แผนบริหารความเสี่ยง
และความปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๕

กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม

สำนักงานเศรษฐกิจอุตสาหกรรม

คำนำ

ปัจจุบันการใช้งานคอมพิวเตอร์และอุปกรณ์ Smart Device (เช่น โทรศัพท์มือถือ แท็บเล็ต ฯลฯ) จะต้องใช้งานผ่านระบบเครือข่ายคอมพิวเตอร์ (Computer Network) เช่น Internet, Cloud เป็นต้น นับวันจะมีความเสี่ยงสูงขึ้น จากการเกิดอาชญากรรมทางไซเบอร์ในหลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการโจมตีทางระบบเครือข่ายเพื่อก่อกวนให้ระบบใช้งานไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ สิ่งเหล่านี้เป็นภัยอันตรายสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมากและมีความรุนแรงเพิ่มขึ้นทุกขณะ ทั้งในประเทศและต่างประเทศ อีกทั้งมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กรภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ขององค์กร

สำนักงานเศรษฐกิจอุตสาหกรรม (สศอ.) ตระหนักและเห็นความสำคัญดังกล่าว จึงได้จัดทำแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ เพื่อเป็นกรอบแนวทางการปฏิบัติงานในการดำเนินงานการบริหารความเสี่ยงของ สศอ. ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้หน่วยงานภายใน สศอ. บรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม รวมทั้งเพื่อให้ผู้บริหารและบุคลากรของ สศอ. มีความรู้ ความเข้าใจในเรื่องการบริหารความเสี่ยงทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

(นายกฤศ จันทร์สุวรรณ)
รองผู้อำนวยการสำนักงานเศรษฐกิจอุตสาหกรรม

สารบัญ

สารบัญ (ต่อ)

บทสรุปผู้บริหาร

สำนักงานเศรษฐกิจอุตสาหกรรมได้นำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานของเจ้าหน้าที่ในสำนักงานหลายด้าน ดังนั้นจึงมีความจำเป็นต้องมีการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้น ทางสำนักงานได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ จึงได้แต่งตั้งคณะทำงานเพื่อดำเนินการจัดทำแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ สศอ. พ.ศ. ๒๕๖๕ ซึ่งการจัดทำแผนบริหารความเสี่ยงฯ ดังกล่าว เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับความปลอดภัยของระบบฐานข้อมูลสารสนเทศ และความปลอดภัยทางไซเบอร์เป็นแนวทางในการดูแลระบบรักษาความมั่นคงปลอดภัยให้มีเสถียรภาพ มีความพร้อมในการใช้งาน และให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอน และภัยพิบัติ

สำหรับความเสี่ยงที่นำมาพิจารณา ประกอบด้วย ความเสี่ยงด้านการบริหารจัดการ ความเสี่ยงจากการปฏิบัติงาน ความเสี่ยงด้านเทคนิค ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน และความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์ ความเสี่ยงทางไซเบอร์ ซึ่งจากการวิเคราะห์สามารถระบุความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยเสี่ยง ผลกระทบ และแนวทางการแก้ไขปัญหา จำนวนทั้งสิ้น ๑๕ 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. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ
๑๓. ความเสี่ยงด้านโปรแกรมประยุกต์
๑๔. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์
๑๕. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ

ซึ่งทั้ง ๑๕ ความเสี่ยงอยู่ในระดับความเสี่ยงต่ำ (สามารถยอมรับได้) จนถึงความเสี่ยงสูงมาก ที่มีแผนรองรับความเสี่ยงเรียบร้อยแล้ว ส่วนแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) สศอ. ได้จัดทำแผนรองรับสถานการณ์ฉุกเฉิน จำนวน ๔ สถานการณ์ ได้แก่ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค เช่น การป้องกันไวรัสล้มเหลว การป้องกันผู้บุกรุกล้มเหลว สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว โรคระบาด สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบ

เรียบร้อยในบ้านเมือง และสถานการณ์ฉุกเฉินที่เกิดจากบุคคล เช่น การโจรกรรม ผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้ เป็นต้น

อย่างไรก็ตามปัญหาของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศสามารถเกิดขึ้นได้ตลอดเวลา ดังนั้น การเตรียมความพร้อมในการรองรับสถานการณ์ เช่น การตรวจสอบช่องโหว่ของระบบเครือข่ายอย่างสม่ำเสมอ การตรวจสอบและคัดกรองผู้เข้าใช้งานในระบบ การสำรองข้อมูลระบบปฏิบัติการและฐานข้อมูลต่าง ๆ ตามรอบระยะเวลา การจัดหาอุปกรณ์คอมพิวเตอร์ที่ทันสมัยเพื่อทดแทนของเดิมที่หมดอายุการใช้งานหรือไม่รองรับกับเทคโนโลยีปัจจุบัน รวมถึงการเสริมสร้างความรู้ในการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัยให้กับผู้ใช้งานในองค์กร เป็นต้น จะทำให้การปฏิบัติงานโดยใช้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพและปลอดภัยจากความเสี่ยงต่าง ๆ ที่อาจจะเกิดขึ้น

คำนิยาม

คำนิยามที่ใช้ในแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์นี้ ประกอบด้วย

"หน่วยงาน" หมายความว่า สำนักงานเศรษฐกิจอุตสาหกรรม

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

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

"ระบบเทคโนโลยีสารสนเทศ (Information Technology System)" หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหารการสนับสนุนการให้บริการการพัฒนา และควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่ายโปรแกรมข้อมูลและสารสนเทศ เป็นต้น

"สิทธิ์ของผู้ใช้งาน" หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"ความมั่นคงปลอดภัย" หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (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 ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

"ระบบอินเทอร์เน็ต (Internet)" หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

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

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานเศรษฐกิจอุตสาหกรรม

"ผู้ใช้บริการ" หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน และให้หมายความรวมถึงเจ้าหน้าที่บริษัทที่ปรึกษาที่เข้ามาปฏิบัติงานในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

"ผู้ดูแลระบบ (System Administrator)" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

"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 มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

"รหัสผ่าน (Password)" หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"บัญชีผู้ใช้บริการ (Account)" หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

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

"ชื่อเครื่องคอมพิวเตอร์ (Computer Name)" หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

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

"การตั้งค่าระบบ (Configuration)" หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

"เลขที่อยู่ไอพี (IP Address)" หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.) ปัจจุบันใช้ IPv4

"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 โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

"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

"อุปกรณ์กระจายสัญญาณ (Access Point)" หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

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

"โดยปริยาย (Default)" หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ

"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 802.11

"MAC Address (Media Access Control Address)" หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

"ไฟร์วอลล์ (Firewall)" หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

"VPN (Virtual Private Network)" หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

"Web Server" หมายความว่า เครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่าง ๆ

"ชื่อโดเมนย่อย (Sub Domain Name)" หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ "ที่อยู่เว็บไซต์" แทนก็ได้

"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 เพื่อตรวจสอบประเภทของ

การสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

“ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (Internal IT Auditor)” หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบระบบสารสนเทศหรือระบบเครือข่ายของหน่วยงาน

“ผู้ตรวจสอบระบบสารสนเทศจากหน่วยงานภายนอก (External IT Auditor)” หมายความว่า ผู้ที่ได้รับมอบหมายจากหน่วยงานให้มีสิทธิ์ในการตรวจสอบระบบสารสนเทศหรือระบบเครือข่ายของหน่วยงาน

“เวลาอ้างอิงสากล (Stratum 0)” หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

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

“Visualization” หมายความว่า เป็นการจำลองเครื่องเสมือนด้วยซอฟต์แวร์ ที่ทำให้คอมพิวเตอร์หนึ่งเครื่อง สามารถทำงานเป็นเครื่องเสมือนหลายๆ ระบบได้ โดยแต่ละระบบมีทรัพยากรหน่วยความจำ, ฮาร์ดดิสก์ และอุปกรณ์เน็ตเวิร์คเสมือนที่เป็นอิสระต่อกัน เครื่องเสมือนแต่ละเครื่องจึงสามารถมีระบบปฏิบัติการและซอฟต์แวร์เป็นของตนเองโดยอิสระ

“VMware” หมายความว่า เป็นชื่อผลิตภัณฑ์ที่มีความสามารถในการทำ **Visualization**

ส่วนที่ ๑
แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ ของสำนักงานเศรษฐกิจอุตสาหกรรม พ.ศ. ๒๕๖๕
(Risk Management)

ส่วนที่ ๑
แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ ของสำนักงานเศรษฐกิจอุตสาหกรรม พ.ศ. ๒๕๖๕ (Risk Management)

สำนักงานเศรษฐกิจอุตสาหกรรมได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ของหน่วยงาน ซึ่งอาจเกิดขึ้นในระบบบริหารงานสั่งการและการปฏิบัติงาน เพื่อสนับสนุนวิสัยทัศน์ในการเป็นองค์กรชี้นำการพัฒนาอุตสาหกรรมของประเทศสู่ความยั่งยืน การดำเนินงานดังกล่าวทำให้ข้อมูลและสารสนเทศต่าง ๆ ที่ใช้ในการบริหารงานมีปริมาณที่มากมาย มีความเคลื่อนไหวตลอดเวลา โดยเฉพาะอย่างยิ่งข้อมูลและสารสนเทศที่ใช้ในการให้บริการประชาชนด้านเศรษฐกิจอุตสาหกรรม รวมทั้งข้อมูลและสารสนเทศต่าง ๆ ที่สำนักงานเศรษฐกิจอุตสาหกรรมต้องรับผิดชอบกระบวนการประมวลผลข้อมูล ตามนโยบายสำคัญต่าง ๆ ของกระทรวงอุตสาหกรรมและรัฐบาล

สำนักงานเศรษฐกิจอุตสาหกรรมโดยกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรมจึงได้จัดทำแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ขึ้นเพื่อใช้เป็นแนวทางปฏิบัติประกอบการบริหารความเสี่ยงเพื่อลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานของสำนักงานเศรษฐกิจอุตสาหกรรม

๑.๑ วัตถุประสงค์

๑) เพื่อให้ฝ่ายบริหาร/ฝ่ายปฏิบัติการ เข้าใจหลักการและกระบวนการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ขององค์กร

๒) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศและการสื่อสารของสำนักงานเศรษฐกิจอุตสาหกรรม

๓) เพื่อให้ผู้ปฏิบัติได้รับทราบและเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ การเผยแพร่ความรู้ความเข้าใจเกี่ยวกับความเสี่ยงและความปลอดภัยทางไซเบอร์ขององค์กร

๔) เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง

๕) เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ความสัมพันธ์ ตลอดจนเชื่อมโยงระหว่างการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์กับกลยุทธ์ขององค์กร

๖) เพื่อใช้เป็นเครื่องมือในการสร้างวัฒนธรรมการบริหารความเสี่ยงในทุก ๆ ระดับขององค์กร

๑.๒ นโยบายการบริหารความเสี่ยง

เพื่อสร้างความตระหนักถึงความสำคัญและกระตุ้นให้ข้าราชการทุกคนของสำนักงานเศรษฐกิจอุตสาหกรรมเห็นถึงความจำเป็นในการระมัดระวังต่อสถานการณ์ที่คุกคามต่อประสิทธิภาพการปฏิบัติงานการบริหารงาน และอาจทำให้เกิดความเสียหายต่อระบบฐานข้อมูลสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญที่สุดในการให้บริการประชาชนและการตัดสินใจของผู้บริหารสำนักงานเศรษฐกิจอุตสาหกรรม ตลอดจนคณะรัฐบาลและผู้บริหารประเทศ

แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ของสำนักงานเศรษฐกิจอุตสาหกรรม จะทำให้เจ้าหน้าที่ทุกคนที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ ซึ่งจะถือเป็นส่วนหนึ่งของการดำเนินงานการปฏิบัติงานเพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายต่าง ๆ ที่อาจเกิดขึ้นต่อระบบปฏิบัติราชการของสำนักงานเศรษฐกิจอุตสาหกรรม

๑.๓ ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๑.๓.๑ ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้สำนักงานเศรษฐกิจอุตสาหกรรมไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อข้อมูลสารสนเทศที่สำนักงานเศรษฐกิจอุตสาหกรรมใช้ในการบริหารงานและปฏิบัติการโดยเฉพาะอย่างยิ่งการบริการประชาชน

๑.๓.๒ การควบคุม (Control) หมายถึง ขั้นตอนการปฏิบัติ กระบวนการดำเนินงานหรือกลไกการปฏิบัติงาน ซึ่งสำนักงานเศรษฐกิจอุตสาหกรรมกำหนดขึ้นเพื่อให้มั่นใจว่าการบริหารงานจะสามารถบรรลุวัตถุประสงค์ที่ได้กำหนดไว้

๑.๓.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ และติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หน่วยงาน หรือกระบวนการดำเนินงานขององค์กร รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้

✓ ๑.๓.๔ การบริหารความเสี่ยงองค์กรโดยรวม (Organization Wide Risk Management) หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการปฏิบัติงานต่าง ๆ โดยต้องลดมูลเหตุของแต่ละโอกาสที่จะทำให้สำนักงานเศรษฐกิจอุตสาหกรรมเสียหาย

๑.๓.๕ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ระบบเครื่องคอมพิวเตอร์ (Hardware) ระบบเครือข่าย (Network System) ระบบฐานข้อมูล (Database System) และอุปกรณ์ประกอบระบบต่าง ๆ รวมทั้งอาคารสถานที่ ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด

๑. ทะเบียนครุภัณฑ์คอมพิวเตอร์ สำนักงานเศรษฐกิจอุตสาหกรรม

๒. ระบบเครือข่าย (Networking) ระบบเครือข่ายที่สำนักงานเศรษฐกิจอุตสาหกรรมใช้ในการปฏิบัติหน้าที่ เช่น Core Switch , Access Switch เป็นต้น

๓. ระบบฐานข้อมูล (Database System) ฐานข้อมูลที่สำนักงานเศรษฐกิจอุตสาหกรรมใช้ในการปฏิบัติหน้าที่ซึ่งประกอบด้วย

๑) ฐานข้อมูลเพื่อการบริการประชาชนด้านเศรษฐกิจอุตสาหกรรม

- ระบบเว็บไซต์อินเทอร์เน็ต
- ระบบห้องสมุดอิเล็กทรอนิกส์ (E-library)
- ระบบเผยแพร่ดัชนีและสถิติอุตสาหกรรม (http://indexes.oie.go.th)
- ระบบการกรอกแบบสอบถาม ร.ง. ๘ และ ร.ง. ๙ ทางอินเตอร์เน็ต (http://isingleform.go.th)
- ระบบ Intelligent Unit
- ระบบเปิดเผยข้อมูล (http://data.oie.go.th)

