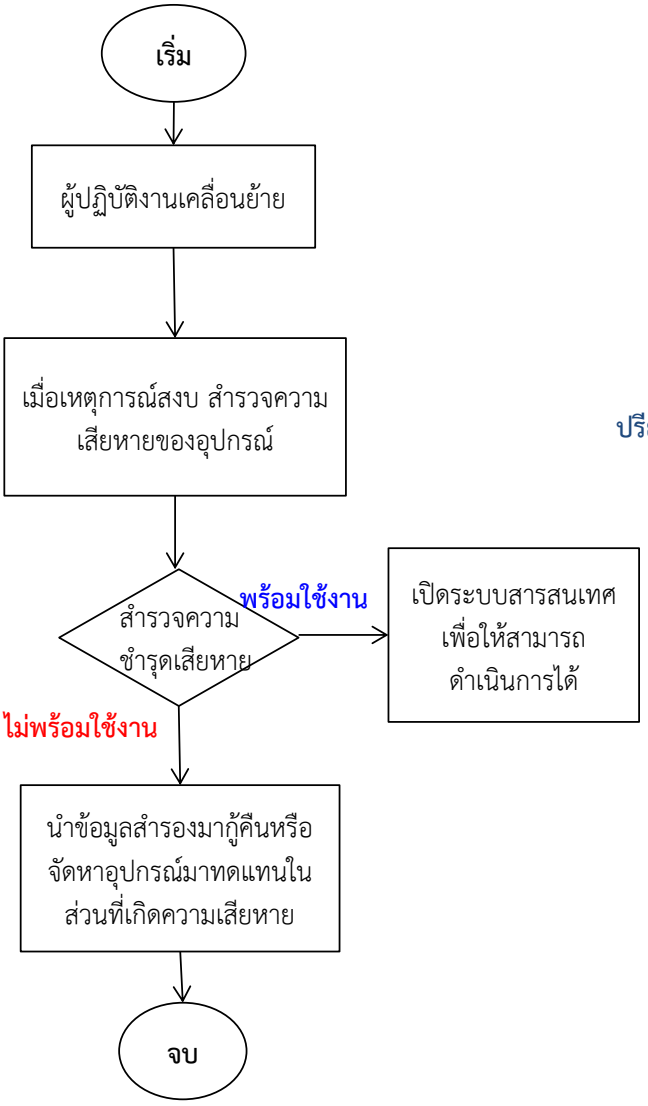
กิตติทัศน์ ณภัทร เอกรัตน์
พิเชษฐ์ วิบูลย์ชัย

ดำรงศักดิ์ วีร์ ทนงศักดิ์

ประพันธ์พงษ์ ดำรงศักดิ์
สพินนา

สพินนา ณัฏฐิณี

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | ๓.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ | แก้ไขครั้งที่ : ๐๐ |
| | ขั้นตอนการปฏิบัติ : ๓.๒.๓ กรณีแผ่นดินไหว | หน้าที่ : ๑๐ |



