กรมโรงงานอุตสาหกรรม

DEPARTMENT OF INDUSTRIAL WORKS

แผนการบริหารความเสี่ยงและความปลอดภัย ด้านเทคโนโลยีสารสนเทศ กรมโรงงานอุตสาหกรรม

Information Technology Risk and Security Management Plan

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

มกราคม ๒๕๖๗

คำนำ

การบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมโรงงานอุตสาหกรรม จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยง ด้านศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทาง หรือมาตรการ ควบคุมเพื่อป้องกัน หรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ระดับที่องค์กรสามารถยอมรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หวังเป็นอย่างยิ่งว่า แผนการบริหารความเสี่ยงและความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรมฉบับนี้ เมื่อนำไปปฏิบัติจะสามารถลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นในอนาคต และเพิ่มระดับของความปลอดภัย ด้านเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรมให้มีประสิทธิภาพมากยิ่งขึ้น

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมโรงงานอุตสาหกรรม
มกราคม ๒๕๖๗

สารบัญ

บทที่ ๑
บทนำ

๑. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจในการวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดโอกาสการสูญเสียที่อาจทำให้เกิดความเสียหายแก่กรมโรงงานอุตสาหกรรม โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยี สารสนเทศ ที่เข้ามามีบทบาทสำคัญในการดำเนินงานของทุกหน่วยภายในกรมโรงงานอุตสาหกรรม ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศล้วนแต่มีความเสี่ยงที่เป็นความไม่แน่นอนที่อาจส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายของกรมโรงงานอุตสาหกรรม จึงจำเป็นต้องมีการจัดการความเสี่ยงอย่างเป็นระบบ โดยการระบุปัจจัยที่มีความเสี่ยง วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง และกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

๒. วัตถุประสงค์ของการจัดทำการบริหารความเสี่ยงและความปลอดภัย

๑. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรม

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอน

๓. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลและระบบสารสนเทศหลัก เช่น เว็บไซต์กรมโรงงานอุตสาหกรรม ระบบสารสนเทศตามกฎหมายด้านโรงงาน ระบบสารสนเทศตามกฎหมายด้านเครื่องจักร ระบบสารสนเทศตามกฎหมายด้านวัตถุอันตราย เป็นต้น

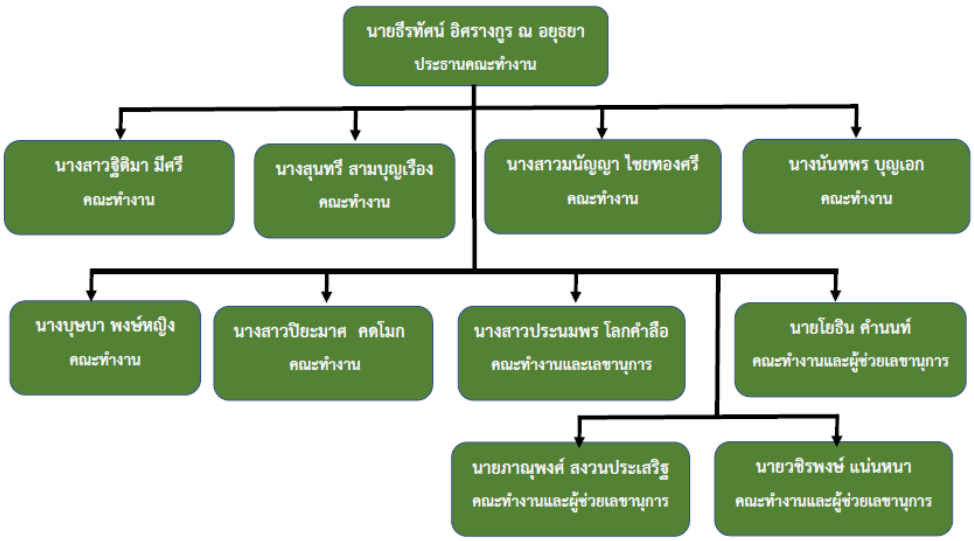
ระบบฐานข้อมูลและระบบสารสนเทศสนับสนุนการบริหารงานภายใน (Back Office) ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ ระบบสารสนเทศทรัพยากรบุคคล ระบบสารสนเทศงาน ระบบงบประมาณ ระบบพัสดุ ระบบการเงิน และระบบบุคลากร เป็นต้น

ระบบบริหารจัดการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) โปรแกรมระบบตรวจสอบและเฝ้าระวังเครือข่าย (Network Monitoring) โปรแกรมป้องกันการบุกรุกเครือข่าย (IPS) เป็นต้น

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ (PC)

เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switch) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Access Point) เป็นต้น

๔. โครงสร้างคณะทำงานบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ



รูปที่ ๑ ผังคณะทำงานบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

รายละเอียดอำนาจหน้าที่ของคณะทำงานสามารถตรวจสอบได้ที่ภาคผนวก ก.

๕. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหารจัดการความเสี่ยง การกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง โดยขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม ๕ ขั้นตอน ดังนี้

รูปที่ ๒ แสดงกระบวนการบริหารความเสี่ยง

๕.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการหรือกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตาม วัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๑) การระดมความคิด เพื่อหาความเป็นไปได้ของความเสี่ยงที่อาจเกิดขึ้น

๒) การใช้ Checklist

๓) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

๔) การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

๕) การรวบรวมปัญหาที่เคยเกิดขึ้น

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๕.๒ การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๕.๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน

เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงได้กำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก)

๕.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงใด และผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

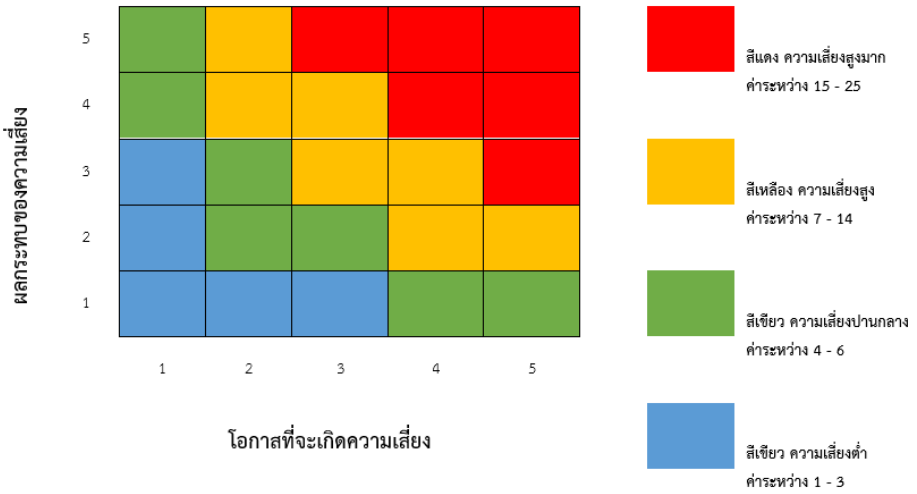
เกณฑ์การประเมิน เป็นการกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	๕ ครั้ง/ปี
๔	สูง	๔ ครั้ง/ปี
๓	ปานกลาง	๓ ครั้ง/ปี
๒	น้อย	๒ ครั้ง/ปี
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**ระดับผลกระทบ**	**คำอธิบาย**
๕	สูงมาก	เกิดความสูญเสียต่อระบบสารสนเทศที่สำคัญทั้งหมด และเกิดความเสียหายอย่างร้ายแรงต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	เกิดความสูญเสียต่อระบบสารสนเทศที่สำคัญบางส่วน และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูล
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก สามารถใช้งานได้ต่อเนื่อง
๒	น้อย	เกิดเหตุการณ์ในบางระบบที่แก้ไขได้ในทันที
๑	น้อยมาก	เกิดเหตุการณ์ที่ไม่มีนัยสำคัญ