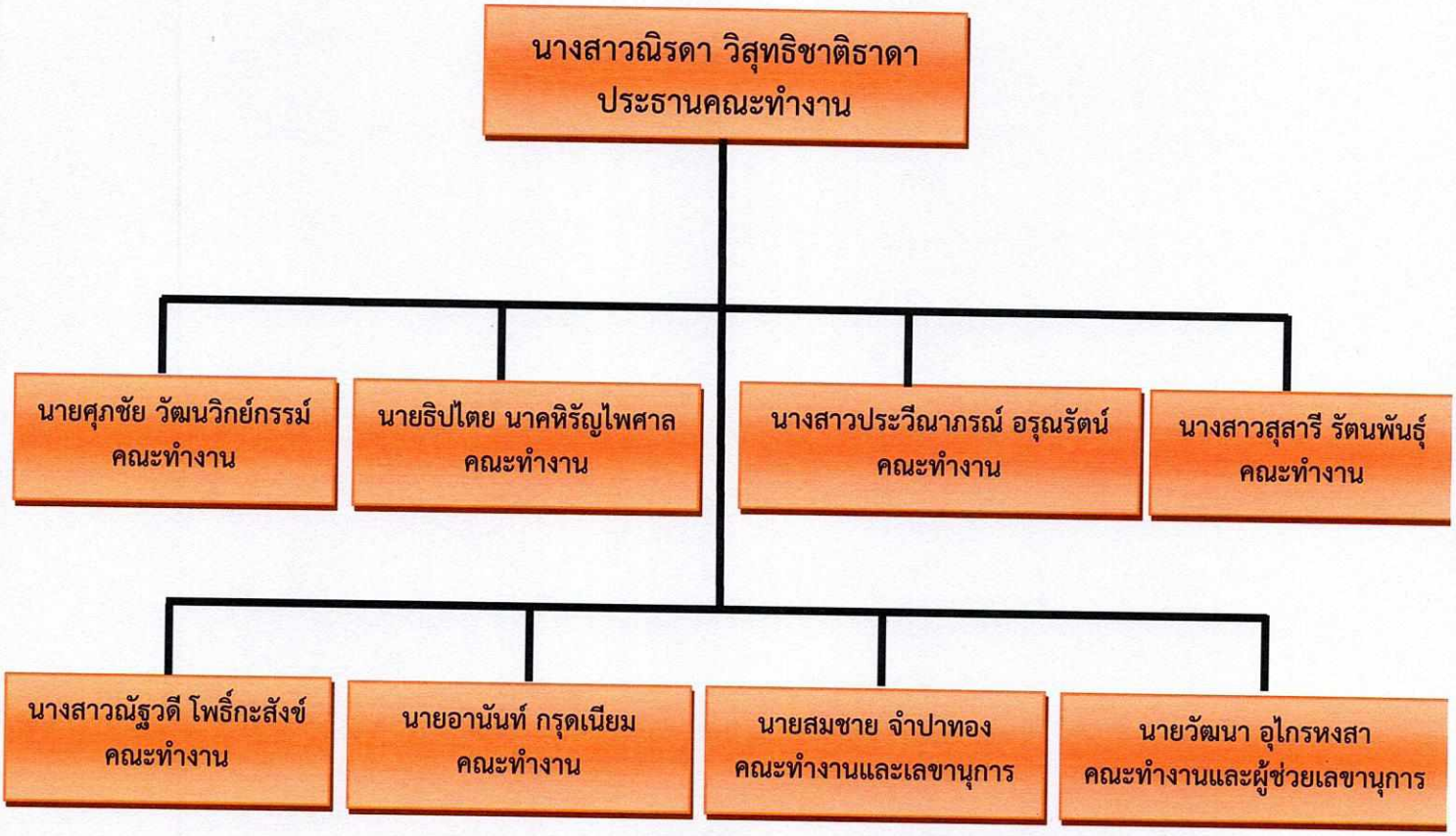
- ระบบดัชนีวัดขีดความสามารถของภาคอุตสาหกรรมไทย (http://ci.oie.go.th)
- ระบบจัดทำตัวชี้วัดผลิตภาพและผลประกอบการอุตสาหกรรม (http://www.oiesurveys.com)
- ระบบ Eco-sticker

๒) ฐานข้อมูลเพื่อการบริหารงานภายใน

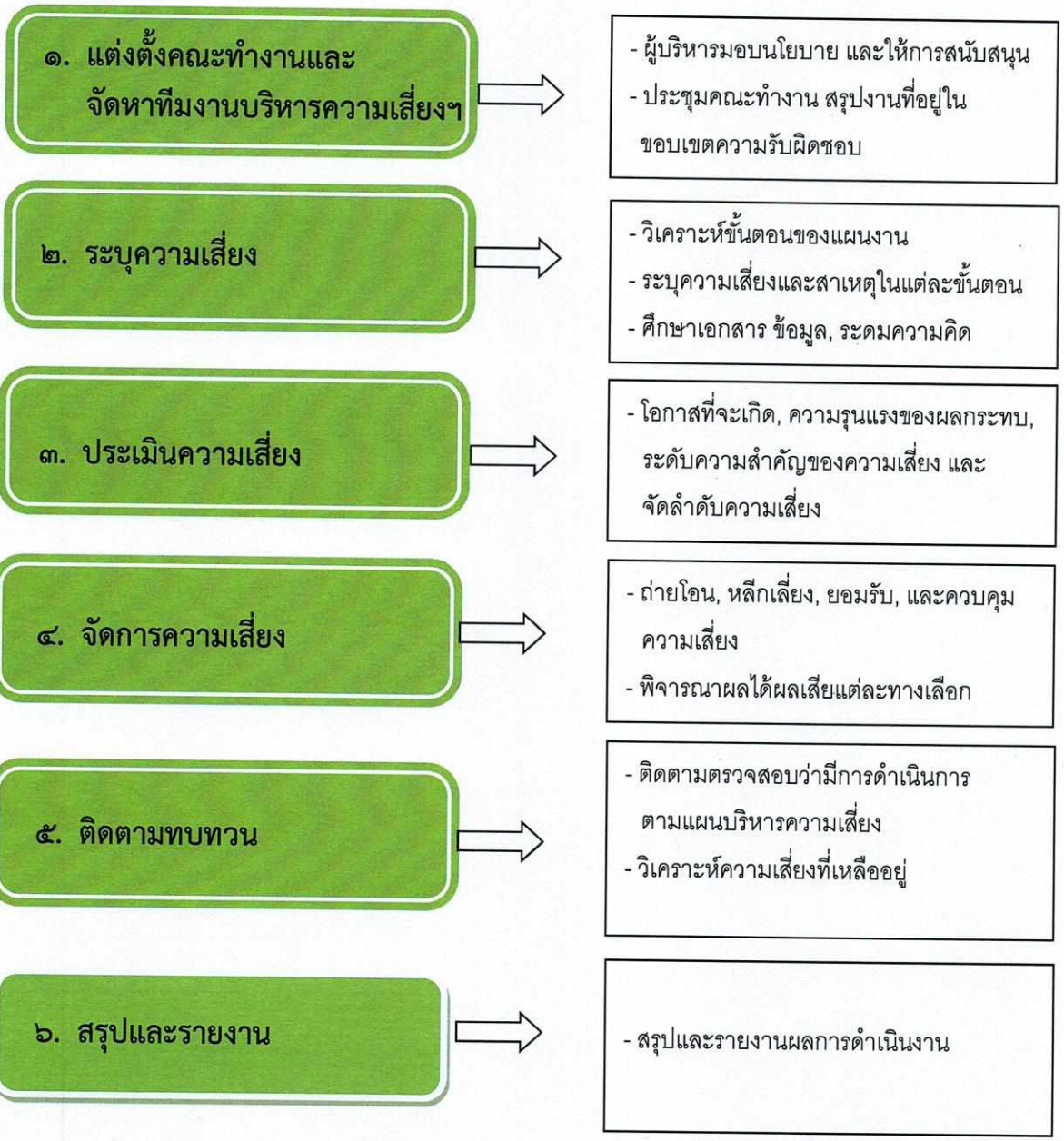
- ระบบห้องสมุดอิเล็กทรอนิกส์ (E-library)
- ระบบการสำรวจข้อมูลอุตสาหกรรมรายเดือน
- ระบบการสำรวจข้อมูลอุตสาหกรรมรายปี
- ระบบสารบรรณอิเล็กทรอนิกส์
- ระบบงานตู้เอกสารอิเล็กทรอนิกส์และหนังสือเวียนอิเล็กทรอนิกส์
- ระบบการมาปฏิบัติราชการ
- ระบบประมวลผลดัชนีอุตสาหกรรม
- ระบบทะเบียนครุภัณฑ์คอมพิวเตอร์
- ระบบติดตามประเมินผลความก้าวหน้า (OIE Monitoring Policy)
- ระบบจดหมายอิเล็กทรอนิกส์ (OIE Webmail)
- ระบบเอกสารอิเล็กทรอนิกส์ (OIE QR Code)
- ระบบตรวจสอบความซ้ำซ้อนของที่ปรึกษาโครงการ (Consult)
- ระบบข้อมูลบุคลากร (DPIS)
- ระบบวันลา (E-Form)
- ระบบจัดเก็บไฟล์กลาง (Share Drive)
- ระบบเผยแพร่ข้อมูล (Data Service)

๑.๓.๖ บุคลากร (People) ได้แก่ บุคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงานสำหรับการดูแลและจัดทำระบบ

๑.๔ โครงสร้างคณะทำงานบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์



๑.๕ ขั้นตอน/กระบวนการบริหารความเสี่ยง



๑.๕.๑ การกำหนดวัตถุประสงค์

๑) เพื่อกำหนดความเสี่ยงที่มีโอกาสเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเศรษฐกิจอุตสาหกรรม

๒) กำหนดกิจกรรมป้องกันรองรับความเสี่ยงที่มีโอกาสเกิดขึ้น เพื่อป้องกันความเสียหายและลดความรุนแรงของความเสียหายที่เกิดขึ้นให้อยู่ในระดับที่น้อยที่สุด

๑.๕.๒ การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเศรษฐกิจอุตสาหกรรมสามารถแยกประเภทความเสี่ยงออกเป็น ๕ ประเภท ดังนี้

๑) ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๒) ความเสี่ยงจากการปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการจัดการความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของสำนักงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓) ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ระบบเครือข่าย เครื่องมือและอุปกรณ์ อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๔) ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๕) ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์ เป็นความเสี่ยงที่เกิดจากเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่มีอายุการใช้งานมานาน และยังไม่มีการจัดซื้อเครื่องใหม่มาทดแทน อาจทำให้เกิดความเสียหายต่อการทำงานได้ เช่น Hard Disk เสีย จะทำให้ข้อมูลสูญหายได้ เป็นต้น

๑.๕.๓ การระบุความเสี่ยง

จากการวิเคราะห์ประเภทความเสี่ยงทั้ง ๕ ด้าน ซึ่งประกอบด้วยความเสี่ยงด้านการบริหารจัดการ ความเสี่ยงจากการปฏิบัติงาน ความเสี่ยงด้านเทคนิค ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน และความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์ และในการระบุความเสี่ยงสามารถจำแนกข้อมูลเกี่ยวกับชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัย/สิ่งคุกคาม และผลกระทบ/ผู้ได้รับผลกระทบ โดยจะแสดงรายละเอียดต่าง ๆ ตามตารางด้านล่างดังนี้

ตารางแสดงรายละเอียดความเสี่ยง (Description of risk) แยกประเภทตามลักษณะของความเสี่ยงแต่ละด้าน

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
๑. ความเสี่ยงด้านระบบฐานข้อมูล ของ สศอ. ประกอบด้วย ฐานข้อมูลระบบเตือนภัยเศรษฐกิจอุตสาหกรรม, ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์, ฐานข้อมูลดัชนีอุตสาหกรรม เป็นต้น	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 - ช่องโหว่ของโปรแกรม เกิดจากไม่มีการอัพเดตระบบอย่างสม่ำเสมอ - โปรแกรมประยุกต์ติดต่อฐานข้อมูลไม่ได้ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์ อาจเกิดการติดไวรัส มัลแวร์ หรือเกิดช่องโหว่ที่นำไปสู่ความไม่ปลอดภัยทางไซเบอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ทดสอบช่องโหว่ของโปรแกรมประยุกต์ โดยกำหนดใน TOR ก่อนใช้งานระบบสารสนเทศ - อบรมผู้ใช้งานระบบสารสนเทศ - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - จัดทำแผนการบำรุงรักษา

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
					เครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - ตรวจสอบการทำงานของโปรแกรมอย่างละเอียด - ให้ผู้ดูแลระบบตรวจสอบโดยเร่งด่วน - ใช้ซอฟแวร์ถูกลิขสิทธิ์ - ไม่อนุญาตให้ผู้ใช้งานติดตั้งซอฟแวร์ด้วยตนเอง
๓. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่ Web Server, Mail Server, File Server, Database Server ระบบอินทราเน็ต, ระบบปริ้นท์เน็ตเวิร์ก	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	- การตั้งค่าอุปกรณ์ผิดพลาด - การทำงานผิดพลาดของอุปกรณ์ - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดต - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - สาย LAN ชำรุดเสียหาย - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- ปรับปรุงระบบเครื่องคอมพิวเตอร์แม่ข่าย - จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างสม่ำเสมอ - ถ่ายโอนระบบงาน สศอ. ไปสู่ระบบ Cloud
๔. ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเตอร์เน็ต, Domain Server, DNS	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์การทำงานมีความผิดพลาดของอุปกรณ์เครือข่ายหลักของเครือข่าย	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่าง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
Server, Firewall, Core Switch			ให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศใช้งาน Internet ไม่ได้	สม่ำเสมอ - ใช้โปรแกรมในการ scan ช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่าย - จัดซื้ออุปกรณ์ทดแทนเพื่อให้สามารถใช้ทดแทน และปฏิบัติงานได้ตามปกติ
๕. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์ส่วนบุคคล (PC) หรืออุปกรณ์ชำรุดเสียหายหรือเกิดขัดข้องทำให้ไม่สามารถทำงานได้ตามปกติ	- Hard disk ชำรุดเสียหาย เช่น Main board, Memory, Power Supply ชำรุดเสียหาย - Software ล้าสมัย - ความเสี่ยงจากภัยคุกคามต่าง ๆ เช่น ผู้ใช้งาน - ผู้ใช้งานไม่มีความรู้ในการใช้งานที่ถูกต้อง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนเพื่อสามารถปฏิบัติงานได้อย่างต่อเนื่อง - บำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - จัดทำคู่มือการใช้งานและจัดอบรมผู้ใช้งาน - ลงระบบปฏิบัติการ (OS) ให้พร้อมใช้งาน
๖. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	ความเสี่ยงด้านเทคนิค	ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถใช้งานได้	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive , Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัส และมีการตรวจสอบอย่างสม่ำเสมอและจัดทำรายงานประจำเดือน - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคาม

