แผนบริหารจัดการความเสี่ยงด้านดิจิทัล และ แผนแก้ไขปัญหาจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงมหาดไทย

บำบัดทุกข์ บำรุงสุข

Change for Good

แผนบริหารจัดการความเสี่ยงด้านดิจิทัล
และแผนแก้ไขปัญหาจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

โดย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงมหาดไทย

กระทรวงมหาดไทย

สารบัญ

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

การบริหารความเสี่ยงเป็นเครื่องมือกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลที่ดี โดยช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ ทั้งนี้ ต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

สำนักงานปลัดกระทรวงมหาดไทย เป็นหน่วยงานที่มีภารกิจเกี่ยวกับการพัฒนายุทธศาสตร์และแปลงนโยบายด้านดิจิทัลของกระทรวงเป็นแผนการปฏิบัติงาน จัดสรรทรัพยากรและบริหารราชการทั่วไปของสำนักงานปลัดกระทรวงมหาดไทย รวมถึงส่งเสริมและสนับสนุนการบริหารราชการส่วนภูมิภาค เพื่อให้บรรลุเป้าหมายและเกิดผลสัมฤทธิ์ตามภารกิจของกระทรวง ตลอดจนการรวบรวมข้อมูลเพื่อใช้ในการนำเสนอผู้บริหาร ดังนั้น การนำเทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน โดยมีศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานกำหนดแนวทางและระเบียบในการจัดระบบการสำรวจ การจัดเก็บ การประมวลผล การใช้ประโยชน์และการพัฒนาระบบข้อมูลสารสนเทศ และบริการสื่อสารของหน่วยงานในสังกัดสำนักงานปลัดกระทรวงมหาดไทย และเป็นศูนย์ข้อมูลสารสนเทศเพื่อการบริหารของกระทรวง และสนับสนุนเครื่องมือและอุปกรณ์สารสนเทศและการสื่อสารแก่ส่วนราชการและจังหวัด จึงมีความจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด และหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้นอันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย รวมถึงลดโอกาสความเสียหายที่อาจเกิดขึ้น ซึ่งการบริหารจัดการความเสี่ยงของสำนักงานปลัดกระทรวงมหาดไทย มีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริง และนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในดำเนินการต่อไป

๑.๒ วัตถุประสงค์

๑. เพื่อให้การจัดการภายในสำนักงานปลัดกระทรวงมหาดไทย มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศและการสื่อสาร

๒. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย

๓. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๕. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

สำนักงานปลัดกระทรวงมหาดไทยได้กำหนดวัตถุประสงค์ให้สอดคล้องกับยุทธศาสตร์และทิศทางโดยใช้หลัก SMART

Specific	:	ชัดเจน
Measurable	:	วัดได้
Achievable	:	ปฏิบัติได้
Reasonable	:	สมเหตุสมผล
Time Constrained	:	มีกรอบเวลา

๑.๓ เป้าหมาย

สำนักงานปลัดกระทรวงมหาดไทย มีแผนสำหรับดำเนินการเพื่อจัดการความเสี่ยง ดังนี้

๑. มีแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒. มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๓. มีแผนบริหารความต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔. สามารถนำแผนบริหารจัดการความเสี่ยงไปใช้เพื่อเป็นกรอบแนวทางในการดำเนินงานขององค์กรได้

๑.๔. ขอบเขตการดำเนินงาน

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการภายในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ซึ่งจะมีการรวบรวมและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงมหาดไทย

๑.๕. ประโยชน์ที่คาดว่าจะได้รับ

๑. หน่วยงานมีความพร้อมในการรับรองสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบสารสนเทศ ระบบฐานข้อมูลและการจัดเก็บข้อมูล

๒. มีแนวทางในการดูแลบำรุงรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีเสถียรภาพและมีความพร้อมใช้งานอย่างต่อเนื่อง

๓. ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน การบริหารจัดการความเสี่ยงทำให้รูปแบบการตัดสินใจการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์วัตถุประสงค์ขององค์กรและรดับความเสี่ยงอย่างชัดเจน

บทที่ ๒
ความเป็นมาและความสำคัญของบริหารความเสี่ยง

๒.๑ ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
๒. การระบุความเสี่ยงต่าง ๆ (Event Identification)
๓. การประเมินความเสี่ยง (Risk Assessment)
๔. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
๕. กิจกรรมการบริหารความเสี่ยง (Control Activities)
๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
๗. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

บทที่ ๓
การประเมินความเสี่ยง (Risk assessment)

๓.๑ การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงมหาดไทยสามารถแยกประเภทความเสี่ยงด้านเป็น ๕ ประเภท ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงจากอุปกรณ์ เป็นความเสี่ยงที่อาจเกิดจากความเสื่อมสภาพของอุปกรณ์ต่าง ๆ ที่อาจส่งผลกระทบกับการดำเนินงานด้านดิจิทัล

๓. ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศและการสื่อสาร หรือใช้ข้อมูลต่าง ๆ ของสำนักงานปลัดกระทรวงมหาดไทยเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศและการสื่อสารได้

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการวางแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านดิจิทัล และความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำ โครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้

๕.ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศและการสื่อสาร เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓.๒ ลักษณะความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสำนักงานปลัดกระทรวงมหาดไทย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงจากอุปกรณ์ /ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศและการสื่อสาร

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๔. ความเสี่ยงจากภัยคุกคามทางไซเบอร์	RIT๐๔	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีทางไซเบอร์ เช่น Hacker, Malware, Phishing Mail และ Cross-site scripting (XSS) เป็นต้น	- แฮ็คเกอร์/แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/มัลแวร์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๕. ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะทางด้านดิจิทัล	RIT๐๕	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้การปฏิบัติงานไม่ต่อเนื่องและไม่มีประสิทธิภาพ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	- นโยบายจากผู้บริหาร	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศและการสื่อสารสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	- งบประมาณ - ทักษะบุคลากร	ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค ความเสื่อมสภาพ/ความสึกกร่อนของอุปกรณ์ หรือความเสียหายจากสัตว์กัดแทะ	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงด้านการบริหารจัดการ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
๑๒. ความเสี่ยงจากผู้รับจ้างว่าจ้างหรือจัดจ้าง	RIT๑๒	ความเสี่ยงด้านการบริหารจัดการ	ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำ โครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ	- ผู้ว่าจ้างหรือจัดจ้างไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้	ผู้ดูแลระบบ ผู้ใช้งาน

.

๓.๓ การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีความถี่มากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับความถี่ที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งกรม ใช้เกณฑ์ดังนี้

ระดับความถี่ในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	**ความถี่ที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	๕ ครั้ง/ปี
๔	สูง	๔ ครั้ง/ปี
๓	ปานกลาง	๓ ครั้ง/ปี
๒	น้อย	๒ ครั้ง/ปี
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**ผลกระทบ**	**คำอธิบาย**
๕	สูงมาก	> ๑๐ ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	> ๕ แสนบาท - ๑๐ ล้านบาท หรือ เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	> ๒.๕ แสนบาท - ๕ แสนบาท หรือ ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	> ๑ แสนบาท - ๒.๕ แสนบาท หรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	ไม่เกิน ๑๐๐,๐๐๐ บาท หรือ เกิดเหตุร้ายที่ไม่มีความสำคัญ

๓.๔ การประมาณความเสี่ยง (Risk estimation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล	๕	๔
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสำนักงานปลัดกระทรวงมหาดไทย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย	๕	๔
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงจากอุปกรณ์ /ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๔. ความเสี่ยงจากภัยคุกคามทางไซเบอร์	RIT๐๔	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีทางไซเบอร์ เช่น Hacker, Malware, Phishing Mail และ Cross-site scripting (XSS) เป็นต้น	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์ แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๓	๔
๕. ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะทางด้านดิจิทัล	RIT๐๕	ความเสี่ยงจากผู้ปฏิบัติงาน /ความเสี่ยงด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้การปฏิบัติงานไม่ต่อเนื่อง และไม่มีประสิทธิภาพ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๑

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศและการสื่อสารสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๕
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ	๑	๒
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค ความเสื่อมสภาพ/ความสึกกร่อนของอุปกรณ์ หรือความเสียหายจากสัตว์กัดแทะ	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๓	๔
๑๑.ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงด้านการบริหารจัดการ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๓	๑

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๑๒.ความเสี่ยงจากผู้รับจ้างว่าจ้างหรือจัดจ้าง	RIT๑๒	ความเสี่ยงด้านการบริหารจัดการ	ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำ โครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ	- ผู้ว่าจ้างหรือจัดจ้างไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้	ผู้ใช้งาน ผู้ดูแลระบบ	๕	๔

๓.๕ การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ

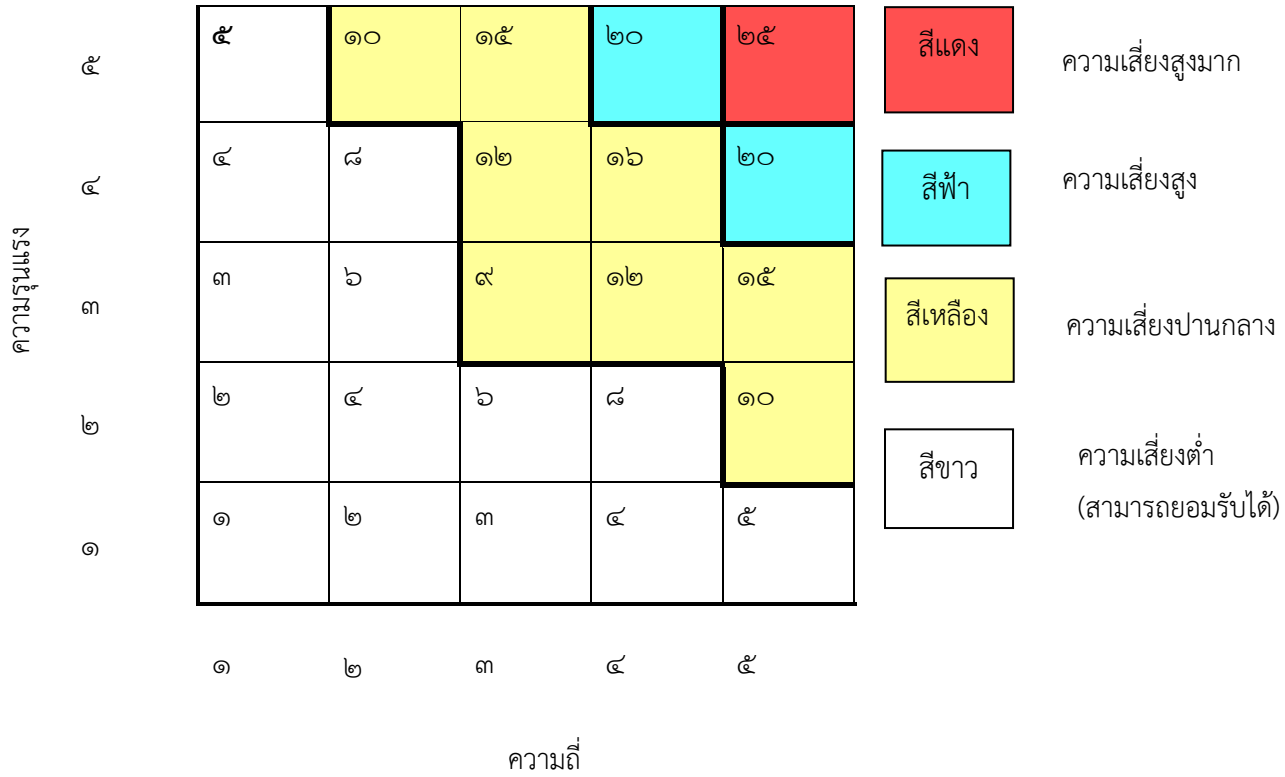
ซึ่งใช้เกณฑ์ในการจัดแบ่ง ดังนี้

ระดับคะแนนความ	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ – ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๙ – ๑๖	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗ – ๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความ	ฟ้า
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

๓.๖ แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง

การประเมินความเสี่ยง



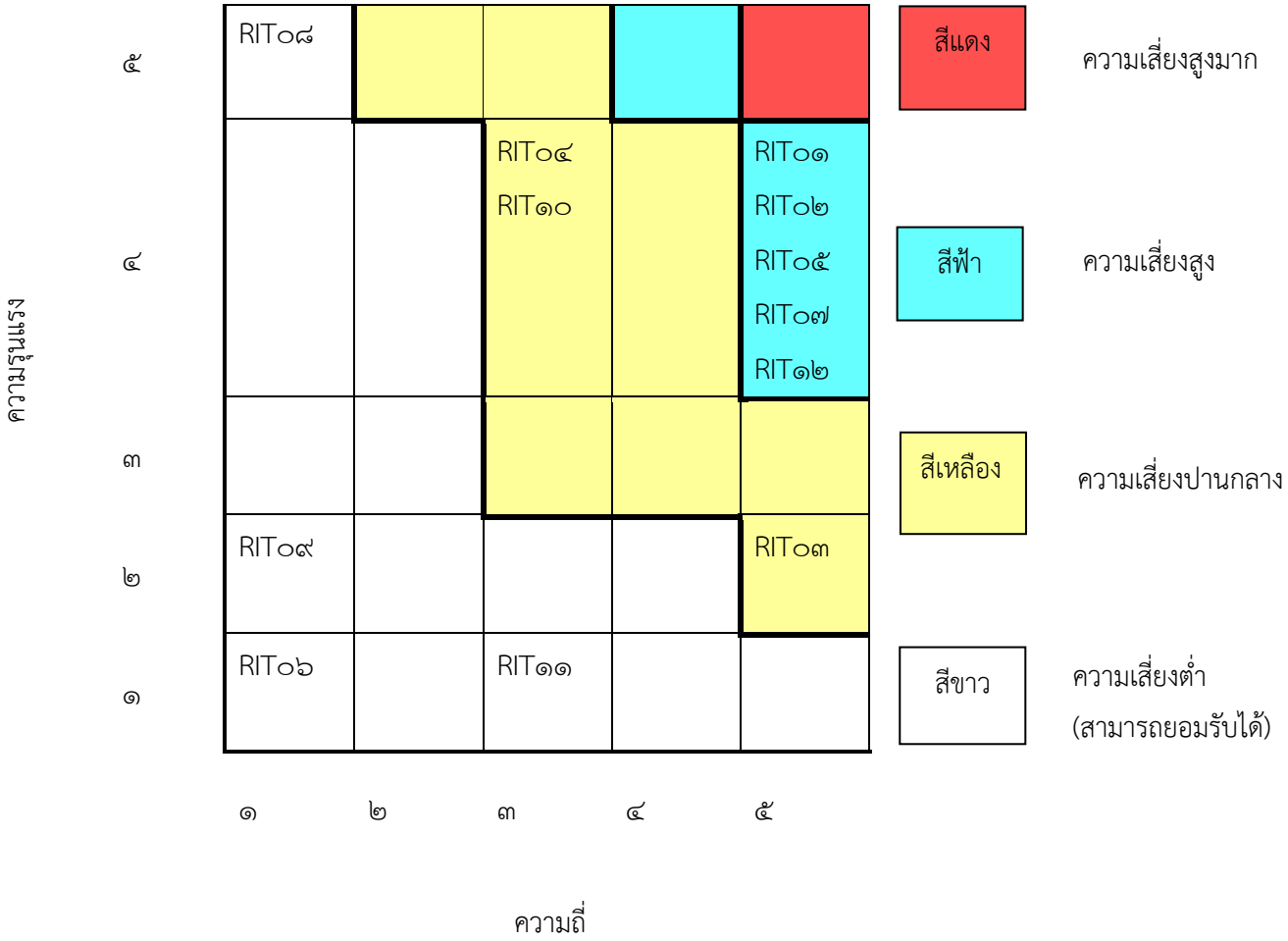
จากแผนภูมิความเสี่ยงสามารถประเมินค่าความเสี่ยง ดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๕	๔	๒๐
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้	๕	๔	๒๐

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
			เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสำนักงานปลัดกระทรวงมหาดไทย			
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงจากอุปกรณ์ /ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๕	๒	๑๐
๔. ความเสี่ยงจากภัยคุกคามทางไซเบอร์	RIT๐๔	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีทางไซเบอร์ เช่น Hacker, Malware, Phishing Mail และ Cross-site scripting (XSS) เป็นต้น	๓	๔	๑๒
๕. ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะทางด้านดิจิทัล	RIT๐๕	ความเสี่ยงจากผู้ปฏิบัติงาน /ความเสี่ยงด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้การปฏิบัติงานไม่ต่อเนื่อง และไม่มีประสิทธิภาพ	๕	๔	๒๐
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	๑	๑	๑
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศและการสื่อสารสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๕	๔	๒๐

