แผนบริหารความเสี่ยง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานเศรษฐกิจการคลัง
พ.ศ. ๒๕๖๘

คำนำ

แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘ จัดทำขึ้นเพื่อใช้เป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และนำไปกำหนดแนวทางการจัดการและรับมือหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม ดังนั้น เพื่อให้การดำเนินภารกิจของสำนักงานเศรษฐกิจการคลังสามารถบรรลุวัตถุประสงค์และเป้าหมายได้อย่างต่อเนื่องและมีประสิทธิภาพมากขึ้น บุคลากรของสำนักงานเศรษฐกิจการคลังโดยเฉพาะบุคลากรด้านไอทีจำเป็นอย่างยิ่งที่จะต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกใช้มาตรการควบคุมหรือวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ในระดับที่สามารถยอมรับได้

ศูนย์เทคโนโลยีสารสนเทศในฐานะหน่วยงานสนับสนุนด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเศรษฐกิจการคลังหวังเป็นอย่างยิ่งว่าการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ตามแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘ ฉบับนี้ จะเป็นแนวทางในการลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเศรษฐกิจการคลังต่อไป

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานเศรษฐกิจการคลัง
๒๕๖๘

สารบัญ

บทสรุปผู้บริหาร

สำนักงานเศรษฐกิจการคลัง (สศค.) ได้นำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานในแต่ละส่วนงานตามภารกิจของสำนักงาน/กอง/ศูนย์/กลุ่ม ดังนั้นจึงมีความจำเป็นต้องมีแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ (บริหารความเสี่ยงฯ) เพื่อป้องกันปัญหาที่เกิดจากความเสี่ยง โดย สศค. ได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงฯ จึงได้จัดทำแผนบริหารความเสี่ยงฯ เพื่อเตรียมความพร้อมรับมือความเสี่ยงในรูปแบบต่าง ๆ รวมถึงรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นและอาจส่งผลกระทบถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล และระบบเครือข่าย โดยสามารถใช้เป็นแนวทางในการดูแลระบบรักษาความมั่นคงปลอดภัยให้มีเสถียรภาพ มีความพร้อมในการใช้งาน และให้การปฏิบัติงานตามภารกิจเป็นไปอย่างมีระบบและต่อเนื่อง สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที หากกรณีที่เกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ประเภทความเสี่ยงที่นำมาพิจารณา มีจำนวน ๕ ประเภทความเสี่ยง ประกอบด้วย (๑) ประเภทความเสี่ยงด้านการบริหารจัดการ (๒) ประเภทความเสี่ยงจากการปฏิบัติงาน (๓) ประเภทความเสี่ยงด้านเทคนิค (ครอบคลุมความเสี่ยงทางไซเบอร์) (๔) ประเภทความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน และ (๕) ประเภทความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์ จากการวิเคราะห์สามารถระบุความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยเสี่ยง ผลกระทบ และแนวทางการแก้ไขปัญหา จำนวนทั้งสิ้น ๑๔ ความเสี่ยง ประกอบด้วย

๑. ความเสี่ยงจากไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่
๒. ความเสี่ยงด้านระบบเครือข่ายคอมพิวเตอร์
๓. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ไม่สามารถทำงานได้
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์ทางไซเบอร์
๕. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ
๖. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้
๘. ความเสี่ยงด้านการขาดแคลนบุคลากร
๙. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม
๑๐. ความเสี่ยงด้านระบบฐานข้อมูล
๑๑. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดีหรือแฮกเกอร์
๑๒. ความเสี่ยงด้านโปรแกรมประยุกต์
๑๓. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์
๑๔. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ

/จากการวิเคราะห์ ...

จากการวิเคราะห์และประเมินความเสี่ยงทั้ง ๑๔ ความเสี่ยงดังกล่าวข้างต้น พบว่า มีระดับความเสี่ยงต่ำที่สามารถยอมรับได้ โดยได้กำหนดกลยุทธ์การจัดการความเสี่ยงและแนวทางการดำเนินการจัดการความเสี่ยงเรียบร้อยแล้ว

อย่างไรก็ตามปัญหาของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล และระบบเครือข่ายสามารถเกิดขึ้นได้ตลอดเวลา ดังนั้นการเตรียมความพร้อมในการรองรับสถานการณ์ เช่น การตรวจสอบและคัดกรองผู้เข้าใช้งานในระบบ การสำรองข้อมูลระบบปฏิบัติการและฐานข้อมูลต่าง ๆ ตามรอบระยะเวลา การจัดหาอุปกรณ์คอมพิวเตอร์ที่ทันสมัยเพื่อทดแทนของเดิมที่หมดอายุการใช้งานหรือไม่รองรับกับเทคโนโลยีปัจจุบัน รวมถึงการเสริมสร้างความรู้ในการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัยให้กับผู้ใช้งาน ใน สศค. เป็นต้น จะทำให้การปฏิบัติงานโดยใช้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพและปลอดภัยจากความเสี่ยงต่าง ๆ ที่อาจจะเกิดขึ้น

คำนิยาม

คำนิยามที่ใช้ในแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ฉบับนี้ ประกอบด้วย

“หน่วยงาน” หมายความว่า สำนักงานเศรษฐกิจการคลัง

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหารการสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

“สิทธิ์ของผู้ใช้งาน” หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

/“ความมั่นคงปลอดภัย” ...

“ความมั่นคงปลอดภัย” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และ ความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“ระบบแลน (Local Area Network)” และ **“ระบบอินทราเน็ต (Intranet)”** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกันเป็นระบบเครือข่าย ที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต (Internet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

“สารสนเทศ (Information)” หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานเศรษฐกิจการคลัง

“ผู้ใช้บริการ” หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน และให้หมายความรวมถึงเจ้าหน้าที่บริษัทที่ปรึกษาที่เข้ามาปฏิบัติงานในหน่วยงานหรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

“ผู้ดูแลระบบ (System Administrator)” หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

/“หน่วยงานภายนอก”...

“หน่วยงานภายนอก” หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

(๑) พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

(๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

(๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

“สินทรัพย์” หมายความว่า ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“จดหมายอิเล็กทรอนิกส์ (E-mail)” หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

“รหัสผ่าน (Password)” หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“บัญชีผู้ใช้บริการ (Account)” หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

“โปรแกรมประสงค์ร้าย (Malware)” หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่ง และ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

“ชื่อเครื่องคอมพิวเตอร์ (Computer Name)” หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

/“สื่อบันทึกพกพา” ...

“สื่อบันทึกพกพา” หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ CD, DVD, Flash Drive หรือ Handy Drive หรือ Thumb Drive, External Hard disk เป็นต้น

“การตั้งค่าระบบ (Configuration)” หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรม หรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

“เลขที่อยู่ไอพี (IP Address)” หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.) ปัจจุบันใช้ IPv๖

“เลขที่อยู่ไอพีสาธารณะ (Public IP Address)” หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

“แบนด์วิดท์ (Bandwidth)” หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

“ชื่อผู้ใช้ (Username)” หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

“ลงบันทึกเข้า (Login)” หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

“ลงบันทึกออก (Logout)” หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

“อัพเดท (Update)” หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

“ช่องโหว่ (Vulnerability)” หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรมทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

“ไฟล์ที่สามารถประมวลผลได้ (Executable file)” หมายความว่า ไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ในขณะที่ไฟล์ข้อมูลอื่น ๆ จะเป็นไฟล์ข้อมูลประกอบ

“การเข้ารหัส (Encryption)” หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

/“อุปกรณ์กระจาย ...

“อุปกรณ์กระจายสัญญาณ (Access Point)” หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

“SSID (Service Set Identifier)” หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

“โดยปริยาย (Default)” หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้าและนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ

“WEP (Wired Equivalent Privacy)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

“WPA (Wi-Fi Protected Access)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

“Wireless LAN Client” หมายความว่า เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE ๘๐๒.๑๑

“MAC Address (Media Access Control Address)” หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

“ไฟร์วอลล์ (Firewall)” หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

“VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

“Web Server” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่าง ๆ

“ชื่อโดเมนย่อย (Sub Domain Name)” หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตนหรืออาจจะใช้ "ที่อยู่เว็บไซต์" แทนก็ได้

/“อุปกรณ์จัดเส้นทาง ...

“อุปกรณ์จัดเส้นทาง (Router)” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“อุปกรณ์กระจายสัญญาณข้อมูล (Switch)” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

“การพิสูจน์ยืนยันตัวตน (Authentication)” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

“แผนผังระบบเครือข่าย (Network Diagram)” หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

“Command Line” หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

“Firewall Log” หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

“ข้อมูลจราจรทางคอมพิวเตอร์ (Log)” หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“Visualization” หมายความว่า เป็นการจำลองเครื่องเสมือนด้วยซอฟต์แวร์ที่ทำให้คอมพิวเตอร์หนึ่งเครื่องสามารถทำงานเป็นเครื่องเสมือนหลาย ๆ ระบบได้ โดยแต่ละระบบมีทรัพยากรหน่วยความจำ, ฮาร์ดดิสก์ และอุปกรณ์เน็ตเวิร์คเสมือนที่เป็นอิสระต่อกัน เครื่องเสมือนแต่ละเครื่องจึงสามารถมีระบบปฏิบัติการและ ซอฟต์แวร์เป็นของตนเองโดยอิสระ

“VMware” หมายความว่า เป็นชื่อผลิตภัณฑ์ที่มีความสามารถในการทำ Visualization

/ส่วนที่ ๑ ...

ส่วนที่ ๑
แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์
ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘

ส่วนที่ ๑

แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ เป็นไปได้อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยงโดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสมด้วย

สำนักงานเศรษฐกิจการคลัง (สศค.) โดยศูนย์เทคโนโลยสารสนเทศ (ศทส.) จึงได้จัดทำแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ (แผนบริหารความเสี่ยงฯ) ขึ้น เพื่อใช้เป็นแนวทางในการปฏิบัติงาน เพื่อลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานของ สศค.

๑.๑ วัตถุประสงค์

๑) เพื่อให้ฝ่ายบริหาร/ฝ่ายปฏิบัติการ เข้าใจหลักการและกระบวนการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์

๒) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล และระบบเครือข่ายของ สศค.

๓) เพื่อให้ผู้ปฏิบัติได้รับทราบและใช้เป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับความเสี่ยงภายในองค์กร

๔) เพื่อให้มีการปฏิบัติตามกระบวนของแผนบริหารความเสี่ยงฯ อย่างเป็นระบบและต่อเนื่อง

๕) เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ความสัมพันธ์ ตลอดจนเชื่อมโยงระหว่างแผนบริหารความเสี่ยงฯ กับกลยุทธ์ขององค์กร

๖) เพื่อใช้เป็นเครื่องมือในการสร้างวัฒนธรรมการบริหารความเสี่ยงในทุก ๆ ระดับของ สศค.

/๑.๒ นโยบาย ...

๑.๒ นโยบายการบริหารความเสี่ยง

เพื่อสร้างความตระหนักถึงความสำคัญและกระตุ้นให้บุคลากรของ สศค. เห็นถึงความจำเป็นในการระมัดระวังต่อสถานการณ์ที่คุกคามต่อประสิทธิภาพการปฏิบัติงาน การบริหารงาน และอาจทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล และระบบเครือข่าย ซึ่งเป็นเครื่องมือที่สำคัญที่สุดในการปฏิบัติงานและการตัดสินใจของผู้บริหาร สศค.

แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ของ สศค. จะทำให้เจ้าหน้าที่ทุกคนที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ ซึ่งจะถือเป็นส่วนหนึ่งของการดำเนินงาน การปฏิบัติงานเพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายต่าง ๆ ที่อาจเกิดขึ้นต่อระบบปฏิบัติงานของ สศค.