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
			- การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์		คอมพิวเตอร์
๗. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต - ข้อมูลหาย หรือมีการแก้ไขโดยไม่ทราบสาเหตุ - ผู้ใช้งานใช้งานไม่เหมาะสมและเกินความจำเป็น	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง และผู้ใช้ขาดความระมัดระวังในการใช้สารสนเทศ	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง
๘. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services/ DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการตั้งค่าของ Firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
		- คำสั่งเจตนาร้าย หรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ ไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย - File ที่ผู้ใช้บริการ Download มา มีการฝังไวรัสคอมพิวเตอร์ หรือคำสั่งอันตราย อันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS , Load Balancer - ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	ปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Load Balancer
๙. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์จากบุคคลภายใน - การลักทรัพย์จากบุคคลภายนอกที่เข้ามาโดยได้รับอนุญาตและไม่ได้รับอนุญาต - ระบบรักษาความปลอดภัยไม่รัดกุม เช่น กล้องวงจรปิดไม่เพียงพอ, เจ้าหน้าที่รักษาความปลอดภัยไม่รัดกุม	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งกล้องวงจรปิดเพิ่มในจุดที่อาจจะมีความเสี่ยง - กวดขันเจ้าหน้าที่รักษาความปลอดภัยให้รัดกุมมากขึ้น
๑๐. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา	- ไม่มีขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้บุคคลอื่นสามารถทำงานทดแทนได้ - การโยกย้ายของบุคลากรด้านคอมพิวเตอร์ - การพัฒนาอย่างรวดเร็วของ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล	- สรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสมและเพียงพอ - จัดทำคู่มือเพิ่มเติมกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ และจัดบุคลากรผู้รับผิดชอบหลักและ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
		และควบคุมดูแลระบบ	เทคโนโลยี	- ระบบสารสนเทศ	ผู้รับผิดชอบรองในกรณีที่ผู้รับผิดชอบหลักไม่สามารถมาปฏิบัติงานได้ - ถ่ายทอดองค์ความรู้ที่สำคัญของระบบงานให้กับเจ้าหน้าที่ใหม่หรือเจ้าหน้าที่รับช่วงงานต่ออย่างน้อย ๑ เดือนเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง
๑๑. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการ ได้ต่อเนื่องอย่างมีประสิทธิภาพ - ไม่สามารถปรับปรุง IT ให้มีประสิทธิภาพดีขึ้นได้	- งบประมาณที่ได้ของ สศอ. มีจำกัด	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- มีแผนการจัดซื้อระบบคอมพิวเตอร์เครือข่าย อุปกรณ์และ Software - ขอรับการจัดสรรงบประมาณในกรณีฉุกเฉิน
๑๒. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่ - ไฟฟ้าดับ - ไม่มีอุปกรณ์สำรองไฟฟ้าที่เพียงพอ - ไม่มีเครื่องกำเนิดไฟฟ้า (เครื่องปั่นไฟฟ้า) เมื่อไฟฟ้าดับเกินระยะเวลาที่กำหนด - เกิดอุบัติเหตุกับสายส่งไฟฟ้า	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดหาเครื่องสำรองไฟฟ้าเพิ่มเติม เช่น เครื่องปั่นไฟฟ้า เครื่องกำเนิดไฟฟ้าสำรอง - บำรุงรักษาเครื่องสำรองไฟฟ้าเมื่อครบกำหนดตามระยะเวลาอย่างสม่ำเสมอ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	แนวทางการแก้ไขปัญหา
๑๓.					- แผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)
๑๔. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การชุมนุมประท้วง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร , การวางเพลิง - ภัยธรรมชาติต่าง ๆ เช่น แผ่นดินไหว , น้ำท่วม - การปิดล้อมสถานที่ราชการ กรณีเกิดการชุมนุมประท้วงทางการเมือง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- มีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) - จัดทำระบบสำรองข้อมูล เช่น สำรองระบบข้อมูลบน Cloud - จัดทำ Data Center สำรองขนาดเล็ก (DR Site) โดยให้อยู่สถานที่อื่น และสามารถใช้ทดแทนได้ ในกรณีที่ Data Center หลักไม่สามารถใช้งานได้
๑๕. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Hard Disk สม่ำเสมอ

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

๑.๕.๔ การประมาณค่าความเสี่ยง (Risk Estimation)

การประมาณค่าความเสี่ยงเป็นการพิจารณาปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งสำนักงานเศรษฐกิจอุตสาหกรรมใช้เกณฑ์ดังนี้

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

การประมาณค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ระดับโอกาสที่เกิด	ความรุนแรง
๑. ความเสี่ยงด้านระบบฐานข้อมูล ของ สศอ. ประกอบด้วย ฐานข้อมูลระบบเตือนภัยเศรษฐกิจอุตสาหกรรม, ฐานข้อมูลระบบสาร-บรรณอิเล็กทรอนิกส์, ฐานข้อมูลดัชนีอุตสาหกรรม เป็นต้น	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ ไม่ว่าจะเป็นฐานข้อมูลหลักเสียหาย ข้อมูลถูกทำลาย การโจรกรรมข้อมูลที่สำคัญ การลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	- ความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	๕	๒
๒.ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	- การทำงานผิดพลาดของโปรแกรม - ช่องโหว่ของโปรแกรม เกิดจากไม่มีการอัพเดตระบบอย่างสม่ำเสมอ - โปรแกรมประยุกต์ติดต่อฐานข้อมูลไม่ได้ - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - การใช้โปรแกรมไม่ถูกลิขสิทธิ์ อาจเกิดการติดไวรัส มัลแวร์ หรือเกิดช่องโหว่ที่นำไปสู่ความไม่ปลอดภัยทางไซเบอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	๕	๑

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ระดับโอกาสที่เกิด	ความรุนแรง
๓. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการกับ user ทั้งภายในและภายนอก เช่น Web Server, Mail Server, File Server, Database Server, ระบบอินทราเน็ต, ระบบปริ้นท์เน็ตเวิร์ก	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	- การตั้งค่าอุปกรณ์ผิดพลาด - การทำงานผิดพลาดของอุปกรณ์ - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดต - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - สาย LAN ชำรุดเสียหาย - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๕	๓
๔. ความเสี่ยงด้านระบบเครือข่าย เช่น ระบบเครือข่ายอินเตอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์การทำงานมีความผิดพลาดของอุปกรณ์เครือข่ายหลักของเครือข่าย	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศใช้งาน Internet ไม่ได้	๕	๑
๕. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้อง ไม่	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากความเสื่อมสภาพของเครื่อง	เครื่องคอมพิวเตอร์ส่วนบุคคล (PC) หรืออุปกรณ์ชำรุดเสียหายหรือเกิดขัดข้อง ทำให้ไม่สามารถทำงานได้ตามปกติ	- Hard disk ชำรุดเสียหาย เช่น Main board, Memory, Power Supply ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์	๕	๒

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ระดับโอกาสที่เกิด	ความรุนแรง
สามารถทำงานได้ตามปกติ	คอมพิวเตอร์		- Software ล้าสมัย - ความเสี่ยงจากภัยคุกคามต่าง ๆ เช่น ผู้ใช้งาน - ผู้ใช้งานไม่มีความรู้ในการใช้งานที่ถูกต้อง	แม่ข่าย - อุปกรณ์เครือข่าย		
๖. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	ความเสี่ยงด้านเทคนิค	ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถใช้งานได้	- 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	๕	๕
๗. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต - ข้อมูลหาย หรือมีการแก้ไขโดยไม่ทราบสาเหตุ	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งาแทน - ผู้ใช้งานเกินความจำเป็น เช่น - ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้	๕	๑

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ระดับโอกาสที่เกิด	ความรุนแรง
			Bandwidth สูง และผู้ใช้ขาดความระมัดระวังในการใช้งานสารสนเทศ			
๘. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services/ DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้าย หรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ ไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย - File ที่ผู้ใช้บริการ Download มา มีการฝังไวรัสคอมพิวเตอร์ หรือคำสั่งอันตราย อันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS , Load Balancer - ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๕
๙. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์จากบุคคลภายใน - การลักทรัพย์จากบุคคลภายนอกที่เข้ามาโดยได้รับอนุญาตและไม่ได้รับอนุญาต - ระบบรักษาความปลอดภัยไม่รัดกุม เช่น กล้องวงจรปิดไม่เพียงพอ,เจ้าหน้าที่รักษาความปลอดภัยไม่รัดกุม	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย	๑	๓

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ระดับโอกาสที่เกิด	ความรุนแรง
๑๐. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- ไม่มีขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้บุคคลอื่นสามารถทำงานทดแทนได้ - การโยกย้ายของบุคลากรด้านคอมพิวเตอร์ - การพัฒนาอย่างรวดเร็วของเทคโนโลยี	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๓
๑๑. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการ ได้ต่อเนื่องอย่างมีประสิทธิภาพ และไม่สามารถพัฒนาหรือปรับปรุงระบบสารสนเทศให้ดีขึ้นได้	- งบประมาณที่ได้ของ สศอ. มีจำกัด	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๓	๓
๑๒. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่ - ไฟฟ้าดับ - ไม่มีอุปกรณ์สำรองไฟฟ้าที่เพียงพอ - ไม่มีเครื่องกำเนิดไฟฟ้า (เครื่องปั่นไฟฟ้า) เมื่อไฟฟ้าดับเกินระยะเวลาที่กำหนด - เกิดอุบัติเหตุกับสายส่งไฟฟ้า	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๓
๑๓. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหาย	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติต่าง ๆ เช่น	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์	๕	๓

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ระดับโอกาสที่เกิด	ความรุนแรง
การชุมนุมประท้วง		ทั้งหมด	แผ่นดินไหว , น้ำท่วม - การปิดล้อมสถานที่ราชการ กรณีเกิดการชุมนุมประท้วงทางการเมือง	แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ		
๑๔. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูล ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๕
๑๕. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	๑	๕

๑.๕.๕ การประเมินค่าความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

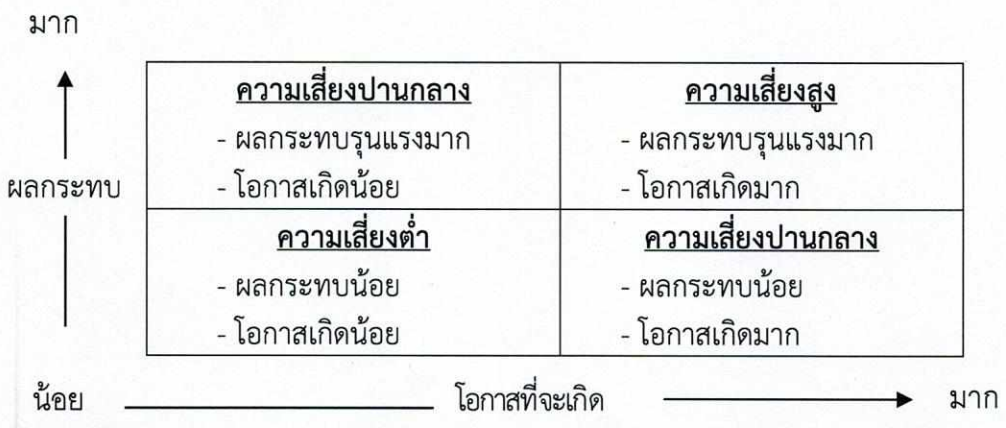
ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ

ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

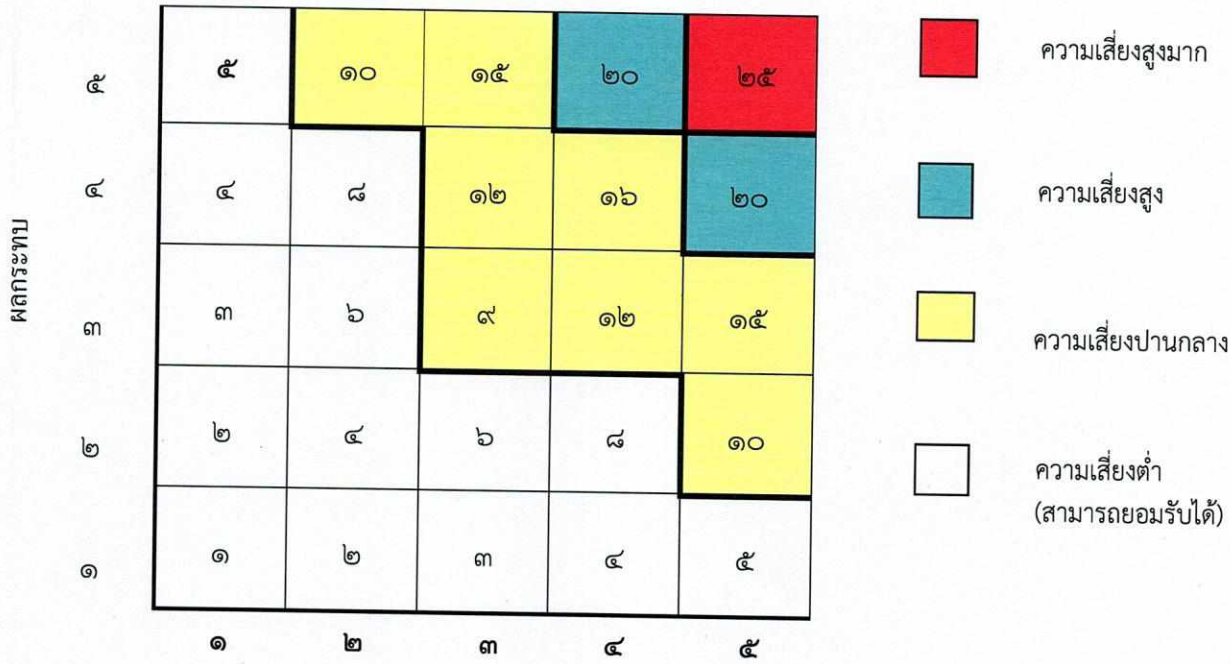
ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ – ๘	ต่ำ	ยอมรับความเสี่ยง (มีแผนรองรับ)	ขาว
๙ – ๑๖	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗ – ๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



การประเมินความเสี่ยง



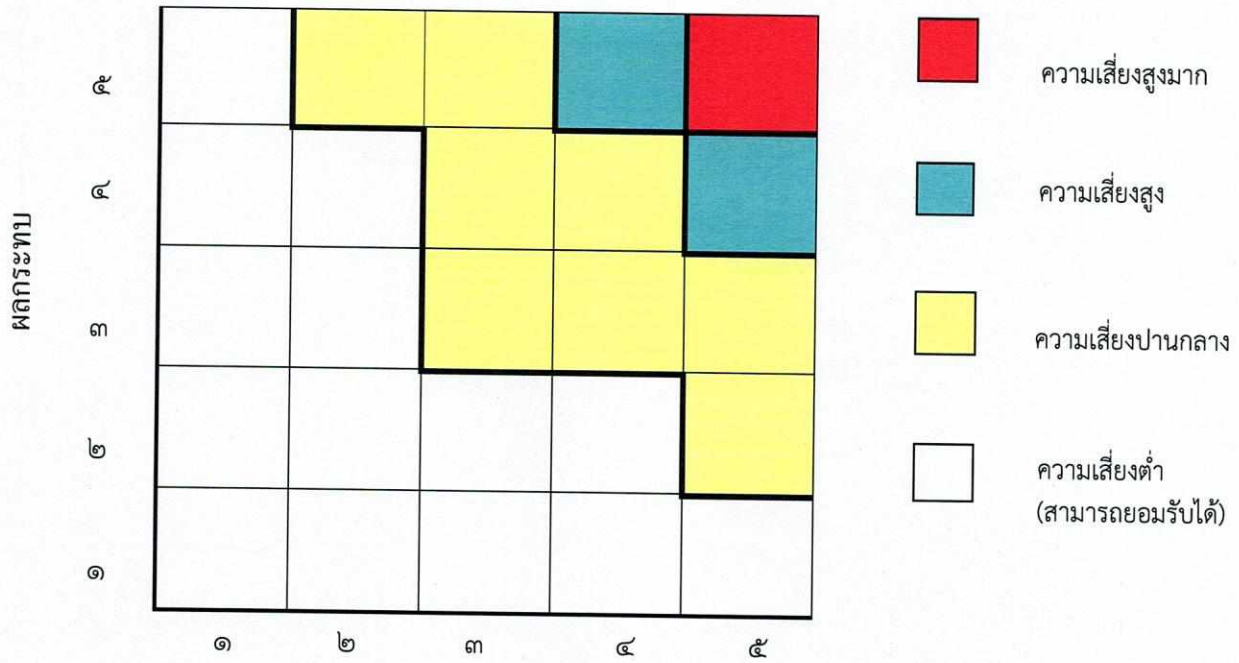
การประเมินค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงด้านระบบฐานข้อมูลของ สศอ. ประกอบด้วย ฐานข้อมูลระบบเตือนภัยเศรษฐกิจอุตสาหกรรม, ฐานข้อมูลระบบสาร-บรรณอิเล็กทรอนิกส์,ฐานข้อมูลดัชนีอุตสาหกรรม เป็นต้น	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ ไม่ว่าจะเป็นฐานข้อมูลหลักเสียหาย ข้อมูลถูกทำลาย การโจรกรรมข้อมูลที่สำคัญ การลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	๕	๒	๑๐
๒. ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรมช่องโหว่ของโปรแกรม	๕	๑	๕
๓. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการกับ User ทั้ง	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	๕	๒	๑๐