๕.๒.๓ การวิเคราะห์ความเสี่ยง

เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อ ระบบสารสนเทศของกรมโรงงานอุตสาหกรรม ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุด ที่จะต้องบริหารจัดการก่อน ดังรูปที่ ๓



รูปที่ ๓ แสดงแผนผังประเมินความเสี่ยง

๕.๒.๔ การจัดลำดับความเสี่ยง

เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อกรมโรงงานอุตสาหกรรม เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับ ความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๕.๓ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผนจะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้นเพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน แก้ไข ควบคุม ความเสี่ยง

ไม่ให้มีผลกระทบต่อระบบที่วางไว้โดยสามารถดำเนินการตามแผนได้การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๕.๓.๑ ควบคุมเพื่อการป้องกัน (Preventive Control)

เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๕.๓.๒ การควบคุมเพื่อให้ตรวจพบ (Detective Control)

เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับการรายงานข้อบกพร่อง เป็นต้น

๕.๓.๓ การควบคุมโดยการชี้แนะ (Direction Control)

เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๕.๓.๔ การควบคุมเพื่อการแก้ไข (Corrective Control)

เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูงมาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

๒) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๕.๔ การติดตามรายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติเพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการหรือกิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยงและนำมาวางแผนจัดการความเสี่ยงทางเลือกในการบริหารความเสี่ยงมีหลายวิธี ซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์อาจเป็นการยอมรับความเสี่ยง การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยงและการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือกเพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๕.๔.๑ พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๕.๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๕.๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๕.๔.๔ ในรอบปีต่อไปให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๕.๕ การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยติดตามผลเป็น รายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน และจัดให้มีการทบทวนการบริหารความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง ก่อนจะมีการประเมินและตรวจสอบ

๖. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กรมโรงงานอุตสาหกรรมได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๕ ประเภท ดังนี้

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดขึ้นและส่งผลกระทบโดยตรงต่อระบบคอมพิวเตอร์ และห้องคอมพิวเตอร์ศูนย์แม่ข่ายกลาง เช่น ไฟไหม้ กระแสไฟฟ้าขัดข้อง รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

๒) ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และ คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

๓) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากไวรัสคอมพิวเตอร์อย่าง Malware, Trojan หรือ Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายในและมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจาก คอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัยเพื่อลดช่องโหว่ที่อาจทำให้เกิดข้อผิดพลาดของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งอาจทำให้กรมโรงงานอุตสาหกรรมถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ อันอาจก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือ และสร้างความเสื่อม เสียแก่กรมโรงงานอุตสาหกรรม ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการ ความเสี่ยงด้านข้อมูลดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศ เป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ อย่างเช่น คน ธรรมชาติ หรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศ

๗. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับ เพื่อให้การบริหารความเสี่ยงเกิดประสิทธิผล ผู้บริหารมีความจำเป็นต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ ให้อยู่ในช่วงที่องค์กรสามารถ ยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๑) การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกไม่แบกรับความเสี่ยง โดยอาจหยุดดำเนินการ ยกเลิกโครงการ หรือกิจกรรม ที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้นโดยมิได้คิดทบทวนถึงผลที่จะได้รับนำมาซึ่งการเสียโอกาสของหน่วยงานได้

๒) การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นและไม่ดำเนินการใดๆ และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่กรมโรงงานอุตสาหกรรม ยอมรับได้หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

๓) การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทาง ป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดหากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมี การจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสีย มีสองวิธี คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือ การหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

๔) การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๘. ปัจจัยเสี่ยง

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) แบ่งออกเป็น

๑.๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๓) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)

๑.๔) ความเสี่ยงจากแมลงสัตว์กัดแทะอุปกรณ์เครือข่ายและสายสัญญาณ

๑.๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครืองแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง

๒) ความเสี่ยงด้านบุคลากร (Human Risk) แบ่งออกเป็น ๒ ข้อ คือ

๒.๑) ความเสี่ยงจากผู้ดูแลระบบ

๒.๒) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย

๓) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk) แบ่งออกเป็น ๗ ข้อ คือ

๓.๑) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย

๓.๒) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์ หรือมัลแวร์

๓.๓) ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร

๓.๔) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน

๓.๕) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)

๓.๖) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)

๓.๗) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) แบ่งออกเป็น ๓ ข้อ คือ

๔.๑) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

๔.๒) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

๔.๓) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)

๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk) แบ่งออกเป็น ๓ ข้อ คือ

๕.๑) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน

๕.๒) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล

๕.๓) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

๙. การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๒. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบ ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบเทคโนโลยีสารสนเทศและฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๑๐. ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบรักษาความปลอดภัยบนเครือข่าย ของกรมโรงงานอุตสาหกรรมได้พัฒนาและปรับปรุงอย่างต่อเนื่อง โดยกำหนดนโยบาย (Policy) บนอุปกรณ์และซอฟต์แวร์ ที่ควบคุมระบบเครือข่าย เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่าย กรมโรงงานอุตสาหกรรม เป็นไปอย่างมีประสิทธิภาพ ตั้งอยู่ที่ ๗๕/๖ ถนนพระรามที่ ๖ แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร

๑๑. ระบบคอมพิวเตอร์และเครือข่ายของกรมโรงงานอุตสาหกรรม

ระบบคอมพิวเตอร์และเครือข่าย ของกรมโรงงานอุตสาหกรรมมีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์ และซอฟต์แวร์ทำงานร่วมกัน เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรอง (Filter Package) ที่ผ่านเข้ามาภายในระบบของกรมโรงงานอุตสาหกรรมจากเครือข่ายภายนอก เช่น เครือข่ายอินเทอร์เน็ต เครือข่าย GIN นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของ DMZ ที่ดูแลเครื่องแม่ข่ายทั้งหมดของกรมโรงงานอุตสาหกรรม รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของกรมโรงงานอุตสาหกรรม มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของกรมโรงงานอุตสาหกรรม มีการแบ่ง Subnet เพื่อให้เป็นระบบกลุ่มบรอดคาสต์โดเมน (Broadcast Domain) เดียวกัน ประกอบกับกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความ ปลอดภัย สะดวกและรวดเร็วต่อการบริหารจัดการระบบกรณีเกิดปัญหาการใช้งาน

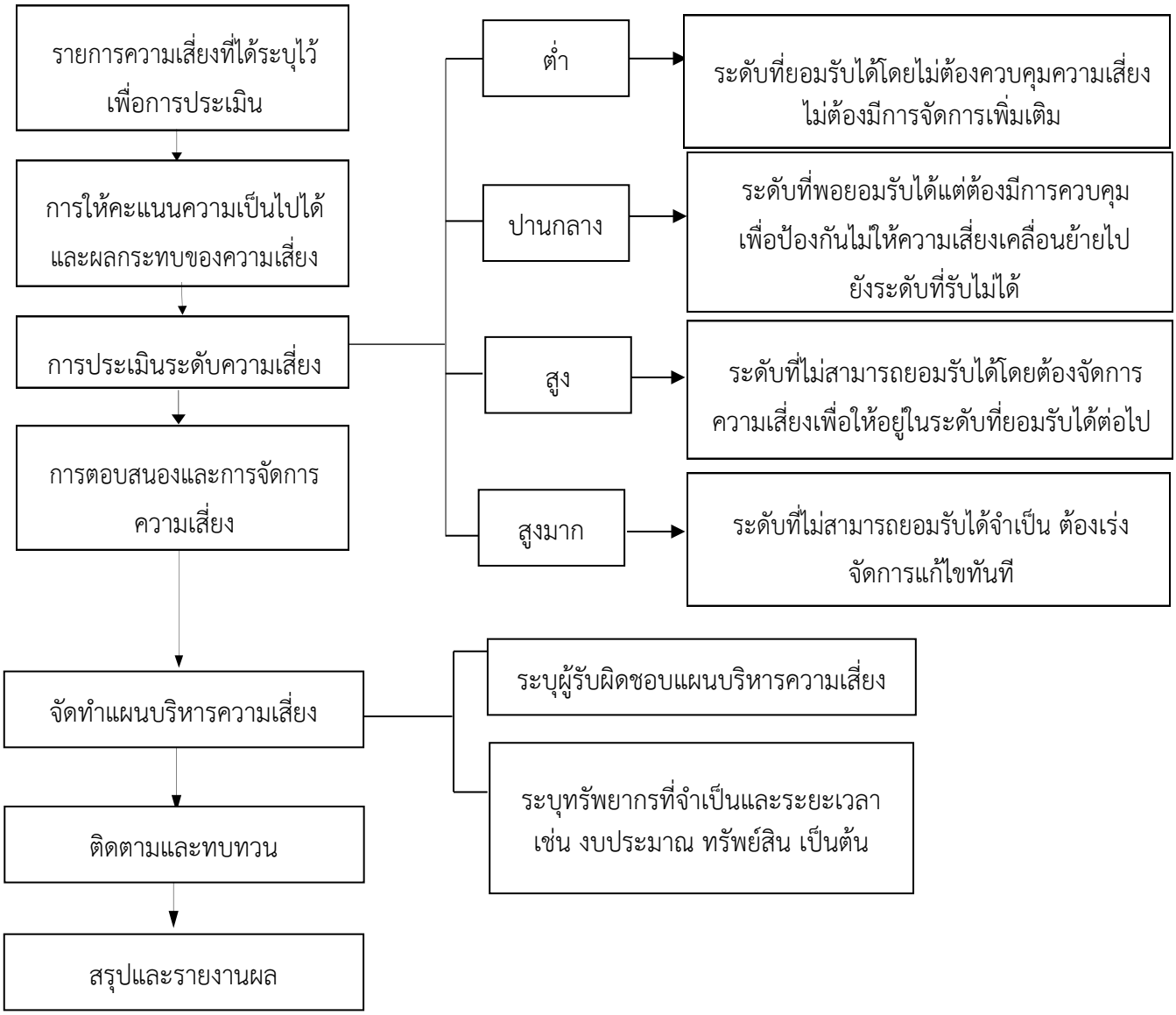
ระบบเครือข่ายหลักของกรมโรงงานอุตสาหกรรม (Core Network) ตั้งอยู่ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบ เครือข่าย ในความเร็วระดับ ๑,๐๐๐ Mbps และระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ต และ GIN เพื่อรองรับภารกิจของกรมโรงงานอุตสาหกรรม ซึ่งลักษณะ งานต้องใช้อุปกรณ์เครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพสูงสามารถรองรับการเชื่อมต่อกับระบบเครือข่าย ภายในและภายนอก เพื่อใช้ระบบงานฐานข้อมูลที่สำคัญของกรมโรงงานอุตสาหกรรม พร้อมทั้งเชื่อมโยงไปยังอุปกรณ์ Distributed Switch (L๓) และ Access Switch(L๒) ภายในอาคาร ซึ่งเป็นที่ตั้งของหน่วยงานในกรมโรงงานอุตสาหกรรม

๑๒. แผนผังระบบและเครือข่ายของกรมโรงงานอุตสาหกรรม (รายละเอียดตามภาคผนวก ก.)