๑.๓ ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๑.๓.๑ ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้ สศค. ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล และระบบเครือข่ายที่ สศค. ใช้ในการบริหารงานและปฏิบัติงาน

๑.๓.๒ การควบคุม (Control) หมายถึง ขั้นตอนการปฏิบัติ กระบวนการดำเนินงานหรือกลไกการปฏิบัติงาน ซึ่ง สศค. กำหนดขึ้นเพื่อให้มั่นใจว่าการบริหารงานจะสามารถบรรลุวัตถุประสงค์ที่ได้กำหนดไว้

๑.๓.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ และติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หน่วยงาน หรือกระบวนการดำเนินงานของ สศค. รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้

๑.๓.๔ การบริหารความเสี่ยงองค์กรโดยรวม (Organization Wide Risk Management) หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการปฏิบัติงานต่าง ๆ โดยต้องลดมูลเหตุของแต่ละโอกาสที่จะทำให้ สศค. เสียหาย

๑.๓.๕ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ระบบเครื่องคอมพิวเตอร์ (Hardware) ระบบเครือข่าย (Network System) ระบบฐานข้อมูล (Database System) และอุปกรณ์ประกอบระบบต่าง ๆ รวมทั้งอาคารสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด ดังนี้

(๑) ทะเบียนครุภัณฑ์คอมพิวเตอร์ สศค.

(๒) ระบบเครือข่าย (Networking) ที่ สศค. ใช้ในการปฏิบัติหน้าที่ เช่น Core Switch , Access Switch เป็นต้น

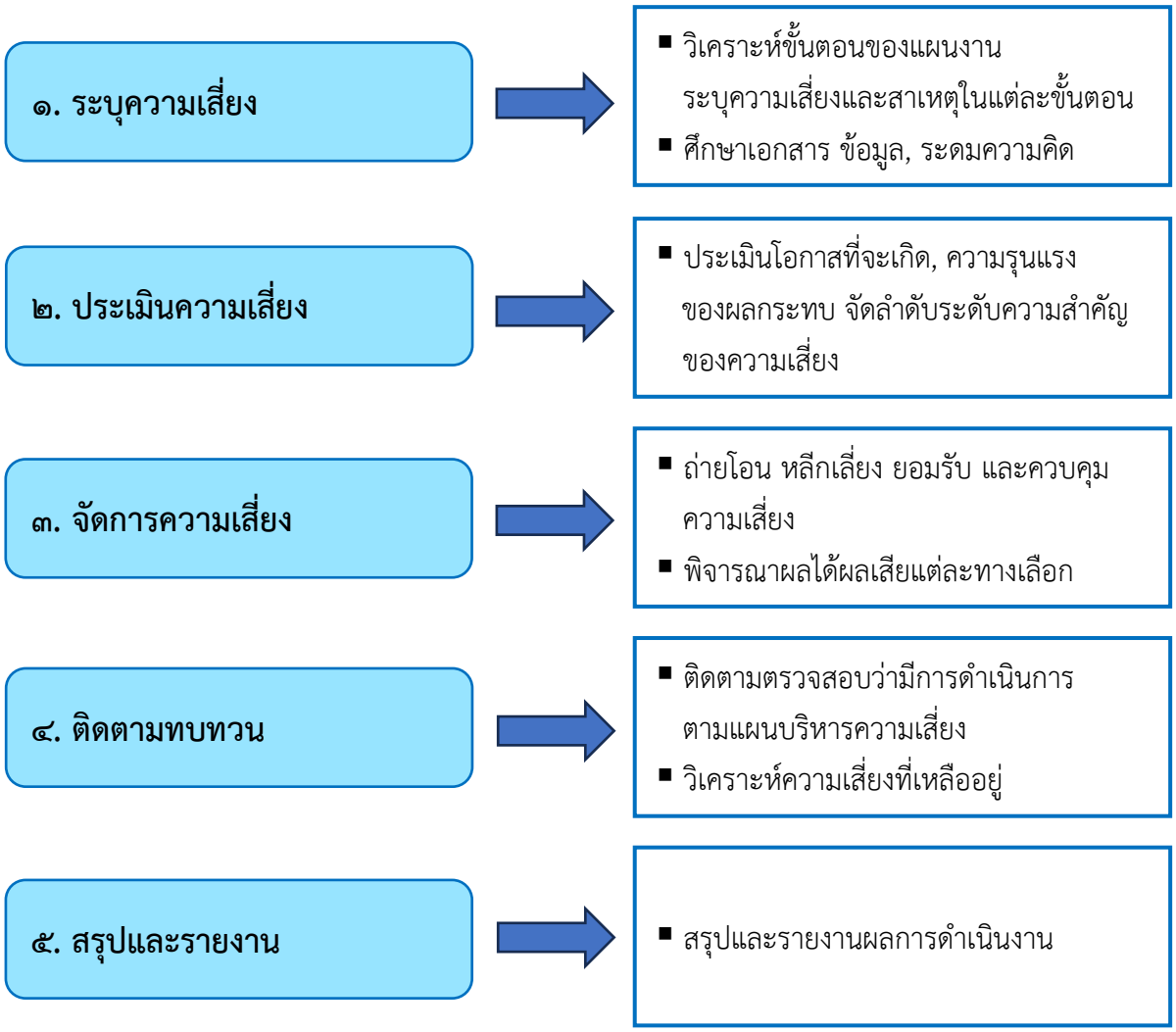
(๓) ระบบฐานข้อมูล (Database System) ฐานข้อมูลที่ สศค.ใช้ในการปฏิบัติหน้าที่ซึ่งประกอบด้วย

/- ระบบอินทราเน็ต ...

- ระบบอินทราเน็ต
- ระบบสารบรรณอิเล็กทรอนิกส์
- ระบบจดหมายอิเล็กทรอนิกส์ (FPO Mail)
- ระบบโครงสร้างผู้ปฏิบัติงาน สศค.
- ระบบลา-ลงเวลา
- ระบบฐานข้อมูลกลางด้านเศรษฐกิจ (ระบบ DOC)
- ระบบข้อมูลสารสนเทศสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (FI&SFI)
- ระบบข้อมูลสารสนเทศการเงินภาคประชาชน (PFI)
- ระบบงานพิโกไฟแนนซ์ (PICO)

๑.๓.๖ บุคลากร (People) ได้แก่ บุคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงานสำหรับการดูแลและจัดทำระบบ

๑.๔ ขั้นตอน/กระบวนการบริหารความเสี่ยง



/๑.๔.๑ การกำหนด ...

๑.๔.๑ <u>การกำหนดวัตถุประสงค์</u>

(๑) เพื่อกำหนดความเสี่ยงที่มีโอกาสเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สศค.

(๒) กำหนดกิจกรรมป้องกันรองรับความเสี่ยงที่มีโอกาสเกิดขึ้นเพื่อป้องกันความเสียหายและลดความรุนแรงของความเสียหายที่เกิดขึ้นให้อยู่ในระดับที่น้อยที่สุด

๑.๔.๒ <u>การวิเคราะห์ความเสี่ยง</u>

จากการวิเคราะห์ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สศค. สามารถแยกประเภทความเสี่ยงออกเป็น ๕ ประเภท ดังนี้

(๑) ***ความเสี่ยงด้านการบริหารจัดการ*** เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

(๒) ***ความเสี่ยงจากการปฏิบัติงาน*** เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการจัดการความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งาน โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศหรือใช้ข้อมูลต่าง ๆ ของ สศค. เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อฐานข้อมูลได้

(๓) ***ความเสี่ยงด้านเทคนิค*** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ ระบบเครือข่าย เครื่องมือ และอุปกรณ์ อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี การถูกก่อกวนจาก Hacker การถูกเจาะทำลายระบบจาก Cracker เป็นต้น

(๔) ***ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน*** เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับระบบเทคโนโลยีสารสนเทศและฐานข้อมูล เช่น ไฟฟ้าขัดข้อง น้ำท่วม แผ่นดินไหว อาคารถล่ม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

(๕) ***ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์*** เป็นความเสี่ยงที่เกิดจากเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่มีอายุการใช้งานมานาน และยังไม่มีการจัดซื้อทดแทนของเดิมอาจทำให้เกิดความเสียหายต่อการทำงานได้ เช่น Hard Disk เสีย จะทำให้ข้อมูลสูญหายได้ เป็นต้น

/๑.๔.๓ <u>การระบุความเสี่ยง</u> ...

๑.๔.๓ <u>การระบุความเสี่ยง</u>

จากการวิเคราะห์ประเภทความเสี่ยงทั้ง ๕ ด้าน ซึ่งประกอบด้วย *(๑) ความเสี่ยงด้านการบริหารจัดการ (๒) ความเสี่ยงจากการปฏิบัติงาน (๓) ความเสี่ยงด้านเทคนิค (๔) ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน และ (๕) ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์* และในการระบุความเสี่ยง สามารถจำแนกข้อมูลเกี่ยวกับชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัย/สิ่งคุกคาม และผลกระทบ/ผู้ได้รับผลกระทบ รวมถึงแนวทางการแก้ไขปัญหา โดยมีรายละเอียดต่าง ๆ ตามตารางด้านล่างดังนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
๑. ความเสี่ยงด้านระบบฐานข้อมูลของ สศค.	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ ไม่ว่าจะเป็นฐานข้อมูลหลักเสียหาย ข้อมูลถูกทำลาย การโจรกรรมข้อมูลที่สำคัญ การลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	- ความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - นำระบบ VMware เข้ามาใช้งาน - เข้มงวดการกำหนดรหัสผ่าน
๒. ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	- การทำงานผิดพลาดของโปรแกรม - ช่องโหว่ของโปรแกรมเกิดจากไม่มีการอัพเดตระบบอย่างสม่ำเสมอ - โปรแกรมประยุกต์ติดต่อฐานข้อมูลไม่ได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ทดสอบช่องโหว่ของโปรแกรมประยุกต์ก่อนใช้งานระบบสารสนเทศ - อบรมผู้ใช้งานระบบสารสนเทศ - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
			- การใช้โปรแกรมไม่ถูกลิขสิทธิ์ อาจเกิดการติดไวรัส มัลแวร์ หรือเกิดช่องโหว่ที่นำไปสู่ความไม่ปลอดภัยทางไซเบอร์		- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - ตรวจสอบการทำงานของโปรแกรมอย่างละเอียด - ใช้ซอฟต์แวร์ถูกลิขสิทธิ์ - ไม่อนุญาตให้ผู้ใช้งานติดตั้งซอฟต์แวร์ด้วยตนเอง
๓. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่ Web Server, Mail Server, Database Server	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	- การตั้งค่าอุปกรณ์ผิดพลาด - การทำงานผิดพลาดของอุปกรณ์ - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดต - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - สาย LAN ชำรุดเสียหาย - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- ปรับปรุงระบบเครื่องคอมพิวเตอร์แม่ข่าย - จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างสม่ำเสมอ

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
					- ถ่ายโอนระบบงาน สศค. ไปสู่ DR Site หรือ ระบบ Cloud
๔. ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์, การทำงานของอุปกรณ์เครือข่ายหลัก มีการทำงานผิดพลาด	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศใช้งาน Internet ไม่ได้	- ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ - ใช้โปรแกรมในการ scan ช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่าย - จัดซื้ออุปกรณ์ทดแทนเพื่อให้สามารถใช้ปฏิบัติงานได้ตามปกติ
๕. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์สำนักงาน (PC) เกิดชำรุดเสียหายหรือเกิดขัดข้องทำให้ไม่สามารถทำงานได้ตามปกติ	- Hard disk ชำรุดเสียหาย เช่น Main board, Memory, Power Supply ชำรุดเสียหาย - Software ล้าสมัย - ความเสี่ยงจากภัยคุกคามต่าง ๆ เช่น ผู้ใช้งานไม่มีความรู้ในการใช้งานที่ถูกต้อง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนเพื่อสามารถปฏิบัติงานได้อย่างต่อเนื่อง - บำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - จัดทำคู่มือการใช้งานและจัดอบรมผู้ใช้งาน - ลงระบบปฏิบัติการ (OS) ให้พร้อมใช้งาน