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
ภายในและภายนอก เช่น Web Server, Mail Server, File Server, Database Server, ระบบอินทราเน็ต, ระบบ ปริ้นท์เน็ตเวิร์ก					
๔. ความเสี่ยงด้านระบบเครือข่าย เช่น ระบบเครือข่ายอินเตอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์การทำงานมีความผิดพลาดของอุปกรณ์เครือข่ายหลักของเครือข่าย	๕	๑	๕
๕. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์ส่วนบุคคล (PC) หรืออุปกรณ์ชำรุดเสียหายหรือเกิดขัดข้อง ทำให้ไม่สามารถทำงานได้ตามปกติ	๕	๒	๑๐
๖. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์ทางไซเบอร์	ความเสี่ยงด้านเทคนิค	ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลงไม่สามารถใช้งานได้	๕	๕	๒๕
๗. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต - ข้อมูลหาย หรือมีการแก้ไขโดยไม่ทราบสาเหตุ - ผู้ใช้งานใช้งานไม่เหมาะสมและเกินความจำเป็น	๕	๑	๕
๘. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services/ DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้าย หรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย - File ที่ผู้ใช้บริการ Download มีการฝังไวรัสคอมพิวเตอร์ หรือคำสั่งอันตราย	๑	๕	๕

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
		อันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี			
๙. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์	๑	๓	๓
๑๐. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๑	๓	๓
๑๑. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	- การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการ ได้ต่อเนื่องอย่างมีประสิทธิภาพ - ไม่สามารถปรับปรุง IT ให้มีประสิทธิภาพดีขึ้นได้	๓	๓	๙
๑๒. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	๑	๓	๓
๑๓. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๕	๓	๑๕
๑๔. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	๑	๕	๑๐
๑๕. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	๑	๕	๕

<u>แผนภูมิความเสี่ยง</u>



๑.๕.๖ การรายงานผลการวิเคราะห์ความเสี่ยง (Risk Reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถใช้งานได้	๒๕
๒	ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ เช่น Web Server, Mail Server, File Server, Database Server, ระบบอินทราเน็ต , ระบบปริ้นท์เน็ตเวิร์ก	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้	๑๕
๓	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การประท้วง และภัยพิบัติอื่นๆ	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๑๕
๔	ความเสี่ยงด้านระบบฐานข้อมูลของ สศอ. ประกอบด้วย ฐานข้อมูลระบบเตือนภัยเศรษฐกิจอุตสาหกรรม, ฐานข้อมูล	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ ไม่ว่าจะเป็นฐานข้อมูลหลักเสียหาย ข้อมูลถูกทำลาย การโจรกรรมข้อมูลที่สำคัญ การลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	๑๐

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
	ระบบสาร-บรรณอิเล็กทรอนิกส์,ฐานข้อมูลดัชนีอุตสาหกรรม เป็นต้น			
๕	ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากความเสื่อมสภาพของเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์ส่วนบุคคล (PC) หรืออุปกรณ์ชำรุดเสียหายหรือเกิดขัดข้อง ทำให้ไม่สามารถทำงานได้ตามปกติ	๑๐
๖	ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการ ได้ต่อเนื่องอย่างมีประสิทธิภาพ และไม่สามารถพัฒนาหรือปรับปรุงระบบสารสนเทศให้ดีขึ้นได้	๙
๗	ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดกับโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	๕
๘	ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเตอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์การทำงานมีความผิดพลาดของอุปกรณ์เครือข่ายหลักของเครือข่าย	๕
๙	ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	๕
๑๐	ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	๕
๑๑	ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต - ข้อมูลหาย หรือมีการแก้ไขโดยไม่ทราบสาเหตุ ผู้ใช้งานใช้งานไม่เหมาะสมและเกินความจำเป็น	๕
๑๒	ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (Denial of Services/ DOS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้าย หรือไฟล์ Auto run อยู่ในเครื่อง - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ - ไวรัส/เวิร์ม เข้ามาสู่ระบบเครือข่าย - File ที่ผู้ใช้บริการ Download มา มีการฝัง	๕

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
			- ไวรัสคอมพิวเตอร์ หรือคำสั่งอันตราย อันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	
๑๓	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากการปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ RAM ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๓
๑๔	ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๓
๑๕	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายอาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	๓

๑.๕.๗ การจัดการความเสี่ยง

จากนโยบายของสำนักงานเศรษฐกิจอุตสาหกรรม ระดับความเสี่ยงที่ยอมรับได้ ≤ ๑๕ โดยกำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูงตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑	ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์ทางไซเบอร์	๒๕	- มีแผนรองรับความเสี่ยง	- ติดตั้งระบบป้องกันไวรัส และมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ
๒	ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ ได้แก่ Web Server, Mail Server, File Server, Database Server, ระบบอินทราเน็ต, ระบบปริ้นท์เน็ตเวิร์ก	๑๕	- มีแผนรองรับความเสี่ยง	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน เพื่อสามารถปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่อง คอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๓	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การประท้วง และภัยพิบัติอื่น ๆ	๑๕	- มีแผนรองรับความเสี่ยง	- มีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
๔	ความเสี่ยงด้านระบบฐานข้อมูลของ สศอ. ประกอบด้วย ฐานข้อมูลระบบเตือนภัยเศรษฐกิจอุตสาหกรรม, ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์,ฐานข้อมูลดัชนีอุตสาหกรรม เป็นต้น	๑๐	- มีแผนรองรับความเสี่ยง	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - จัดเก็บข้อมูลไว้บนระบบ Cloud
๕	ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๑๐	- มีแผนรองรับความเสี่ยง	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนเพื่อสามารถปฏิบัติงานได้อย่างต่อเนื่อง - บำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอตลอดจนจัดอบรมผู้ใช้งาน - จัดทำคู่มือการใช้งานลงระบบปฏิบัติการ (OS) ให้พร้อมใช้งาน
๖	ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๙	- มีแผนรองรับความเสี่ยง	- ขอรับงบประมาณในกรณีฉุกเฉิน - จัดทำแผนรองรับความต้องการใช้งานล่วงหน้าให้ทันท่วงที - นำเสนอแผนให้ผู้บริหารรับรู้
๗	ความเสี่ยงด้านโปรแกรมประยุกต์ เช่น การทำงานผิดพลาดของโปรแกรม ช่องโหว่ของโปรแกรม	๕	- มีแผนรองรับความเสี่ยง	- จัดทำแผนการบำรุงรักษาเครื่อง คอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - ตรวจสอบการทำงานของโปรแกรมอย่างละเอียด - ให้ผู้ดูแลระบบตรวจสอบโดยเร่งด่วน
๘	ความเสี่ยงด้านระบบเครือข่าย ได้แก่ ระบบเครือข่ายอินเตอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	๕	- มีแผนรองรับความเสี่ยง	- บำรุงรักษาระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ - มีแผนจัดซื้ออุปกรณ์ทดแทนอุปกรณ์ที่หมดสภาพเพื่อให้สามารถใช้งานได้ตามปกติ
๙	ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ	๕	- มีแผนรองรับความเสี่ยง	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่อง ระบบสำรองข้อมูล

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
				อย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Hard Disk สม่ำเสมอ
๑๐	ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	๕	- มีแผนรองรับความเสี่ยง	- ปรับปรุงระบบเครื่องคอมพิวเตอร์ แม่ข่าย - จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่อง คอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างสม่ำเสมอ - ถ่ายโอนระบบงาน สศอ. ไปสู่ระบบ Cloud
๑๑	ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	๕	- มีแผนรองรับความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง
๑๒	ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	๕	- มีแผนรองรับความเสี่ยง	- นำระบบงานที่สำคัญเข้าสู่ระบบ VM เพื่อเพิ่มประสิทธิภาพในการ Backup และ Restore หากเกิดเหตุการบุกรุกโดยผู้ไม่ประสงค์ดี - ตรวจสอบและปรับปรุงการตั้งค่าของ firewall อย่างสม่ำเสมอ - ปรับปรุงระบบตรวจสอบการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
๑๓	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๓	- มีแผนรองรับความเสี่ยง	- มีการจัดเวรยามรักษาความปลอดภัยของสำนักงาน - ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจสอบการทำงานของกล้องวงจรปิดภายในอาคาร - ตรวจสอบระบบป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพใช้งานได้ปกติ - สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้าน

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
				ความมั่นคงปลอดภัยสารสนเทศ กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง
๑๔	ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๓	- มีแผนรองรับความเสี่ยง	- สรรหาบุคลากรทดแทนตำแหน่งว่าง - จัดทำคู่มือเพิ่มเติมกระบวนการทำงานเพื่อให้บุคลากรอื่น - สามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ - ถ่ายทอดองค์ความรู้ที่สำคัญของระบบงานให้กับเจ้าหน้าที่ใหม่หรือเจ้าหน้าที่รับช่วงงานต่ออย่างน้อย ๑ เดือน
๑๕	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๓	- มีแผนรองรับความเสี่ยง	- มีแผนจัดหาเครื่องกำเนิดไฟฟ้า - จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - แผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)

๑.๖ เจ้าหน้าที่ผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยง

เพื่อให้การดำเนินงานตามแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ เป็นไปอย่างรวดเร็วทันต่อการดำเนินการ จึงกำหนดให้เจ้าหน้าที่ต่อไปนี้ เป็นผู้รับผิดชอบดำเนินการจัดการความเสี่ยงที่เกิดขึ้น

๑.๖.๑ ให้กลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดำเนินการ

๑.๖.๒ ให้ผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม กำกับดูแลควบคุมการดำเนินการ

ส่วนที่ ๒
แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบสารสนเทศ
(IT Contingency Plan)

ส่วนที่ ๒
แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบสารสนเทศ
(IT Contingency Plan)

ในส่วนที่ ๒ ของแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ จะประกอบด้วยรายละเอียดเกี่ยวกับแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) ดังนี้

๒.๑ แผนรองรับสถานการณ์ฉุกเฉิน แบ่งออกเป็น ๔ สถานการณ์ คือ

๒.๑.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

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

๒.๑.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ

๑) กรณีไฟไหม้
๒) กรณีน้ำท่วม
๓) กรณีแผ่นดินไหว

๒.๑.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด

๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้
๒) กรณีหลังเหตุการณ์ความไม่สงบ

๒.๑.๔ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

๑) กรณีโจรกรรม
๒) กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

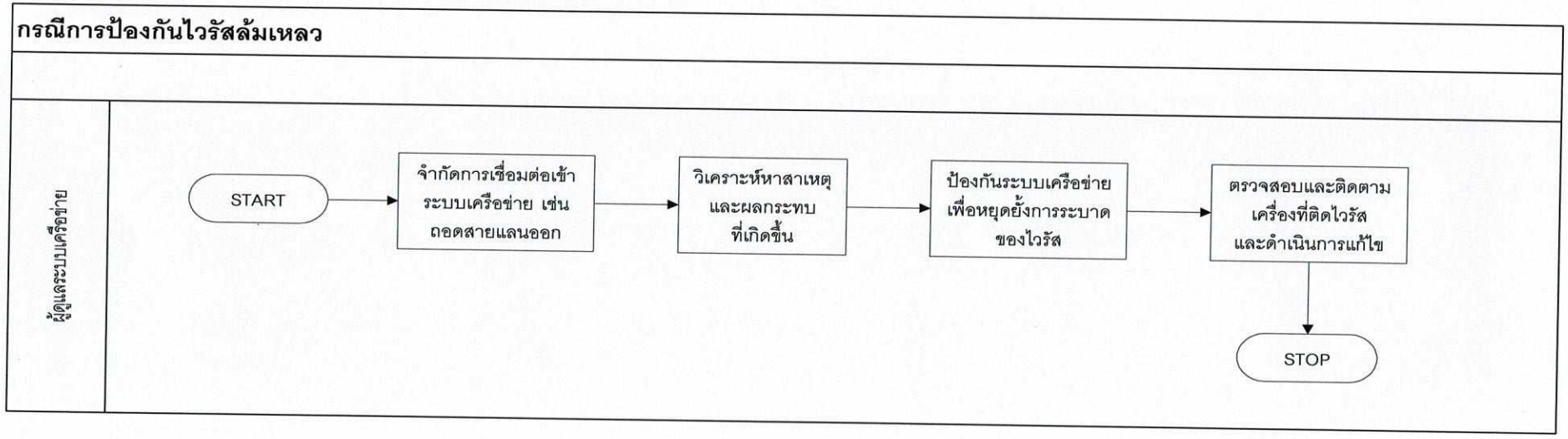
๒.๑ แผนรองรับสถานการณ์ฉุกเฉิน

๒.๑.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๑) กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรมทราบ หรือกรณีมีเหตุอันทำให้กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรมไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรมจะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