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	๑	๕	๕
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	๑	๒	๒
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค ความเสื่อมสภาพ/ความสึกกร่อนของอุปกรณ์ หรือความเสียหายจากสัตว์กัดแทะ	๓	๔	๑๒
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงด้านการบริหารจัดการ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๓	๑	๓
๑๒. ความเสี่ยงจากผู้รับจ้างว่าจ้างหรือจัดจ้าง	RIT๑๒	ความเสี่ยงด้านการบริหารจัดการ	ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ	๕	๔	๒๐

เมื่อดำเนินการประเมินความเสี่ยงและระดับคะแนนเรียบร้อยแล้ว สามารถนำความเสี่ยงดังกล่าว (รหัสความเสี่ยง) ลงในตารางแผนภูมิความเสี่ยง (Risk Map) ดังนี้



๓.๗ การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพ ดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๒๐
๒	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสำนักงานปลัดกระทรวงมหาดไทย	๒๐
๓	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะทางด้านดิจิทัล	ความเสี่ยงจากผู้ปฏิบัติงาน /ความเสี่ยงด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้การปฏิบัติงานไม่ต่อเนื่อง และไม่มีประสิทธิภาพ	๒๐
๔	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศและการสื่อสารสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๒๐
๕	RIT๑๒ ความเสี่ยงจากผู้รับจ้างว่าจ้างหรือจัดจ้าง	ความเสี่ยงด้านการบริหารจัดการ	ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำ โครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ	๒๐
๖	RIT๐๔ ความเสี่ยงจากภัยคุกคามทางไซเบอร์	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีทางไซเบอร์ เช่น Hacker, Malware, Phishing Mail และ Cross-site scripting (XSS) เป็นต้น	๑๒
๗	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค ความเสื่อมสภาพ/ความสึกกร่อนของอุปกรณ์ หรือความเสียหายจากสัตว์กัดแทะ	๑๒

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๘	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากอุปกรณ์/ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๑๐
๙	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วมแผ่นดินไหว	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่มไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๕
๑๐	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงด้านการบริหารจัดการ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๓
๑๑	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	๒
๑๒	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๑

๓.๘ การจัดการความเสี่ยง

นโยบายของสำนักงานปลัดกระทรวงมหาดไทย ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ ๙

สำนักงาน ก.พ.ร. กำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

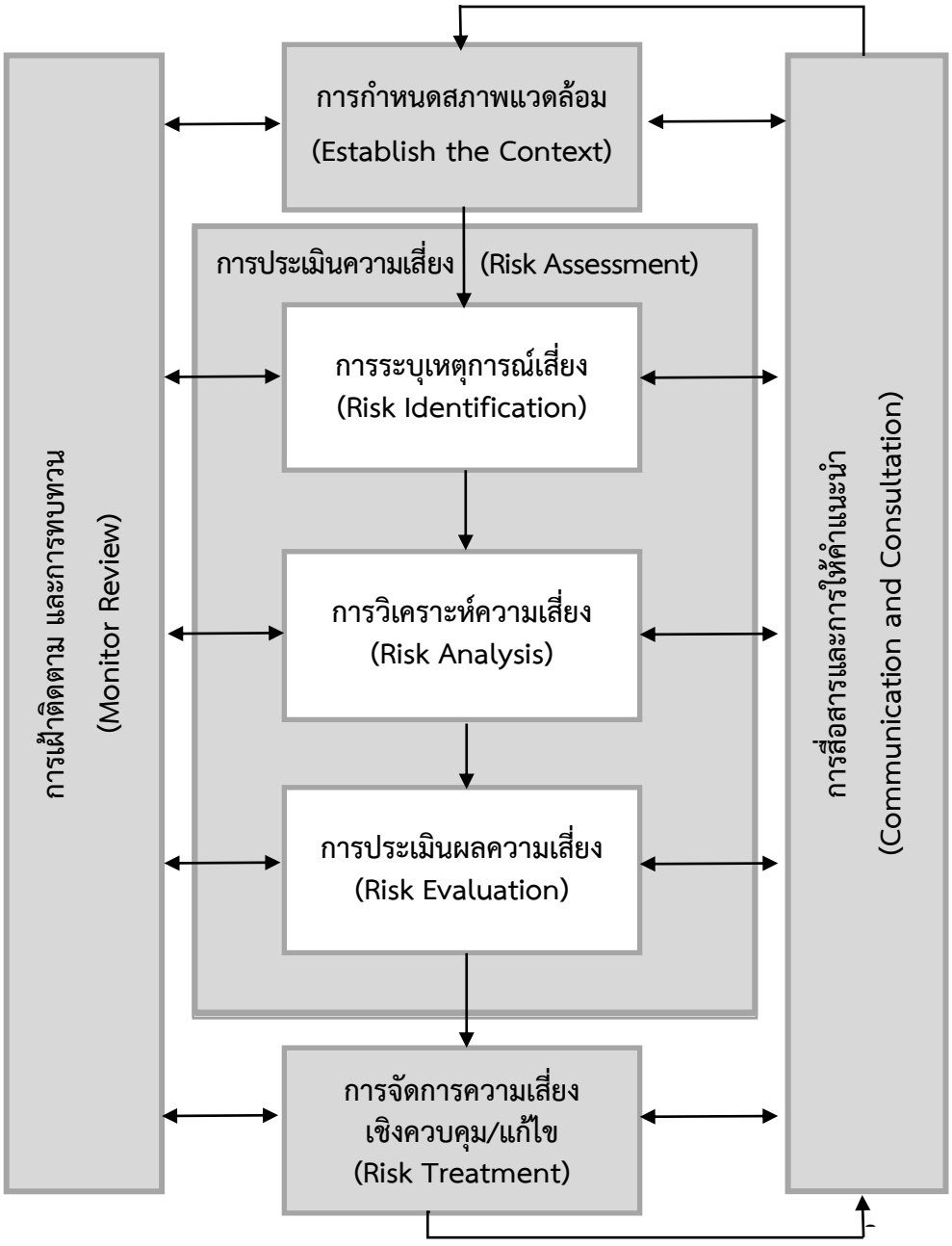
ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๒	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	
๓	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะทางด้านดิจิทัล	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดอบรม/สัมมนา เพื่อเพิ่มทักษะบุคลากรด้านดิจิทัล
๔	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	
๕	RIT๑๒ ความเสี่ยงจากผู้รับจ้างว่าจ้างหรือจัดจ้าง	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- หาทางป้องกันสัตว์กัดแทะอุปกรณ์ - จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ
๖	RIT๐๔ ความเสี่ยงจากภัยคุกคามทางไซเบอร์	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบรักษาความมั่นคงปลอดภัยไซเบอร์
๗	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- ตรวจสอบ บำรุง ซ่อมแซมอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ - จัดหาอุปกรณ์คอมพิวเตอร์สำรองเพื่อเตรียมพร้อมในกรณีอุปกรณ์ชำรุดขัดข้อง
๘	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๑๐	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๙	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วมแผ่นดินไหว	๕	- ยอมรับความเสี่ยง	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
๑๐	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๓	- ยอมรับความเสี่ยง	- รักษาความปลอดภัยอาคารสถานที่ คัดกรองคนจากภายนอกที่เข้ามาติดต่อราชการ - ปลูกฝังคุณธรรมจริยธรรมแก่บุคลากรภายใน
๑๑	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๒	- ยอมรับความเสี่ยง	
๑๒	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๑	- ยอมรับความเสี่ยง	

๓.๙ การกำหนดสภาพแวดล้อม

กระบวนการบริหารความเสี่ยงมีขั้นตอนการดำเนินงาน และหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม ประกอบด้วย ๔ ขั้นตอน คือ



๑) การระบุเหตุการณ์เสี่ยง (Risk Identification) การค้นหาความเสี่ยง สำรวจเหตุการณ์ที่เป็นความเสี่ยง ปัจจัยหรือสาเหตุของความเสี่ยง รวมทั้งความเสียหายหรือผลกระทบที่อาจเกิดขึ้น ซึ่งสามารถหาได้จากคำร้องเรียนจากผู้ใช้บริการ การสัมภาษณ์ผู้ปฏิบัติงาน การออกแบบสอบถาม การศึกษาเอกสารและตำราวิชาการต่างๆ เป็นต้น

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis) การพิจารณาถึงความถี่ ความรุนแรง และความสำคัญของเหตุการณ์แต่ละเหตุการณ์ว่ามีความถี่และความรุนแรงมากน้อยเพียงใด ซึ่งต้องอาศัยประสบการณ์ ข้อมูลในอดีต และความมีวิสัยทัศน์ เพื่อให้สามารถประเมินผลกระทบได้อย่างค่อนข้างแม่นยำ

๓) การประเมินผลความเสี่ยง (Risk Evaluation) การประเมินผลการจัดการความเสี่ยงจะบ่งบอกถึงความสามารถที่จะทำให้ความเสี่ยงที่ได้ดำเนินการบริหารความเสี่ยงนั้นลดลง โดยศึกษาถึงเหตุการณ์ที่เกิดขึ้นย้อนหลังเพื่อดูความสำเร็จของการบริหารความเสี่ยง

การรายงาน เป็นการรายงานผลการวิเคราะห์ ประเมิน และจัดการความเสี่ยงว่ายังมีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้ายังเหลืออยู่มีอยู่ในระดับใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไร

การติดตามผล เป็นการติดตามผลหลังจากได้ดำเนินการตามแผนบริหารความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งสาเหตุของความเสี่ยงที่มีผลต่อความสำเร็จ ความรุนแรงของผลกระทบ วิธีการบริหารจัดการความเสี่ยง รวมถึงค่าใช้จ่ายในการควบคุมมีความเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป โดยมีเป้าหมายในการติดตามผล คือ

๑. การประเมินคุณภาพและความเหมาะสมกับวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการไปแล้วว่าบรรลุผลของการบริหารความเสี่ยงหรือไม่

๒. การติดตามความคืบหน้าของมาตรการควบคุมที่มีการทำเพิ่มเติมว่าแล้วเสร็จตามกำหนดหรือไม่สามารถโอกาสหรือไม่

๔) การจัดการความเสี่ยง (Risk Treatment) การหาวิธีการเพื่อนำมาใช้ในการจัดการกับความเสี่ยงที่เกิดขึ้น โดยวิธีการที่นำมาใช้นั้นต้องสอดคล้องกับนโยบายและเป้าหมายของหน่วยงานหรือองค์กร

บทที่ ๔
แผนแก้ไขปัญหาจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)
สำนักงานปลัดกระทรวงมหาดไทย

การปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัลเป็นการนำเทคโนโลยีดิจิทัลมาใช้ในการปรับปรุงประสิทธิภาพการบริหารจัดการของหน่วยงานรัฐ ทั้งส่วนกลางและส่วนภูมิภาคในการบริการภาครัฐหรือบริการสาธารณะ ในรูปแบบดิจิทัลอย่างมีแบบแผนและเป็นระบบเพื่อตอบสนองความต้องการของประชาชนหรือผู้ใช้บริการ ซึ่งผู้ใช้บริการ ประชาชนทุกคนสามารถเข้าถึงข้อมูลสารสนเทศได้โดยไม่มีข้อจำกัด และสามารถให้บริการผ่านระบบเชื่อมโยงข้อมูลอัตโนมัติการเปิดเผยข้อมูลของภาครัฐที่ไม่กระทบต่อสิทธิส่วนบุคคลและความมั่นคงของชาติผ่านการจัดเก็บ รวบรวม และแลกเปลี่ยนอย่างมีมาตรฐาน รวมถึงการให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์และข้อมูล

เพื่อให้มีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เกิดความมั่นคงปลอดภัย มีความพร้อมใช้ข้อมูลได้อย่างเต็มประสิทธิภาพตลอดเวลา และนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กร ตลอดจนการเลือกใช้วิธีการที่เหมาะสมในการบริหารจัดการความเสี่ยงที่ได้รับความเสียหายจากการถูกโจมตีทางไซเบอร์ ไวรัสคอมพิวเตอร์ บุคลากร ปัญหาไฟฟ้าลัดวงจร อัคคีภัย สถานการณ์โรคระบาด หรือปัจจัยอื่น ๆ ทั้งภายในและภายนอก ซึ่งเป็นการบุกรุกระบบ การโจรกรรมข้อมูลที่ก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และเพื่อให้การดำเนินงานอยู่ในระดับที่สามารถรองรับได้ ดังนั้น สำนักงานปลัดกระทรวงมหาดไทย โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เห็นถึงความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ ระบบเครือข่าย จึงมีการจัดทำแผนการแก้ไขปัญหาจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกัน หรือลดความเสี่ยงที่อาจนำไปสู่ผลเสีย หรือความเสียหายได้ทั้งทางตรงและทางอ้อม

๔.๑ วัตถุประสงค์

(๑) เพื่อบริหารจัดการภัยคุกคามระบบสารสนเทศรูปแบบต่าง ๆ ให้สามารถรองรับการเปลี่ยนแปลงรูปแบบอย่างต่อเนื่อง

(๒) เพื่อใช้เป็นแนวทางในการดำเนินการ การกำกับดูแล การตรวจสอบการบริหารจัดการ และดูแลรักษาระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารให้มีความเสถียรภาพ มีความพร้อมในการใช้งาน และเฝ้าระวังความเสี่ยงใหม่ ๆ ที่อาจเกิดขึ้นได้ตลอดเวลา

(๓) เพื่อลดความเสี่ยงจากการโจมตีระบบหรือภัยคุกคามระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงมหาดไทย

(๔) เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย

(๕) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

(๖) เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

(๗) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย

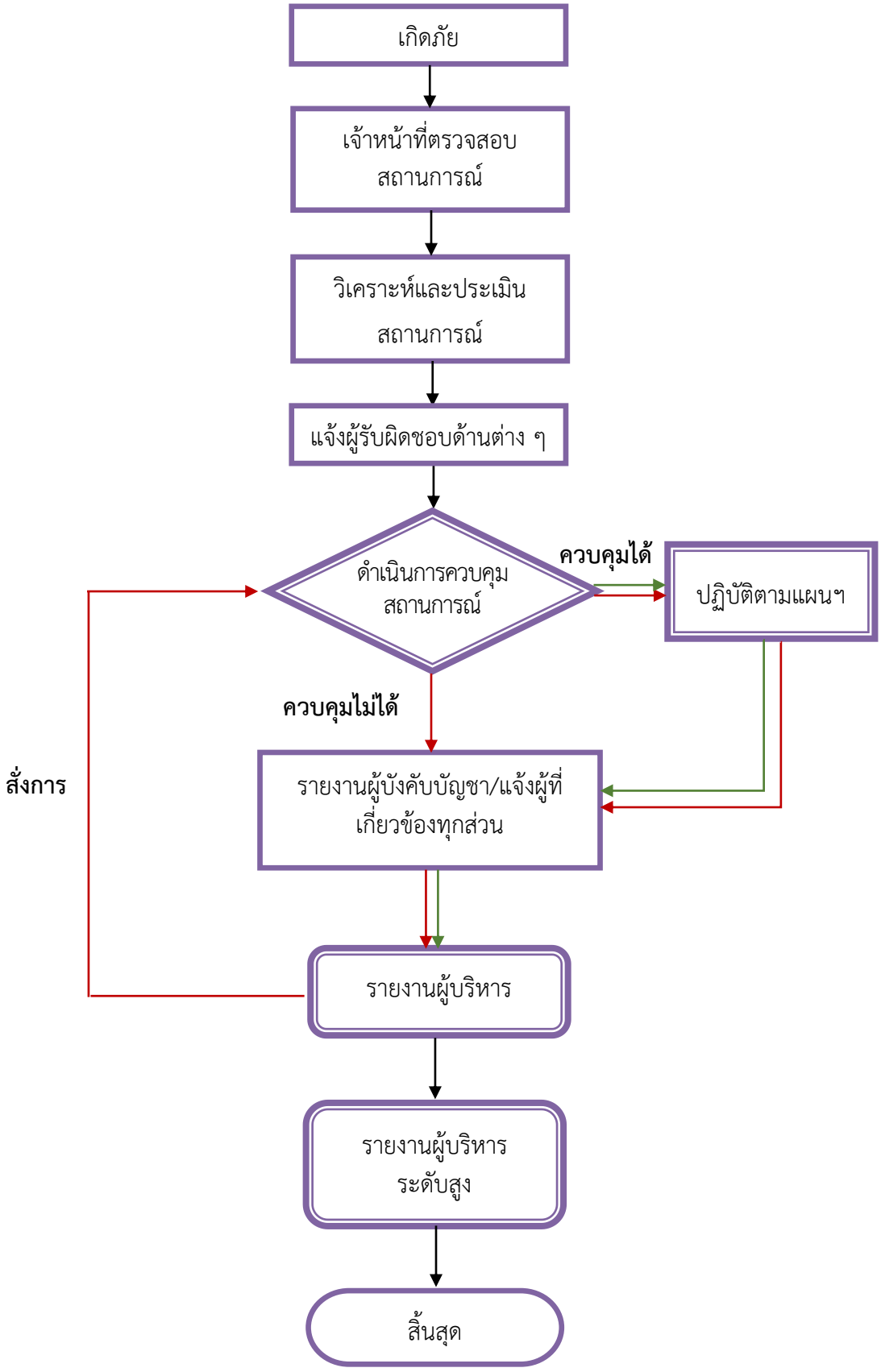
(๘) สร้างความเข้าใจ กรอบและแนวทางในการดำเนินงานให้แก่บุคลากรในองค์กร เพื่อให้สามารถบริหารจัดการความไม่แน่นอนที่จะเกิดขึ้นกับองค์กรได้อย่างเป็นระบบและมีประสิทธิภาพ