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
๖. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถใช้งานได้ - มัลแวร์ทำให้เกิดช่องโหว่ให้ผู้ไม่หวังดี เข้ามาควบคุมคอมพิวเตอร์ หรือโจรกรรมข้อมูล - Ransomeware ทำให้เครื่องคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้ และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive , Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งานตระหนักถึงภัยคุกคามคอมพิวเตอร์
๗. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services: DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้ายหรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ ไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS , Load Balancer	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- ตรวจสอบการตั้งค่าของ Firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
		- File ที่ผู้ใช้บริการ Download มา มีการฝังไวรัสคอมพิวเตอร์ หรือคำสั่งอันตรายอันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	- ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข		- เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Load Balancer
๘. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์จากบุคคลภายใน - การลักทรัพย์จากบุคคลภายนอกที่เข้ามาโดยได้รับอนุญาตและไม่ได้รับอนุญาต - ระบบรักษาความปลอดภัยไม่รัดกุม เช่น กล้องวงจรปิดไม่เพียงพอ, เจ้าหน้าที่รักษาความปลอดภัยไม่รัดกุม	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย	- สร้างความตระหนักรู้ในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งกล้องวงจรปิดเพิ่มในจุดที่อาจจะมีความเสี่ยง - กวดขันเจ้าหน้าที่รักษาความปลอดภัยให้รัดกุมมากขึ้น
๙. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา และควบคุมดูแลระบบ	- ไม่มีขั้นตอนการปฏิบัติงานที่ชัดเจนเพื่อให้บุคคลอื่นสามารถทำงานทดแทนได้ - การโยกย้ายของบุคลากรด้านคอมพิวเตอร์ - การพัฒนาอย่างรวดเร็วของเทคโนโลยี	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- สรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสมและเพียงพอ - จัดทำคู่มือเพิ่มเติมกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้และจัดบุคลากรผู้รับผิดชอบหลักและผู้รับผิดชอบรองในกรณีที่ผู้รับผิดชอบหลักไม่สามารถมาปฏิบัติงานได้

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
๑๐. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	- การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ - ไม่สามารถปรับปรุงระบบสารสนเทศให้มีประสิทธิภาพดีขึ้นได้	- งบประมาณที่ได้ของ สศค. มีจำกัด	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- ถ่ายทอดองค์ความรู้ที่สำคัญของระบบงานให้กับเจ้าหน้าที่ใหม่หรือเจ้าหน้าที่ที่รับช่วงงานต่ออย่างน้อย ๑ เดือนเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง - มีแผนการจัดซื้อระบบคอมพิวเตอร์เครือข่าย อุปกรณ์และ Software - ขอรับการจัดสรรงบประมาณในกรณีฉุกเฉิน
๑๑. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่ - ไฟฟ้าดับ - ไม่มีอุปกรณ์สำรองไฟฟ้าที่เพียงพอ - ไม่มีเครื่องกำเนิดไฟฟ้าเมื่อไฟฟ้าดับเกินระยะเวลาที่กำหนด - เกิดอุบัติเหตุกับสายส่งไฟฟ้า	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดหาเครื่องสำรองไฟฟ้าเพิ่มเติม เช่น เครื่องปั่นไฟฟ้า เครื่องกำเนิดไฟฟ้าสำรอง - บำรุงรักษาเครื่องสำรองไฟฟ้าเมื่อครบกำหนดตามระยะเวลาอย่างสม่ำเสมอ

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
๑๒. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การชุมนุมประท้วง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติต่าง ๆ เช่น แผ่นดินไหว น้ำท่วม - การปิดล้อมสถานที่ราชการกรณีเกิดการชุมนุมประท้วงทางการเมือง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- แผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ - มีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ - จัดทำระบบสำรองข้อมูล เช่น สำรองระบบข้อมูลบน Cloud - จัดทำ DR Site โดยให้อยู่สถานที่อื่น และสามารถใช้ทดแทนได้ ในกรณีที่ Data Center หลักไม่สามารถใช้งานได้
๑๓. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูล ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
๑๔. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- ปรับปรุงระบบเครื่องคอมพิวเตอร์แม่ข่าย - จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างสม่ำเสมอ - ถ่ายโอนระบบงาน สศค. ไปสู่ระบบ Cloud

/๑.๔.๔ <u>การประมาณค่า</u> ...

๑.๔.๔ <u>การประมาณค่าความเสี่ยง</u> (Risk Estimation)

การประมาณค่าความเสี่ยงเป็นการพิจารณาปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ ระดับความรุนแรงของผลกระทบของความเสี่ยง และระดับความเสี่ยง ซึ่ง สศค. ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	๑๖ ครั้งขึ้นไป/ปี
๔	สูง	๑๑ - ๑๕ ครั้ง/ปี
๓	ปานกลาง	๖ - ๑๐ ครั้ง/ ปี
๒	น้อย	๒ - ๕ ครั้ง/ปี
๑	น้อยมาก	๑ ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
๔	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	เกิดเหตุร้ายแรงหรือระบบมีปัญหา แต่มีความสูญเสียไม่มาก
๒	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

/การประมาณค่า ...

การประมาณค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ	ระดับโอกาส ที่เกิด	ความรุนแรง
๑. ความเสี่ยงด้านระบบฐานข้อมูลของ สศค.	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ ไม่ว่าจะเป็นฐานข้อมูลหลักเสียหาย ข้อมูลถูกทำลาย การโจรกรรมข้อมูลที่สำคัญ การลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	- ความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	๑	๕
๒. ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	- การทำงานผิดพลาดของโปรแกรม - ช่องโหว่ของโปรแกรมเกิดจากไม่มีการอัพเดตระบบอย่างสม่ำเสมอ - โปรแกรมประยุกต์ติดต่อฐานข้อมูลไม่ได้ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์ อาจเกิดการติดไวรัส มัลแวร์ หรือเกิดช่องโหว่ที่นำไปสู่ความไม่ปลอดภัยทางไซเบอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	๒	๓
๓. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	- การตั้งค่าอุปกรณ์ผิดพลาด - การทำงานผิดพลาดของอุปกรณ์ - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย	๑	๓

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ	ระดับโอกาส ที่เกิด	ความรุนแรง
Web Server, Mail Server, Database Server			- ระบบปฏิบัติการไม่อัพเดต - ความเสียงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่าย อินเทอร์เน็ต - สาย LAN ชำรดเสียหาย - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker	- อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ		
๔. ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์, การทำงานของอุปกรณ์เครือข่ายหลัก มีการทำงานผิดพลาด	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศใช้งาน Internet ไม่ได้	๒	๓
๕. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์สำนักงาน (PC) เกิดชำรุดเสียหายหรือเกิดขัดข้องทำให้ไม่สามารถทำงานได้ตามปกติ	- Hard disk ชำรุดเสียหาย เช่น Main board, Memory, Power Supply ชำรุดเสียหาย - Software ล้าสมัย - ความเสี่ยงจากภัยคุกคามต่าง ๆ จากผู้ใช้งาน	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย	๕	๑

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ	ระดับโอกาส ที่เกิด	ความรุนแรง
๖. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถใช้งานได้ - มัลแวร์ทำให้เกิดช่องโหว่ให้ผู้ไม่หวังดี เข้ามาควบคุมคอมพิวเตอร์ หรือโจรกรรมข้อมูล - Ransomeware ทำให้เครื่องคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้ และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	- ผู้ใช้งานไม่มีความรู้ในการใช้งานที่ถูกต้อง - การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive, Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์ มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	๑	๕
๗. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services: DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้ายหรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS , Load Balancer	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๕

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ	ระดับโอกาส ที่เกิด	ความรุนแรง
		ไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย - File ที่ผู้ใช้บริการ Download มา มีการฝังไวรัสคอมพิวเตอร์ หรือคำสั่งอันตรายอันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	- ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข			
๘. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์จากบุคคลภายใน - การลักทรัพย์จากบุคคลภายนอกที่เข้ามาโดยได้รับอนุญาตและไม่ได้รับอนุญาต - ระบบรักษาความปลอดภัยไม่รัดกุม เช่น กล้องวงจรปิดไม่เพียงพอ, เจ้าหน้าที่รักษาความปลอดภัยไม่รัดกุม	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย	๑	๕
๙. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา และควบคุมดูแลระบบ	- ไม่มีขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้บุคคลอื่นสามารถทำงานทดแทนได้ - การโยกย้ายของบุคลากรด้านคอมพิวเตอร์ - การพัฒนาอย่างรวดเร็วของเทคโนโลยี	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๕

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ	ระดับโอกาส ที่เกิด	ความรุนแรง
๑๐. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	- การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ - ไม่สามารถปรับปรุง IT ให้มีประสิทธิภาพดีขึ้นได้	- งบประมาณที่ได้ของ สศค. มีจำกัด	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๒	๓
๑๑. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่ - ไฟฟ้าดับ - ไม่มีอุปกรณ์สำรองไฟฟ้าที่เพียงพอ - ไม่มีเครื่องกำเนิดไฟฟ้าเมื่อไฟฟ้าดับเกินระยะเวลาที่กำหนด - เกิดอุบัติเหตุกับสายส่งไฟฟ้า	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล	๒	๓
๑๒. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การชุมนุมประท้วง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติต่าง ๆ เช่น แผ่นดินไหว น้ำท่วม - การปิดล้อมสถานที่ราชการ กรณีเกิดการชุมนุมประท้วงทางการเมือง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๓

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ	ระดับโอกาส ที่เกิด	ความรุนแรง
๑๓. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๕
๑๔. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๕

/๑.๔.๕ การประเมินค่า ...

๑.๔.๕ <u>การประเมินค่าความเสี่ยง</u> (Risk Evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้นรวมถึงขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

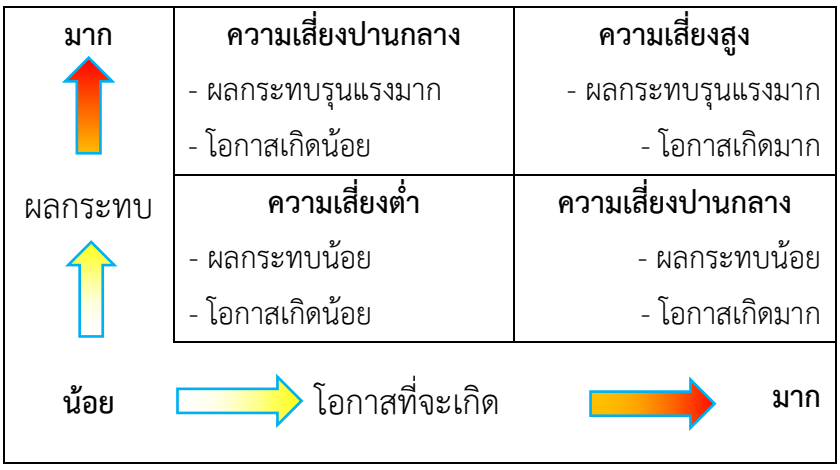
ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ

ซึ่งการจัดระดับความสำคัญของความเสี่ยง สศค. ใช้เกณฑ์ดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ – ๘	ต่ำ	ยอมรับความเสี่ยง (มีแผนรองรับ)	ขาว
๙ – ๑๖	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗ – ๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุม)	ส้ม
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

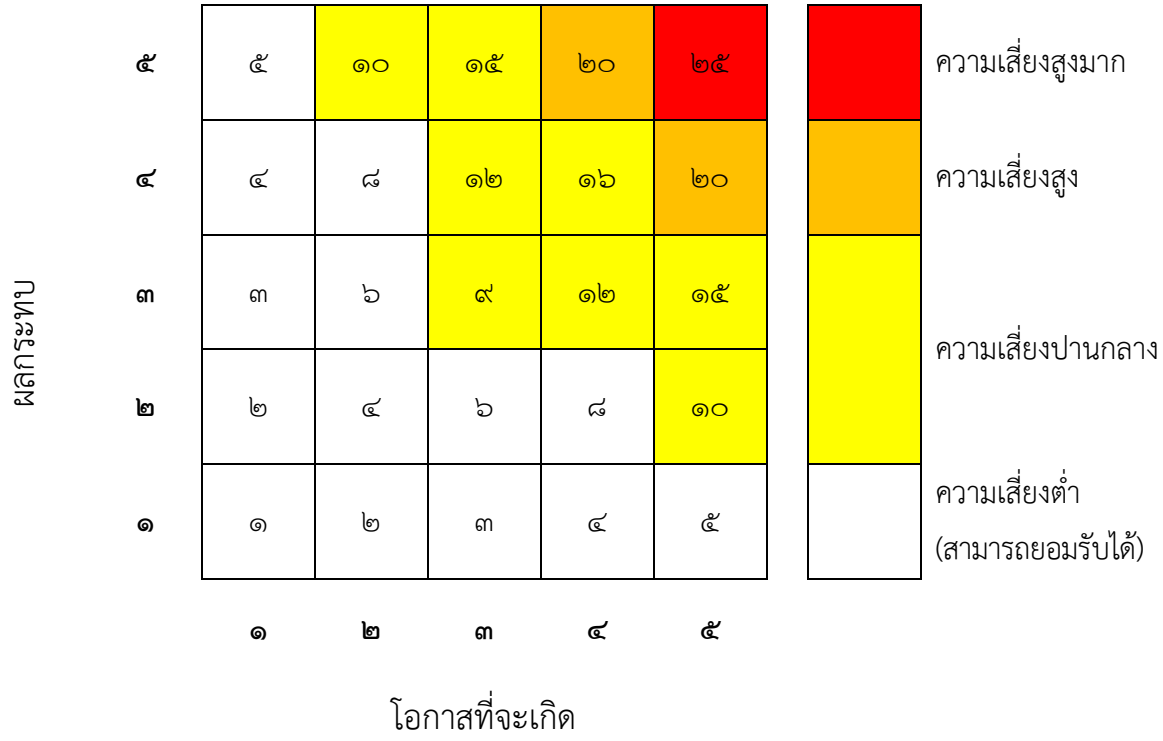
แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



/การประเมินความเสี่ยง ...