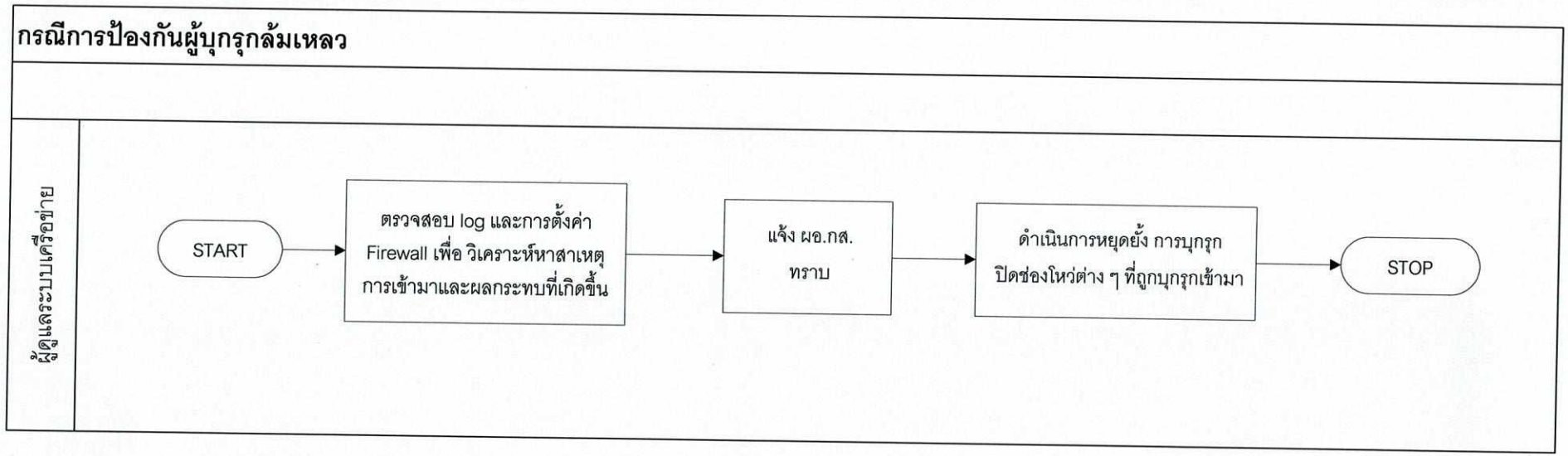
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



๒) กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log file และตรวจสอบการตั้งค่าของ Firewall
- ผู้ดูแลระบบแจ้งผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรมให้ทราบโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

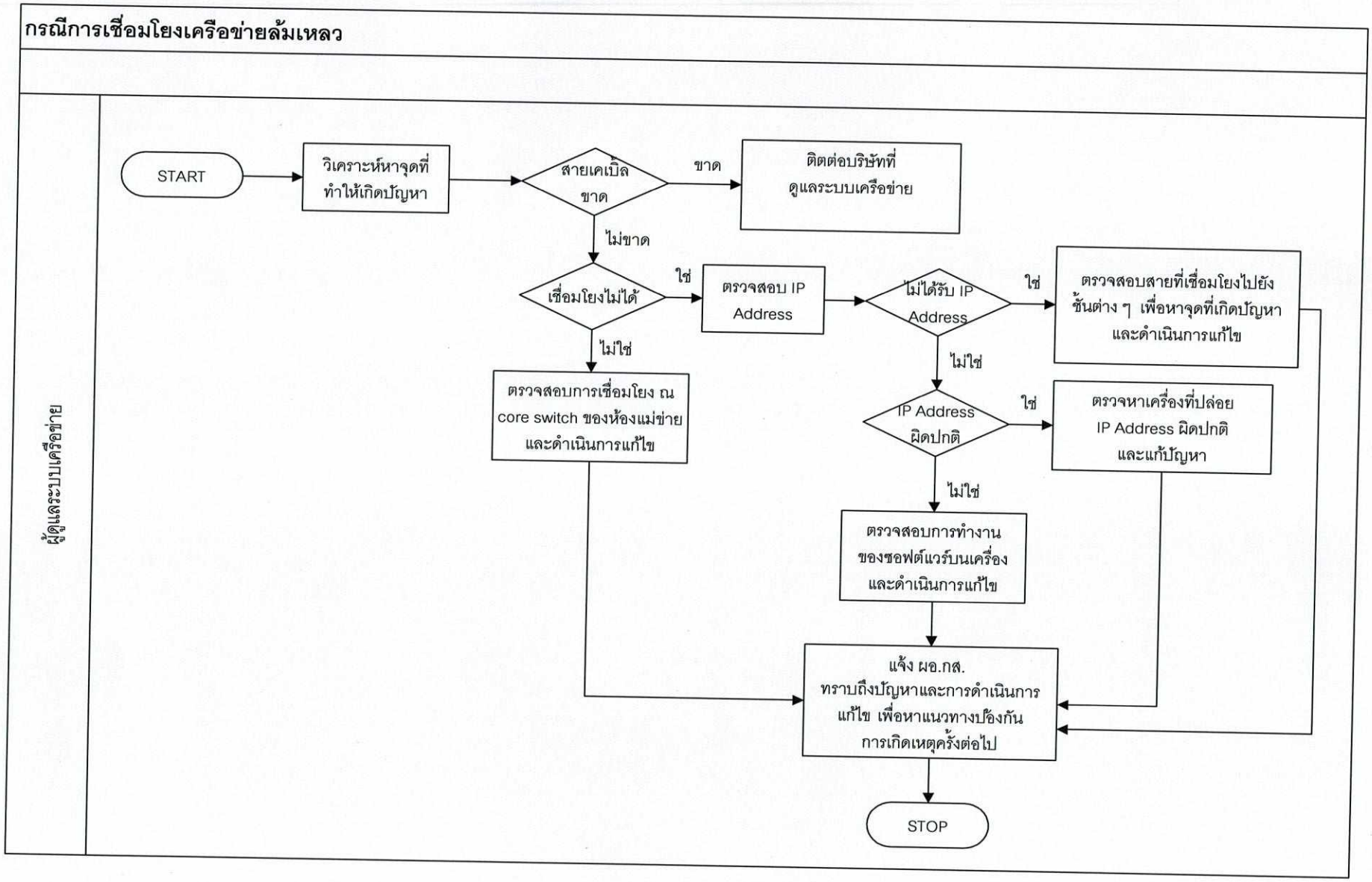
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



๓) กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้ ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อของแต่ละชั้นภายในอาคาร

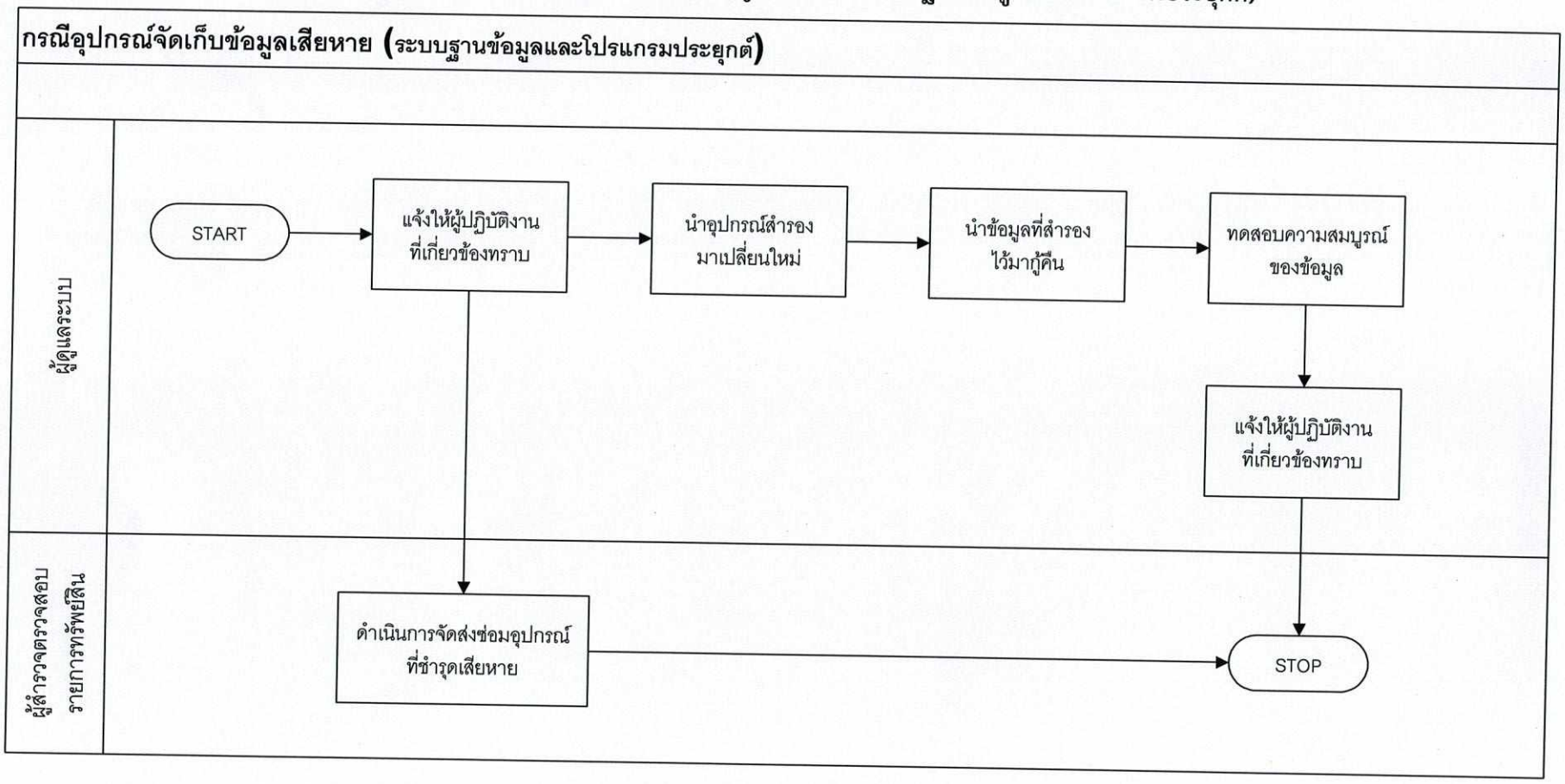
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



๔) กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

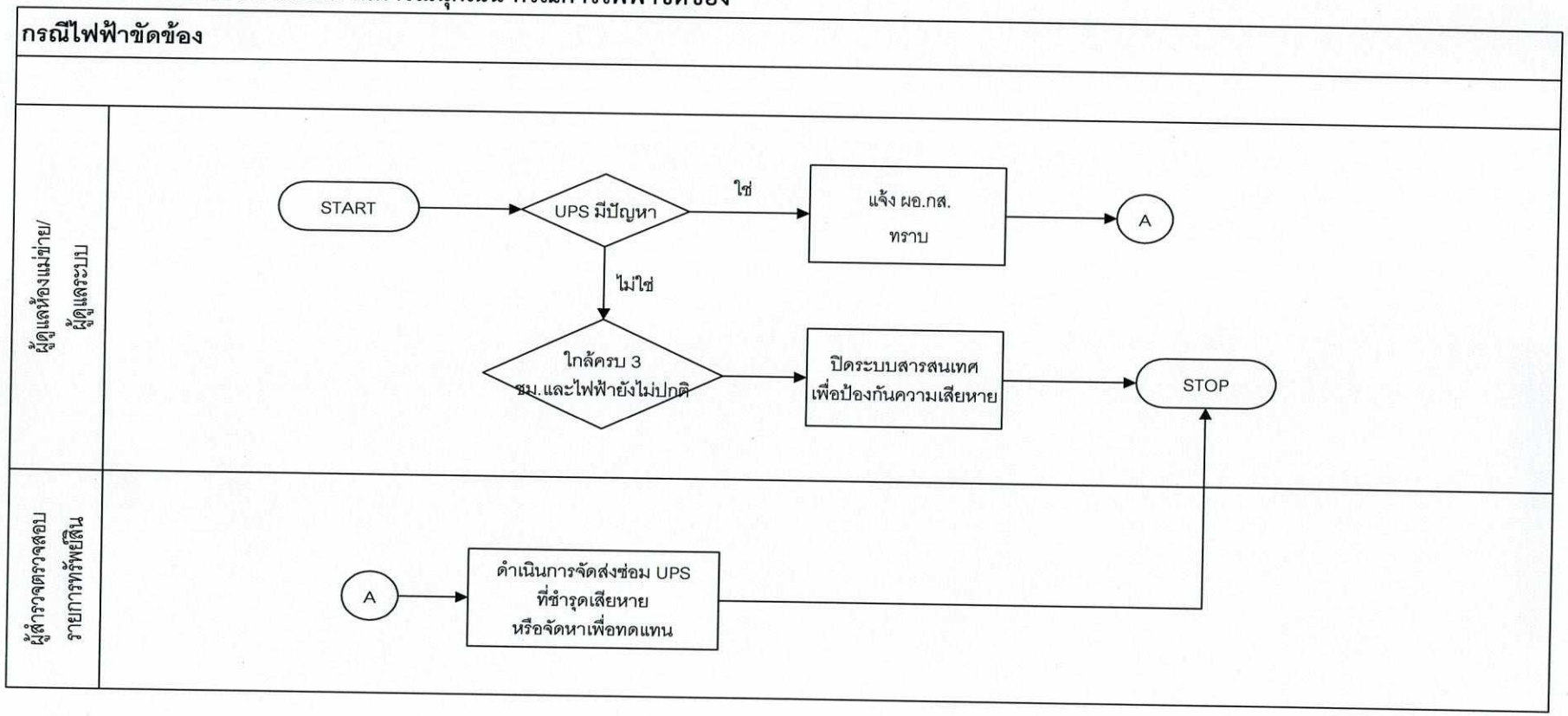
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)



๕) กรณีไฟฟ้าขัดข้อง

- ระบบฐานข้อมูลสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ ๓ ชั่วโมง
- หากใกล้ครบ ๓ ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม (ผอ.กส.)
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