๔.๒ กรอบแนวทางในการจัดทำแผน

การจัดทำแผนรับสถานการณ์ฉุกเฉินภัยพิบัติ อาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) มีแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

(๑) การวิเคราะห์และประเมินความรุนแรงของสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
(๒) แนวทางการป้องกันและเตรียมการเบื้องต้น
(๓) การเตรียมความพร้อม
(๔) การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
(๕) มาตรการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
(๖) กระบวนการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
(๗) แผนกู้คืนระบบกลับสู่สภาพปกติ
(๘) การติดตามและรายงานผล

ขั้นตอนการแก้ไขปัญหาจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ
ของงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย



กรอบแนวทางการแก้ไขปัญหาจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

๔.๒.๑ การวิเคราะห์และประเมินความรุนแรงของสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ

สำนักงานปลัดกระทรวงมหาดไทย มีภารกิจเกี่ยวกับการพัฒนายุทธศาสตร์และแปลงนโยบายของกระทรวงเป็นแผนการปฏิบัติงานจัดสรรทรัพยากรและบริหารราชการทั่วไปของกระทรวง การรักษาความมั่นคงภายในการรักษาความสงบเรียบร้อยและอำนวยความเป็นธรรม และการส่งเสริมและสนับสนุนการบริหารราชการส่วนภูมิภาคเพื่อให้บรรลุเป้าหมายและเกิดผลสัมฤทธิ์ตามภารกิจขององค์กร โดยให้มีอำนาจหน้าที่ ดังต่อไปนี้

• ศึกษา วิเคราะห์และจัดทำข้อมูลเพื่อใช้ในการกำหนดนโยบาย เป้าหมาย และผลสัมฤทธิ์ของกระทรวง

• พัฒนายุทธศาสตร์การบริหารของกระทรวง

• แปลงนโยบายเป็นแนวทางและแผนการปฏิบัติงาน

• จัดสรรและบริหารทรัพยากรของกระทรวงเพื่อให้เกิดการประหยัด คุ้มค่า และสมประโยชน์

• ดำเนินการเกี่ยวกับการตรวจราชการและตรวจสอบภายในราชการทั่วไปของกระทรวง

• พัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อใช้ในการบริหารงานและให้บริการด้านการสื่อสารแก่ส่วนราชการต่าง ๆ และจังหวัด

• ดำเนินการเกี่ยวกับงานของคณะกรรมการมาตรฐานการบริหารงานบุคคลส่วนท้องถิ่นตามกฎหมายว่าด้วยระเบียบบริหารงานบุคคลส่วนท้องถิ่น

• ดำเนินการและประสานการแปลงยุทธศาสตร์และแผนพัฒนาเศรษฐกิจและสังคมในระดับชาติไปสู่การบริหารงานแบบบูรณาการในจังหวัดและกลุ่มจังหวัด ส่งเสริมและสนับสนุนการวางแผนยุทธศาสตร์การพัฒนาจังหวัดและกลุ่มจังหวัด การยื่นคำของบประมาณของจังหวัดและกลุ่มจังหวัด ตลอดจนติดตามและประเมินผลการบริหารและพัฒนาจังหวัดและกลุ่มจังหวัด และสนับสนุนการปฏิบัติราชการส่วนภูมิภาค

• ดำเนินการเกี่ยวกับระบบการบริหารทรัพยากรบุคคลของสำนักงานปลัดกระทรวงและกระทรวง ตลอดจนการส่งเสริมและสนับสนุนการบริหารทรัพยากรบุคคลของจังหวัดและกลุ่มจังหวัด

• ดำเนินการเกี่ยวกับกฎหมายในความรับผิดชอบของกระทรวงและกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งงานนิติกรรมและสัญญา งานเกี่ยวกับความรับผิดทางแพ่งและอาญา งานคดีปกครอง และงานคดีอื่นที่อยู่ในอำนาจหน้าที่ของกระทรวง

• ดำเนินการเกี่ยวกับความช่วยเหลือและความร่วมมือกับต่างประเทศ

• อำนวยการ บูรณาการ และเป็นศูนย์กลางของกระทรวงในการประสานงานด้านการข่าวที่อาจส่งผลกระทบต่อความสงบเรียบร้อยและความมั่นคงภายใน รวมถึงการข่าวที่เกี่ยวกับการก่อการร้ายและอาชญากรรมข้ามชาติ

• ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของสำนักงานปลัดกระทรวงหรือตามที่รัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย

จากภารกิจและอำนาจหน้าที่ข้างต้น สำนักงานปลัดกระทรวงมหาดไทยจึงได้พัฒนาระบบสารสนเทศเพื่อรองรับภารกิจต่าง ๆ อาทิ ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เว็บไซต์กระทรวงมหาดไทย (https://moi.go.th/moi/) เว็บไซต์สำนักงานปลัดกระทรวงมหาดไทย

(http://smoi.moi.go.th/) เว็บไซต์แม่บ้านมหาดไทย (http://www.dokkaew.moi.go.th/) ระบบงานสารบรรณอิเล็กทรอนิกส์ ระบบแพลตฟอร์มกลาง ระบบให้บริการเครือข่าย อุปกรณ์คอมพิวเตอร์ ฯลฯ เป็นต้น

จากการวิเคราะห์และตรวจสอบความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร สามารถจำแนกได้ ดังนี้

(๑) สถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติจากภายนอก

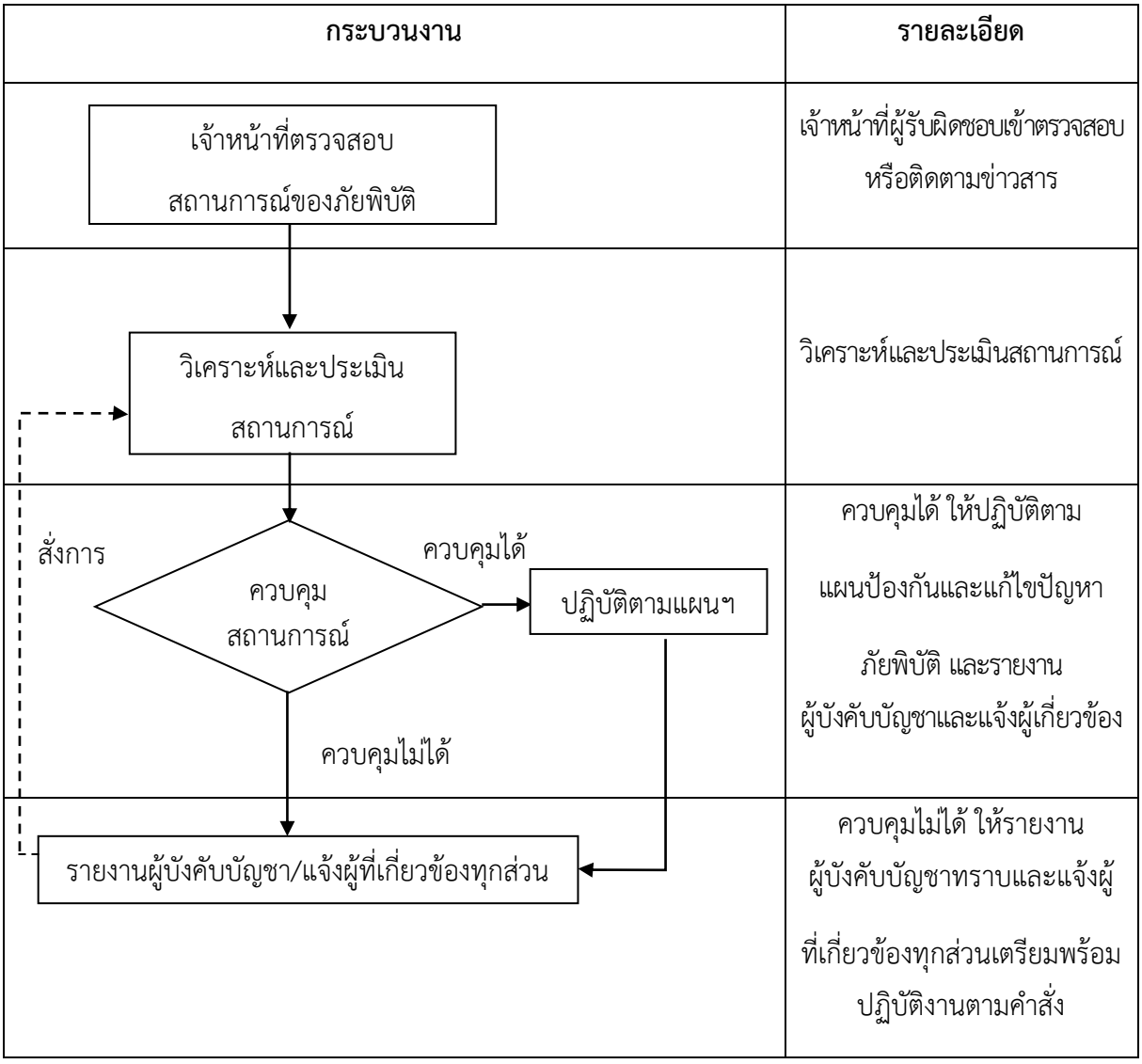
- ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย อาทิ อัคคีภัย อุทกภัย หรือการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ
- การโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- การเชื่อมโยงระบบเครือข่ายล้มเหลว หรือเกิดความขัดข้อง
- ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/เพลิงไหม้/น้ำท่วม/แผ่นดินไหว
- ภัยการบุกรุกหรือโจมตีจากภายนอกเพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายฐานข้อมูล ไวรัสคอมพิวเตอร์ หรือการก่อกวนจาก Hacker หรือการเจาะทำลายระบบจาก Cracker รวมถึงการนำอุปกรณ์ที่ไม่ได้ลงทะเบียนจากภายนอกมาเชื่อมต่อกับระบบภายในสังกัดสำนักงานปลัดกระทรวงมหาดไทย
- เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบเรียบร้อย
- สถานการณ์โรคระบาด
- การจ้างผู้ว่าจ้าง

(๒) สถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติจากภายใน

- ระบบโครงสร้างพื้นฐาน ระบบเครื่องข่ายต่าง ๆ เสียหาย ระบบสารสนเทศและคอมพิวเตอร์ขัดข้อง
- ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายใน
- ภัยจากผู้ใช้งานระบบ
- การเปลี่ยนแปลงของนโยบาย
- การได้รับการสนับสนุนงบประมาณไม่เพียงพอ

๔.๒.๒ แนวทางการป้องกัน และการเตรียมการเบื้องต้น

๔.๒.๒.๑ แนวทางการดำเนินการเบื้องต้น



๔.๒.๒.๒ แนวทางการป้องกันและเตรียมการเบื้องต้น

(๑) การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วยโดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะทำการแจ้งให้ CEO หรือ CIO ขององค์กรทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

(๒) กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กรโดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้นทั้งการรวบรวมเหตุการณ์การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

(๓) การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอกเพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้าสถานีดับเพลิงสถานีตำรวจเป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

(๔) การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบสื่อสารและเครือข่ายคอมพิวเตอร์ โดยได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ซึ่งเตรียมอุปกรณ์ ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลของระบบงานที่สำคัญ เช่น External Hard disk/SAN Storage/Cloud
- แผนโปรแกรม' Antivirus/Spyware
- แผ่น Driver อุปกรณ์ต่าง ๆ
- ระบบสำรองไฟฉุกเฉิน

(๕) การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้โดยองค์กรมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

(๖) การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้โดยองค์กรมีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy)

(๗) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

- ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที
- เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
- เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และ อุปกรณ์ต่างๆ
- ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ปริมาณน้ำมันแบตเตอรี่ และตั้งเวลาทดสอบการทำงานอัตโนมัติสัปดาห์ละ ๑ ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้าถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่องเป็นระยะเวลาประมาณ ๘ ชั่วโมง

(๘) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทาง ดังนี้

- มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหายโดยห้าม บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม
- มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา
- มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
- มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป
- การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

(๙) การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

- เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ
- ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
- ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า
- ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง
- ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๔.๓ การเตรียมความพร้อม

๔.๓.๑ ภัยพิบัติจากภายนอก

(๑) ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้น และอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

(๑.๑) การดำเนินการและการป้องกันด้านอัคคีภัย ได้แก่

- กำหนดเวรรักษาการณ์รักษาความปลอดภัย
- มีการซ้อมแผนดับเพลิง
- ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย
- จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

(๑.๒) การดำเนินการ และการป้องกันด้านอุทกภัย ความชื้น อุณหภูมิที่ไม่เหมาะสม

- เปิดเครื่องปรับอากาศ สำหรับเครื่องแม่ข่ายตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ
- ติดตามข่าวสารภัยพิบัติตามสถานการณ์ที่เกิดขึ้น

(๑.๓) การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

- เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ
- ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
- ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า
- ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง
- ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

(๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

(๒.๑) ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย โดยใช้ระบบสแกนลายนิ้วมือและใบหน้าก่อนเข้าห้องคอมพิวเตอร์แม่ข่าย

- จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ
- ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

(๓) ระบบการเชื่อมโยงเครือข่ายขัดข้อง

(๓.๑) ตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

(๓.๒) จัดให้มีเครือข่ายสำรอง สำหรับใช้ในกรณีที่เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้

(๓.๓) ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขปัญหา

(๔) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

(๔.๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(๔.๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ

(๔.๓) เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้หยุดบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่าง ๆ

(๔.๔) สำรองข้อมูลที่สำคัญบนสื่อที่สามารถจัดเก็บข้อมูลได้อย่างเหมาะสม (DVD, CD, External Hard disk, Handy drive ฯลฯ)

(๕) ภัยการบุกรุกหรือโจมตีจากภายนอกเพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายฐานข้อมูล ไวรัสคอมพิวเตอร์ หรือการก่อกวนจาก Hacker หรือการเจาะทำลายระบบจาก Cracker

(๕.๑) สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

(๕.๒) ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทยได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

(๕.๓) ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย และกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

(๕.๔) จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตของกรมส่งเสริมการปกครองท้องถิ่น เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

(๕.๕) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

(๕.๖) กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติ ดังนี้

- ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
- ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น
- จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
- เปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น
- ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย ๘ อักขระ

- ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้
- เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว
- เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน
- ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ อาทิ บันทึกไว้ในหน้าจอล็อกอิน ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง จะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง
- ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
- หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

(๕.๗) ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอกโดยการนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย

(๕.๘) ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS

(๖) ไวรัสคอมพิวเตอร์

(๖.๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอและต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

(๖.๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

(๖.๓) ใช้ความระมัดระวังในการเปิด E-mail

- ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

(๖.๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ
- ไม่ควรเปิด website ที่แนะนำมาทาง E-mail
- ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

(๖.๕) ปิดการใช้งานฟังก์ชัน Autoplay เพื่อป้องกันไม่ให้ไวรัสที่แพร่ระบาดผ่านทางสื่อเก็บข้อมูลแบบพกพาใช้เป็นช่องทางในการรันไฟล์ไวรัสโดยอัตโนมัติ

(๗) ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบเรียบร้อย

เนื่องจากเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ ในการป้องกันหากไม่สามารถย้ายสถานที่หรือป้องกันสถานที่ได้ ควรมีการ Back Up ข้อมูลไว้มากกว่า ๑ Back Up และแยกสถานที่จัดเก็บ และถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการ Back Up ไว้ และอุปกรณ์คอมพิวเตอร์ สำรองมาใช้แทนหากเกิดความเสียหายร้ายแรงควรมีศูนย์คอมพิวเตอร์สำรองเพิ่ม