การประเมินความเสี่ยง



การประเมินค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงด้านระบบฐานข้อมูลของ สศค.	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ ไม่ว่าจะเป็นฐานข้อมูลหลักเสียหาย ข้อมูลถูกทำลาย การโจรกรรมข้อมูลที่สำคัญ การลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	๑	๕	๕
๒. ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	๒	๓	๖

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๓. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่ Web Server, Mail Server, Database Server	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	๑	๓	๓
๔. ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์การทำงานของอุปกรณ์เครือข่ายหลักมีการทำงานผิดพลาด	๒	๓	๖
๕. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์สำนักงาน (PC) เกิดชำรุดเสียหายหรือเกิดขัดข้องทำให้ไม่สามารถทำงานได้ตามปกติ	๕	๑	๕
๖. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถใช้งานได้ - มัลแวร์ทำให้เกิดช่องโหว่ให้ผู้ไม่หวังดีเข้ามาควบคุมคอมพิวเตอร์ หรือโจรกรรมข้อมูล - Ransomeware ทำให้เครื่องคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้ และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	๑	๕	๕
๗. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดีหรือ Hacker	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services: DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้ายหรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย	๑	๕	๕

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
		- ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ ไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย - File ที่ผู้ใช้บริการ Download มา มีการฝังไวรัสคอมพิวเตอร์ หรือคำสั่งอันตรายอันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี			
๘. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๑	๕	๕
๙. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา และควบคุมดูแลระบบ	๑	๕	๕
๑๐. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	- การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ - ไม่สามารถปรับปรุง IT ให้มีประสิทธิภาพดีขึ้นได้	๒	๓	๖
๑๑. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	๒	๓	๖
๑๒. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การชุมนุม ประท้วง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหว จนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และ อุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๑	๓	๓

/ชื่อความเสี่ยง ...

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑๓. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	๑	๕	๕
๑๔. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	๑	๕	๕

/๑.๔.๖ การรายงานผล ...

๑.๔.๖ <u>การรายงานผลการวิเคราะห์ความเสี่ยง</u> (Risk Reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศจากมากไปน้อยได้ดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	- การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ - ไม่สามารถปรับปรุง IT ให้มีประสิทธิภาพดีขึ้นได้	๖
๒	ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	๖
๓	ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์, การทำงานของอุปกรณ์เครือข่ายหลัก มีการทำงานผิดพลาด	๖
๔	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	๖
๕	ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถใช้งานได้ - มัลแวร์ทำให้เกิดช่องโหว่ให้ผู้ไม่หวังดีเข้ามาควบคุมคอมพิวเตอร์หรือโจรกรรมข้อมูล - Ransomeware ทำให้เครื่อคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้ และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	๕
๖	ความเสี่ยงด้านระบบฐานข้อมูลของ สศค.	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ ไม่ว่าจะเป็นฐานข้อมูลหลักเสียหาย ข้อมูลถูกทำลาย การโจรกรรมข้อมูลที่สำคัญการลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	๕
๗	ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์สำนักงาน (PC) เกิดชำรุดเสียหายหรือเกิดขัดข้องทำให้ไม่สามารถทำงานได้ตามปกติ	๕

/ลำดับ ...

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๘	ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	๕
๙	ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	๕
๑๐	ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดีหรือ Hacker	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services: DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้ายหรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ ไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย - File ที่ผู้ใช้บริการ Download มามีการฝังไวรัสคอมพิวเตอร์หรือคำสั่งอันตราย อันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	๕
๑๑	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ /ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๕
๑๒	ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๕
๑๓	ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่ Web Server, Mail Server, Database Server	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	๓

/ลำดับ ...

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑๔	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การชุมนุม ประท้วง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๓

/๑.๔.๗ การจัดความเสี่ยง ...

๑.๔.๗ <u>การจัดการความเสี่ยง</u>

จากผลการวิเคราะห์ความเสี่ยงจำนวน ๑๔ ความเสี่ยงข้างต้น ได้รับการพิจารณาว่าเป็นความเสี่ยงที่มีระดับความเสี่ยงเป็นที่ยอมรับได้ (ค่าระดับความเสี่ยงอยู่ที่ ≤ ๑๕) โดยกำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการบริหารจัดการความเสี่ยง คือ ความเสี่ยงที่มีค่าระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีค่าระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำ แต่อาจนำมาพิจารณาดำเนินการบริหารจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ ทั้งนี้ได้กำหนดแนวทางการดำเนินการบริหารจัดการความเสี่ยงที่มีระดับความเสี่ยงที่ยอมรับได้ ≤ ๑๕ ต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการบริหารจัดการความเสี่ยง
๑	ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	**๖**	- มีแผนรองรับความเสี่ยง	- จัดทำแผนรองรับความต้องการใช้งานล่วงหน้าให้ทันท่วงที - นำเสนอแผนเพื่อเสนอผู้บริหารพิจารณา
๒	ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	**๖**	- มีแผนรองรับความเสี่ยง	- จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - ตรวจสอบการทำงานของโปรแกรมอย่างละเอียด - ให้ผู้ดูแลระบบตรวจสอบโดยเร่งด่วน
๓	ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	**๖**	- มีแผนรองรับความเสี่ยง	- บำรุงรักษาระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ - มีแผนจัดซื้ออุปกรณ์ทดแทนอุปกรณ์ที่หมดสภาพเพื่อให้สามารถใช้งานได้ตามปกติ
๔	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	**๖**	- มีแผนรองรับความเสี่ยง	- มีแผนจัดหาเครื่องกำเนิดไฟฟ้า - จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - แผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ
๕	ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	**๕**	- มีแผนรองรับความเสี่ยง	- ติดตั้งระบบป้องกันไวรัส และมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ

/ลำดับ ...

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการบริหารจัดการความเสี่ยง
๖	ความเสี่ยงด้านระบบฐานข้อมูลของ สศค.	๕	- มีแผนรองรับความเสี่ยง	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - จัดเก็บข้อมูลไว้บนระบบ Cloud
๗	ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	๕	- มีแผนรองรับความเสี่ยง	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนเพื่อสามารถปฏิบัติงานได้อย่างต่อเนื่อง - บำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ ตลอดจนจัดอบรมผู้ใช้งาน จัดทำคู่มือการใช้งานระบบปฏิบัติการ (OS)
๘	ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	๕	- มีแผนรองรับความเสี่ยง	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่อง ระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ
๙	ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	๕	- มีแผนรองรับความเสี่ยง	- ปรับปรุงระบบเครื่องคอมพิวเตอร์แม่ข่าย - จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่อง คอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างสม่ำเสมอ - ถ่ายโอนระบบงาน สศค. ไปสู่ระบบ Cloud
๑๐	ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดีหรือ Hacker	๕	- มีแผนรองรับความเสี่ยง	- นำระบบงานที่สำคัญเข้าสู่ระบบ VM เพื่อเพิ่มประสิทธิภาพในการ Backup และ Restore หากเกิดเหตุการณ์บุกรุกโดยผู้ไม่ประสงค์ดี - ตรวจสอบและปรับปรุงการตั้งค่าของ firewall อย่างสม่ำเสมอ - ปรับปรุงระบบตรวจสอบการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

/ลำดับ ...

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการบริหารจัดการความเสี่ยง
๑๑	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๕	- มีแผนรองรับความเสี่ยง	- มีการจัดเวรยามรักษาความปลอดภัยในอาคารสำนักงาน - ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจสอบการทำงานของกล้องวงจรปิดภายในอาคาร - ตรวจสอบระบบป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพใช้งานได้ปกติ - สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง
๑๒	ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๕	- มีแผนรองรับความเสี่ยง	- สรรหาบุคลากรทดแทนตำแหน่งว่าง - จัดทำคู่มือเพิ่มเติมกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ - ถ่ายทอดองค์ความรู้ที่สำคัญของระบบงานให้กับเจ้าหน้าที่ใหม่หรือเจ้าหน้าที่รับช่วงงานต่ออย่างน้อย ๑ เดือน
๑๓	ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่ Web Server, Mail Server, Database Server	๓	- มีแผนรองรับความเสี่ยง	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนเพื่อสามารถปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ
๑๔	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การชุมนุม ประท้วง	๓	- มีแผนรองรับความเสี่ยง	- มีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ - สำรองข้อมูลระบบสารสนเทศ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด

๑.๕ เจ้าหน้าที่ผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยง

เพื่อให้การดำเนินงานตามแผนบริหารความเสี่ยงฯ เป็นไปอย่างรวดเร็วทันต่อการดำเนินการ จึงกำหนดให้บุคลากรของ สศค. เป็นผู้รับผิดชอบดำเนินการบริหารจัดการความเสี่ยงที่เกิดขึ้น ดังนี้

๑.๕.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศกำกับดูแลควบคุมการดำเนินการ

๑.๕.๒ ศูนย์เทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการ

/ส่วนที่ ๒ ...

ส่วนที่ ๒
แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบสารสนเทศ

ส่วนที่ ๒
แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบสารสนเทศ

ในส่วนที่ ๒ ของแผนบริหารความเสี่ยงฯ ประกอบด้วย แผนการเตรียมการและการป้องกันความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล และระบบเครือข่าย รวมถึงแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น ดังนี้

๒.๑ แผนการเตรียมการและการป้องกันความเสี่ยง

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ฐานข้อมูลและระบบเครือข่าย ได้กำหนดแผนปฏิบัติการในการจัดการความเสี่ยงในแต่ละเรื่อง โดยกำหนดระยะเวลาการดำเนินการและระบุหน่วยงานผู้รับผิดชอบ ดังนี้

ความเสี่ยง	แผนปฏิบัติการ	ระยะเวลาการดำเนินการ	ผู้รับผิดชอบ
๑. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	- จัดทำแผนรองรับความต้องการใช้งานล่วงหน้าให้ทันท่วงที	ภายในไตรมาสที่ ๑ ก่อนที่จะเริ่มปีงบประมาณใหม่	ศทส.
	- นำเสนอแผนให้ผู้บริหารพิจารณา		
	- ประเมินและจัดลำดับโครงการที่จำเป็นที่สุดในการแก้ไขความเสี่ยง		
๒. ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	- จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ	ภายในไตรมาสที่ ๑ ก่อนที่จะเริ่มปีงบประมาณใหม่	ศทส.
	- ตรวจสอบการทำงานของโปรแกรมอย่างละเอียด	ทุก ๆ ๓ เดือน	
	- ให้ผู้ดูแลระบบตรวจสอบโดยเร่งด่วน		

/ความเสี่ยง ...