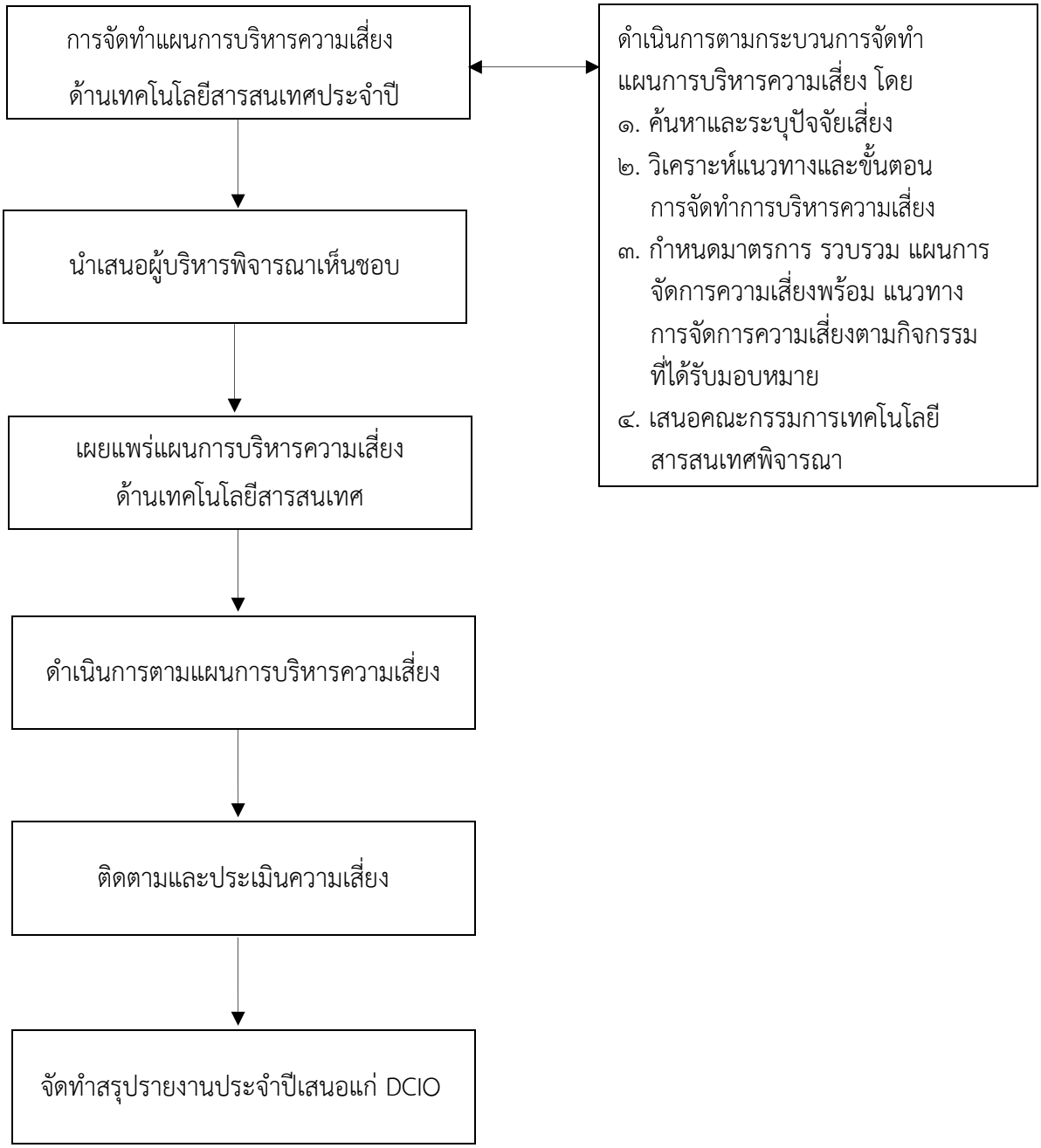
บทที่ ๒
การวิเคราะห์และการจัดทำแผนบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

กรมโรงงานอุตสาหกรรม ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหาย จากปัจจัยเสี่ยงแต่ละด้าน จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศส.) จัดทำแผนบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๗ โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจาก การรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม การวิเคราะห์ปัจจัยเสี่ยง และกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังต่อไปนี้

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๒. กระบวนการจัดทำแผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



๓. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

จากการวิเคราะห์ความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศของกรมโรงงานอุตสาหกรรม สามารถสรุปความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization) จำแนกได้ ๕ ด้าน ดังนี้ ๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) แบ่งออกเป็น ๕ ข้อ คือ

๑.๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

๑.๓) ความเสี่ยงจากอุณหภูมิและความชื้นและตรวจจับน้ำรั่วซึมของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)

๑.๔) ความเสี่ยงจากแมลงสัตว์กัดแทะอุปกรณ์เครือข่ายและสายสัญญาณ

๑.๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่ายและอุปกรณ์ต่อพ่วง

๒) ความเสี่ยงด้านบุคลากร (Human Risk) แบ่งออกเป็น ๒ ข้อ คือ

๒.๑) ความเสี่ยงจากผู้ดูแลระบบ

๒.๒) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย

๓) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk) แบ่งออกเป็น ๗ ข้อ คือ

๓.๑) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย

๓.๒) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์

๓.๓) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร

๓.๔) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต อินเทอร์เน็ตภายใน และภายนอกสถานที่ทำงาน

๓.๕) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)

๓.๖) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)

๓.๗) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) แบ่งออกเป็น ๓ ข้อ คือ

๔.๑) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

๔.๒) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

๔.๓) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือบำรุงรักษาระบบโดยผู้รับจ้างภายนอก (Outsource)

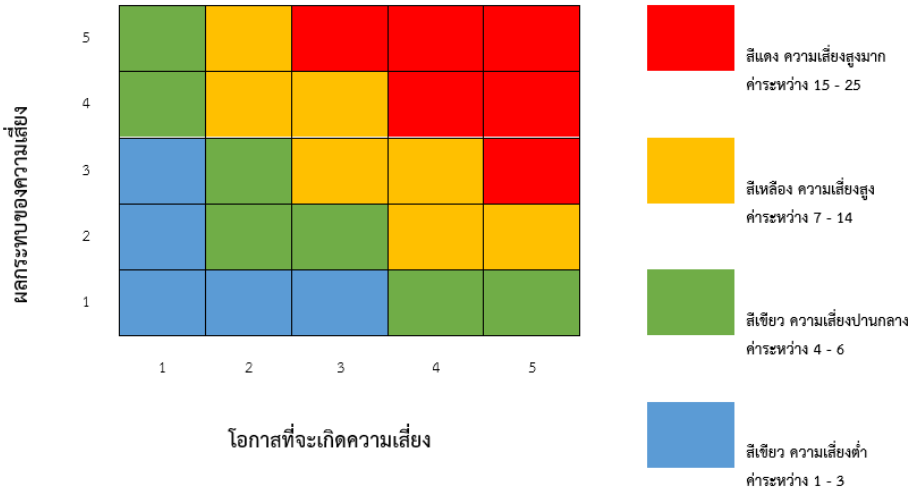
๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk) แบ่งออกเป็น ๓ ข้อ คือ

๕.๑) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้องไม่เป็นปัจจุบัน และไม่ครบถ้วน

๕.๒) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล

๕.๓) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

การระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่กรมโรงงานอุตสาหกรรมเผชิญอยู่ ผลสรุปการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้



ตารางแสดงประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศตามค่าคะแนนความเสี่ยง (รายละเอียดตามภาคผนวก ข.)