(๘) สถานการณ์โรคระบาด/โรคติดต่ออุบัติใหม่

ปัจจุบันสถานการณ์การแพร่ระบาดอย่างรวดเร็วและต่อเนื่องของเชื้อไวรัส COVID-19 มีแนวโน้มสร้างภาวะชะงักงันให้กับหน่วยงานและส่งผลกระทบเหมือนกับการบุกรุกทางด้านไซเบอร์หรือเป็นภัยพิบัติทางธรรมชาติ หน่วยงานต้องควบคุมสถานการณ์โดยการสร้างความเชื่อมั่นในการควบคุมโรคให้กับบุคลากรและสามารถปฏิบัติงานได้อย่างต่อเนื่อง โดยการใช้เครื่องมือดิจิทัลเพื่อทำงานร่วมกันในการควบคุมความปลอดภัย และมีเครือข่ายรองรับมาตรการกักกันต่าง ๆ และข้อจำกัดการเดินทาง ในเบื้องต้นหน่วยงานที่ยังไม่มีความสามารถนำระบบทำงานแบบระยะไกลมาปรับใช้ได้นั้น อาจต้องแก้ไขโดยการระบุข้อกำหนดกรณีการใช้งาน อาทิ การส่งข้อความทันทีเพื่อสื่อสารทั่วไป การแชร์ไฟล์ หรือการประชุม และการเข้าถึงแอปพลิเคชันต่าง ๆ ขององค์กร อาทิ ระบบสารสนเทศต่าง ๆ และเตรียมการด้านความปลอดภัยทั้งหมดเพื่อให้เข้าถึงแอปพลิเคชันและข้อมูลได้อย่างปลอดภัยใช้ช่องทางดิจิทัลเป็นช่องทางหลักในการติดต่อสื่อสารกับบุคลากรและหน่วยงานอื่นที่เกี่ยวข้อง มีการนำแพลตฟอร์มดิจิทัลมาใช้ติดต่อสื่อสาร อาทิ เว็บไซต์ หรือแอปพลิเคชันต่าง ๆ โซเชียลมีเดีย ทั้งนี้ การติดต่อแบบออฟไลน์ยังคงมีบทบาทสำคัญ การทำงานร่วมกันในสถานที่ทำงาน การประชุมผ่านวิดีโอ และไลฟ์สตรีมมิ่ง สร้างแหล่งข้อมูลหลักที่เชื่อถือได้ให้แก่องค์กร และการเตรียมแผนรับมือตอนกลับเข้าสู่โหมดการดำเนินงานในภาวะปกติขององค์กร

๔.๓.๒ ภัยพิบัติจากภายใน

(๑) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

(๑.๑) การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

(๑.๒) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนดทุกสัปดาห์ โดยจะสำรองข้อมูลโครงสร้างข้อมูล Source Code และบันทึกข้อมูลลงในสื่อบันทึก

(๑.๓) ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้สำรองไว้ในสื่อบันทึก

(๑.๔) จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายเพื่อลดความเสียหายของข้อมูล

(๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

(๒.๑) ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้

(๒.๒) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

(๒.๓) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

(๒.๔) สร้างความรู้ความเข้าใจในการป้องกันและแก้ไขปัญหาจากไวรัสคอมพิวเตอร์เบื้องต้น

(๓) การจัดเตรียมอุปกรณ์ที่จำเป็น

(๓.๑) แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

(๓.๒) สำรองข้อมูลและระบบงานที่สำคัญ

(๓.๓) แผ่นโปรแกรม antivirus/spyware

(๓.๔) แผ่น Driver อุปกรณ์ต่าง ๆ

(๓.๕) ระบบสำรองไฟฉุกเฉิน

(๓.๖) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

(๔) การสำรองข้อมูล (Back Up)

(๔.๑) การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลแม่ข่าย โดยสำรองข้อมูลไว้ในสื่อบันทึก จำนวน ๑ ชุด

(๔.๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิด ขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

(๔.๓) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๔.๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และ อุปกรณ์ต่างๆ

(๔.๕) ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ ปริมาณน้ำมันแบตเตอรี่ และตั้งเวลาทดสอบการทำงานอัตโนมัติสัปดาห์ละ ๑ ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้าถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่องเป็นระยะเวลาประมาณ ๘ ชั่วโมง

(๔.๖) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนด โดยสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในสื่อบันทึก

(๕) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้ระบบสารสนเทศและระบบเครือข่ายมีแนวทาง ดังนี้

(๕.๑) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้าม บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

(๕.๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

(๕.๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

(๕.๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

(๕.๕) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๔.๔ การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ

หน้าที่ความรับผิดชอบในการแก้ไขปัญหาด้านเทคโนโลยีสารสนเทศ

๔.๔.๑ ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของหน่วย (DCIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามการกำกับ ดูแล ควบคุม และตรวจสอบ

๔.๔.๒ ระดับอำนวยการ

การแก้ไขปัญหาจากภัยพิบัติ มีหน้าที่ในควบคุม ตรวจสอบ กำกับดูแลการประเมินสถานการณ์และตัดสินใจในกรณีที่ฝ่ายปฏิบัติงานประเมินสถานการณ์และรายงานการประเมินเบื้องต้นว่าอาจไม่สามารถควบคุมสถานการณ์ได้ จำเป็นจะต้องปฏิบัติงานนอกเหนือจากแผนป้องกันแก้ไขปัญหาจากภัยพิบัติที่กำหนดไว้ หรือสถานการณ์ยังไม่เกิดแต่มีสภาวการณ์หรือแนวโน้มที่อาจเกิดขึ้น รายงานผลต่อผู้บังคับบัญชา ประกอบด้วย

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

- ผู้อำนวยการกลุ่มงานเทคโนโลยีสารสนเทศ
- ผู้อำนวยการกลุ่มงานโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร
- ผู้อำนวยการกลุ่มงานเทคโนโลยีสื่อสาร
- ผู้อำนวยการกลุ่มงานยุทธศาสตร์สารสนเทศและการสื่อสาร

๔.๔.๓ ระดับปฏิบัติ

ดำเนินการตามแผนป้องกันและแก้ไขปัญหาเกี่ยวกับภัยพิบัติรายงานผลการดำเนินการตามแผนฯ ทบทวนแผนฯ ประเมินสถานการณ์ ติดต่อประสานงานฝ่ายต่าง ๆ ที่เกี่ยวข้อง รวมทั้งขอรับการสนับสนุนจากหน่วยงานภายนอกหรือบริษัทคู่สัญญาตรวจสอบและประเมินผล รวมทั้งด้าน Hardware และ Software พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน โดยแบ่งออกเป็น ๔ ด้าน ดังนี้

(๑) ด้านฐานข้อมูลและระบบสารสนเทศ มีหน้าที่ในการจัดการแก้ไขปัญหาที่เกิดภัยต่าง ๆ การประสานงาน การกู้คืนข้อมูลระบบงาน การประเมินสถานการณ์ต่าง ๆ เช่น เครือข่าย/ระบบงาน ตลอดจนติดตั้งระบบงาน และฐานข้อมูลให้พร้อมใช้งาน ประกอบด้วย

- ผู้อำนวยการกลุ่มงานเทคโนโลยีสารสนเทศ
- เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ

สถานที่ปฏิบัติงาน: อาคารศูนย์เทคโนโลยีสารสนเทศ กลุ่มงานเทคโนโลยีสารสนเทศ ชั้น ๒
เบอร์ติดต่อ : มท ๕๑๑๔๓

(๒) ด้านโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร มีหน้าที่ในการแก้ไขปัญหาการจัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบแอร์ให้พร้อมใช้งาน ประกอบด้วย

- ผู้อำนวยการกลุ่มงานโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร
- เจ้าหน้าที่กลุ่มงานโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร

สถานที่ปฏิบัติงาน: อาคารศูนย์เทคโนโลยีสารสนเทศ กลุ่มงานโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร ชั้น ๕
เบอร์ติดต่อ : มท ๕๑๔๕๓

(๓) ด้านระบบสื่อสารและเครือข่าย มีหน้าที่หลักในการจัดการจัดเตรียมสถานที่รวมถึงอุปกรณ์/ระบบสื่อสาร ให้พร้อมใช้งาน รวมทั้งตรวจสอบและประเมินความเสียหาย ประกอบด้วย

- ผู้อำนวยการกลุ่มงานเทคโนโลยีการสื่อสาร
- เจ้าหน้าที่กลุ่มงานเทคโนโลยีการสื่อสาร

สถานที่ปฏิบัติงาน: อาคารศูนย์เทคโนโลยีสารสนเทศ กลุ่มงานเทคโนโลยีสื่อสาร ชั้น ๔
เบอร์ติดต่อ : มท ๕๑๔๓๘

(๔) ด้านสนับสนุนการแก้ไขปัญหาจากภัยพิบัติ มีหน้าที่ในการสนับสนุนการแก้ไขปัญหาจากภัยพิบัติตามที่ฝ่ายปฏิบัติงานแก้ไขปัญหาจากภัยพิบัติร้องขอ ประกอบด้วย

- ผู้อำนวยการกลุ่มงานอำนวยการ
- ผู้อำนวยการกลุ่มงานยุทธศาสตร์สารสนเทศและการสื่อสาร
- เจ้าหน้าที่กลุ่มงานอำนวยการ
- เจ้าหน้าที่กลุ่มงานยุทธศาสตร์สารสนเทศและการสื่อสาร

สถานที่ปฏิบัติงาน: อาคารศูนย์เทคโนโลยีสารสนเทศ กลุ่มงานอำนวยการ ชั้น ๓ และกลุ่มงานยุทธศาสตร์สารสนเทศและการสื่อสาร ชั้น ๒
เบอร์ติดต่อ : มท ๕๑๕๔๐ และ มท ๕๑๔๐๔

๔.๕ มาตรการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติ ดังนี้

๔.๕.๑ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client)

(๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศของหน่วยงานทราบ หรือในกรณีเกิดจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

(๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

(๓) ให้เจ้าหน้าที่ด้านระบบสารสนเทศของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบเพื่อแก้ไขปัญหาต่อไป

๔.๕.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

(๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ ประสิทธิภาพของเครื่องสำรองไฟฟ้าและเครื่องกำเนิดไฟฟ้า

(๓) ตัดระบบจ่ายไฟ

(๔) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

(๕) กรณีไฟไหม้ให้ดับเพลิงด้วยระบบดับเพลิงอัตโนมัติซึ่งเป็นการดับเพลิงด้วยการฉีดก๊าซสารสะอาด FM ๒๐๐

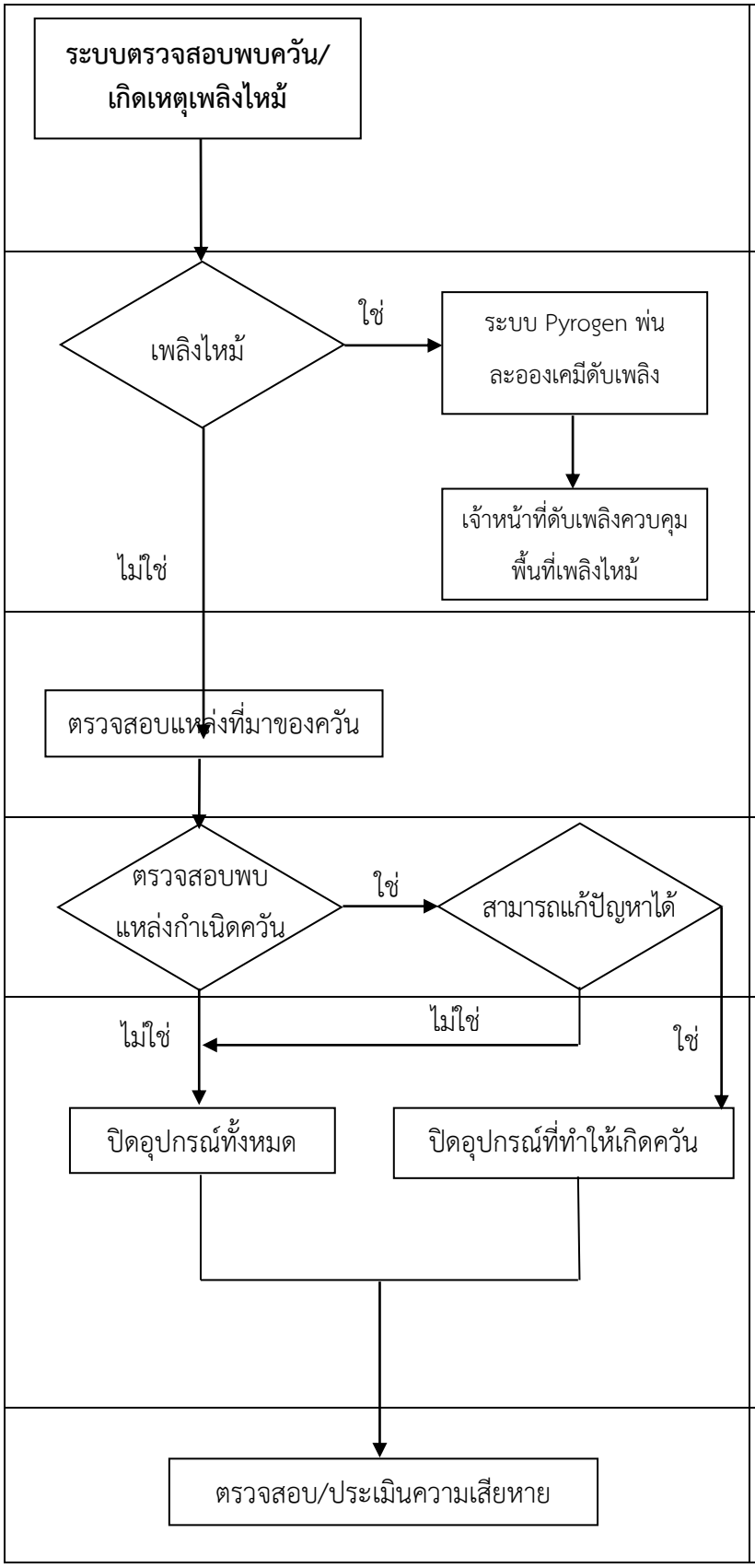
(๖) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือขายโดยเร็วที่สุด

(๗) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

(๘) ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยเร็ว

๔.๖ กระบวนการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ

๔.๖.๑ ข้อปฏิบัติกรณีเกิดเพลิงไหม้



- ระบบไฟฟ้าดับ ระบบ Tale Alarm แจ้งว่าตรวจพบควัน (SMOKE DETECTER)
- แจ้งบริษัทคู่สัญญาให้มาตรวจสอบความเสียหาย/แก้ไข

- ฝ่ายปฏิบัติตรวจสอบประเมินเหตุการณ์ว่าเกิดเพลิงไหม้หรือไม่ แจ้งฝ่ายอำนวยการ ฝ่ายสนับสนุน ทราบให้บุคลากรออกจากพื้นที่แจ้งสถานีดับเพลิงดุสิต
- หากเกิดเพลิงไหม้ระบบ Pyrogen จะทำงานอัตโนมัติ

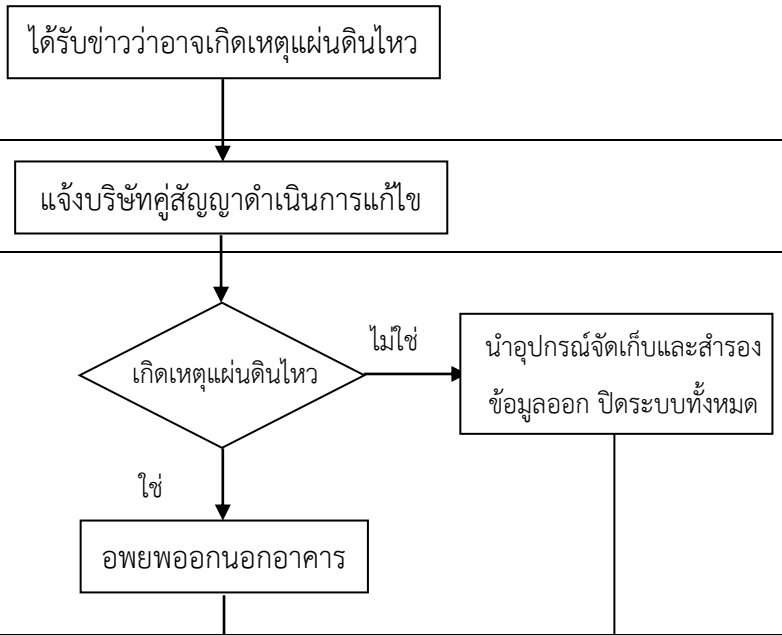
- หากไม่เกิดเพลิงไหม้ ให้ฝ่ายปฏิบัติตรวจสอบแหล่งที่มาของควันและประเมินสถานการณ์และแจ้งให้ฝ่ายอำนวยการทราบ