ความเสี่ยง	แผนปฏิบัติการ	ระยะเวลาการดำเนินการ	ผู้รับผิดชอบ
๓. ความเสี่ยงด้านระบบ เครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	- บำรุงรักษาระบบตรวจสอบการใช้งาน เครือข่าย	ทุก ๆ ๓ เดือน	ศทส.
	- ตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ	ภายในไตรมาสที่ ๑ ก่อนที่จะเริ่มปีงบประมาณใหม่	
	- มีแผนจัดซื้ออุปกรณ์ทดแทนอุปกรณ์ที่หมดสภาพเพื่อให้สามารถใช้งานได้ตามปกติ		
๔. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- มีแผนการบำรุงรักษาเครื่องกำเนิดไฟฟ้าอย่างต่อเนื่อง	ภายในไตรมาสที่ ๑ ก่อนที่จะเริ่มปีงบประมาณใหม่	ศทส.
	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่	ในกรณีเกิดเหตุฉุกเฉินเครื่องสำรองไฟฟ้าขัดข้อง	
๕. ความเสี่ยงจากไวรัส คอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	- ติดตั้งระบบป้องกันไวรัส และมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน	ทุก ๆ ๑ เดือน	ศทส.
	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ	ทุกครั้งที่ระบบมีการแจ้งเตือนการอัพเดท	
	- ต้องอัพเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ		
๖. ความเสี่ยงด้านระบบฐานข้อมูลของ สศค.	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	ทุก ๆ ๑ เดือน	ศทส.
	- จัดเก็บข้อมูลไว้บนระบบ Cloud		
	- จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ	ภายในไตรมาสที่ ๑ ก่อนที่จะเริ่มปีงบประมาณใหม่	
๗. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน เพื่อสามารถปฏิบัติงานได้อย่างต่อเนื่อง	ในทันทีที่เกิดเหตุฉุกเฉินเครื่องเครื่องคอมพิวเตอร์ (PC) หรือ อุปกรณ์ขัดข้องไม่สามารถทำงานได้	ศทส.
	- บำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ ตลอดจนจัดอบรมผู้ใช้งาน จัดทำคู่มือการใช้งานระบบปฏิบัติการ (OS)	ทุก ๆ ๓ เดือน	

/ความเสี่ยง ...

ความเสี่ยง	แผนปฏิบัติการ	ระยะเวลาการดำเนินการ	ผู้รับผิดชอบ
๘. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	- ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย	ในทันทีที่มีการสร้างเครื่องคอมพิวเตอร์เสมือน	ศทส.
	- ตรวจสอบและบำรุงรักษาเครื่องและระบบสำรองข้อมูลอย่างสม่ำเสมอ	ทุก ๆ ๑ เดือน	
	- จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ		
๙. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	- ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย	ในทันที	ศทส.
	- ปรับปรุงระบบเครื่องคอมพิวเตอร์แม่ข่าย	ทุก ๆ ๓ เดือน	
	- ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างสม่ำเสมอ		
	- ถ่ายโอนระบบงาน สศค. ไปสู่ระบบ Cloud	ทุก ๆ ๑ เดือน	
๑๐. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดีหรือ Hacker	- ตรวจสอบและปรับปรุงการตั้งค่าของ Firewall อย่างสม่ำเสมอ	ทุก ๆ ๓ เดือน	ศทส.
	- ปรับปรุงระบบตรวจสอบการบุกรุกเครือข่ายอย่างสม่ำเสมอ		
	- ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ		
	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ		
	- เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ		
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	- มีการจัดเวรยามรักษาความปลอดภัยภายในอาคารสำนักงาน	ทุกวัน	สำนักงานเลขานุการกรม (สลข.), ศทส.
	- ตรวจสอบการเข้าออกของบุคคลภายนอก		

/ความเสี่ยง ...

ความเสี่ยง	แผนปฏิบัติการ	ระยะเวลาการดำเนินการ	ผู้รับผิดชอบ
	- ตรวจสอบการทำงานของกล้องวงจรปิดภายในอาคาร		
	- ตรวจสอบระบบป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพใช้งานได้ปกติ - สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง		
๑๒. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	- สรรหาบุคลากรทดแทนตำแหน่งว่าง	ภายในไตรมาสที่ ๑ ก่อนที่จะเริ่มปีงบประมาณใหม่	สลข., ศทส.
	- จัดทำคู่มือเพิ่มเติมกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถศึกษาและปฏิบัติงานได้	ทุกครั้งที่มีการติดตั้งระบบงานใหม่ก่อนที่จะได้บุคลากร	
	- ถ่ายทอดองค์ความรู้ที่สำคัญของระบบงานให้กับเจ้าหน้าที่ใหม่หรือเจ้าหน้าที่ที่รับช่วงงานต่ออย่างน้อย ๑ เดือน	ทุก ๆ ๑ เดือน	
๑๓. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่ Web Server, Mail Server, Database Server	- ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย	ในทันที	ศทส.
	- ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ	ทุก ๆ ๓ เดือน	
๑๔. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การชุมนุมประท้วง	- มีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ	ภายในไตรมาสที่ ๑ ก่อนที่จะเริ่มปีงบประมาณใหม่	ศทส.
	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	ทุก ๆ ๑ เดือน	

/๒.๒ แผนรองรับ ...

๒.๒ แผนรองรับสถานการณ์ฉุกเฉิน

จากการพิจารณากรณีการเกิดเหตุการณ์ที่ไม่คาดคิดซึ่งอาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ระบบฐานข้อมูลและระบบเครือข่ายของ สศค. แบ่งออกเป็น ๔ สถานการณ์หลัก ๆ ที่สำคัญ ดังนี้

๒.๒.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

(๑) กรณีการป้องกันไวรัสล้มเหลว

(๒) กรณีการป้องกันผู้บุกรุกล้มเหลว

(๓) กรณีการเชื่อมโยงเครือข่ายล้มเหลว

(๔) กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)

(๕) กรณีไฟฟ้าขัดข้อง

๒.๒.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ

(๑) กรณีไฟไหม้

(๒) กรณีน้ำท่วม

(๓) กรณีแผ่นดินไหว

๒.๒.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด

(๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้

(๒) กรณีหลังเหตุการณ์ความไม่สงบ

๒.๒.๔ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

(๑) กรณีโจรกรรม

(๒) กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

/สถานการณ์ ...

➢ **สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค**

(๑) กรณีการป้องกันไวรัสล้มเหลว

– กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

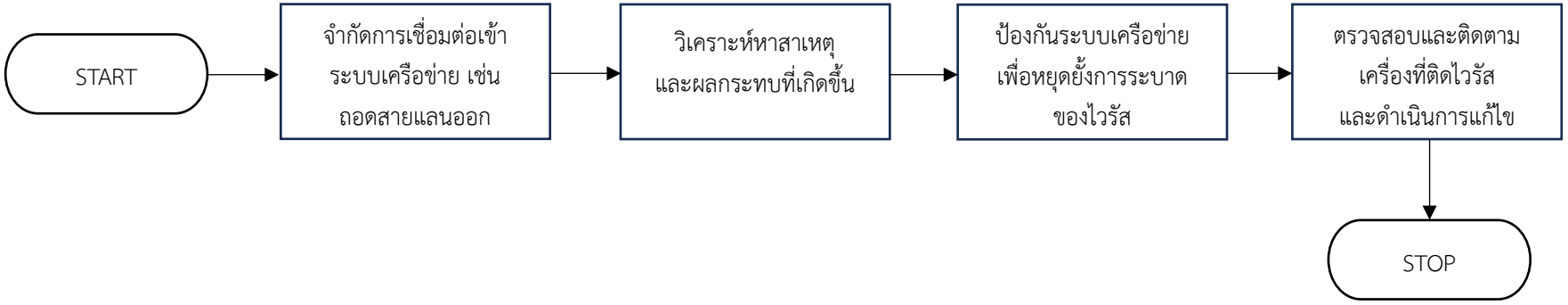
– วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

– ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

– ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

– กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุให้เจ้าหน้าที่ ศทส. ทราบ หรือกรณีมีเหตุอันทำให้ ศทส. ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศทส. จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



/(๒) กรณีการป้องกัน ...

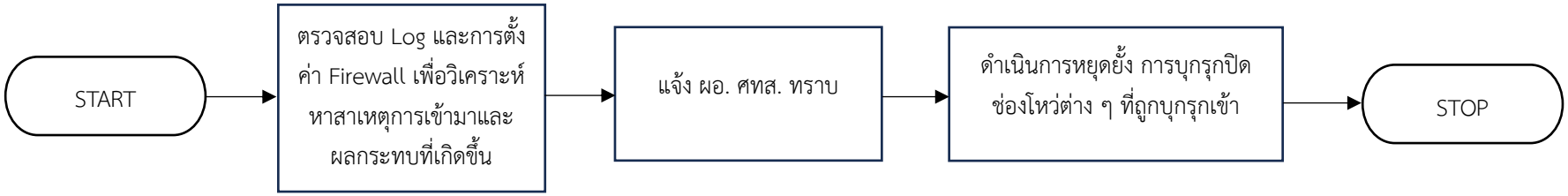
(๒) กรณีการป้องกันผู้บุกรุกล้มเหลว

– กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log file และตรวจสอบการตั้งค่าของ Firewall

– ผู้ดูแลระบบแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศให้ทราบโดยด่วน

– ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



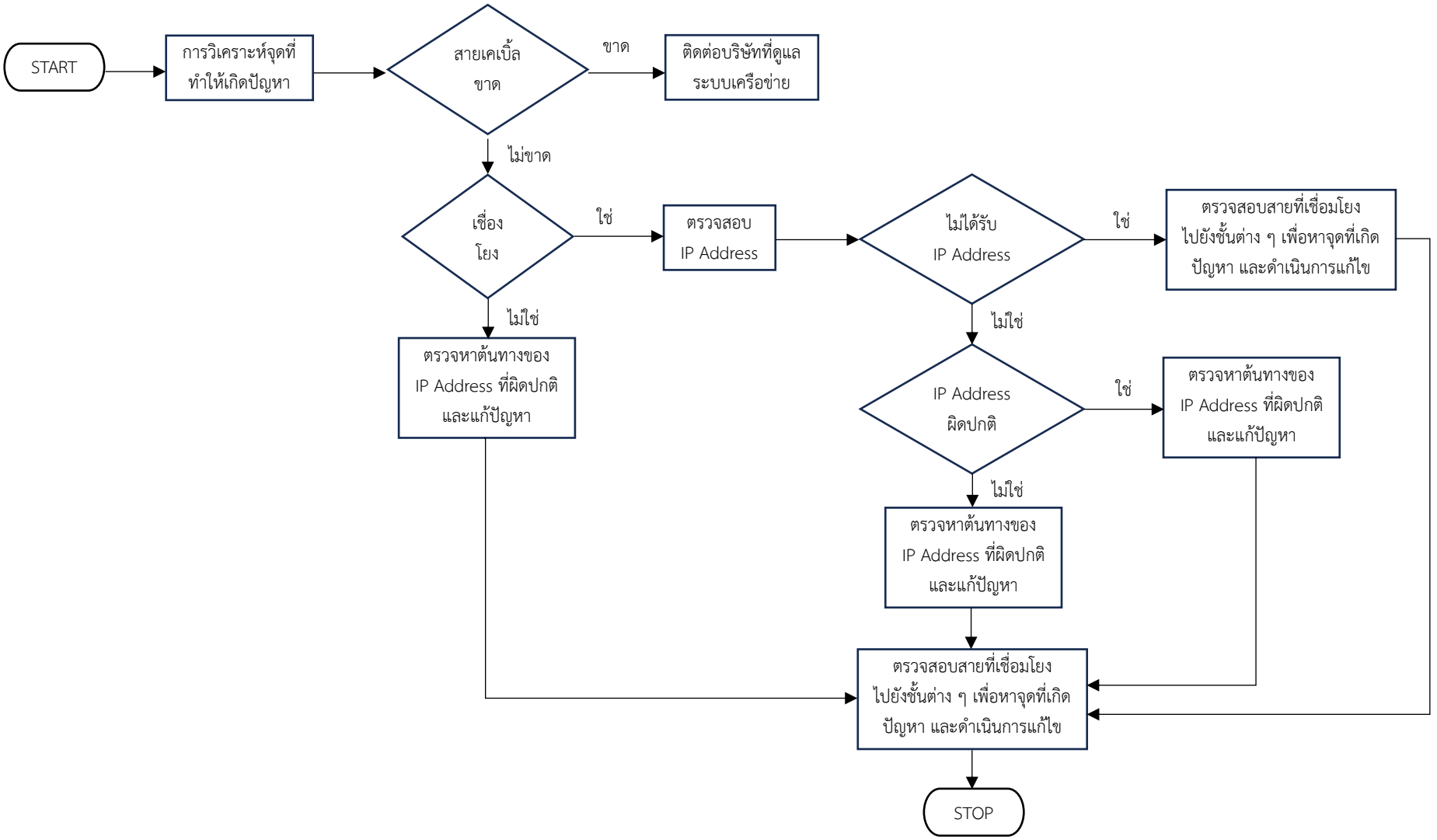
/(๓) กรณีการ ...