๔. ผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและแนวทางการควบคุมที่มีอยู่

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑. ระบบคอมพิวเตอร์และระบบเครือข่ายถูกทำลาย ๒. ระบบสารสนเทศและระบบฐานข้อมูลถูกทำลาย	๑	๕	๕	๑. มีระบบดับเพลิงอัตโนมัติ (Fire Suppression System) ตรวจสอบ ทุก ๓ เดือน ๒.มีระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (environment Monitoring System) ตรวจสอบ ทุก ๓ เดือน	การควบคุม (Treat)	กลุ่มบริการระบบสารสนเทศ ๒ ศส.
๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑. ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้ ๒. ไม่สามารถใช้งานระบบสารสนเทศและระบบฐานข้อมูลได้ ๓. ระบบปฏิบัติการ และระบบฐานข้อมูลเกิดความเสียหายจากเครื่องไม่ได้ถูกทำการปิดอย่างเหมาะสม	๑	๕	๕	๑. มีระบบสำรองไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่ายกลาง ตรวจสอบ ทุก ๓ เดือน ๒. มีระบบสลับจ่ายกระแสไฟฟ้า ตรวจสอบ ทุก ๓ เดือน ๓.มีระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environment Monitoring System) ตรวจสอบ ทุก ๓ เดือน	การถ่ายโอน (Transfer)	กลุ่มบริการระบบสารสนเทศ ๒ ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓) ความเสี่ยงจากอุณหภูมิและความชื้นและตรวจจับน้ำรั่วซึมของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	เกิดความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย	๑	๕	๕	๑. มีระบบเครื่องปรับอากาศควบคุมอุณหภูมิและความชื้น(Precision Air Conditioning System)และระบบตรวจจับการรั่วซึมของน้ำ ตรวจสอบ ทุก ๓ เดือน (Water Leak Detection System) ๒.มีระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (environment Monitoring System) ตรวจสอบ ทุก ๓ เดือน	การถ่ายโอน (Transfer)	กลุ่มบริการระบบสารสนเทศ ๒ ศส.
๔) ความเสี่ยงจากแมลงสัตว์กัดแทะอุปกรณ์เครือข่ายและสายสัญญาณ	๑. ไม่สามารถใช้งานระบบเครือข่ายได้ ๒. ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง	๑	๕	๕	ทำการแก้ไขเมื่อได้รับแจ้งจากผู้ใช้งาน	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.
๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่ายและอุปกรณ์ต่อพ่วง (Data Center)	๑. อุปกรณ์และข้อมูลที่มีความสำคัญสูญหาย ๒. เสียภาพลักษณ์ของหน่วยงาน	๑	๕	๕	มีระบบควบคุมกำหนดสิทธิ์การปิด-เปิด ประตูอัตโนมัติ (Access Control System) และกล้องวงจรปิดภายในห้อง Data Center ตรวจสอบ ทุก ๓ เดือน	การยอมรับ (Take)	๑. กลุ่มบริการระบบสารสนเทศ ๒ ๒. กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๒. ความเสี่ยงด้านบุคลากร (Human Risk)							
๖) ความเสี่ยงจากผู้ดูแลระบบ	ข้อมูลที่อยู่ในชั้นความลับรั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือของหน่วยงาน	๑	๕	๕	๑. การทำ Authentication การเข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ) ๒. การจัดระดับการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล ทุก ๖ เดือน	การยอมรับ (Take)	กลุ่มบริการระบบสารสนเทศกลาง ศส.
๗) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย	๑. สูญเสีย Bandwidth ในระบบเครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้นเนื่องจากการใช้งานนอกเหนือจากงานราชการ ๒. เครื่องคอมพิวเตอร์ เสียหายและเสื่อมอายุการใช้งานเร็วกว่าปกติ	๒	๕	๑๐	๑. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และการเฝ้าระวังเครือข่าย ทุก ๑ เดือน ๒. ตรวจสอบและเมื่อพบสิ่งผิดปกติจะให้คำแนะนำผู้ใช้งานให้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างเหมาะสม	การควบคุม (Treat)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
๘) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๑. เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล ๒. ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	๓	๕	๑๕	๑. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลักทุกวัน ๒. สำรองระบบและข้อมูล (Backup) ทุกวัน ๓. ทดสอบการกู้คืนระบบแม่ข่ายหลัก เดือนละ ๑ ครั้ง	การควบคุม (Treat)	๑. กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส. ๒.กลุ่ม/กอง ที่ดูแลระบบงานต่าง ๆ
๙) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	๑. โปรแกรมหรือข้อมูลถูกทำลาย ๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ ๓. การถูกขโมยข้อมูลที่สำคัญ	๓	๕	๑๕	๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ) ๒. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งคัด	การควบคุม (Treat)	๑. กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๐) ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	๑.ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้ ๒. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ๓. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของหน่วยงาน ๔. ถูกโจรกรรมข้อมูลที่เป็นความลับ ๕. ไม่สามารถเข้าใช้ระบบสารสนเทศได้	๔	๕	๒๐	๑. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และการเฝ้าระวังเครือข่ายทุก ๑ เดือน	การควบคุม (Treat)	๑. กลุ่มบริการอุปกรณ์และระบบเครือข่าย ๒. กลุ่มบริการระบบสารสนเทศกลาง ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๑) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน	๑. ระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตไม่สามารถใช้งานได้ ๒. ไม่สามารถเข้าใช้งานระบบสารสนเทศ ผ่านเครือข่ายอินทราเน็ตและอินเทอร์เน็ตได้	๒	๕	๑๐	๑. ตรวจสอบระบบเครือข่าย (Monitoring) ทุกวัน ๒. ควบคุมการเข้าใช้เครือข่ายอินทราเน็ต และอินเทอร์เน็ต โดยใช้ระบบยืนยันตน (Authentication)	การยอมรับ (Take)	๑. กลุ่มบริการอุปกรณ์และระบบเครือข่าย ๒. กลุ่มบริการระบบสารสนเทศกลาง ศส.
๑๒) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)	๑. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ ๒. ลดความน่าเชื่อถือของหน่วยงาน	๑	๕	๕	๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ) ๒. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และการเฝ้าระวังเครือข่าย ทุก ๑ เดือน ๓. ตรวจสอบระบบเครือข่าย (Monitoring) ทุกวัน	การยอมรับ (Take)	๑.กลุ่มบริการอุปกรณ์และระบบเครือข่าย ๒.กลุ่มบริการระบบสารสนเทศกลาง ศส.
๑๓) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องไม่สามารถเข้าร่วมประชุมได้	๑	๓	๓	ตรวจสอบการเชื่อมต่ออุปกรณ์การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนการใช้งานและแก้ไขเมื่อได้รับแจ้ง	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๔) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)	๑. ระบบโทรศัพท์ (IP Phone) ขัดข้อง ทำให้เจ้าหน้าที่ในหน่วยงานไม่สามารถใช้งานระบบโทรศัพท์ติดต่อประสานงานทั้งภายใน/ภายนอก ได้อย่างต่อเนื่อง	๑	๕	๕	ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) ทุก ๑ เดือน	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
๑๕) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑. การถูกฟ้องร้อง และเสื่อมเสียชื่อเสียง และ ความน่าเชื่อถือของหน่วยงาน ๒. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ ๓. หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	๑	๕	๕	๑. การจัดหาซอฟต์แวร์พื้นฐานที่ถูกกฎหมายมาใช้งาน ๒. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งครัด	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.
๑๖) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศและระบบฐานข้อมูล ๒. ลดความน่าเชื่อถือต่อหน่วยงาน	๑	๕	๕	๑. อัพเดทเครื่องมือและโปรแกรมที่ใช้พัฒนา ๒. ตรวจสอบช่องโหว่และดำเนินการแก้ไข ทุก ๑ เดือน	การยอมรับ (Take)	ศส. หรือ กลุ่ม/กองที่มีการพัฒนาโปรแกรม