- หากตรวจสอบพบแหล่งที่มาของควัน ให้ประเมินสถานการณ์ว่าสามารถควบคุมและแก้ไขได้ หรือไม่

- หากตรวจสอบไม่พบแหล่งที่มาของควันให้ทำการหรือตรวจพบแหล่งที่มาแต่ไม่สามารถแก้ไขปัญหาได้ ให้ปิดอุปกรณ์ทั้งหมดปิดเครื่องปรับอากาศและระบบไฟฟ้า
- หากตรวจพบแหล่งกำเนิดควันและสามารถแก้ไขปัญหาได้ให้ปิดอุปกรณ์ที่ทำให้เกิดควัน

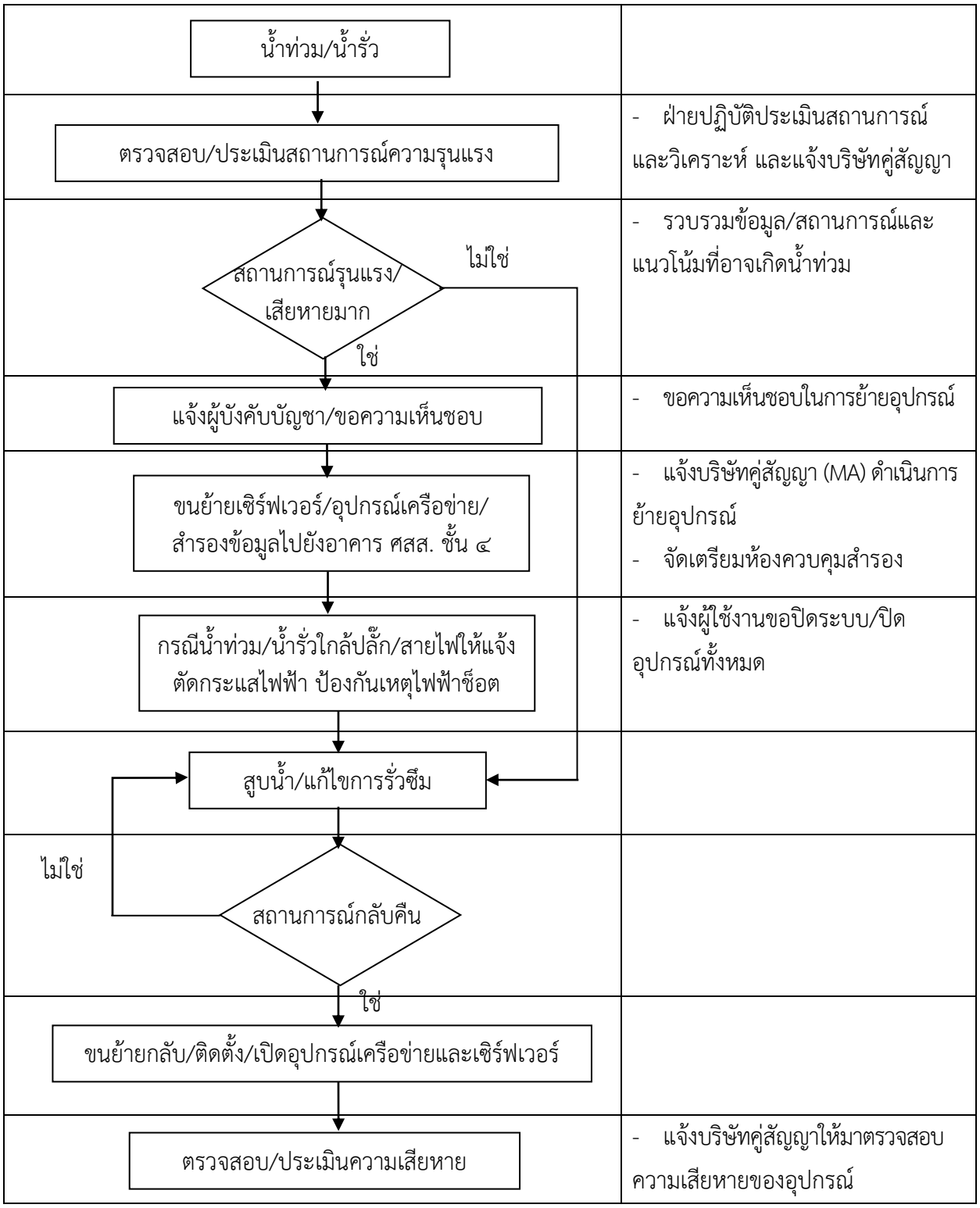
- แจ้งบริษัทคู่สัญญาให้มาตรวจสอบความเสียหายของอุปกรณ์

๔.๖.๒ ข้อปฏิบัติกรณีเกิดเหตุแผ่นดินไหว

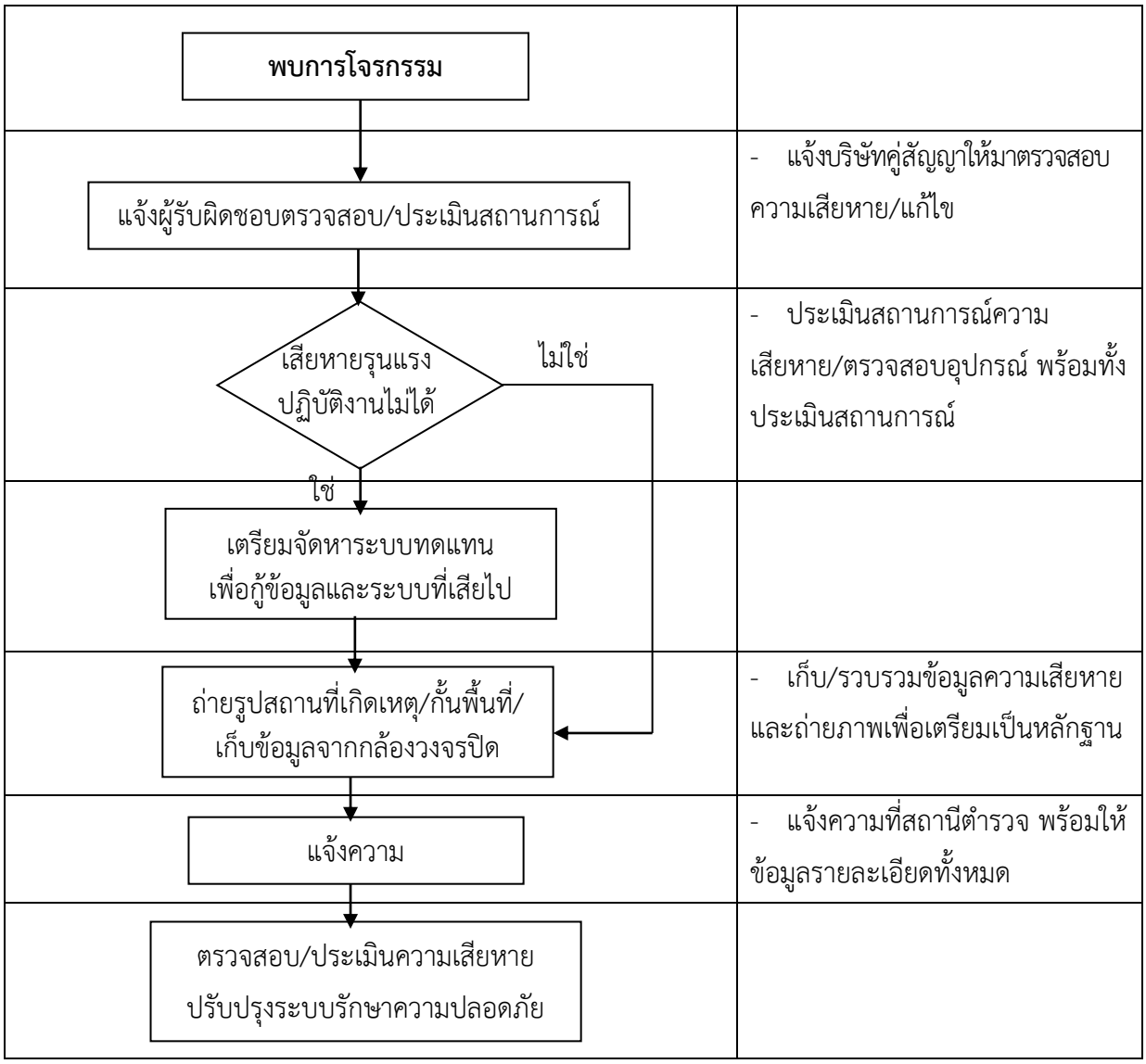


	- ได้รับแจ้งจากหน่วยงานที่เกี่ยวข้อง แจ้งว่าจะเกิดเหตุแผ่นดินไหว
	- แจ้งบริษัทคู่สัญญาให้มาตรวจสอบความเสียหาย/แก้ไข
	- ประเมินสถานการณ์หากเกิดขึ้นแล้วให้อพยพออกนอกอาคาร - หากยังไม่เกิดขึ้นแต่ได้รับการแจ้งเตือนให้นำอุปกรณ์สำรองข้อมูลออกและปิดระบบทั้งหมด
	- รอเหตุการณ์สงบหรือพ้นระยะเวลาที่ได้รับแจ้งว่าอาจเกิดแผ่นดินไหวให้ดำเนินการตรวจสอบความเสียหายและความพร้อมใช้งานของอุปกรณ์
	- ตรวจสอบอุปกรณ์ทั้งหมดว่าได้รับความเสียหายหรือไม่ หากไม่ได้รับความเสียหายให้ประเมินความพร้อมใช้งาน หากมีความพร้อมใช้งานให้เปิดระบบทั้งหมดดังเดิม
	- กรณีอุปกรณ์ได้รับความเสียหายให้แจ้งผู้บังคับบัญชาทราบและแจ้งบริษัทคู่สัญญาบำรุงรักษาระบบมาตรวจสอบดำเนินการแก้ไขหรือจัดหาอุปกรณ์มาทดแทน

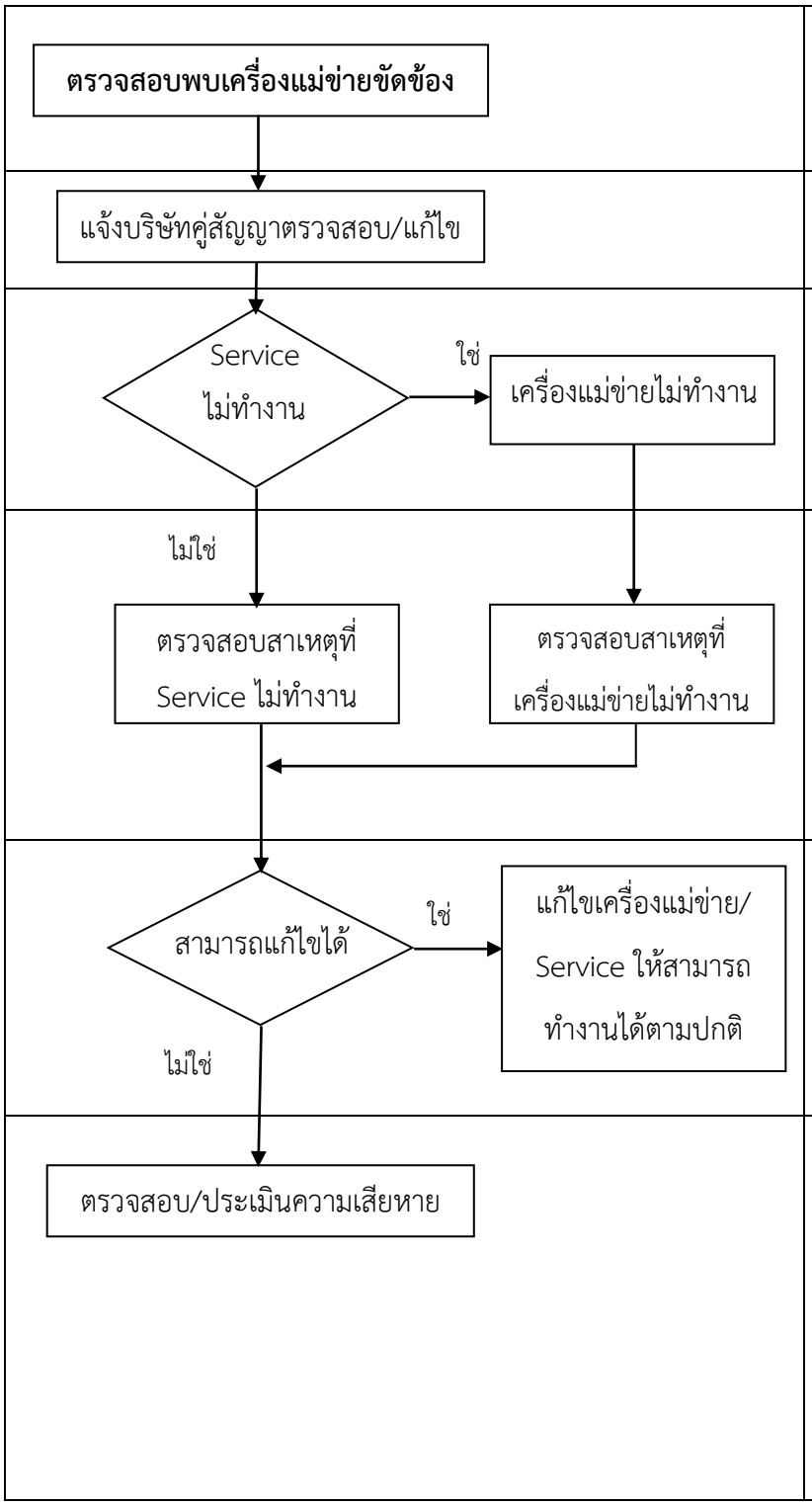
๔.๖.๓ ข้อปฏิบัติกรณีเกิดน้ำท่วม/น้ำรั่วซึม