(๓) กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่ายเพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้ ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อของแต่ละชั้นภายในอาคาร

/แผนผัง ...

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

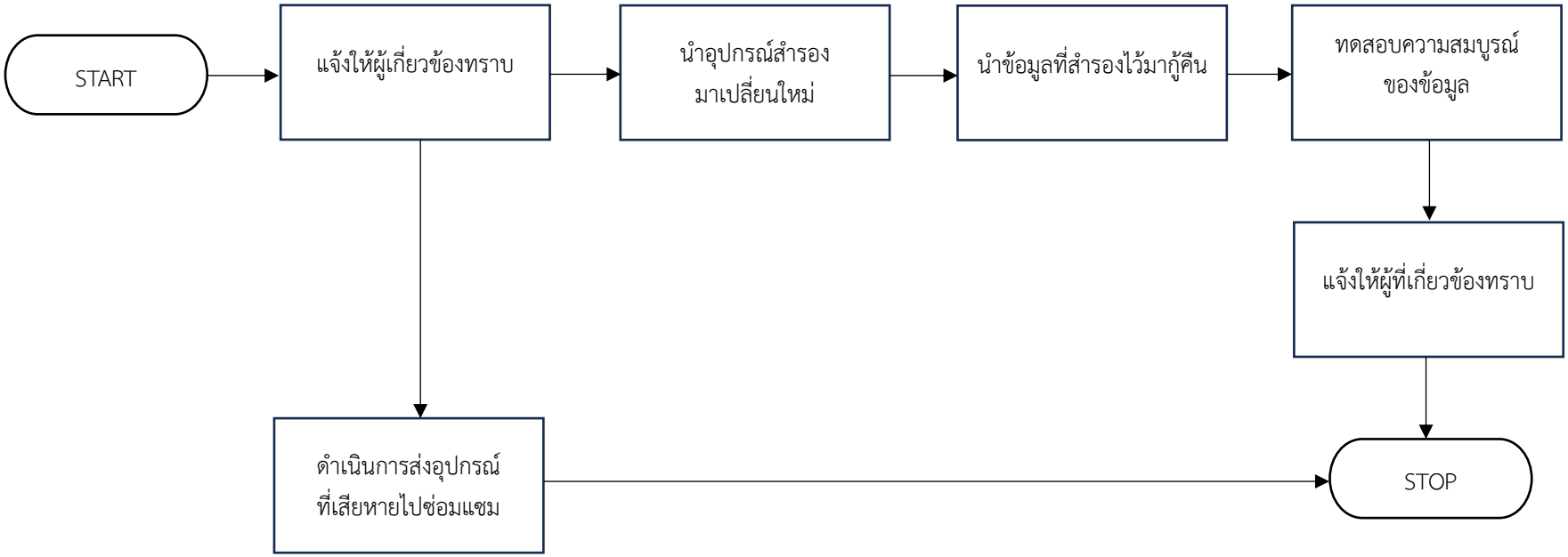


/(๔) กรณีอุปกรณ์ ...

(๔) กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่และนำข้อมูลที่ได้สำรองไว้มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)

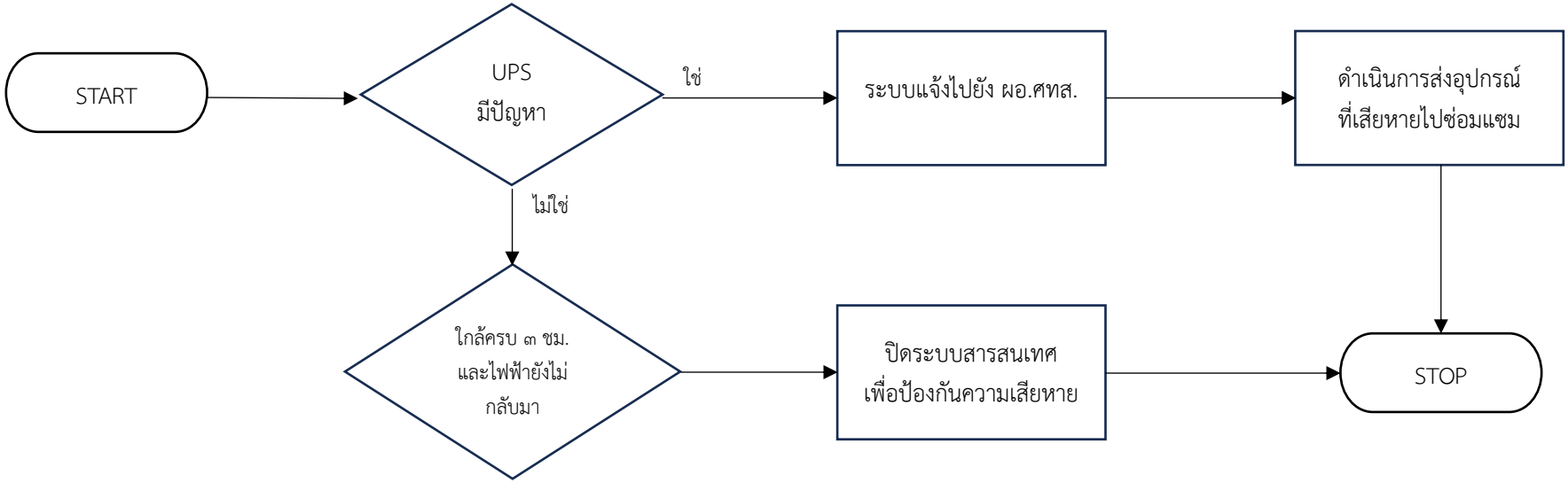


/(๕) กรณีไฟฟ้า ...

(๕) กรณีไฟฟ้าขัดข้อง

- ระบบเทคโนโลยีสารสนเทศและฐานข้อมูลมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ ๓ ชั่วโมง
- หากใกล้ครบ ๓ ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังผู้อำนวยการ ศทส.
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟฟ้าขัดข้อง



/สถานการณ์ ...

➢ **สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ**

(๑) กรณีไฟไหม้แยกเป็น ๒ กรณี คือ กรณีไฟไหม้ขณะมีผู้ปฏิบัติงานอยู่ และกรณีไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน

– หากเกิดไฟไหม้ขณะมีผู้ปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

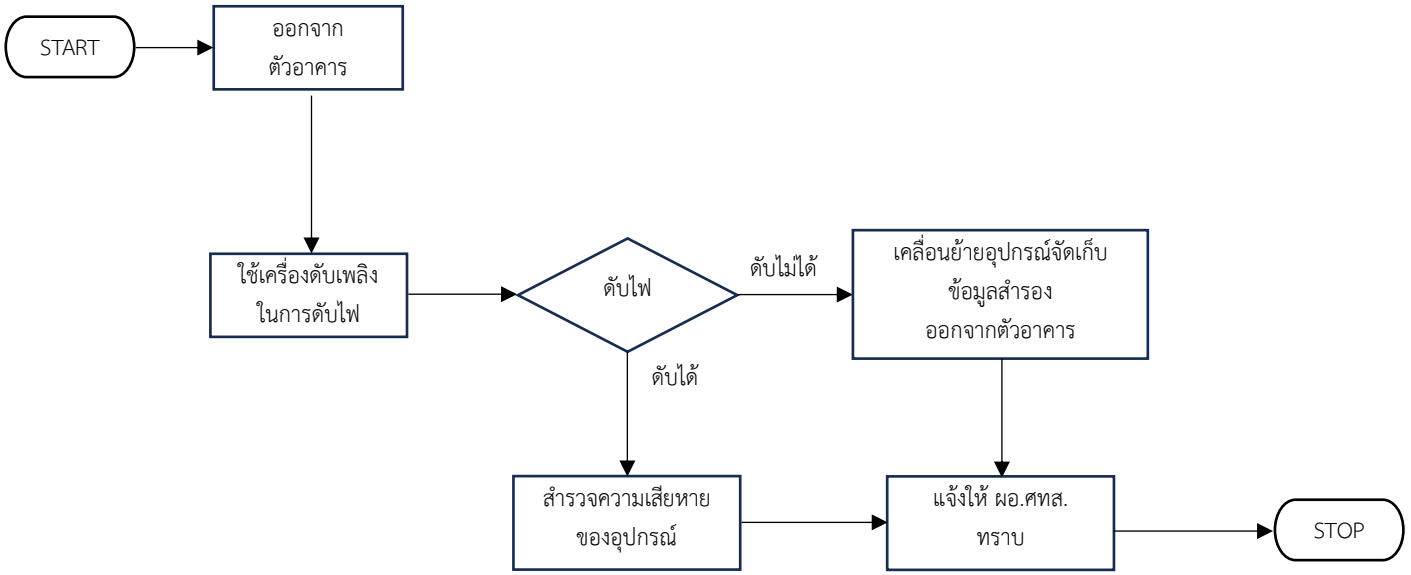
– หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงาน กับผู้ที่เกี่ยวข้องให้รีบดำเนินการแก้ไขอย่างเร่งด่วน

– หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบแจ้งเหตุเพลิงไหม้และดับไฟอัตโนมัต

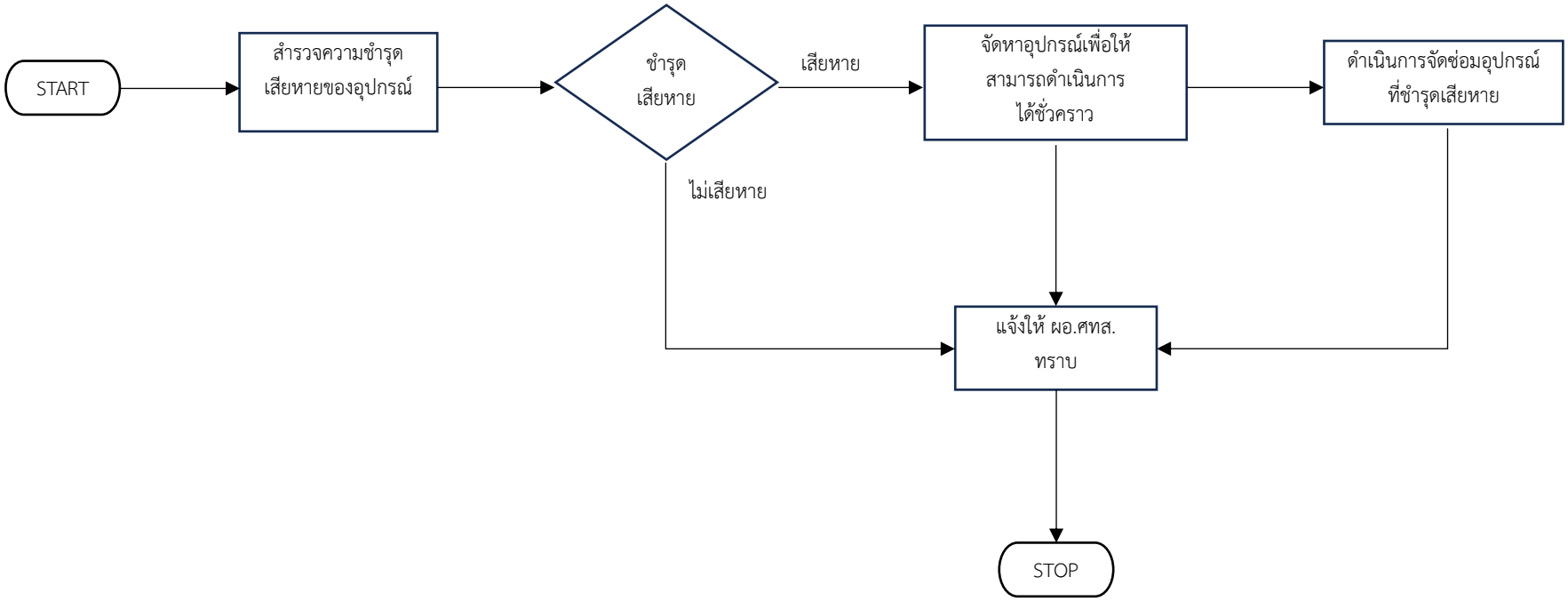
– อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

กรณีที่ ๑ แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)

/กรณีที่ ๒ ...