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๗) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือบำรุงรักษาระบบโดยผู้รับจ้างภายนอก (Outsource)	๑. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ผิดพลาดได้อย่างทันท่วงที ๒. ขาดการดูแลบำรุงรักษาโปรแกรม และข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว เนื่องจากโปรแกรมหมดลิขสิทธิ์ และขาดการปรับปรุง (Update) โปรแกรม	๑	๕	๕	๑. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการวิเคราะห์ออกแบบการพัฒนาระบบและชุดคำสั่ง (Source Code) ฉบับสมสมบูรณ์ ทั้งในกรณีพัฒนาเสร็จสิ้นและเมื่อมีการปรับปรุงแก้ไข ๒. ส่งมอบชุดคำสั่ง (Source Code) ชุดสมบูรณ์ ๓. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ ๔. ขอรับการจัดสรรงบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลให้มีความทันสมัยและใช้งานได้อย่างต่อเนื่อง	การควบคุม (Treat)	ศส. หรือกลุ่ม/กองที่มีการจัดจ้างผู้รับจ้างภายนอก

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๕. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)							
๑๘) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้องไม่เป็นปัจจุบันและไม่ครบถ้วน	๑. ระบบฐานข้อมูลไม่สามารถนำไปใช้สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ ๒. ลดความน่าเชื่อถือของหน่วยงาน	๒	๕	๑๐	๑. จัดทำรายงานข้อมูลทุก ๑ เดือน ๒. กำหนดนโยบาย/แนวทางปฏิบัติของผู้บันทึกข้อมูลที่ลงในระบบให้ครบถ้วนและถูกต้อง	การยอมรับ (Take)	1.(ทุกกลุ่มที่ดูแลระบบงานต่างๆ) ศส ๒ .ผู้บันทึกข้อมูลระบบงานต่างๆ
๑๙) ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถกู้คืนระบบฐานข้อมูล	๑.เกิดการสูญหายของข้อมูล และกระทบต่อการทำงานตามปกติ ๒.ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้สนับสนุนการปฏิบัติงานได้	๑	๕	๕	๑. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุก ๑ เดือน	การยอมรับ (Take)	(ทุกกลุ่มที่ดูแลระบบงานต่างๆ) ศส.
๒๐) ความเสี่ยงจากการโจมตีระบบฐานข้อมูล	๑.ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ ๒. ข้อมูลที่สำคัญสูญหายและถูกทำลาย	๑	๕	๕	๑. ตรวจสอบระบบเครือข่าย (Monitoring) ทุกวัน ๒. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่าย ทุก ๑ เดือน	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

แผนปฏิบัติการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. ๒๕๖๗

กรมโรงงานอุตสาหกรรม
กระทรวงอุตสาหกรรม

ผู้รับผิดชอบหลัก
หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรมบรรลุเป้าประสงค์ของการบริหารความเสี่ยง

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๑. มีระบบดับเพลิงอัตโนมัติ (Fire Suppression System)	ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	ทุก ๓ เดือน			/			/			/			/
๒.ระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (environment Monitoring System)		ทุก ๓ เดือน			/			/			/			/

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๓. มีระบบสำรองไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่ายกลาง	ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	ทุก ๓ เดือน			/			/			/			/
๔. มีระบบสลับจ่ายกระแสไฟฟ้า		ทุก ๓ เดือน			/			/			/			/
๕. มีระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environment Monitoring System)		ทุก ๓ เดือน			/			/			/			/
๖. มีระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detection System)	ความเสี่ยงจากอุณหภูมิและความชื้นและตรวจจับน้ำรั่วซึมของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	ทุก ๓ เดือน			/			/			/			/
๗. มีระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environment Monitoring System) ทุก ๓ เดือน		ทุก ๓ เดือน			/			/			/			/
๘. ทำการแก้ไขเมื่อได้รับแจ้งจากผู้ใช้งาน	ความเสี่ยงจากแมลงสัตว์กัดแทะอุปกรณ์เครือข่ายและสายสัญญาณ	กรณีเมื่อได้รับแจ้งจากผู้ใช้งาน	←											→

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๙. มีระบบควบคุมกำหนดสิทธิ์การปิด-เปิด ประตูอัตโนมัติ (Access Control System) และกล้องวงจรปิดภายในห้อง (Data Center)	ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่ายและอุปกรณ์ต่อพ่วง (Data Center)	ทุก ๓ เดือน			/			/			/			/
๑๐. การทำ Authenticationการเข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน(เกษียณอายุ/ลาออก ฯลฯ)	ความเสี่ยงจากผู้ดูแลระบบ	กรณีเมื่อได้รับแจ้งเกษียณอายุ/ลาออก	←											→
๑๑. การจัดระดับการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล		ทุก ๖ เดือน						/						/
๑๒. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS,IPS และการเฝ้าระวังเครือข่าย ทุก ๑ เดือน	- ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย - ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
	- ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List) - ความเสี่ยงจากการโจมตีระบบฐานข้อมูล													
๑๓. ตรวจสอบและเมื่อพบสิ่งผิดปกติจะให้คำแนะนำผู้ใช้งานให้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างเหมาะสม	ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย	กรณีเมื่อได้รับแจ้ง	←											→
๑๔. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลักทุกวัน	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	ทุกวัน	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*
๑๕. สำรองระบบและข้อมูล (Backup) ทุกวัน		ทุกวัน	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*
๑๖. ทดสอบการกู้คืนระบบแม่ข่ายหลัก		เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
๑๗. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ)	- ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์ - ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ตและ	ทุกวัน	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
	อินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน - ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)													
๑๘. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งคัด *ไม่มีแผนปฏิบัติงาน	- ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์ - ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	ให้ปฏิบัติตามแผน	←											→
๑๙. ตรวจสอบระบบเครือข่าย (Monitoring) ทุกวัน	- ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน -ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)	ทุกวัน	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
	-ความเสี่ยงจากการโจมตีระบบฐานข้อมูล													
๒๐. ควบคุมการเข้าใช้เครือข่ายอินทราเน็ตและอินเทอร์เน็ตโดยใช้ระบบยืนยันตน (Authentication)	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน	ควบคุมการเข้าใช้งาน	←											→
๒๑. ตรวจสอบการเชื่อมต่ออุปกรณ์การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนการใช้งานและแก้ไขเมื่อได้รับแจ้ง	ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	กรณีเมื่อได้รับแจ้ง	←											→
๒๒. ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone)	ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
๒๓. การจัดหาซอฟต์แวร์พื้นฐานที่ถูกกฎหมายมาใช้งาน	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	กรณีมีการซื้อซอฟต์แวร์ที่มีลิขสิทธิ์หรือดาวน์โหลดมาใช้งาน	←											→