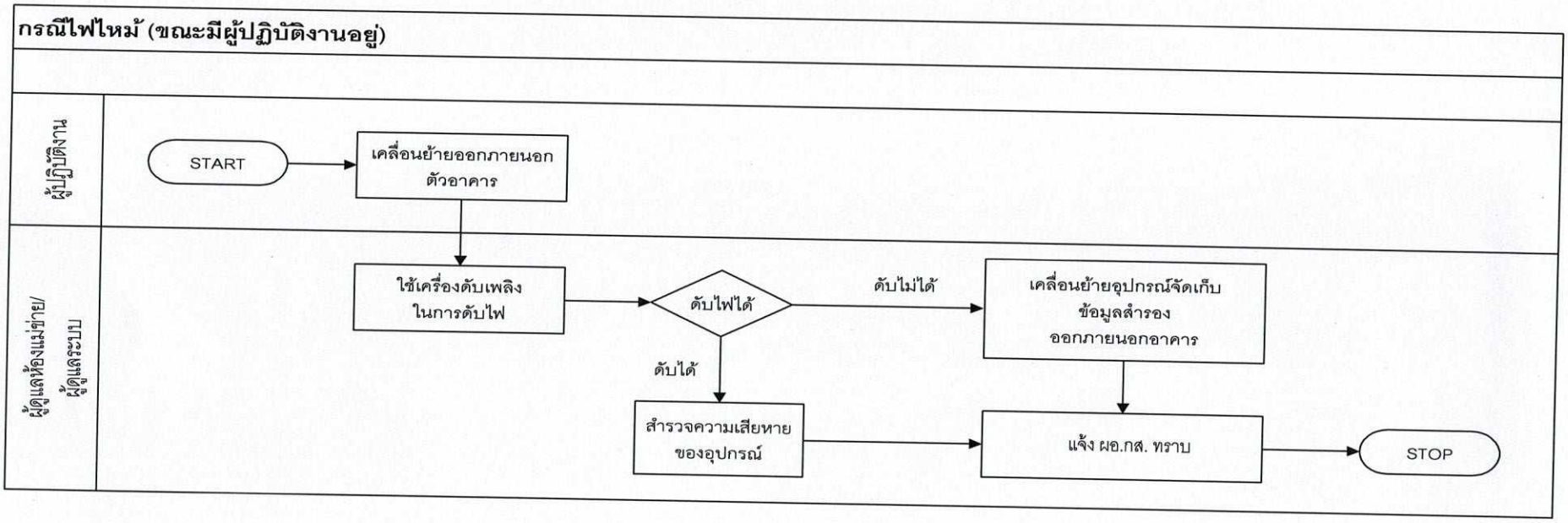


๒.๑.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ

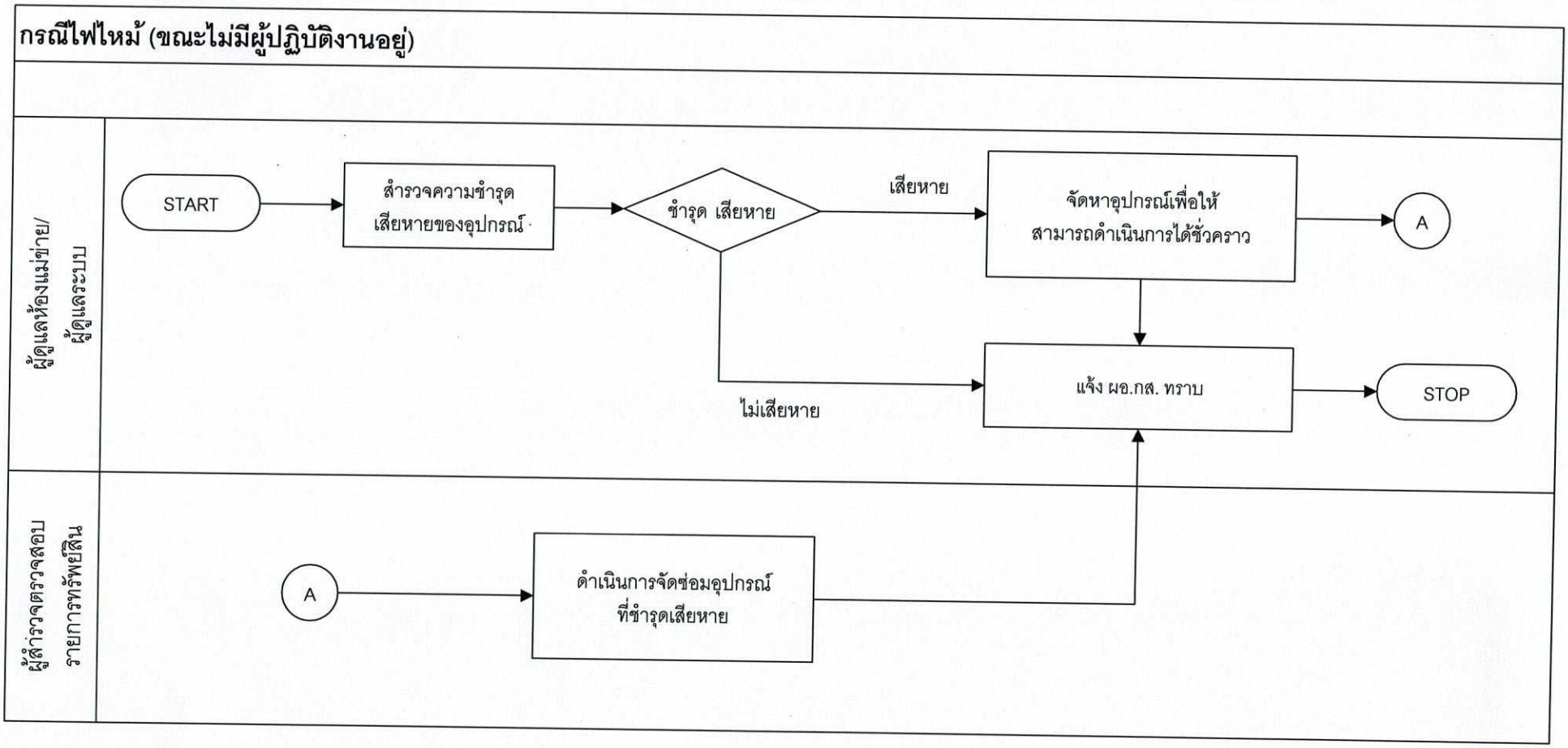
๑) กรณีไฟไหม้ แยกเป็น ๒ กรณี คือ กรณีไฟไหม้ขณะมีผู้ปฏิบัติงานอยู่ และกรณีไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงานอยู่

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานกับผู้ที่เกี่ยวข้องให้รีบดำเนินการแก้ไขอย่างเร่งด่วน
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

กรณีที่ ๑ แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



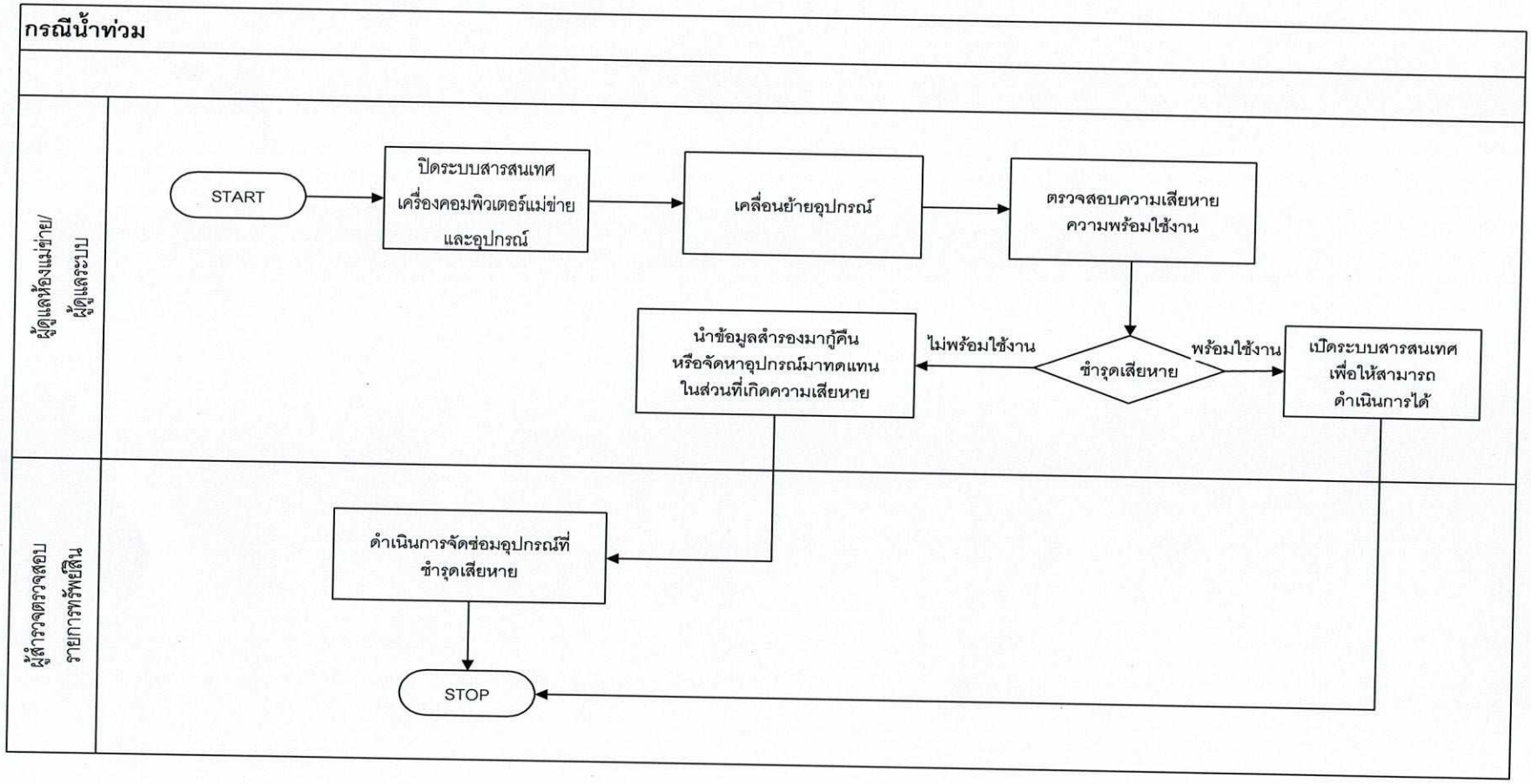
กรณีที่ ๒ แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)



๒) กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

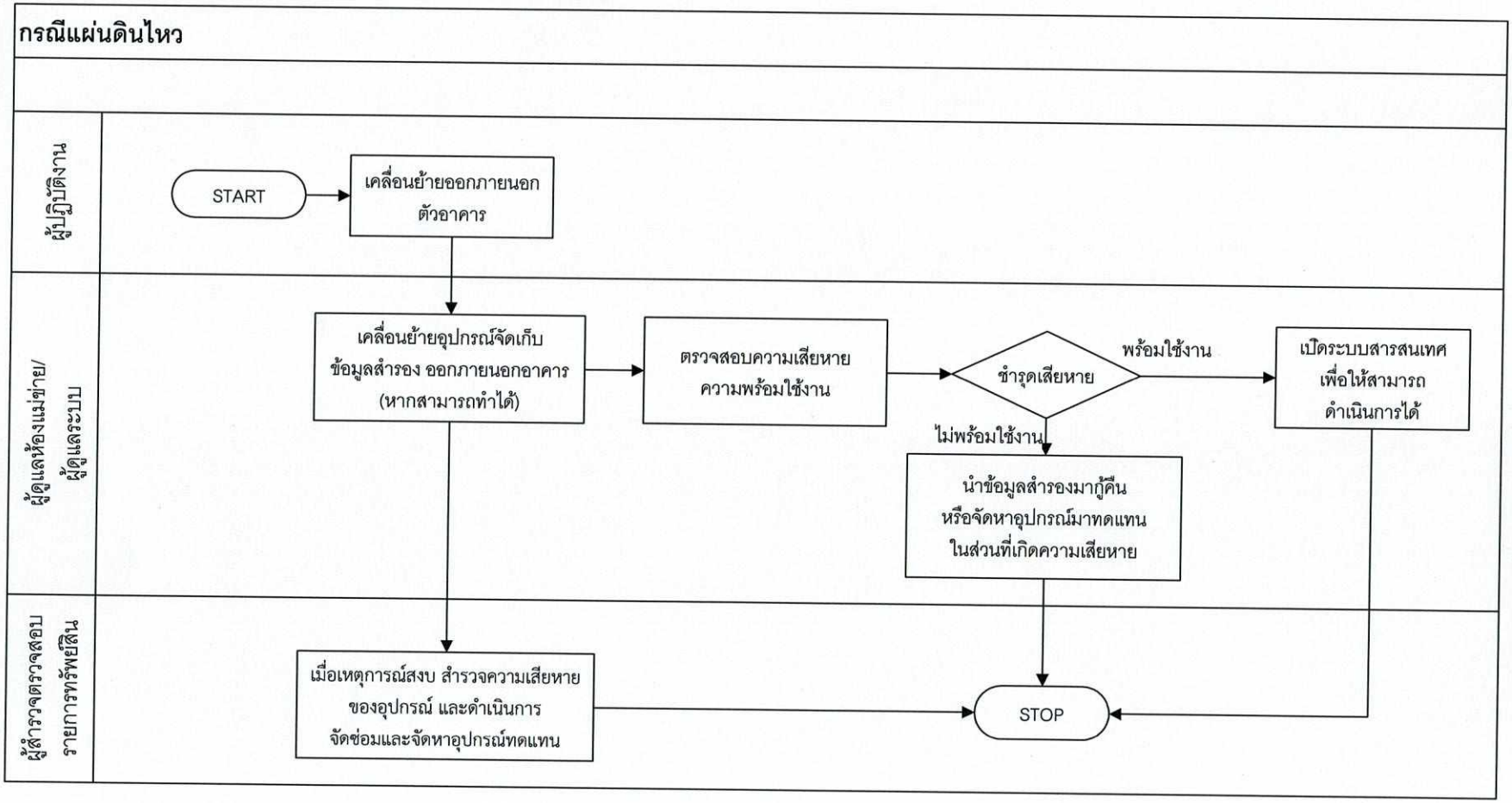
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม



๓) กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

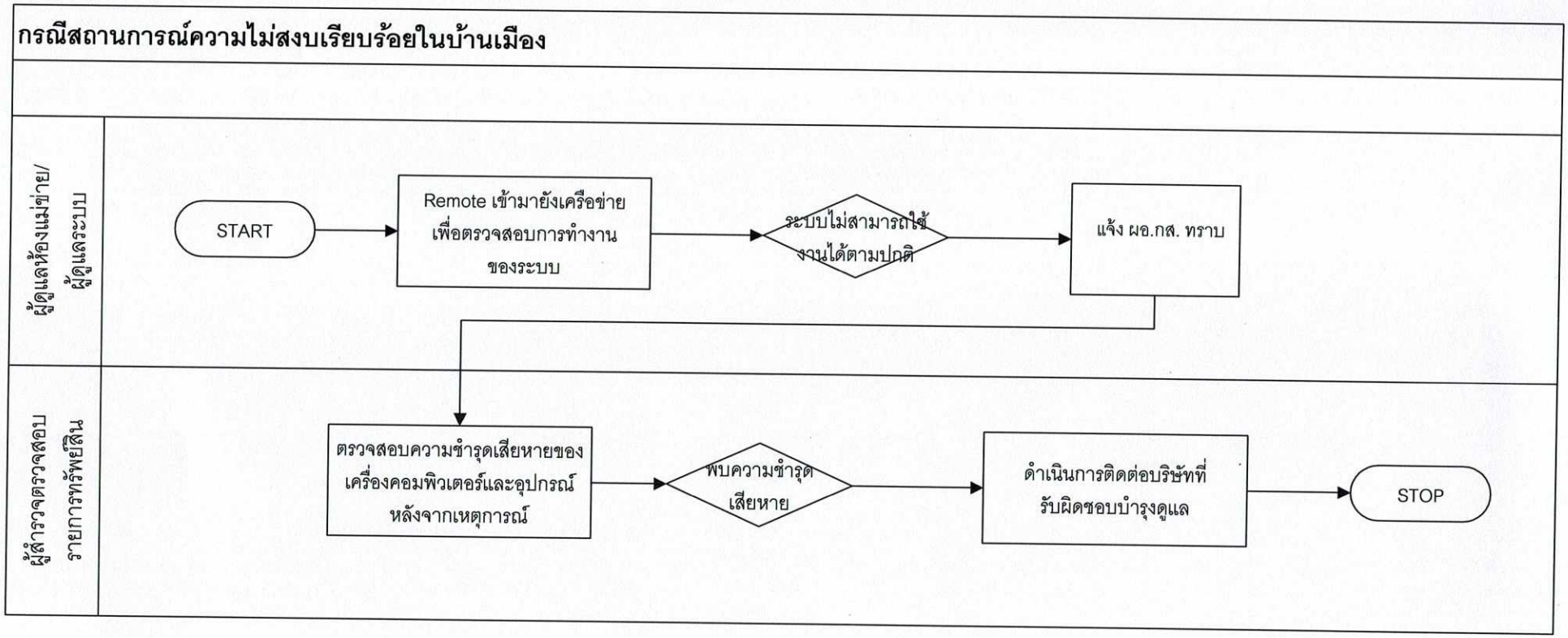


๒.๑.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด

สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรมทราบ
- กรณีหลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด

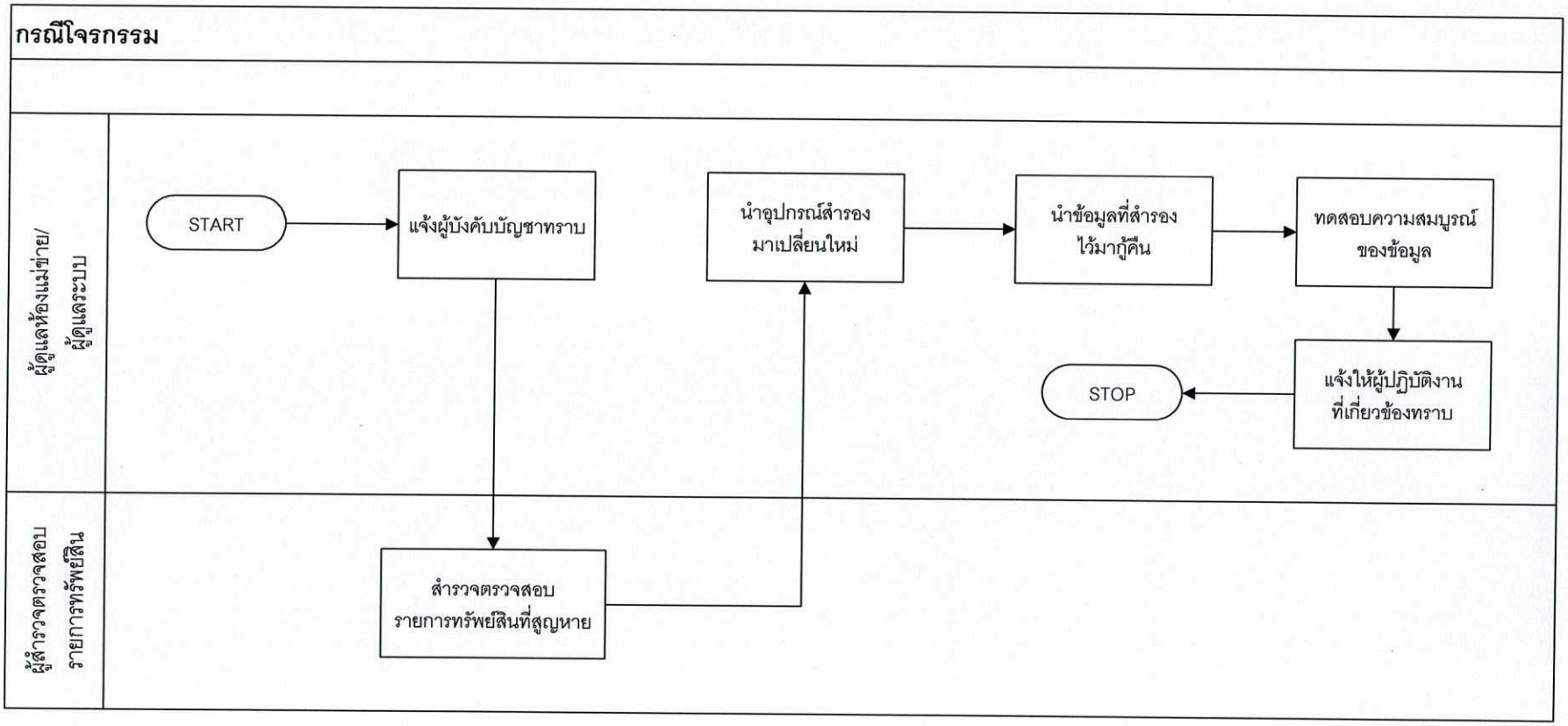


๒.๑.๔ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

๑) กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

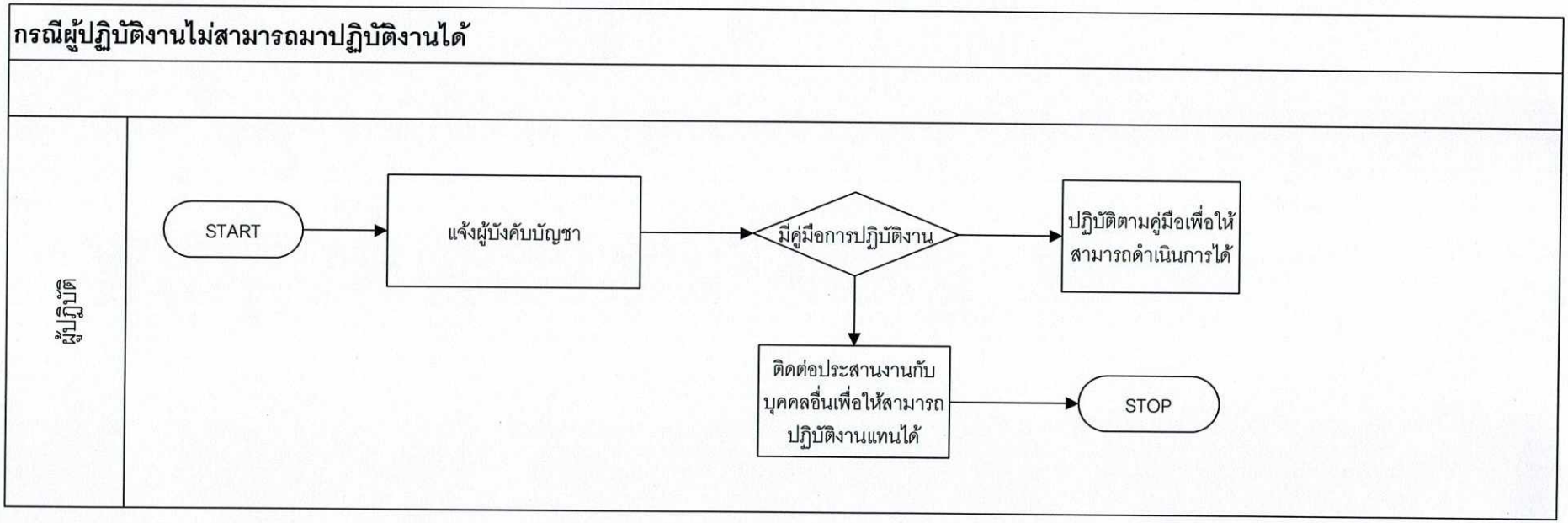
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



๒) กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

- แจ้งผู้บังคับบัญชาทราบ
- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



๒.๒ การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เป็นดังนี้

๒.๒.๑ ผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบปฏิบัติงาน ได้แก่

๒.๒.๑.๑ รองผู้อำนวยการสำนักงานเศรษฐกิจอุตสาหกรรม ที่ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ประจำสำนักงานเศรษฐกิจอุตสาหกรรม

๒.๒.๑.๒ นางสาวณิรดา วิสุทธิชาติธาดา ดำรงตำแหน่งผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม

๒.๒.๒ ผู้รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย (Server room) คือ

นายสมชาย จำปาทอง นักวิชาการคอมพิวเตอร์ชำนาญการ

นางสาวณัฐวดี โพธิ์กะสังข์ นักวิชาการคอมพิวเตอร์ชำนาญการ

นายอานันท์ กรุดเนียม นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายวัฒนา อุไกรหงสา นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๒.๒.๓ ผู้รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน คือ

นางสาวทิพาพร ยิ้มวิลัย นักวิชาการการเงินและบัญชีชำนาญการพิเศษ

จากแผนผังแสดงขั้นตอนการรองรับสถานการณ์ฉุกเฉินในกรณีต่าง ๆ รวม ๔ สถานการณ์ ได้แก่ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องทางด้านเทคนิค สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง และสถานการณ์ฉุกเฉินที่เกิดจากบุคคล ดังที่กล่าวแล้วข้างต้น สามารถนำมาจำแนกข้อมูล ซึ่งประกอบด้วยระบบต่าง ๆ หน้าที่/กิจกรรม การแก้ไขปัญหา และผู้รับผิดชอบ โดยจะแสดงรายละเอียดตามตารางด้านล่าง ดังนี้

๒.๓ ตารางแสดงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนที่เกิดจากความขัดข้องด้านเทคนิค

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
๒.๓.๑ ระบบ Firewall เป็น Hardware Firewall รุ่น Fortigate 600D ใช้เป็นระบบป้องกันข้อมูลเครือข่าย	๑) ติดตั้งระบบ Firewall ในเครือข่ายสำนักงานเศรษฐกิจอุตสาหกรรม ๒) กำหนดสิทธิ์ผู้ใช้ระบบเพื่อการบริหารจัดการ ๓) อบรมผู้ดูแลระบบเกี่ยวกับเทคโนโลยีการรักษาความปลอดภัย ๔) จัดทำคู่มือการใช้งานระบบ และ Configuration ทั้งหมด ๕) ทำการ Backup Configuration ของระบบ	๑) Restore ระบบ Firewall จากที่ได้ Backup ไว้ ๒) กำหนด Configuration ใหม่ของ Firewall ตามคู่มือที่ได้จัดทำไว้	นายสมชาย จำปาทอง นางสาวณัฐวดี โพธิ์กะสังข์ นายอานันท์ กรุดเนียม นายวัฒนา อุไกรหงสา
๒.๓.๒ ระบบปฏิบัติการ	ระบบปฏิบัติการ ๑) ได้ทำการตรวจสอบและติดตั้ง Patch ใหม่ ๆ เพื่อทำให้ระบบปฏิบัติการมีความเสถียรภาพและความปลอดภัย ๒) ทำการ Backup	๑) Restore ระบบปฏิบัติการตามที่ได้ Backup	นายสมชาย จำปาทอง นางสาวณัฐวดี โพธิ์กะสังข์ นายอานันท์ กรุดเนียม นายวัฒนา อุไกรหงสา
	Windows Server OS ๑) ทำการตรวจสอบ Critical และ Security Patch จากเว็บไซต์ windowsupdate.microsoft.com ๒) ทำการ Backup	๑) Restore Windows ตามที่ได้ Backup	นายสมชาย จำปาทอง นางสาวณัฐวดี โพธิ์กะสังข์ นายอานันท์ กรุดเนียม นายวัฒนา อุไกรหงสา
	Linux OS ๑) ทำการ Download และติดตั้ง Recommended Patch Cluster ๒) ทำการ Backup	๑) Restore LINUX ตามที่ได้ Backup	นายสมชาย จำปาทอง นางสาวณัฐวดี โพธิ์กะสังข์ นายอานันท์ กรุดเนียม นายวัฒนา อุไกรหงสา

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
๒.๓.๓ ระบบฐานข้อมูล	<u>ฐานข้อมูลระบบ open data สศอ.</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายสมชาย จำปาทอง นางสาวพัชราวดี คำรอด
	<u>ฐานข้อมูลระบบการสำรวจข้อมูลอุตสาหกรรมรายปี</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวภูริตา มณียม
	<u>ฐานข้อมูลระบบห้องสมุดอิเล็กทรอนิกส์</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายอานันท์ กรุดเนียม นายวัฒนา อุไกรหงสา
	<u>ฐานข้อมูลระบบการสำรวจข้อมูลอุตสาหกรรมรายเดือน</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวประวีณาภรณ์ อรุณรัตน์

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
	<u>ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์และระบบงานตู้เอกสารอิเล็กทรอนิกส์ หนังสือเวียนอิเล็กทรอนิกส์</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวสุสารี รัตนพันธุ์
	<u>ฐานข้อมูลระบบวันลาอิเล็กทรอนิกส์ (E-Form)</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวณัฐวดี โพธิ์กะสังข์
	<u>ฐานข้อมูลระบบเว็บไซต์ สำนักงานเศรษฐกิจอุตสาหกรรม</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๔) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวสุสารี รัตนพันธุ์ นายอานันท์ กรุดเนียม
	<u>ฐานข้อมูลระบบรายงานดัชนีอุตสาหกรรมบนเว็บไซต์ สำนักงานเศรษฐกิจอุตสาหกรรม</u> ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวสุสารี รัตนพันธุ์ นายอานันท์ กรุดเนียม

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
	ฐานข้อมูลระบบรายงานสถิติอุตสาหกรรม บนเว็บไซต์ สำนักงานเศรษฐกิจอุตสาหกรรม ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวสุสารี รัตนพันธุ์ นายอานันท์ กรุดเนียม
	ฐานข้อมูลระบบ iSingle form ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นางสาวประวีณาภรณ์ อรุณรัตน์
	ฐานข้อมูลระบบติดตามประเมินผลความก้าวหน้า ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายอานันท์ กรุดเนียม
	ฐานข้อมูลระบบจดหมายอิเล็กทรอนิกส์ (OIE Webmail) ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายวัฒนา อุไกรหงสา

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
	ฐานข้อมูลระบบเอกสารอิเล็กทรอนิกส์ (OIE QR Code) ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายอานันท์ กรุดเนียม นางสาวณัฐวดี โพธิ์กะสังข์
	ฐานข้อมูลระบบตรวจสอบความซ้ำซ้อนของที่ปรึกษาโครงการ (OIE Consult) ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายอานันท์ กรุดเนียม
	ฐานข้อมูลระบบข้อมูลบุคลากร (DPIS) ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายอานันท์ กรุดเนียม
	ฐานข้อมูลระบบเผยแพร่ข้อมูล (Data Service) ๑) กำหนดสิทธิ์ผู้ใช้ระบบ ๒) กำหนดขอบเขตการเข้าถึงข้อมูลของผู้ใช้แต่ละคน ๓) อบรมผู้ใช้ระบบฐานข้อมูล ๔) จัดทำคู่มือติดตั้งระบบฐานข้อมูล ๕) ทำการ Backup	๑) Restore ระบบฐานข้อมูลที่ได้ Backup ไว้ ๒) กำหนดสิทธิ์ผู้ใช้ระบบใหม่อีกครั้งตามคู่มือการใช้งาน ๓) กำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน	นายวัฒนา อุไกรหงสา

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
๒.๓.๔ โปรแกรมประยุกต์ (Application program)	<u>ระบบ Smart mail สศอ.</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอชั่น(ถ้ามี) ๓) จัดทำคู่มือการใช้งานโปรแกรม	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นายสมชาย จำปาทอง นายวัฒนา อุไกรหงสา
	<u>ระบบงานสำรวจข้อมูลอุตสาหกรรมรายปี</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น (ถ้ามี) ๓) จัดทำคู่มือการใช้งานโปรแกรม	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นางสาวภูริตา มณียม
	<u>ระบบตู้เอกสารอิเล็กทรอนิกส์และหนังสือเวียนอิเล็กทรอนิกส์</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น (ถ้ามี) ๓) จัดทำคู่มือการใช้งานโปรแกรม	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นางสาวสุสารี รัตนพันธุ์
	<u>ระบบสารบรรณอิเล็กทรอนิกส์</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น ๓) จัดทำคู่มือการใช้งาน	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นางสาวสุสารี รัตนพันธุ์
	<u>ระบบ open data สศอ.</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น ๓) จัดทำคู่มือการใช้งาน	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นายสมชาย จำปาทอง
	<u>ระบบ ธรรมาภิบาล สศอ.</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น ๓) จัดทำคู่มือการใช้งาน	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นายสมชาย จำปาทอง