กรณีที่ ๒ แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะที่ไม่มีผู้ปฏิบัติงานอยู่)

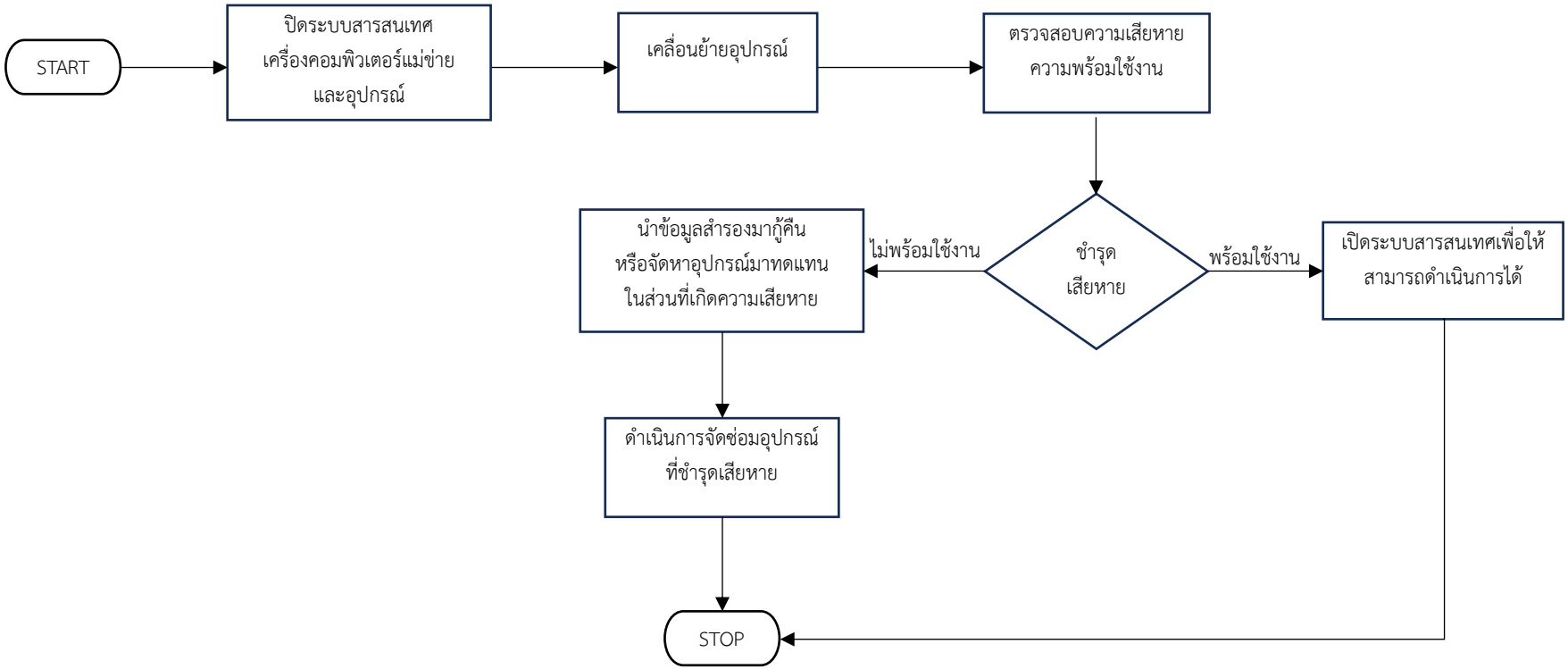

START
สำรวจความชำรุด
เสียหายของอุปกรณ์
ชำรุด
เสียหาย
เสียหาย
จัดหาอุปกรณ์เพื่อให้
สามารถดำเนินการ
ได้ชั่วคราว
ดำเนินการจัดซ่อมอุปกรณ์
ที่ชำรุดเสียหาย
ไม่เสียหาย
แจ้งให้ ผอ.ศทส.
ทราบ
STOP

/(๒) กรณีน้ำ ...

(๒) กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- สำรวจความชำรุดเสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม

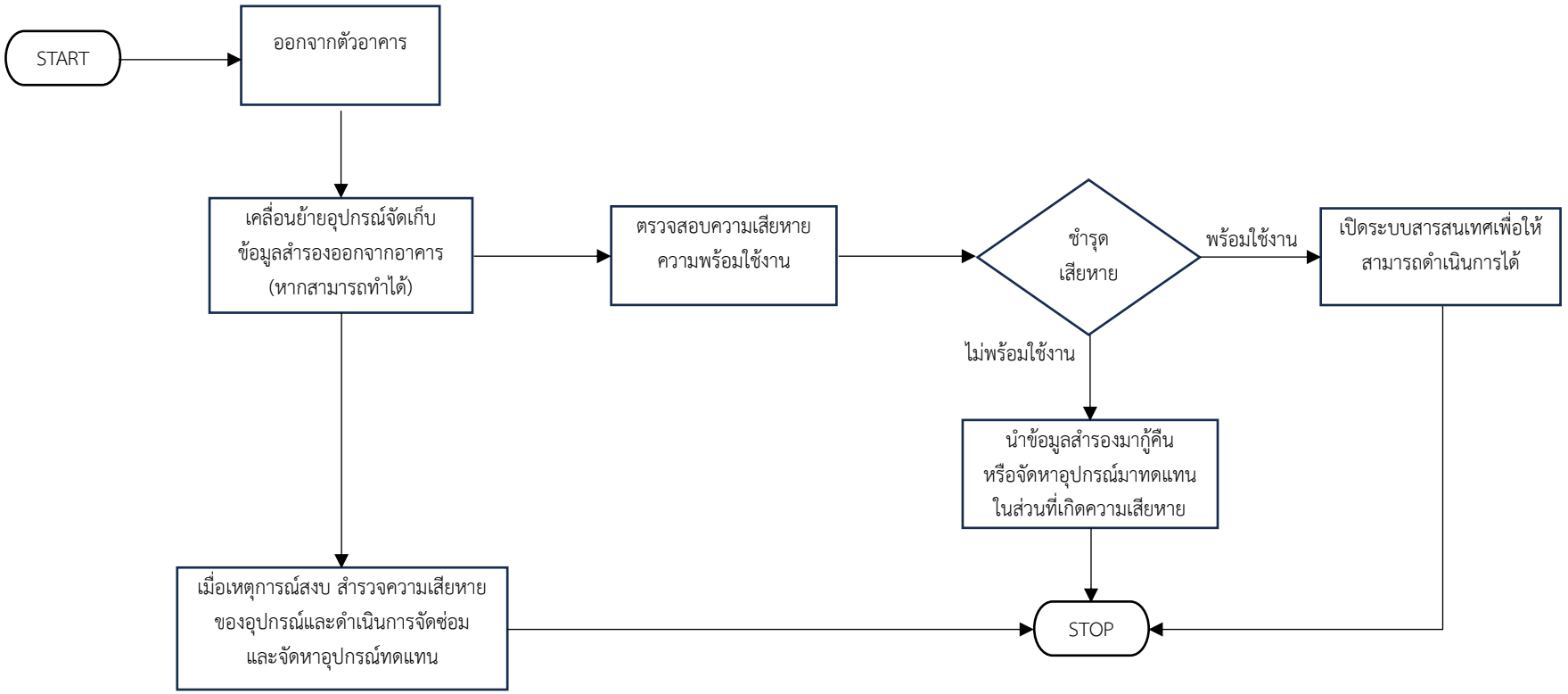


/(๓) กรณีแผ่น ...

(๓) กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรองเคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุดเสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



/สถานการณ์ ...

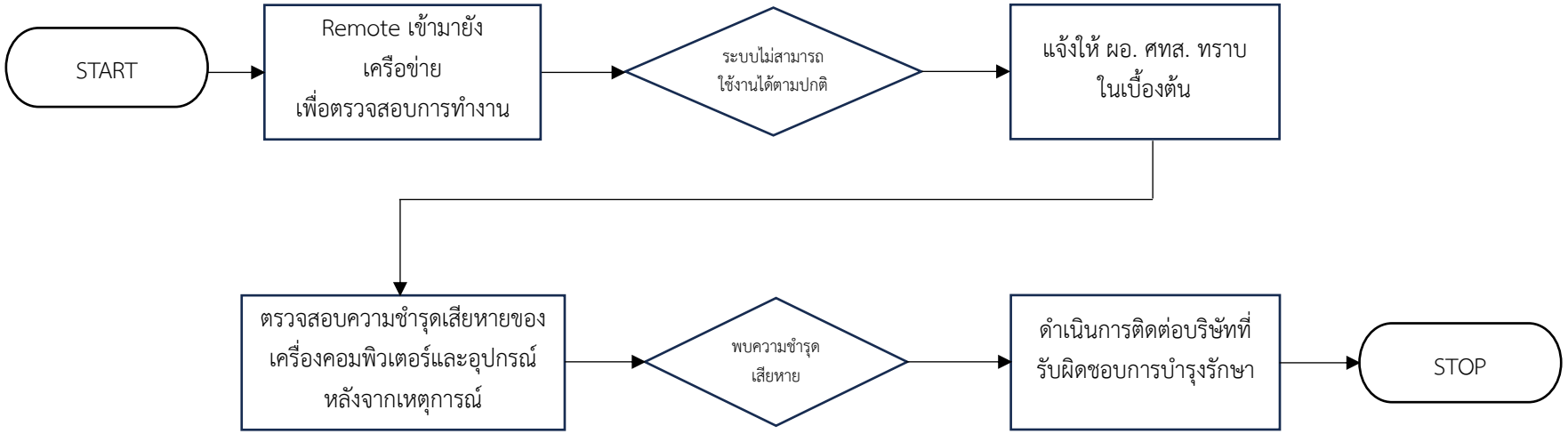
➢ **สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด**

สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

– กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ให้ผู้ดูแลระบบทำการ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ ให้แจ้งไปยัง ผอ. ศทส. ทราบในเบื้องต้น

– กรณีหลังเหตุการณ์ความไม่สงบต้องตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด



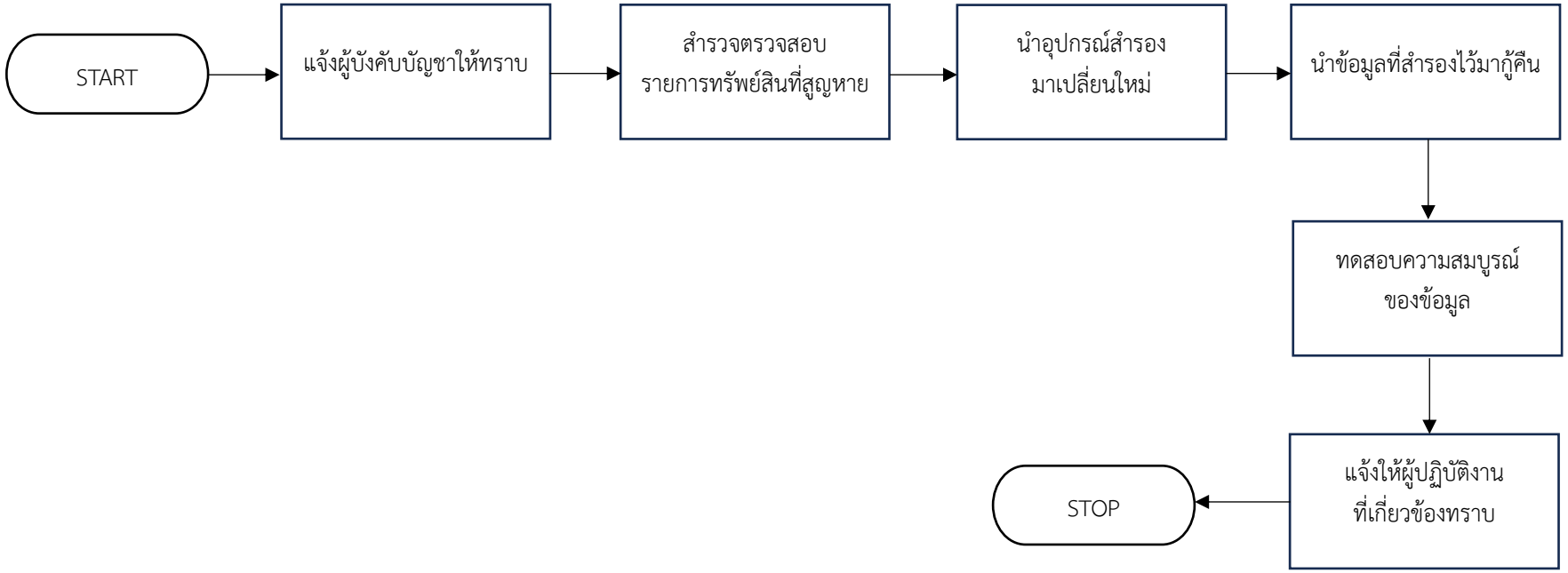
/สถานการณ์ ...