๔.๖.๔ ข้อปฏิบัติกรณีโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์

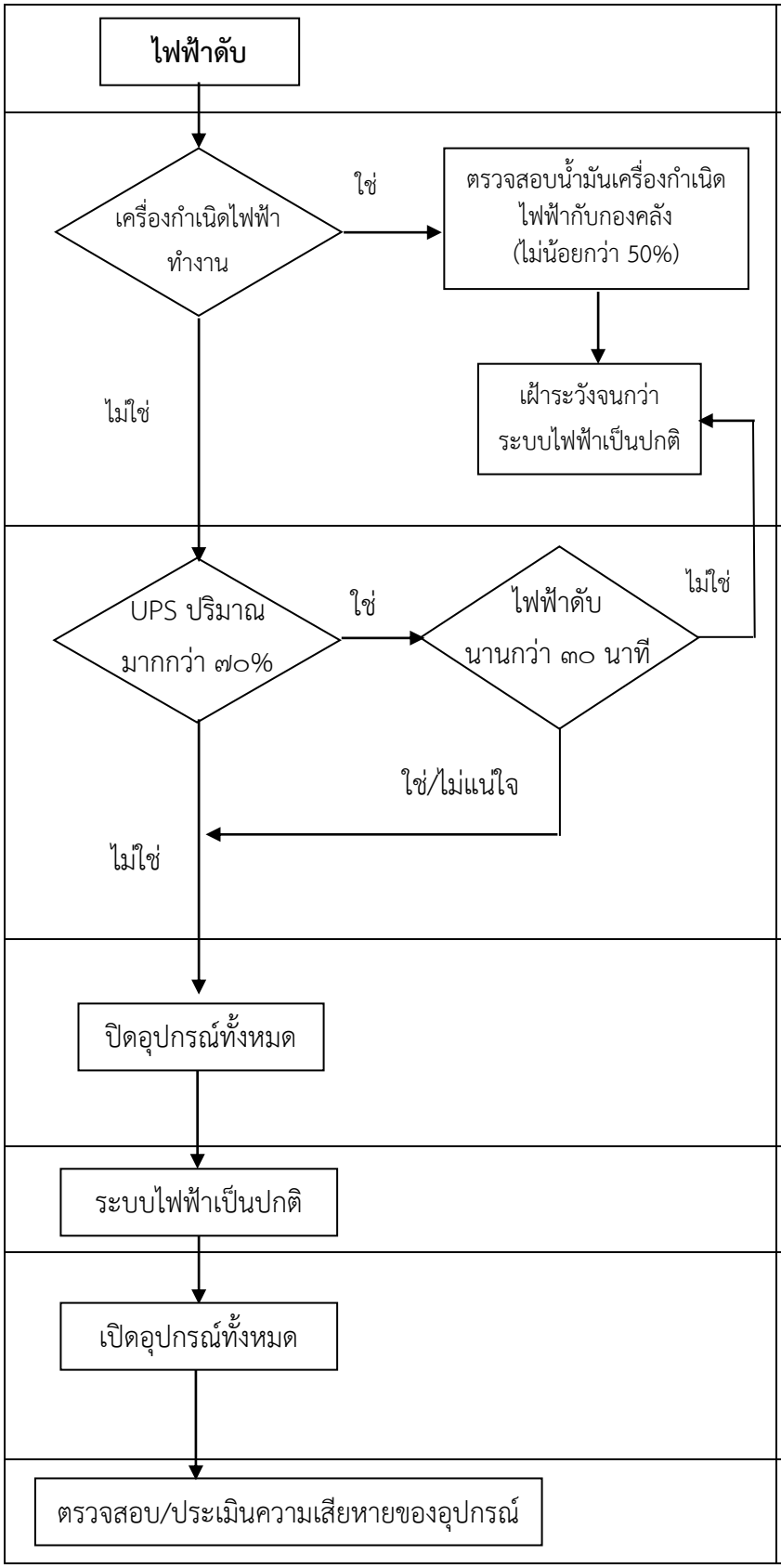


๔.๖.๕ ข้อปฏิบัติกรณีเกิดเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง



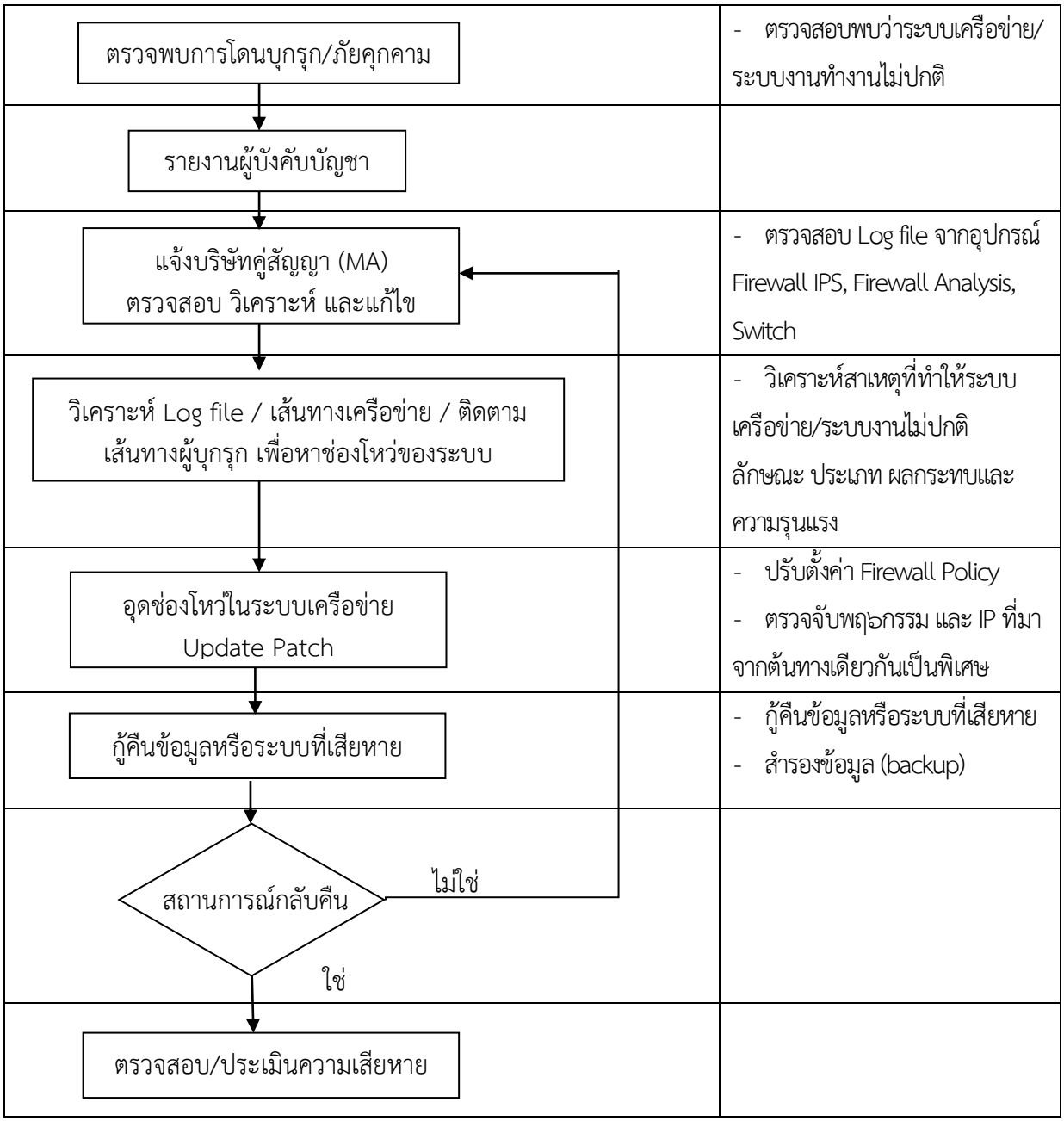
หมายเหตุ : อุปกรณ์ทั้งหมดได้รับการบำรุงรักษา ตามโครงการบำรุงรักษาระบบเครือข่ายและระบบ Antivirus (MA)

๔.๖.๖ ข้อปฏิบัติกรณีไฟฟ้าดับ

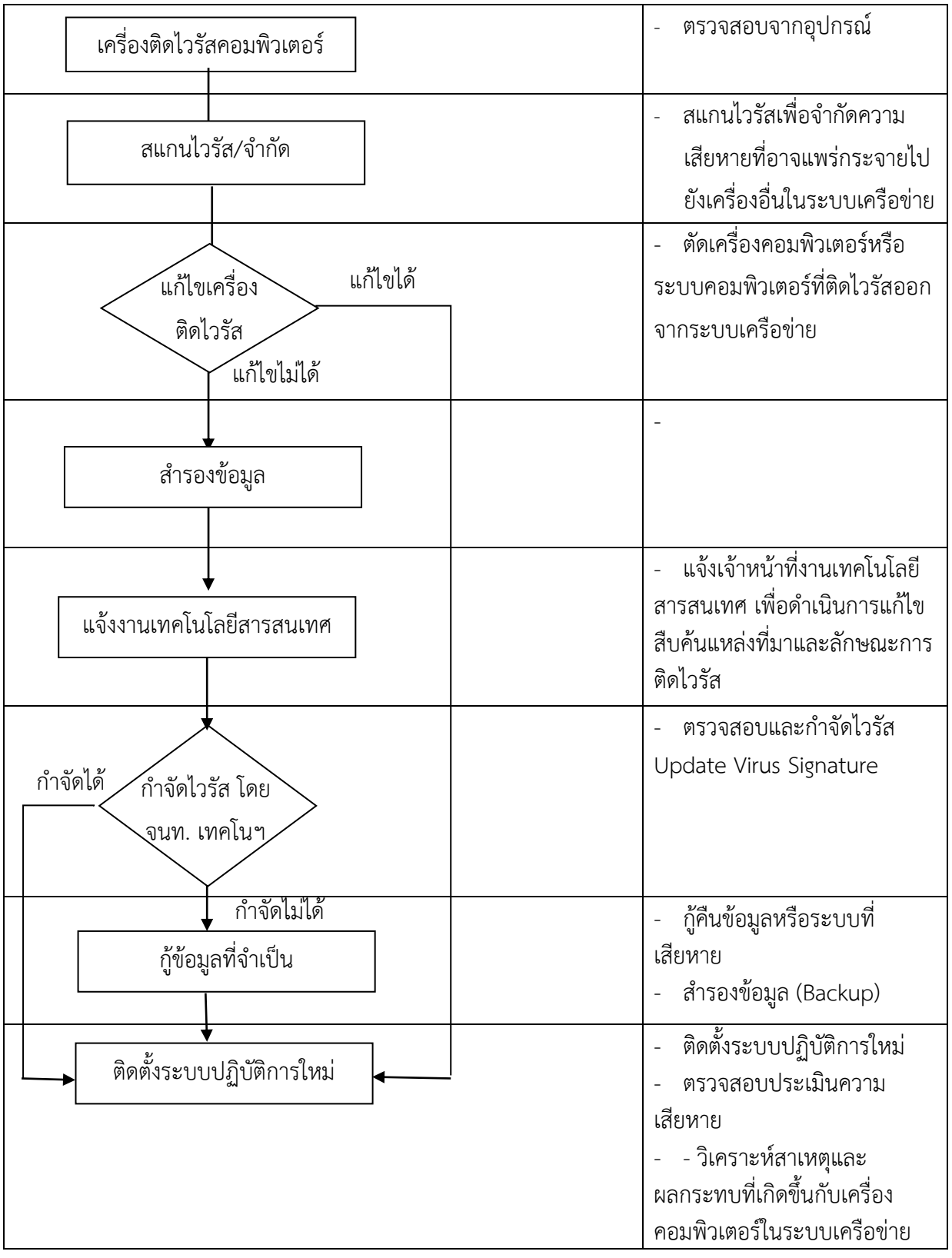


	- ระบบไฟฟ้าดับ ระบบ Tale Alarm แจ้งว่าไฟฟ้าดับ (Main Power FAIL)
	- ตรวจสอบเครื่องกำเนิดไฟฟ้าว่าทำงานหรือไม่ - กรณีที่เครื่องกำเนิดไฟฟ้าทำงานให้ฝ่ายปฏิบัติตรวจสอบปริมาณน้ำมันและแจ้งกองคลังสำรองน้ำมันหากมีน้ำมันน้อยกว่า ๕๐% และเฝ้าระวังจนกว่าระบบไฟฟ้าจะเป็นปกติ
	- กรณีเครื่องกำเนิดไฟฟ้าไม่ทำงาน ฝ่ายปฏิบัติตรวจสอบ UPS ว่าปริมาณไฟฟ้าสำรองมากกว่า ๗๐% ให้สอบถาม กฟน. ถึงระยะเวลาที่ไฟฟ้าจะกลับเป็นปกติ - หากไฟฟ้าดับน้อยกว่า ๓๐ นาที ให้เฝ้าระวังจนกว่าระบบไฟฟ้าจะเป็นปกติ
	- ปิดอุปกรณ์หากปริมาณไฟฟ้าสำรองของ UPS น้อยกว่า ๗๐% หรือไฟฟ้าดับนานกว่า ๓๐ นาที หรือไม่แน่ใจสถานการณ์
	- ตรวจสอบระบบไฟฟ้าว่าทำงานเป็นปกติหรือไม่
	- หากระบบไฟฟ้าเป็นปกติให้เปิดระบบไฟฟ้าเครื่องปรับอากาศและให้อุณหภูมิอยู่ที่ ๒๕°C แล้วเปิดอุปกรณ์ทั้งหมด
	แจ้งบริษัทคู่สัญญาให้มาตรวจสอบความเสียหายของอุปกรณ์

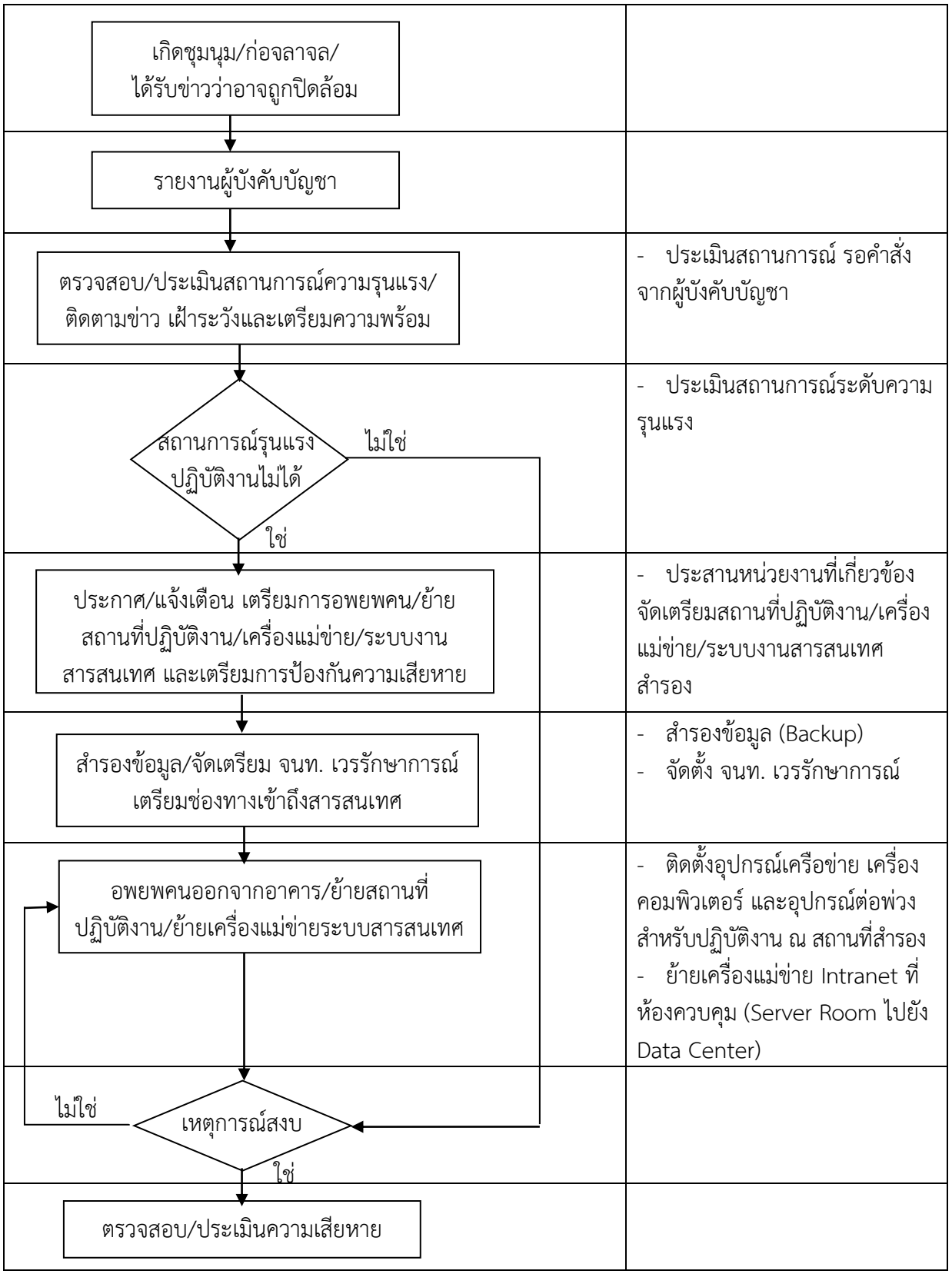
๔.๖.๗ ข้อปฏิบัติกรณีโดนบุกรุก และภัยคุกคามทางคอมพิวเตอร์