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๒๔. อัพเดทเครื่องมือและโปรแกรมที่ใช้พัฒนา	ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	กรณีเมื่อมีการอัพเดทโปรแกรมที่ใช้พัฒนาระบบ	←											→
๒๕. ตรวจสอบช่องโหว่และดำเนินการแก้ไขทุก ๑ เดือน		เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
๒๖. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการวิเคราะห์ออกแบบการพัฒนาระบบและชุดคำสั่ง (Source Code) ฉบับสมสมบูรณ์ทั้งในกรณีพัฒนาเสร็จสิ้นและเมื่อมีการปรับปรุงแก้ไข	ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือบำรุงรักษาระบบโดยผู้รับจ้างภายนอก (Outsource)	กรณีมีการปรับปรุงชุดคำสั่ง	←											→
๒๗. ส่งมอบชุดคำสั่ง (Source Code) ชุดสมบูรณ์	(ต่อ) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือบำรุงรักษาระบบโดยผู้รับจ้างภายนอก (Outsource)	กรณีมีการปรับปรุงชุดคำสั่ง	←											→
๒๘. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่		กรณีมีการปรับปรุงชุดคำสั่ง	←											→
๒๙. ขอรับการจัดสรรงบประมาณเพื่อทำการบำรุงรักษาโปรแกรม		กรณีมีการปรับปรุงชุดคำสั่ง	←											→

แผนปฏิบัติ	ประเภทความเสี่ยง	ระยะเวลา	เดือน											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
และข้อมูลให้มีความทันสมัยและใช้งานได้อย่างต่อเนื่อง														
๓๐. จัดทำรายงานข้อมูล ทุก ๑ เดือน	ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้องไม่เป็นปัจจุบันและไม่ครบถ้วน	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/
๓๑. กำหนดนโยบาย/แนวทางปฏิบัติของผู้บันทึกข้อมูลที่ลงในระบบให้ครบถ้วนและถูกต้อง		ให้ปฏิบัติตามนโนบาย	←											→
๓๒. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน	ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถกู้คืนระบบฐานข้อมูล	ทุกวัน	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*	/*
๓๓. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุก ๑ เดือน	(ต่อ) ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถกู้คืนระบบฐานข้อมูล	เดือนละ ๑ ครั้ง	/	/	/	/	/	/	/	/	/	/	/	/

หมายเหตุ /* คือมีการทำเป็นประจำทุกวันใน ๑ เดือน

แผนปฏิบัติงานบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. ๒๕๖๗		
ลำดับ	**แผนการปฏิบัติงาน**	**กลุ่มงาน/ผู้รับผิดชอบ**
๑	แผนการตรวจสอบการทำงานของระบบดับเพลิงอัตโนมัติ	กลุ่มบริการระบบสารสนเทศ ๒
๒	แผนการตรวจสอบการทำงานของระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ	กลุ่มบริการระบบสารสนเทศ ๒
๓	แผนการตรวจสอบการทำงานของระบบสลับจ่ายกระแสไฟฟ้า	กลุ่มบริการระบบสารสนเทศ ๒
๔	แผนการตรวจสอบระบบตรวจจับการรั่วซึมของน้ำ	กลุ่มบริการระบบสารสนเทศ ๒
๕	แผนการตรวจสอบเครื่องปรับอากาศควบคุมอุณหภูมิและความชื้น	กลุ่มบริการระบบสารสนเทศ ๒
๖	แผนการตรวจสอบระบบควบคุมการปิด-เปิด ประตูอัตโนมัติ	กลุ่มบริการระบบสารสนเทศ ๒
๗	แผนการตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และการเฝ้าระวังเครือข่าย	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๘	แผนการตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลัก (Server) และระบบเครือข่าย (Network)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๙	แผนการสำรองข้อมูล (Backup) ระบบให้บริการอุปกรณ์และระบบเครือข่าย (Mtn System)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๑๐	แผนการ Backup & Restore เครื่องคอมพิวเตอร์แม่ข่าย	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๑๑	แผนการตรวจสอบ อัพเดตโปรแกรมป้องกันไวรัส Kaspersky Server	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๑๒	แผนปฏิบัติงาน การประชุมทางไกลผ่านเครือข่าย (VDO Conference)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๑๓	แผนการตรวจสอบการทำงานของระบบโทรศัพท์บนเครือข่ายอินเทอร์เน็ต (IP Phone)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๑๔	แผนการสำรอง (Backup) ฐานข้อมูลระบบขอรับบริการด้านอุปกรณ์และระบบเครือข่าย	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๑๕	แผนการนำข้อมูลกลับคืน (Restore) ระบบขอรับบริการด้านอุปกรณ์และระบบเครือข่าย	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๑๖	แผนการสำรอง (Backup) ฐานข้อมูลระบบรายงานชนิดและปริมาณมลพิษที่ระบายจากโรงงาน	กลุ่มบริการระบบสารสนเทศ ๒
๑๗	แผนการสำรองข้อมูล (Backup) ระบบการจัดการวัสดุที่ไม่ใช้แล้วทางอิเล็กทรอนิกส์	กลุ่มบริการระบบสารสนเทศ ๒
๑๘	แผนปฏิบัติงานการจัดหาซอฟต์แวร์พื้นฐานที่ถูกกฎหมายมาใช้งานกรมโรงงานอุตสาหกรรม	กลุ่มบริการอุปกรณ์และระบบเครือข่าย

แผนปฏิบัติงานบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. ๒๕๖๗		
ลำดับ	**แผนการปฏิบัติงาน**	**กลุ่มงาน/ผู้รับผิดชอบ**
๑๙	แผนการสำรอง (Backup) ฐานข้อมูลและระบบงานวัตถุอันตราย - บุคลากรเฉพาะด้านวัตถุอันตราย (เครื่อง OPMS หรือ Dell-server16) - ระบบติดตามการอนุญาตวัตถุอันตราย (เครื่อง Eis) - ระบบการเชื่อมโยงข้อมูลการส่งไปกรมศุลกากร NSW (EBMSDB) - ฐานข้อมูลระบบการอนุญาตวัตถุอันตราย (Oracle๕)	กลุ่มบริการระบบสารสนเทศ ๔
๒๐	แผนจัดทำรายงานข้อมูล	ศูนย์ข้อมูลธุรกิจอุตสาหกรรม
๒๑	แผนทำการแก้ไขเมื่อได้รับแจ้งจากผู้ใช้งาน	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๒๒	แผนการทำ Authentication การเข้าใช้ระบบสารสนเทศรวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ)	กลุ่มบริการระบบสารสนเทศกลาง
๒๓	แผนการจัดระดับการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล	กลุ่มบริการระบบสารสนเทศกลาง
๒๔	แผนตรวจสอบช่องโหว่และดำเนินการแก้ไข ระบบขอรับบริการด้านอุปกรณ์และระบบเครือข่าย	กลุ่มบริการอุปกรณ์และระบบเครือข่าย
๒๕	แผนตรวจสอบช่องโหว่และดำเนินการแก้ไข ระบบทะเบียนโรงงาน	กลุ่มบริการระบบสารสนเทศ ๓
๒๖	แผนตรวจสอบช่องโหว่และดำเนินการแก้ไข ระบบงานวัตถุอันตราย	กลุ่มบริการระบบสารสนเทศ ๔
๒๗	แผนตรวจสอบช่องโหว่และดำเนินการแก้ไข เว็บไซต์กรมโรงงานอุตสาหกรรม	กลุ่มบริการระบบสารสนเทศกลาง
๒๘	แผนตรวจสอบช่องโหว่และดำเนินการแก้ไข ระบบงานทะเบียนเครื่องจักร และระบบจดทะเบียนเครื่องจักรออนไลน์	กลุ่มบริการระบบสารสนเทศ ๑
๒๙	แผนตรวจสอบช่องโหว่และดำเนินการแก้ไข ระบบการจัดการวัสดุที่ไม่ใช้แล้วทางอิเล็กทรอนิกส์	กลุ่มบริการระบบสารสนเทศ ๒
๓๐	แผนการสำรองข้อมูล (Backup) ระบบงานทะเบียนเครื่องจักร และระบบจดทะเบียนเครื่องจักรออนไลน์	กลุ่มบริการระบบสารสนเทศ ๑
๓๑	แผนการสำรองข้อมูล (Backup) ระบบทะเบียนโรงงาน	กลุ่มบริการระบบสารสนเทศ ๓
๓๒	แผนการสำรองข้อมูล (Backup) เว็บไซต์กรมโรงงานอุตสาหกรรม	กลุ่มบริการระบบสารสนเทศกลาง

บทที่ ๓
การติดตามและรายงานผล

การติดตามและรายงานผล มีการดำเนินงานดังต่อไปนี้

๑. ติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารระหว่างปฏิบัติงาน เพื่อให้เป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที โดยทำการติดตามและประเมินผลรายไตรมาส

๒. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ ต่อคณะทำงานบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมโรงงานอุตสาหกรรม ทุกสิ้นไตรมาส เพื่อทราบและมั่นใจว่าการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศมีคุณภาพ และมีความเหมาะสม

๓. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ทุกสิ้นปีงบประมาณ เพื่อทราบและมั่นใจว่าการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศมีคุณภาพ และมีความเหมาะสม

๔. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (DCIO) ภายในไตรมาสแรกของงบประมาณถัดไป เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และวิเคราะห์ถึงปัญหาที่เกิดขึ้นเพื่อเสนอแนวทางแก้ไขอย่างถูกต้องและมีประสิทธิภาพ

คำสั่งกรมโรงงานอุตสาหกรรม
ที่ ๑๙๕ /๒๕๖๗
เรื่อง แต่งตั้งคณะทำงานบริหารความเสี่ยงและความปลอดภัย
ด้านเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรม

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบกับปัจจุบันกรมโรงงานอุตสาหกรรม มีการใช้ระบบสารสนเทศเป็นเครื่องมือในการปฏิบัติงานโดยมีการเข้าถึงระบบเครือข่ายทั้งภายในและภายนอกหน่วยงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงเพื่อให้เกิดความมั่นคงและปลอดภัยทางด้านเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรม ให้เป็นไปตามแนวทางปฏิบัติและกรอบมาตรฐานต่าง ๆ ภายใต้กฎหมายดังกล่าว

ดังนั้น อธิบดีกรมโรงงานอุตสาหกรรม จึงมีคำสั่งแต่งตั้งคณะทำงานบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรม โดยมีองค์ประกอบและอำนาจหน้าที่ ดังนี้

องค์ประกอบ

๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ประธานคณะทำงาน
๒. ผู้อำนวยการกลุ่มบริการระบบสารสนเทศ ๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงาน
๓. ผู้อำนวยการกลุ่มบริการระบบสารสนเทศ ๒ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงาน
๔. ผู้อำนวยการกลุ่มบริการระบบสารสนเทศ ๓ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงาน
๕. ผู้อำนวยการกลุ่มบริการระบบสารสนเทศ ๔ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงาน
๖. ผู้อำนวยการกลุ่มบริการระบบสารสนเทศกลาง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงาน
๗. ผู้อำนวยการศูนย์ข้อมูลธุรกิจอุตสาหกรรม ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงาน

๘. ผู้อำนวย...

๘. ผู้อำนวยการกลุ่มบริการอุปกรณ์และระบบเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร — คณะทำงานและเลขานุการ

๙. นายโยธิน คำนนท์ นักวิชาการคอมพิวเตอร์ชำนาญการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร — คณะทำงานและผู้ช่วยเลขานุการ

๑๐. นายภาณุพงศ์ สงวนประเสริฐ นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร — คณะทำงานและผู้ช่วยเลขานุการ

๑๑. นายวชิรพงษ์ แน่นหนา นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร — คณะทำงานและผู้ช่วยเลขานุการ

อำนาจหน้าที่

๑. จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมโรงงานอุตสาหกรรม

๒. บริหารจัดการด้านการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมโรงงานอุตสาหกรรม

๓. ติดตามและประเมินผลการดำเนินงานด้านการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

๔. นำผลการประเมินการบริหารความเสี่ยงไปปรับปรุงแผนบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศในปีต่อไป

๕. ปฏิบัติงานอื่น ๆ ที่เกี่ยวข้องตามที่อธิบดีกรมโรงงานอุตสาหกรรม มอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๘ มิถุนายน พ.ศ. ๒๕๖๗

(นายจุลพงษ์ ทวีศรี)
อธิบดีกรมโรงงานอุตสาหกรรม