➢ **สถานการณ์ฉุกเฉินที่เกิดจากบุคคล**

(๑) กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืนให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

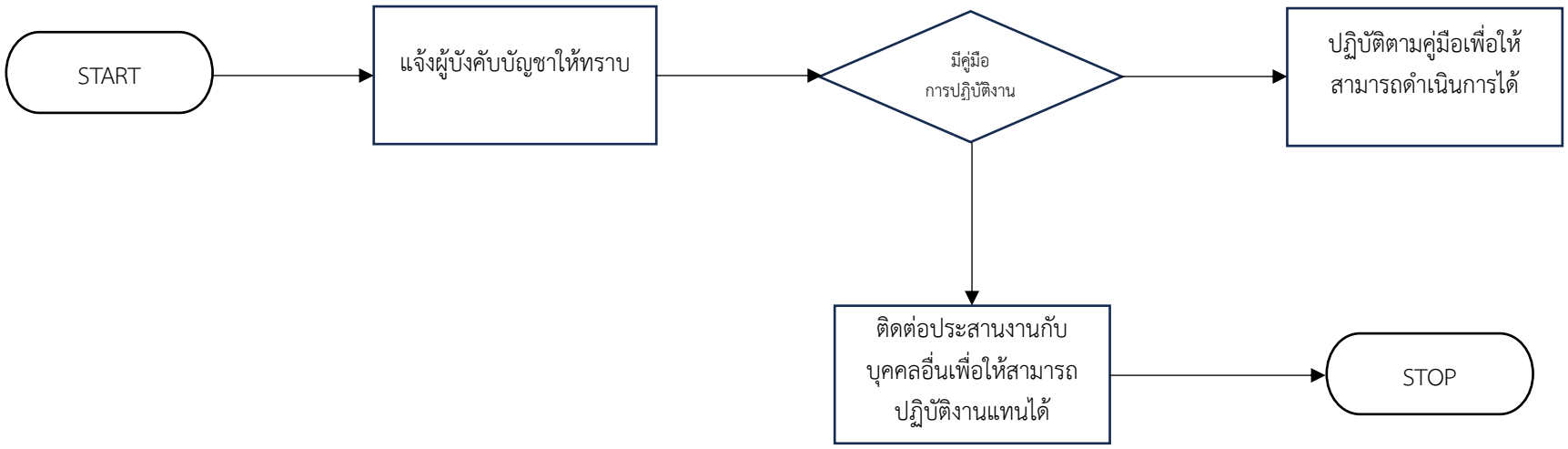


/(๒) กรณีผู้ปฏิบัติ ...

(๒) กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

- แจ้งผู้บังคับบัญชาให้ทราบ
- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



/๒.๓ การกำหนด ...

๒.๓ การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เป็นดังนี้

๒.๓.๑ ผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบปฏิบัติงาน ได้แก่

(๑) ผู้ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ประจำสำนักงานเศรษฐกิจการคลัง

(๒) นายสุภชัย ภูริเกษม ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒.๓.๒ ผู้รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย (Server room) ได้แก่

(๑) นายนิติสิริ ประสาทกุล	ผู้อำนวยการส่วนระบบข้อมูลและนวัตกรรมเทคโนโลยีสารสนเทศ
(๒) นางสาวณาตยา เด่นพงศ์สันต์	ผู้อำนวยการส่วนกลยุทธ์เทคโนโลยีสารสนเทศ
(๓) นางเรณุกา ยังมีสุข	ผู้อำนวยการส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย
(๔) นางสาวพิมลชญา สุขโข	นักวิชาการคอมพิวเตอร์ชำนาญการ
(๕) นายสุขุมภัทร จุฬุวรรณ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(๖) นายปิยวรรษ เกียรติกูล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(๗) นางสาวนัยรัตน์ อารีประยูรกิจ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(๘) นายสุชาติ จงพ่วง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ

/ส่วนที่ ๓ ...

ส่วนที่ ๓
บทสรุปและข้อเสนอแนะ

ส่วนที่ ๓
บทสรุปและข้อเสนอแนะ

เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในการใช้เป็นเครื่องมือและกลไกอันทรงพลังในการขับเคลื่อนการดำเนินงานตามภารกิจในทุกขั้นตอนและกิจกรรมที่เกิดขึ้นล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศ ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกส่วนงานภายใน สศค. โดยที่ปฏิเสธไม่ได้ว่า “ข้อมูล” นับว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลและอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม สศค. ได้ตระหนักถึงความสุ่มเสี่ยงดังกล่าวมาโดยตลอด ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การบริหารจัดการความเสี่ยงในองค์กรซึ่งการบริหารจัดการความเสี่ยง (Risk Management) จะครอบคลุมกระบวนการเริ่มตั้งแต่การระบุ วิเคราะห์ ประเมิน ดูแลตรวจสอบ จัดการและควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้ สศค. สามารถลดความเสียหายจากความเสี่ยงมากที่สุดอันเนื่องมาจากภัยที่ต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง

๓.๑ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยงเป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่ สศค. เผชิญอยู่ และจากการวิเคราะห์และกำหนดแนวทางการดำเนินการบริหารจัดการความเสี่ยงเพื่อควบคุมความเสี่ยงที่มีค่าระดับความเสี่ยงสูงสุด ๕ ลำดับแรก สรุปได้ดังนี้

๓.๑.๑ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ

<u>แนวทางการดำเนินการบริหารจัดการความเสี่ยง</u>

- จัดทำแผนรองรับความต้องการใช้งานล่วงหน้าให้ทันท่วงที
- นำเสนอแผนเพื่อเสนอผู้บริหารพิจารณา

๓.๑.๒ ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม

<u>แนวทางการดำเนินการจัดการความเสี่ยง</u>

- จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ
- ตรวจสอบการทำงานของโปรแกรมอย่างละเอียด
- ให้ผู้ดูแลระบบตรวจสอบโดยเร่งด่วน

/๓.๑.๓ ความเสี่ยง ...

๓.๑.๓ ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server , DNS Server, Firewall, Core Switch

แนวทางการดำเนินการบริหารจัดการความเสี่ยง

- บำรุงรักษาระบบตรวจสอบการใช้งานเครือข่าย
- ตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ
- มีแผนจัดซื้ออุปกรณ์ทดแทนอุปกรณ์ที่หมดสภาพเพื่อให้สามารถใช้งานได้ตามปกติ

๓.๑.๔ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่

แนวทางการดำเนินการบริหารจัดการความเสี่ยง

- มีแผนจัดหาเครื่องกำเนิดไฟฟ้า
- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่
- แผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ

๓.๑.๕ ความเสี่ยงจากไวรัส คอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์

แนวทางการดำเนินการจัดการความเสี่ยง

- ติดตั้งระบบป้องกันไวรัส และมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน
- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ
- ต้องอัพเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ

๓.๒ แผนรองรับสถานการณ์ฉุกเฉินและเจ้าหน้าที่ผู้รับผิดชอบ

มีแผนรองรับสถานการณ์ฉุกเฉินแบ่งออกเป็น ๔ สถานการณ์หลัก ๆ ดังนี้

๓.๒.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

(๑) กรณีการป้องกันไวรัสล้มเหลว
(๒) กรณีการป้องกันผู้บุกรุกล้มเหลว
(๓) กรณีการเชื่อมโยงเครือข่ายล้มเหลว
(๔) กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)
(๕) กรณีไฟฟ้าขัดข้อง

๓.๒.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ

(๑) กรณีไฟไหม้
(๒) กรณีน้ำท่วม
(๓) กรณีแผ่นดินไหว

/๓.๒.๓ สถานการณ์ ...

๓.๒.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด

(๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้

(๒) กรณีหลังเหตุการณ์ความไม่สงบ

๓.๒.๔ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

(๑) กรณีโจรกรรม

(๒) กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

กำหนดให้มีเจ้าหน้าที่ผู้รับผิดชอบหากมีสถานการณ์ฉุกเฉินเกิดขึ้น ดังต่อไปนี้

๑. *สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค*
เจ้าหน้าที่ผู้รับผิดชอบ คือ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ (ผอ. ศทส.)
เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ (ศทส.)
และผู้ดูแลระบบงาน

๒. *สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ กรณี ไฟไหม้ น้ำท่วม แผ่นดินไหว*
เจ้าหน้าที่ผู้รับผิดชอบ คือ ผู้ปฏิบัติงานส่วนต่าง ๆ ผู้ดูแลห้องปฏิบัติการคอมพิวเตอร์
ผู้ดูแลระบบงาน ผู้สำรวจตรวจสอบรายการทรัพย์สิน
ผู้บริหารของหน่วยงาน

๓. *สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง*
กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบจะทำการ Remote เข้ามา
เพื่อตรวจสอบการทำงานของระบบ หากพบว่า
ระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งให้
ผอ.ศทส. ทราบ

กรณีหลังเหตุการณ์ความไม่สงบ ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สิน
ตรวจสอบความชำรุด เสียหาย ซึ่งอาจได้รับ
จากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย
ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

๔. *สถานการณ์ฉุกเฉินที่เกิดจากบุคคล*
ทั้งในกรณีโจรกรรม และกรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้
เจ้าหน้าที่ผู้รับผิดชอบ คือ เจ้าหน้าที่ของ ศทส. และฝ่ายดูแลอาคารสถานที่
สำนักงานเลขานุการกรม

/๓.๓ ข้อเสนอแนะ ...

๓.๓ ข้อเสนอแนะ

๑. การดูแลระบบรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ฐานข้อมูลและระบบเครือข่ายให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน เช่น ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ เช่น Domain Server, Web Server, Mail Server, DNS Server และ Database Server ซึ่งกำหนดแนวทางจัดการความเสี่ยงไว้คือ ต้องจัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนการปฏิบัติงานได้ตามปกติ ควรจัดทำเป็นโครงการที่จะต้องได้รับการสนับสนุนงบประมาณในการจัดหาทดทนอุปกรณ์ดังกล่าวด้วยเช่นกัน

๒. การบริหารจัดการความเสี่ยงเกี่ยวกับข้อมูลส่วนบุคคลถูกละเมิด ควรมีการจัดหาเครื่องมือ วิธีการ หรือเสริมสร้างองค์ความรู้ใหม่ ๆ แก่บุคลากรของ สศค. ให้ตระหนักถึงความสำคัญของบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (พระราชบัญญัติฯ) พร้อมทั้งพัฒนา/ปรับปรุงระบบและมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลให้สอดคล้องตามข้อกำหนดแห่งพระราชบัญญัติฯ รวมถึงสอดคล้องตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๓. การพัฒนาระบบงานต่าง ๆ ควรพิจารณาการออกแบบระบบงานให้เป็นสถาปัตยกรรมแบบ ๓-tier Architecture โดยรองรับการจัดแบ่งระบบงานออกเป็น ๓ ส่วน ได้แก่ ส่วนแสดงผล ส่วนประมวลผล และส่วนฐานข้อมูล ซึ่งจะส่งผลให้เกิดความยืดหยุ่นในด้านการบริหารจัดการทรัพยากร และการเปลี่ยนแปลงของระบบงาน รวมถึงการเพิ่มความปลอดภัยทางด้านไซเบอร์ เนื่องจากการทำงานของระบบงานถูกแบ่งออกเป็นส่วน ๆ

๔. การสำรองข้อมูลของระบบงานต่าง ๆ ของ สศค. ควรจัดหาระบบสำรองข้อมูลให้เพียงพอกับระบบงานของ สศค. ทั้งระบบงานที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย และติดตั้งบนระบบคอมพิวเตอร์แม่ข่ายเสมือน