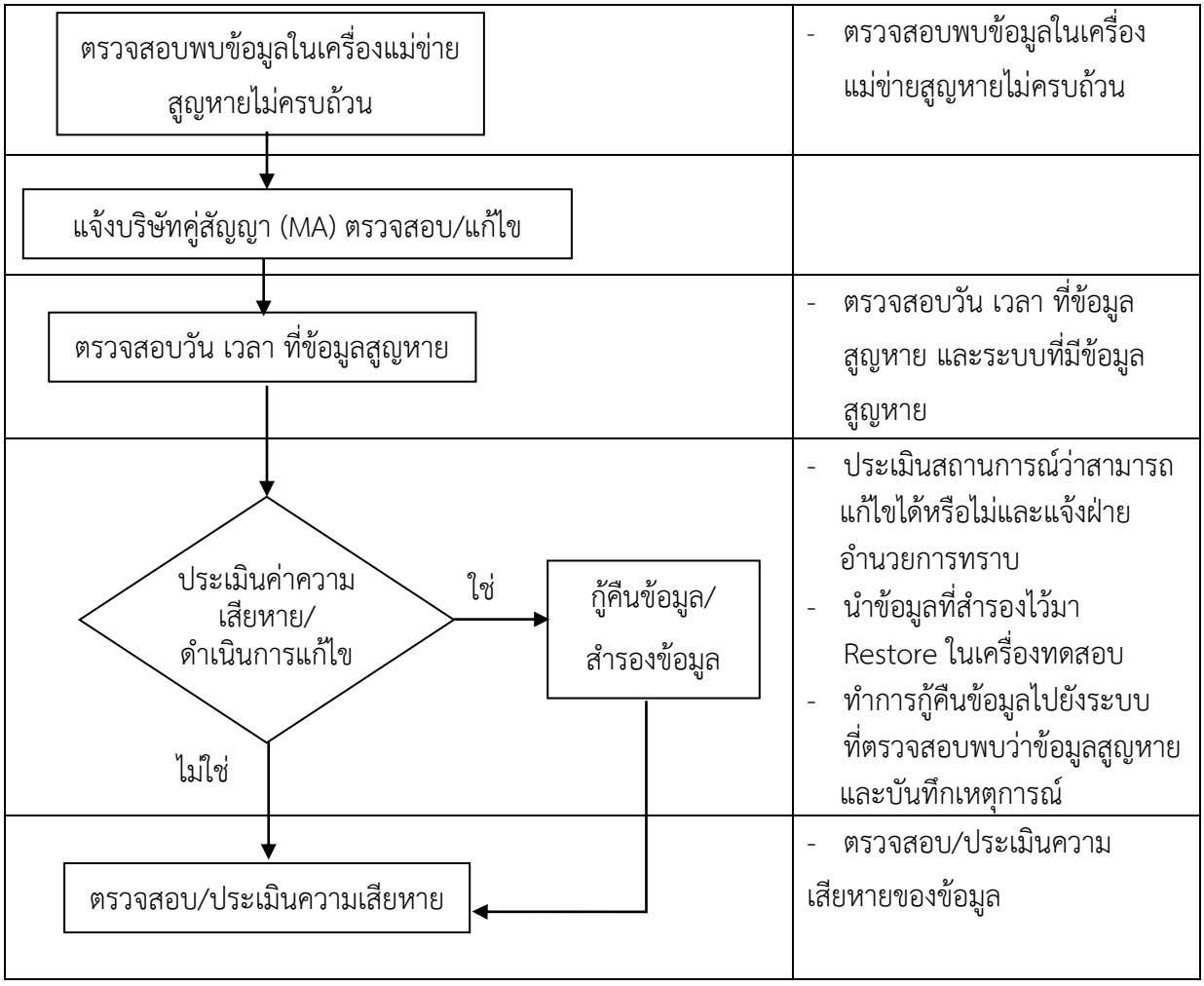
๔.๖.๘ ข้อปฏิบัติกรณีเครื่องติดไวรัสคอมพิวเตอร์



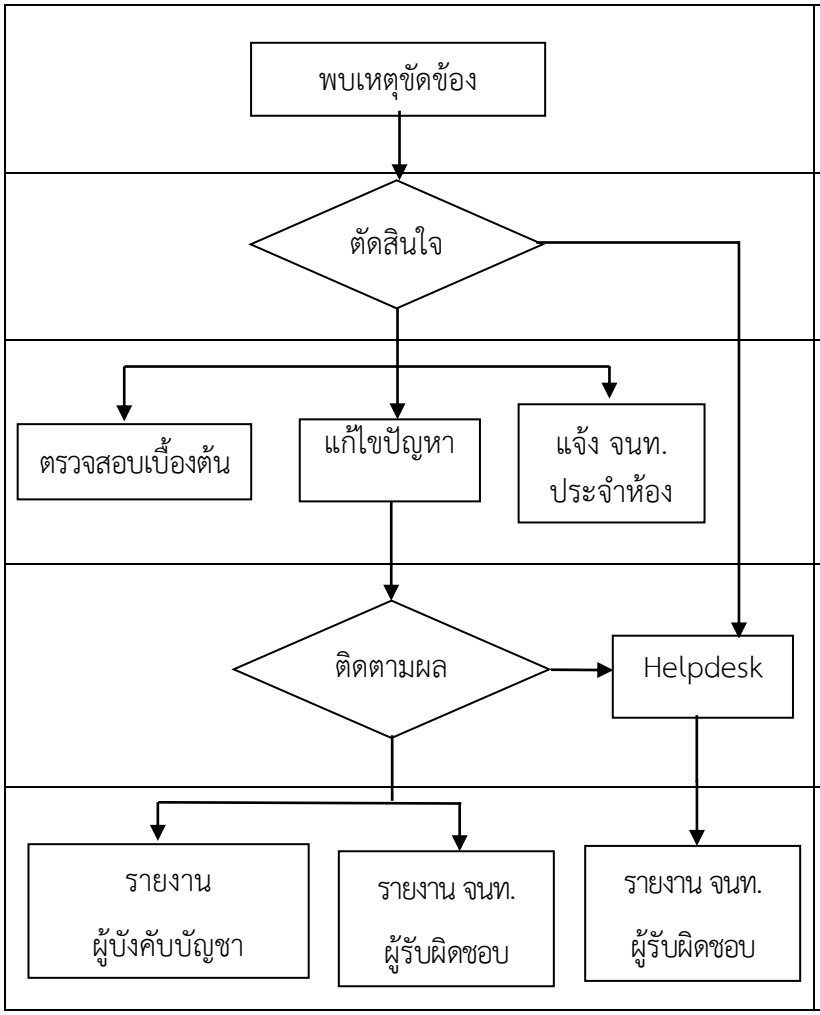
๔.๖.๙ ข้อปฏิบัติกรณีโดนปิดล้อมสถานที่ปฏิบัติงาน (ชุมนุม/ประท้วง/ก่อจลาจล)



๔.๖.๑๐ ข้อปฏิบัติกรณีการกู้คืนข้อมูล

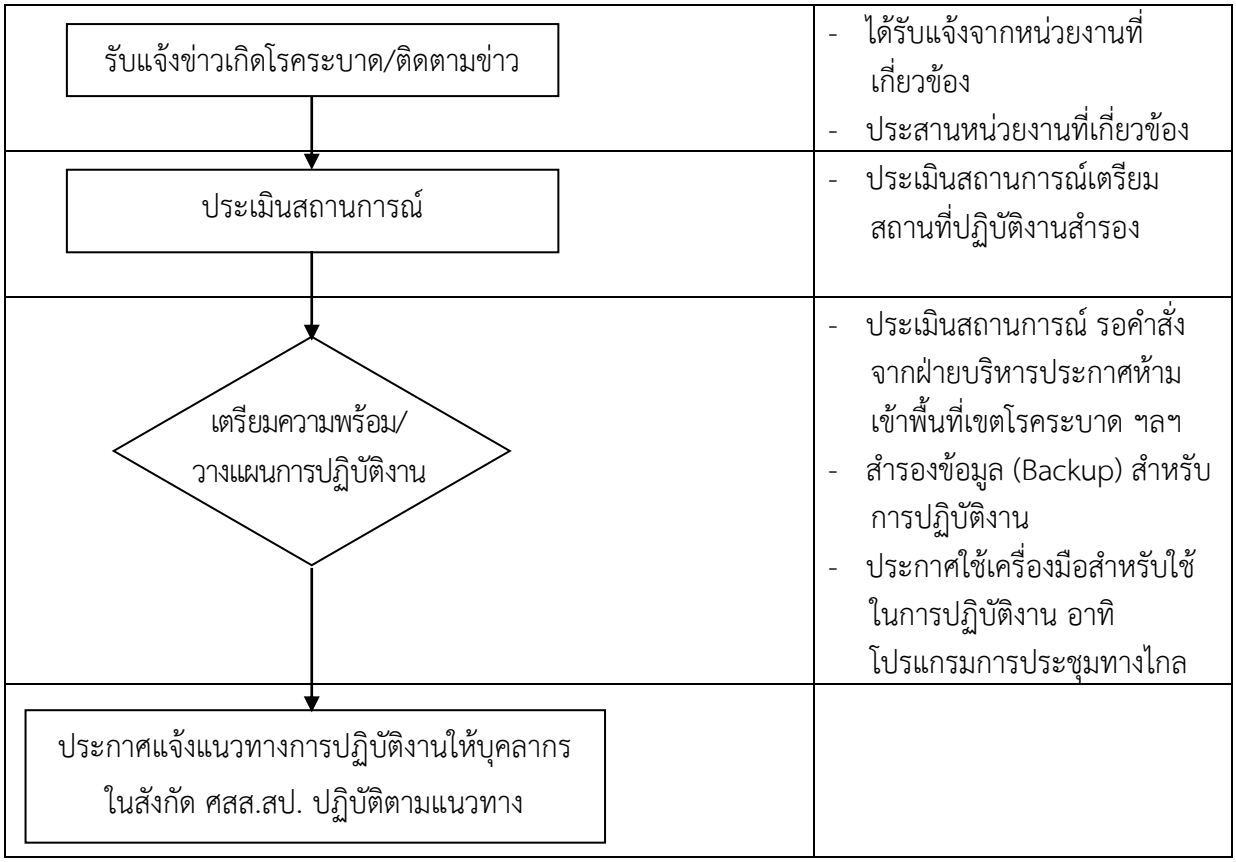


๔.๖.๑๑ ข้อปฏิบัติกรณีพบเหตุเครื่องมือสื่อสารขัดข้อง



	- ตรวจพบเหตุขัดข้อง
	- ประเมินสถานการณ์ เพื่อประสานแจ้งผู้ที่เกี่ยวข้อง
	- -ตรวจสอบวัน เวลา และข้อมูล - แก้ไขปัญหา - ดำเนินการแจ้งเจ้าหน้าที่ประจำห้อง
	- ติดตามผลการแก้ไขปัญหา - แก้ไขปัญหา ดำเนินการแจ้งเจ้าหน้าที่ประจำห้อง
	- รายงานผู้บังคับบัญชา - แจ้งเจ้าหน้าที่ผู้รับผิดชอบเพื่อดำเนินการแก้ไข

๔.๖.๑๒ ข้อปฏิบัติกรณีเกิดโรคระบาดในสถานที่ปฏิบัติงาน



๔.๗ มาตรการปฏิบัติในการสำรองระบบงาน (Backup) และการนำข้อมูลกลับมาใช้ (Recovery)

๔.๗.๑ ขั้นตอนในการสำรองระบบงาน (Backup)

(๑) ระบบสารบรรณอิเล็กทรอนิกส์

การสำรองข้อมูลของระบบงานทั้งหมดจะดำเนินการโดย ใช้ Hyper-V Replica ในการสำรองข้อมูล จากศูนย์ข้อมูลหลักไปยังศูนย์สำรองข้อมูล โดยข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายเสมือนทั้งหมดในระบบจะถูกทำสำเนาตัวเองและส่งไปจัดเก็บที่ศูนย์สารองข้อมูลทุก ๑๕ นาที โดยไฟล์จะถูกจัดเก็บที่ C:\ClusterStorage\VMStore-DR\replica\Hyper-V Replica และไฟล์จะถูกเขียนทับข้อมูลเดิมเพื่อป้องกันปัญหาเรื่องพื้นที่จัดเก็บเต็ม

(๒) ระบบเว็บไซต์ (Web Server) และระบบจดหมายอิเล็กทรอนิกส์ (E-Mail Server)

การสำรองข้อมูลโดยการใช้ระบบปฏิบัติการ windows server มีขั้นตอนดังนี้

๑. ทำการ map drive จาก server ที่ต้องการ backup

๒. Click ที่ Start > All Programs > Accessories > System Toolsแลว click เลือก Backup จะแสดงหน้าต่าง Welcome to the Backup or Restore Wizard

๓. Click เลือก Advanced Mode

๔. Click ที่แถบ Schedule Jobs

๕. Click ที่ Add Job

๖. แสดงหน้าต่าง Welcome to the Backup Wizard Click ที่ Next

๗. หน้าต่าง what to Back Up เลือกรายการ Back up selected files, drives, or Network dataแลว click ที่ Next

๘. หน้าต่างItems to Back Up จะแสดงรายชื่อ drive หรือ folder ให้click เลือกในชองCheck boxes รายชื่อ files, folders หรือ drives ที่ต้องการจะ backup แลว clickที่ Next

๙. หน้าต่าง Backup Type, Destination, and Name ที่ช่อง Choose a place to saveyourbackup : ให้click Browse เพื่อระบุชื่อ file และ path ที่จะใช้ในการ save (.bkf) file เสร็จแล้ว click Save และ click ที่ Next

๑๐. หน้าต่าง Type of Backup > Select he type of backup : เป็นการเลือกประเภทของการ Backup ได้แก่ รายวัน เลือก Incremental และ รายสัปดาห์ เลือก Normal จาก click ที่ Next

๑๑. หน้าต่าง How to Back Up ให้click ที่ Next

๑๒. หน้าต่าง Backup Options > Replace the existing backups แลว click ที่ Next

๑๓. หน้าต่าง When to Back Up > Later ช่อง Job name: ระบุชื่อ Monday เลือก Set Schedule

๔.๗.๒ แผนการสำรองข้อมูล

(๑) ระบบสารบรรณอิเล็กทรอนิกส์

ทุก ๑๕ นาที จะทำการสำรองข้อมูลแบบ Replicate และเก็บข้อมูลไฟล์ที่สารองไว้ที่ C:\ClusterStorage\VMStore-DR\replica\Hyper-V Replica โดยไฟล์สารองข้อมูลจะเป็นข้อมูลล่าสุดเสมอ เพื่อความเป็นปัจจุบันของข้อมูลและจะถูกเขียนทับข้อมูลเดิมเพื่อป้องกันปัญหาเรื่องพื้นที่จัดเก็บข้อมูล

(๒) ระบบศูนย์ข้อมูลกลางกระทรวงมหาดไทยและจังหวัด

Database Server

- ทุกวัน เวลา ๑๒.๓๐ น. และ ๑๘.๓๐ น. จะทำการสำรองข้อมูลลงดิสก์ (Disk)
- ทุกวันเสาร์ เวลา ๒๑.๐๐ น. จะทำการสำรองข้อมูลแบบ Full Backup ลงเทป (Tape)
- แบ่งและเก็บ File Backup ไว้ที่ /oradata/oracle,/export/home โดย File Backup จะถูกเก็บไว้เป็นเวลา ๑ สัปดาห์

Application Server

- ทุกวันที่ ๑๕ ของทุกเดือน เวลา ๐๐.๐๐ น. จะทำการสำรองข้อมูลแบบ Full Backup ลงเทป (Tape)
- แบ่งและเก็บ File Backup ไว้ที่ /data,/export/home ,/export/home2,app

(๓) ระบบเว็บไซต์ (Web Server) และระบบจดหมายอิเล็กทรอนิกส์ (E-Mail Server)

ระบบทำการจำลองการใช้งานแบบเซิร์ฟเวอร์เสมือน (Could Solution) จะเริ่มทำการ Backup โดยระบบจะทำกระบวนการ Snap Shotted โดยไม่รบกวนการใช้งานระบบตามระยะเวลาที่กำหนด เป็นรายวัน รายสัปดาห์ รายเดือน โดยจะทำเป็นไฟล์ข้อมูล ที่รวมข้อมูลทั้งหมดเอาไว้ ทั้งในส่วน ฐานข้อมูล รูปภาพ ไฟล์เว็บไซต์ (HTML, CSS, Java Script) โดยจัดทำการสำรองข้อมูล โดย "Direct Admin" ในรูปแบบ Full Backup ประจำสัปดาห์

๔.๗.๓ การจัดเก็บข้อมูลสำรอง

(๑) ระบบสารบรรณอิเล็กทรอนิกส์

(๑.๑) การสำรองฐานข้อมูล (Database)

- ทำการสำรองข้อมูลเป็น Database ลงดิสก์ (Disk) เก็บไว้ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) อาคาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๔ ถนนวิสุทธิกษัตริย์
- ทุกวัน เวลา ๒๒.๐๐ น.

(๑.๒) การสำรองโปรแกรมประยุกต์ (Application)

- ทำการสำรองข้อมูลลงเทป (Tape) เก็บไว้ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) อาคาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๔ ถนนวิสุทธิกษัตริย์
- ทำการคัดลอก (Copy) เก็บไว้อีกชุดที่ห้องกลุ่มงานเทคโนโลยีสารสนเทศ อาคาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๒ ถนนวิสุทธิกษัตริย์
- ทุกวันที่ ๒๘ ของเดือน เวลา ๒๐.๐๐ น.