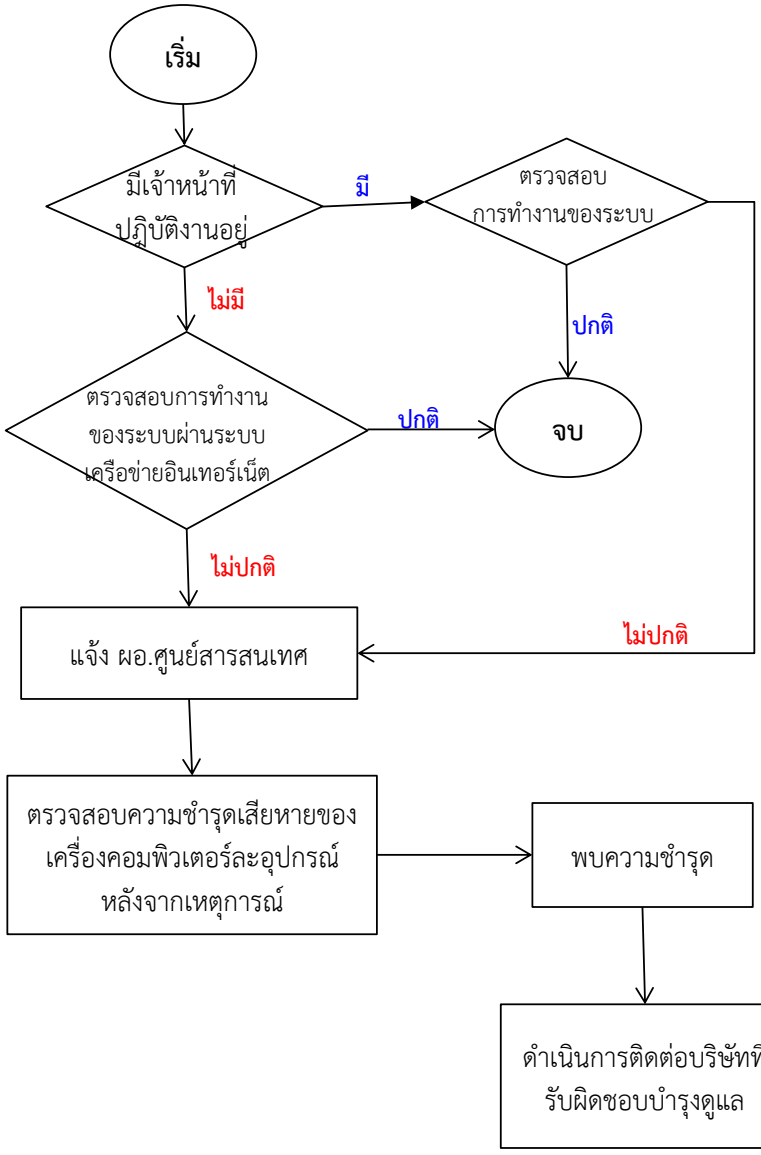

ผู้รับผิดชอบ

ปรียานุช กิตติทัศน์ วีร์ นรนันท์

ดำรงศักดิ์ วีร์ พิทยา

ดำรงศักดิ์ วีร์ พิทยา

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | ๓.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง | แก้ไขครั้งที่ : ๐๐ |
| | ขั้นตอนการปฏิบัติ : ๓.๓.๑ กรณีความไม่สงบเรียบร้อยในบ้านเมือง | หน้าที่ : ๑๑ |




ผู้รับผิดชอบ

ดำรงศักดิ์ พิทยา

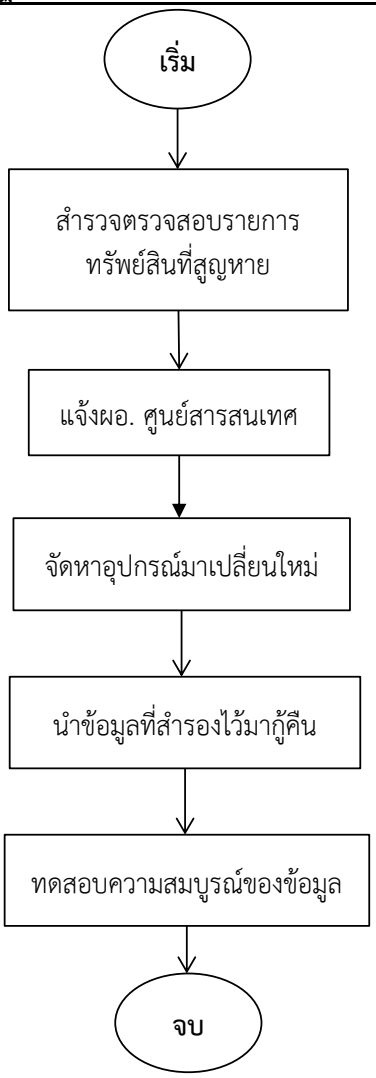
ดำรงศักดิ์ พิทยา

ทนงศักดิ์

ประพันธ์พงษ์ ทนงศักดิ์

ประพันธ์พงษ์
ทนงศักดิ์ สพินนา

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | ๓.๔ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล | แก้ไขครั้งที่ : ๐๐ |
| | ขั้นตอนการปฏิบัติ : ๓.๔.๑ กรณีโจรกรรม | หน้าที่ : ๑๒ |




| ผู้รับผิดชอบ |
|---|
| ทนงศักดิ์ |
| ณัฏฐิณี |
| ประพันธ์พงษ์ พิทยา |
| ดำรงศักดิ์ วีร์ นรนันท์ |
| ดำรงศักดิ์ วีร์ นรนันท์ |

| กรมป่าไม้ | แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ | |
|---|---|---|
| | **๓.๔ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล** | **แก้ไขครั้งที่ : ๐๐** |
| | **ขั้นตอนการปฏิบัติ :** ๓.๔.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้ | **หน้าที่ : ๑๓** |