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
	<u>ระบบงานเว็บไซต์ สำนักงานเศรษฐกิจอุตสาหกรรม</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น (ถ้ามี) ๓) จัดทำคู่มือการใช้งานโปรแกรม	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นางสาวสุสารี รัตนพันธุ์ นายอานันท์ กรุดเนียม
	<u>ระบบงานรายงานดัชนีอุตสาหกรรม บนเว็บฯ</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น (ถ้ามี) ๓) จัดทำคู่มือการใช้งานโปรแกรม	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นางสาวสุสารี รัตนพันธุ์ นายอานันท์ กรุดเนียม
	<u>ระบบงานรายงานสถิติอุตสาหกรรม บนเว็บไซต์ สำนักงานเศรษฐกิจอุตสาหกรรม</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอร์ชั่น (ถ้ามี) ๓) จัดทำคู่มือการใช้งานโปรแกรม	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นางสาวสุสารี รัตนพันธุ์ นายอานันท์ กรุดเนียม
	<u>ระบบ OIE QR Code</u> ๑) ทำการ Backup ๒) ทำการปรับปรุงเวอชั่น(ถ้ามี) ๓) จัดทำคู่มือการใช้งานโปรแกรม	๑) Restore โปรแกรมตามที่ได้ Backup ไว้	นายอานันท์ กรุดเนียม นางสาวณัฐวดี โพธิ์กะสังข์

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
๒.๓.๖ ไฟดับ ไฟตก	๑) ติดตั้งอุปกรณ์สำรองไฟ (UPS) ๒) จัดจ้าง บริการบำรุงรักษา ซ่อมแซมแก้ไข ระบบคอมพิวเตอร์ เครือข่ายและอุปกรณ์ ๓) จัดทำคู่มือการเปิด-ปิดระบบคอมพิวเตอร์	๑) ปิดระบบคอมพิวเตอร์ เครือข่ายและอุปกรณ์ ๒) เปิดเครื่องอีกครั้ง ตามขั้นตอนที่ระบุไว้ในคู่มือการเปิด-ปิดระบบคอมพิวเตอร์ ๓) ตรวจสอบแก้ไขอุปกรณ์และข้อมูลที่เกิดความเสียหาย	- เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน
๒.๓.๗ ผู้บุกรุก ขโมย	๑) มีเจ้าหน้าที่รักษาความปลอดภัย ๒) ติดสัญลักษณ์เป็นเขตเฉพาะผู้ดูแลระบบ ๓) การควบคุมการเข้าออกห้องควบคุมคอมพิวเตอร์แม่ข่าย	๑) ตรวจสอบคอมพิวเตอร์ และอุปกรณ์ ๒) จัดหาระบบที่พอใช้งานได้มาทำงานทดแทน เพื่อให้ระบบทำงานได้ ๓) Restore ระบบต่างๆ ที่ได้ Backup ไว้ ๔) Restore ข้อมูลที่ Backup ไว้ ๕) จัดหาคอมพิวเตอร์และอุปกรณ์ทดแทน	- เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน - เจ้าหน้าที่ในส่วนกลุ่มบริหารการคลังและพัสดุ สำนักเลขานุการกรม
๒.๓.๘ Hacker	๑) Backup ข้อมูลตามระยะเวลาของข้อมูล ๒) กระจายการจัดเก็บข้อมูลไว้หลายๆ ที่ ป้องกันข้อมูลสูญหาย ๓) ติดตั้งระบบรักษาความปลอดภัย Firewall ๔) หมั่น Update Security เพื่ออุดรอยรั่วของระบบรักษาความปลอดภัย ๕) ให้ความรู้ด้านความปลอดภัยเจ้าหน้าที่ที่เกี่ยวข้อง	๑) Restore ระบบที่ได้ Backup ไว้ ขึ้นมา ๒) Restore ข้อมูลที่ Backup ไว้ ๓) ตรวจสอบ Log ของระบบเครือข่ายเพื่อวิเคราะห์หาหมายเลข IP แปลกปลอม และทำการปิดกั้นการเข้าถึง	เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน
๒.๓.๙ Virus Computer	๑) Backup ข้อมูลตามระยะเวลาของข้อมูล ๒) ติดตั้งโปรแกรมป้องกันไวรัส ๓) Update โปรแกรมป้องกันไวรัส ๔) ให้ความรู้แก่เจ้าหน้าที่ ๕) จัดทำคู่มือการใช้งาน	๑) ตรวจสอบและทำลายไวรัส ๒) Update โปรแกรมป้องกันไวรัส ๓) Restore ระบบที่ได้ Backup ไว้ ขึ้นมา ๔) Restore ข้อมูลที่ Backup ไว้	เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน

ระบบ	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
๒.๓.๑๐ เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ เช่น Computer UPS เสีย	๑) จัดจ้างบริการ บำรุงรักษา ซ่อมแซม แก้ไขระบบคอมพิวเตอร์ เครือข่ายและอุปกรณ์ ๒) อบรมเจ้าหน้าที่ ให้มีความรู้ในการดูแลรักษาอุปกรณ์สำนักงาน	๑) เจ้าหน้าที่จากบริษัทรับจ้างบริการบำรุงรักษา ซ่อมแซม แก้ไขระบบคอมพิวเตอร์ เครือข่ายและอุปกรณ์ ๒) จัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ทดแทนที่ชำรุด ใช้งานไม่ได้	เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน

๒.๔ ตารางแสดงแผนแก้ไขปัญหาความไม่แน่นอนที่เกิดจากภัยธรรมชาติต่าง ๆ

ความเสี่ยง	หน้าที่ / กิจกรรม	การแก้ไขปัญหา	ผู้รับผิดชอบ
๒.๔.๑ แผ่นดินไหว	๑) Backup ข้อมูลตามระยะเวลาของข้อมูล ๒) กระจายการจัดเก็บข้อมูลไว้หลาย ๆ ที่ ป้องกันข้อมูลสูญหาย	๑) จัดหาเครื่อง Server ที่สามารถทำงานได้ ๒) Restore ระบบต่าง ๆ ที่ได้ Backup ไว้ ๓) Restore ข้อมูลที่ Backup ไว้	เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน
๒.๔.๒ ไฟไหม้	๑) Backup ข้อมูลตามระยะเวลาของข้อมูล ๒) กระจายการจัดเก็บข้อมูลไว้หลายๆ ที่ ป้องกันข้อมูลสูญหาย ๓) ติดตั้งระบบเตือนภัยหากเกิดไฟไหม้สำนักงาน ๔) ติดตั้งอุปกรณ์ตัดไฟ หากเกิดไฟฟ้าลัดวงจร	๑) จัดหาเครื่อง Server ที่สามารถทำงานได้ ๒) Restore ระบบต่าง ๆ ที่ได้ Backup ไว้ ๓) Restore ข้อมูลที่ Backup ไว้	เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน และฝ่ายดูแลอาคารสถานที่
๒.๔.๓ น้ำท่วม	๑) Backup ข้อมูลตามระยะเวลาของข้อมูล ๒) กระจายการจัดเก็บข้อมูลไว้หลาย ๆ ที่ ป้องกันข้อมูลสูญหาย	๑) จัดหาเครื่อง Server ที่สามารถทำงานได้ ๒) Restore ระบบต่าง ๆ ที่ได้ Backup ไว้ ๓) Restore ข้อมูลที่ Backup ไว้	เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน
๒.๔.๔ การชุมนุมทางการเมือง	๑) Backup ข้อมูลตามระยะเวลาของข้อมูล ๒) กระจายการจัดเก็บข้อมูลไว้หลาย ๆ ที่ ป้องกันข้อมูลสูญหาย	๑) จัดหาเครื่อง Server ที่สามารถทำงานได้ ๒) Restore ระบบต่าง ๆ ที่ได้ Backup ไว้ ๓) Restore ข้อมูลที่ Backup ไว้	เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน

ส่วนที่ ๓
สรุปผลและข้อเสนอแนะ

ส่วนที่ ๓
บทสรุปและข้อเสนอแนะ

สำนักงานเศรษฐกิจอุตสาหกรรม (สศอ.) ได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงของหน่วยงาน ซึ่งอาจเกิดขึ้นในระบบบริหารงานสั่งการและการปฏิบัติงานเพื่อสนับสนุนวิสัยทัศน์ในการเป็นองค์กรชี้นำการพัฒนาอุตสาหกรรมของประเทศ การดำเนินงานดังกล่าวทำให้ข้อมูลและสารสนเทศต่าง ๆ ที่ใช้ในการบริหารงานมีปริมาณที่มากมาย มีความเคลื่อนไหวตลอดเวลา โดยเฉพาะอย่างยิ่งข้อมูลและสารสนเทศที่ใช้ในการให้บริการประชาชนด้านเศรษฐกิจอุตสาหกรรม รวมทั้งข้อมูลและสารสนเทศต่าง ๆ ที่สำนักงานเศรษฐกิจอุตสาหกรรมต้องรับผิดชอบกระบวนการประมวลผลข้อมูลตามนโยบายสำคัญต่าง ๆ ของกระทรวงอุตสาหกรรมและรัฐบาล ซึ่งหากข้อมูลและสารสนเทศดังกล่าวเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายและถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกสำนักงานโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหาครั้งนี้ จึงควรเริ่มตั้งแต่การบริหารจัดการความเสี่ยงในสำนักงาน

๓.๑ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยงเป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่สำนักงานเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด ๕ ลำดับแรก ได้ข้อสรุป ดังนี้

๑. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์
แนวทางการดำเนินการจัดการความเสี่ยง
- ติดตั้งระบบป้องกันไวรัส และมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน
- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ
- ต้องอัพเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ

๒. ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ
แนวทางการดำเนินการจัดการความเสี่ยง
- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน เพื่อสามารถปฏิบัติงานได้ตามปกติ
- ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย
- ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ

๓. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม การประท้วง และภัยพิบัติอื่นๆ
แนวทางการดำเนินการจัดการความเสี่ยง
- มีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)
- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด

๔. ความเสี่ยงด้านระบบฐานข้อมูลของ สศอ.
แนวทางการดำเนินการจัดการความเสี่ยง
- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
- จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ
- จัดเก็บข้อมูลไว้บนระบบ Cloud

๕. ความเสี่ยงจากเครื่องคอมพิวเตอร์ (PC) หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ

- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน เพื่อสามารถปฏิบัติงานได้อย่างต่อเนื่อง
- บำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอตลอดจน จัดอบรมผู้ใช้งาน
- จัดทำคู่มือการใช้งาน
- ลงระบบปฏิบัติการ (OS) ให้พร้อมใช้งาน

๓.๒ แผนรองรับสถานการณ์ฉุกเฉินและเจ้าหน้าที่ผู้รับผิดชอบ ซึ่งแผนรองรับสถานการณ์ฉุกเฉินแบ่งออกเป็น ๔ สถานการณ์ คือ

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 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้
๒) กรณีหลังเหตุการณ์ความไม่สงบ

๓.๒.๔ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

๑) กรณีโจรกรรม
๒) กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

เจ้าหน้าที่ผู้รับผิดชอบหากมีสถานการณ์ฉุกเฉินเกิดขึ้น

๑. สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค เจ้าหน้าที่ผู้รับผิดชอบคือ เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน ผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม และฝ่ายดูแลอาคารรสถานที่ สำนักงานเลขานุการกรม

๒. สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ กรณี ไฟไหม้ น้ำท่วม แผ่นดินไหว เจ้าหน้าที่ผู้รับผิดชอบคือ ผู้ปฏิบัติงานส่วนต่าง ๆ ผู้ดูแลห้องแม่ข่าย/ผู้ดูแลระบบงาน ผู้สำรวจตรวจสอบรายการทรัพย์สิน ผู้บริหารของหน่วยงาน

๓. สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบจะ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้อำนวยการศูนย์สารสนเทศเศรษฐกิจอุตสาหกรรมทราบ กรณีหลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหาย ซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว

หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

๔. สถานการณ์ฉุกเฉินที่เกิดจากบุคคล ในกรณีโจรกรรม กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้ เจ้าหน้าที่ผู้รับผิดชอบคือ เจ้าหน้าที่ในกลุ่มระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม ผู้ดูแลระบบงาน ผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม และฝ่ายดูแลอาคารสถานที่ สำนักงานเลขานุการกรม

การกำหนดผู้รับผิดชอบหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

ผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบปฏิบัติงาน ได้แก่

- รองผู้อำนวยการสำนักงานเศรษฐกิจอุตสาหกรรม ที่ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ประจำสำนักงานเศรษฐกิจอุตสาหกรรม
- นางสาวณิรดา วิสุทธิชาติธาดา ดำรงตำแหน่งผู้อำนวยการกองสารสนเทศและดัชนีเศรษฐกิจอุตสาหกรรม
- ผู้รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย (Server room) คือ นายสมชาย จำปาทอง นักวิชาการคอมพิวเตอร์ชำนาญการ
  นางสาวณัฐวดี โพธิ์กะสังข์ นักวิชาการคอมพิวเตอร์ชำนาญการ
  นายอานันท์ กรุดเนียม นักวิชาการคอมพิวเตอร์ปฏิบัติการ
  นายวัฒนา อุไกรหงสา นักวิชาการคอมพิวเตอร์ปฏิบัติการ
- ผู้รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน คือ นางสาวทิพาพร ยิ้มวิลัย นักวิชาการการเงินและบัญชีชำนาญการพิเศษ

๓.๓ ข้อเสนอแนะ

๑) การดูแลระบบรักษาความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน เช่น ความเสี่ยงด้านเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ เช่น Domain Server, Web Server, Mail Server, DNS Server, File Server และ Database Server ที่มีแนวทางดำเนินการต้องจัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนการปฏิบัติงานได้ตามปกติ นั่นคือต้องได้รับการสนับสนุนงบประมาณจัดหาอุปกรณ์ดังกล่าวด้วยเช่นกัน

๒) จัดหาระบบป้องกันการบุกรุกที่ทันสมัย เช่น EDR (Endpoint Detection and Response) เพราะภัยคุกคามในปัจจุบันได้รับการออกแบบเพื่อหลบเลี่ยงระบบรักษาความปลอดภัยแบบดั้งเดิม ระบบดังกล่าวสามารถตรวจจับ วิเคราะห์พฤติกรรมและเรียนรู้ที่จะป้องกันภัยคุกคามแบบใหม่ได้โดยอัตโนมัติ ทำให้ระบบงานของ สศอ. มีความปลอดภัยมากขึ้น

๓) ให้ความสำคัญกับข้อมูลส่วนบุคคล ในเชิงป้องกันทั้งภายในและภายนอก จัดหาเครื่องมือหรือวิธีการเพื่อสนับสนุน ระบบงานของ สศอ. ให้สอดคล้องพรบ.คุ้มครองข้อมูลส่วนบุคคล