(๒) ระบบศูนย์ข้อมูลกลางกระทรวงมหาดไทยและจังหวัด

(๒.๑) การสำรองฐานข้อมูล (Database)

- ทำการสำรองข้อมูลเป็น Full Backup ลงเทป (Tape) เก็บไว้ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) อาคารศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๔ ถนนวิสุทธิกษัตริย์
- ทุกวันเสาร์ เวลา ๒๑.๐๐ น

(๒.๒) การสำรองโปรแกรมประยุกต์ (Application)

- ทำการสำรองข้อมูลลงเทป (Tape) เก็บไว้ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) อาคารศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๔ ถนนวิสุทธิกษัตริย์
- ทุกวันที่ ๑๕ ของทุกเดือน เวลา ๐๐.๐๐ น.

๔.๗.๔ ขั้นตอนในการนำข้อมูลกลับมาใช้ (Recovery)

(๑) ระบบสารบรรณอิเล็กทรอนิกส์

การกู้คือระบบงานจะต้องดำเนินการสั่ง Failover ที่เมนู Replication ใน Failover Cluster Manager เพื่อเริ่มต้นการทำงานของเครื่องแม่ข่ายเสมือนที่ศูนย์สำรองข้อมูล

(๒) ระบบศูนย์ข้อมูลกลางกระทรวงมหาดไทยและจังหวัด

(๒.๑) นำแผ่นระบบปฏิบัติการมาติดตั้งใหม่

(๒.๒) ติดตั้งโปรแกรมพื้นฐานตามการใช้งาน

(๒.๓) นำเทป (Tape) มากู้คืนระบบ (Restore)

(๓) ระบบเว็บไซต์ (Web Server) และระบบจดหมายอิเล็กทรอนิกส์ (E-Mail Server)

(๓.๑) จุดกู้คืน (กู้คืน จากภาพรวม)

สาเหตุ : เมื่อเซิร์ฟเวอร์เสมือนมีความเสียหายของข้อมูลที่ไม่สามารถซ่อมแซมแบบปกติได้ สามารถกู้คืน (Recovery) เซิร์ฟเวอร์เสมือนเฉพาะจาก VDR ภาพรวม

ขั้นตอนการกู้คืน <u>ด้วยตนเอง</u> โดย

(ก) จุดที่ต้องการเรียกคืน Recovery

(ข) การ Recovery

(๓.๒) หากต้องการข้อมูลที่ต้องการกู้คืนมีความเสียหายบางส่วนที่เกิดขึ้นกับไฟล์หรือฐานข้อมูล : จะกู้คืนไฟล์ที่เสียหายจาก "Direct Admin " ไฟล์สำรอง

ขั้นตอนการกู้คืน <u>ด้วยตนเอง</u> โดยเลือกจุดกู้คืนซึ่งต้องการที่จะเรียกคืน (แก้ไข) บราว์เซอร์ระบุไฟล์เป้าหมาย (ข) การเลือกสถานที่ปลายทางจะเรียกคืนการคืนค่า

๔.๘ แผนการกู้คืนระบบกลับสู่สภาพปกติ

๔.๘.๑ การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

(๑) จัดหาอุปกรณ์/ชิ้นส่วนเพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

(๒) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้แล้วเสร็จภายใน ๔๘ ชั่วโมง (ตามเงื่อนไข)

(๓) จัดหาอุปกรณ์คอมพิวเตอร์ทดแทนจากหน่วยงานอื่นมาใช้เป็นการชั่วคราว

(๔) นำสื่อที่ได้จัดเก็บข้อมูลที่สำรองไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง

(๕) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

๔.๘.๒ การกู้คืนระบบสารสนเทศและฐานข้อมูลให้สู่สภาวะปกติ ดังนี้

(๑) ปิดระบบสารสนเทศที่ต้องการกู้คืนข้อมูล

(๒) ตรวจสอบวันเวลาที่ข้อมูลสูญหาย

(๓) เตรียมไฟล์ Database ที่ทำการ Backup ไว้ในแต่ละวันเพื่อใช้ในการ Restore ข้อมูล

(๔) ทำการกู้คืนข้อมูล Restore

(๕) เปิดใช้งานระบบสารสนเทศ

(๖) ตรวจสอบข้อมูลที่ได้ทำการกู้คืนโดยผู้ดูแลระบบ

(๗) แจ้งผู้ใช้งานให้ดำเนินการตรวจสอบข้อมูลหลังจาก Restore

๔.๙ การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ เมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้หัวหน้ากลุ่มงาน / สำนักงาน ทราบ เพื่อนำเสนอรายงานสรุปการเกิดปัญหา และผลการแก้ไขให้ผู้บังคับบัญชาทราบ ในทันทีตามแผนกระบวนการในการป้องกันและแก้ไขปัญหาภัยพิบัติในทุกกรณี พร้อมทั้งสรุปรายงานผลการดำเนินการ การตรวจสอบ และการแก้ไขปัญหาต่าง ๆ ให้ผู้บังคับบัญชาทราบ

ภาคผนวก

ศูนย์ความมั่นคงปลอดภัยไซเบอร์ของออสเตรเลีย (Australian Cyber Security Centre หรือ ACSC) แนวโน้มรูปแบบการโจมตีทางไซเบอร์ที่พบในระหว่างปี ๒๐๑๙-๒๐๒๐ โดยภาพรวมเป็นการวิเคราะห์กลยุทธ์ เทคนิค และวิธีการที่ผู้โจมตีใช้เพื่อบุกรุกระบบหรือขโมยข้อมูล อ้างอิงตาม MITRE ATT&CK โดยรูปแบบการโจมตีที่พบมีดังนี้

๑. Initial Access การโจมตีโดยการเข้าถึงระบบของเป้าหมาย เช่น
- เจาะระบบผ่านช่องโหว่ของแอปพลิเคชันที่เปิดให้เข้าถึงได้แบบสาธารณะ เช่น ช่องโหว่การอัปโหลดไฟล์ขึ้นไปบนเว็บไซต์ ช่องโหว่ของโปรแกรมบริหารจัดการเว็บไซต์ หรือช่องโหว่ของโปรแกรม VPN
- เดารหัสผ่านของบัญชีผู้ใช้ หากระบบไม่ได้ถูกตั้งค่าให้ป้องกันการ brute force ก็มีโอกาสสูงที่รหัสผ่านจะหลุดได้ง่าย
- ส่งอีเมลฟิชชิ่งแบบกำหนดเป้าหมาย ซึ่งโดยส่วนใหญ่มักเป็นการส่งมัลแวร์แนบไปกับอีเมลเพื่อให้เหยื่อเปิดไฟล์มัลแวร์นั้น

๒. Execution การเรียกโปรแกรมหรือคำสั่งอันตราย (มัลแวร์) ขึ้นมาประมวลผล เช่น
- เรียกใช้งานโปรแกรมผ่าน command line หรือ PowerShell ซึ่งเป็นช่องทางที่ถูกออกแบบมาไว้เพื่อใช้สั่งรันโปรแกรมบน Windows อยู่แล้ว
- รันโค้ดผ่านสคริปต์ เช่น ไฟล์ .BAT, JavaScript, หรือ Microsoft Office macro
- หลอกให้เหยื่อดาวน์โหลดไฟล์มัลแวร์ไปเรียกใช้งานเอง

๓. Persistence ทำให้มัลแวร์ยังคงทำงานอยู่ในระบบถึงแม้จะถูกรีสตาร์ท เช่น
- เพิ่มข้อมูลใน Registry หรือสร้าง shortcut ในโฟลเดอร์ Startup เพื่อให้มีการเรียกมัลแวร์ขึ้นมาทำงานทุกครั้งที่เปิดเครื่อง
- ในกรณีการโจมตีเว็บไซต์ เทคนิคที่มักถูกใช้คือการฝัง web shell ซึ่งเป็นการอัปโหลดหน้าเว็บไซต์สำหรับใช้เป็นช่องทางรับคำสั่งหรือเชื่อมต่อเข้าไปยังระบบในภายหลัง

๔. Privilege escalation การทำเพื่อให้ได้สิทธิ์การทำงานที่สูงกว่าสิทธิ์ของผู้ใช้ทั่วไป จุดประสงค์เพื่อเข้าถึงหรือแก้ไขไฟล์ด้วยสิทธิ์ที่มากขึ้น หรือเปลี่ยนแปลงการตั้งค่าของระบบ ตัวอย่างรูปแบบการโจมตีที่พบ เช่น ใช้เครื่องมือ RottenPotato ในการโจมตีเพื่อให้ได้สิทธิ์สูงสุดของระบบ

๕. Defence evasion เป็นเทคนิคที่ใช้เพื่อหลบเลี่ยงการตรวจจับหรือการสังเกตความผิดปกติของระบบ เช่น
- ใช้เทคนิค Timestomp เพื่อแก้ไขวันเวลาที่ไฟล์มัลแวร์ถูกติดตั้งลงในระบบ เช่น แก้ให้ไฟล์ web shell ถูกสร้างขึ้นในวันเวลาเดียวกับไฟล์อื่น ๆ ในเว็บไซต์ จุดประสงค์เพื่อให้ผู้ดูแลระบบมองข้ามไฟล์ดังกล่าวหรือเกิดความสับสนหากต้องตรวจสอบว่าระบบถูกโจมตีเมื่อใด
- ลบไฟล์ล็อกของระบบ เช่น Windows event log หรือ web access log เพื่อไม่ให้ตรวจสอบได้ว่าถูกโจมตีด้วยวิธีใดหรือวันเวลาใด
- ลบไฟล์มัลแวร์ทิ้งหลังโจมตีสำเร็จ หรือซ่อนไฟล์ไม่ให้ปรากฏเมื่อเรียกดูข้อมูลด้วยวิธีปกติ
- ใช้วิธีบีบอัดข้อมูลของไฟล์มัลแวร์ จุดประสงค์เพื่อทำให้ค่า signature ของไฟล์เปลี่ยนไป ทำให้ระบบตรวจจับที่อาศัยแค่การวิเคราะห์จากข้อมูล signature เพียงอย่างเดียวนั้นไม่สามารถตรวจพบความผิดปกติได้

๖. Credential access เป็นการขโมยหรือรวบรวมข้อมูลบัญชีผู้ใช้ในระบบ เช่น
- ใช้เครื่องมือ เช่น Mimikatz ในการ dump บัญชีผู้ใช้และรหัสผ่าน
- ใช้เครื่องมือในลักษณะ keylogging เพื่อบันทึกข้อมูลที่ผู้ใช้พิมพ์ ซึ่งจะได้ชื่อผู้ใช้และรหัสผ่านด้วย
- อ่านข้อมูลจากไฟล์การตั้งค่า เช่น ระบบเว็บไซต์บางแห่งจะเก็บชื่อบัญชีและรหัสผ่านสำหรับเข้าถึงฐานข้อมูลไว้ในไฟล์ตั้งค่า หากสามารถอ่านข้อมูลจากไฟล์ดังกล่าวได้ก็จะสามารถเข้าถึงฐานข้อมูลได้

๗. Discovery เป็นเทคนิคที่ใช้เพื่อรวบรวมข้อมูลที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เป้าหมายหรือเครื่องคอมพิวเตอร์อื่น ๆ ที่อยู่ในเครือข่ายเดียวกัน เพื่อศึกษาสภาพแวดล้อมของระบบหรือใช้หาช่องทางโจมตีคอมพิวเตอร์เครื่องอื่น ๆ ต่อ เช่น
- ใช้เครื่องมือพื้นฐานที่ติดตั้งมาในระบบ เช่น คำสั่ง ping, net, หรือ sc เพื่อรวบรวมข้อมูล
- ใช้เครื่องมือ PowerSploit เพื่อรวบรวมข้อมูลบัญชีผู้ใช้และอุปกรณ์อื่น ๆ ในเครือข่าย หรือใช้เครื่องมือ SharpHound เพื่อรวบรวมข้อมูล Active Directory

๘. Lateral movement หลายครั้งการโจมตีจะไม่ได้เกิดขึ้นแค่ในคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง แต่จะเป็นการรวบรวมข้อมูลเครือข่ายแล้วเจาะไปยังคอมพิวเตอร์เครื่องอื่นต่อ ซึ่งอาจมีข้อมูลสำคัญหรือมีสิทธิ์ในการทำงานมากกว่าเครื่องที่เจาะได้ตอนแรก เช่น
- เชื่อมต่อไปยังคอมพิวเตอร์เครื่องอื่นผ่านช่องทาง secure shell (SSH) หรือ remote desktop (RDP)
- โจมตีผ่าน SMB โดยอาศัยฟีเจอร์ Windows Admin Shares เพื่อขโมยข้อมูลหรือสั่งรันโปรแกรมที่เครื่องปลายทาง
- เพิ่มไฟล์มัลแวร์ลงในโฟลเดอร์ที่มีการแชร์ผ่านเครือข่าย โดยตั้งชื่อไฟล์ให้ดูเหมือนว่าเป็นไฟล์ทั่วไป ซึ่งผู้ใช้คนอื่นในระบบก็มีโอกาสที่จะหลงเชื่อและเปิดไฟล์ดังกล่าว

๙. Collection เป็นการรวบรวมข้อมูลจากระบบของเป้าหมาย เช่น
- ขโมยไฟล์จากเครื่องคอมพิวเตอร์ของเป้าหมาย หรือไฟล์ที่แชร์ผ่านเครือข่าย
- ในบางกรณีผู้โจมตีอาจใช้วิธีรวบรวมข้อมูลแล้วสร้างเป็นไฟล์บีบอัดขึ้นมา จากนั้นค่อยส่งไฟล์ดังกล่าวออกไปในภายหลัง

๑๐. Command and control เป็นเทคนิคที่ผู้โจมตีใช้เพื่อเชื่อมต่อเข้ามาควบคุมเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ ตัวอย่างรูปแบบการโจมตีที่พบ เช่น ส่งคำสั่งผ่าน web shell

๑๑. Exfiltration เป็นรูปแบบของการส่งข้อมูลที่รวบรวมได้ออกไปให้ผู้โจมตี เช่น
- ส่งข้อมูลออกไปในรูปแบบของไฟล์ที่ถูกบีบอัดเพื่อลดขนาดของข้อมูล โดยอาจมีการตั้งรหัสผ่านของไฟล์บีบอัดไว้ด้วยเพื่อป้องกันระบบตรวจจับ
- ส่งข้อมูลผ่านช่องทางพิเศษที่มัลแวร์ใช้ติดต่อกับเครื่องสั่งการและควบคุม
- ใช้ช่องทางปกติเพื่อทำให้ดูเหมือนเป็นการใช้งานทั่วไป เช่น หลังจากที่ขโมยข้อมูลออกมาได้ก็สร้างเป็นไฟล์ไว้ในหน้าดาวน์โหลดของเว็บไซต์ แล้วตั้งชื่อไฟล์ให้ดูเหมือนเป็นไฟล์ปกติ จากนั้นดาวน์โหลดไฟล์ดังกล่าวจากหน้าเว็บไซต์โดยตรง

๑๒. Impact คือผลกระทบหรือความเสียหายที่เกิดขึ้นจากการโจมตี ซึ่งอาจมีได้หลายรูปแบบ ไม่ว่าจะเป็นข้อมูลรั่วไหล ระบบไม่สามารถให้บริการต่อได้ หรือข้อมูลสำคัญถูกเข้ารหัสลับเพื่อเรียกค่าไถ่

คณะจัดทำแผนบริหารจัดการความเสี่ยงด้านดิจิทัลและแผนแก้ไขปัญหาจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) สำนักงานปลัดกระทรวงมหาดไทย

คณะที่ปรึกษา

นายสุทธิพงษ์ จุลเจริญ	ปลัดกระทรวงมหาดไทย
นายสมคิด จันทมฤก	รองปลัดกระทรวงมหาดไทย ด้านบริหาร
นายพรพจน์ เพ็ญพาส	รองปลัดกระทรวงมหาดไทย ด้านพัฒนาชุมชนและส่งเสริมการปกครองท้องถิ่น
นายชำนาญวิทย์ เตรัตน์	รองปลัดกระทรวงมหาดไทย ด้านกิจการความมั่นคงภายใน
นายโชตินรินทร์ เกิดสม	รองปลัดกระทรวงมหาดไทย ด้านสาธารณภัยและพัฒนาเมือง

คณะผู้จัดทำ

นายศักดาวุธ ศักดิเศรษฐ์	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย
นางสาวอัญชลี เสียงระฆัง	ผู้อำนวยการกลุ่มงานยุทธศาสตร์สารสนเทศและการสื่อสาร
นางสาวมนัสวีช์ ทรัพย์พร้อม	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
นางสาวณิชนันท์ สิทธิพรหม	นักวิเคราะห์นโยบายและแผนปฏิบัติการ
นายกิตติธัช พรายงาม	นักวิเคราะห์นโยบายและแผนปฏิบัติการ
นางสาวสิริขวัญ ฟักสมบูรณ์	เจ้าหน้าที่สนับสนุนงานมหาดไทย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงมหาดไทย