แผนบริหารความเสี่ยง
และความปลอดภัยทางไซเบอร์

พ.ศ. ๒๕๖๗

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

การบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์
กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑. หลักการและเหตุผล

การบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์ มีบทบาทสำคัญในการป้องกันระบบเทคโนโลยีสารสนเทศและข้อมูลที่เป็นสินทรัพย์ของหน่วยงาน และเป็นการป้องกันภารกิจของหน่วยงานให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง หน่วยงานจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อความสามารถในการดำเนินภารกิจของหน่วยงานให้บรรลุผลสำเร็จได้ด้วย ดังนั้นการประเมินความเสี่ยงและความปลอดภัยทางไซเบอร์จึงเป็นหนึ่งในเครื่องมือที่ใช้สำหรับการจัดการความมั่นคงปลอดภัยของทรัพยากรด้านสารสนเทศของหน่วยงาน

๒. วัตถุประสงค์

(๑) เพื่อเป็นแนวทางปฏิบัติในการบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์ของหน่วยงาน

(๒) เพื่อป้องกันความเสียหายที่เกิดจากเหตุการณ์ที่ไม่พึงประสงค์ต่อทรัพยากรด้านเทคโนโลยีสารสนเทศและมีผลต่อการดำเนินงานของหน่วยงาน

(๓) เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๓. ขอบเขตการดำเนินการ

การบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์เป็นการบริหารจัดการภายในความรับผิดชอบของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๔. ความหมายและคำจำกัดความของการบริหารจัดการความเสี่ยง

๔.๑ ความเสี่ยง (Risk)

ความเสี่ยง คือ โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร

การบริหารความเสี่ยง คือ กระบวนการดำเนินงานขององค์กรที่เป็นระบบและต่อเนื่อง เพื่อช่วยให้องค์กรลดมูลเหตุของแต่ละโอกาสที่จะเกิดความเสียหายทั้งจากการกำหนดนโยบาย การปฏิบัติงานและการทุจริตให้ระดับของความเสียหายและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรประเมินได้ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายและภาพลักษณ์ขององค์กรเป็นสำคัญ

๔.๒ ปัจจัยความเสี่ยง (Risk Factor)

ปัจจัยความเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้องค์กรไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน กระบวนงานใด เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไมถึงเกิด ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการป้องกันความเสี่ยงในภายหลังได้อย่างถูกต้อง

๔.๓ การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด ผลกระทบ และระดับของความเสี่ยงนั้น

๑) โอกาสที่จะเกิด หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง

๒) ผลกระทบ หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุความเสี่ยง

๓) ระดับของความเสี่ยง หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น ๕ ระดับ คือ สูงมาก สูง ปานกลาง ต่ำ และต่ำมาก

๔.๔ การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยง หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง หรืออยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยงมีหลายวิธี ดังนี้

๑) การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้น เนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง

๒) การลดการควบคุมความเสี่ยง (Risk Reduction) เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

๓) การกระจายความเสี่ยง หรือการโอนความเสี่ยง (Risk Sharing) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งความรับผิดชอบไป

๔) หลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการความเสี่ยงที่อยู่ในระดับความสูงมากและหน่วยงานไม่อาจยอมรับได้ จึงต้องตัดสินใจยกเลิกโครงการหรือกิจกรรมนั้น

๔.๕ การควบคุม (Control)

การควบคุม หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการขององค์กรบรรลุวัตถุประสงค์ตามเป้าหมาย แบ่งได้ ๔ ประเภท คือ

๑) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยง และข้อผิดพลาดตั้งแต่แรก

๒) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว

๓) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดการป้องกัน

๔) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

๕. กระบวนการบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์

๕.๑ การระบุความเสี่ยง (Risk Identification)

การชี้ให้เห็นถึงความเสี่ยงที่หน่วยงานเผชิญอยู่ กระบวนการนี้จำเป็นต้องอาศัยความรู้ความเข้าใจหน่วยงาน ภารกิจและกิจกรรมสิ่งแวดล้อมด้านกฎหมาย สังคม วัฒนธรรม พัฒนาการและปัจจัยทีมีต่อความสำเร็จของหน่วยงาน รวมทั้งโอกาสและภัยคุกคามที่มีต่อหน่วยงาน การชี้ระบุความเสี่ยงควรดำเนินการอย่างทั่วถึงครอบคลุมกิจกรรมในทุก ๆ ด้านของหน่วยงาน สาเหตุสำคัญของความเสี่ยง คือ การมีภัยคุกคาม (Threat) ที่อาจส่งผลให้เกิดการละเมิดความมั่นคงปลอดภัยทางไซเบอร์และส่งผลเสียตามมา

การชี้ระบุความเสี่ยง อาจพิจารณาถึงเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีตกับหน่วยงานนั้นหรือหน่วยงานอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ตาม กระบวนการในการชี้ระบุความเสี่ยงอาจใช้วิธีการต่าง ๆ ร่วมกัน ดังนี้

(๑) การระดมสมอง (Brain Storming)
(๒) การออกแบบสอบถาม (Questionnaire)
(๓) การวิเคราะห์กระบวนการการทำงานหรือกิจกรรมในภารกิจ (Business Process Analysis)
(๔) การวิเคราะห์สภาพการณ์เหตุการณ์ละเมิดความมั่นคง (Scenario Analysis)
(๕) การประชุมเชิงปฏิบัติการด้านการประเมินความเสี่ยง (Risk Assessment Workshop)
(๖) การสืบสวนเหตุการณ์ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (Incident Investigation)
(๗) การตรวจสอบและการตรวจสภาพระบบ (Auditing and Inspection)
(๘) การวิเคราะห์สถานการณ์ (SWOT Analysis)

การบรรยายลักษณะรายละเอียดของความเสี่ยง (Description of Risk) เมื่อชี้ระบุความเสี่ยงได้แล้วและบรรยายรายละเอียดและลักษณะของความเสี่ยงได้ ดังนี้

(๑) ชื่อความเสี่ยง
(๒) ขอบเขต
(๓) ลักษณะความเสี่ยง
(๔) ผู้ที่มีผลกระทบ
(๕) ลักษณะเชิงประมาณ
(๖) การยอมรับความเสี่ยง
(๗) การบำบัดและการควบคุม
(๘) แนวทางการปรับปรุง
(๙) การพัฒนากลยุทธ์และนโยบาย

๕.๒ การประมาณความเสี่ยง (Risk Estimation) ขั้นตอนนี้เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

โอกาส หรือความน่าจะเป็น (Probability or Likelihood) หรือความบ่อยครั้งของการเกิดเหตุ หรือเหตุการณ์ อาจแบ่งเป็น ๕ ระดับ ดังนี้

(๑) สูงมาก
(๒) สูง
(๓) ปานกลาง
(๔) น้อย
(๕) น้อยมาก

ความรุนแรงของสิ่งที่เกิดขึ้นตามมา (Severity of Consequence) อาจแบ่งเป็น ๕ ระดับ ดังนี้

(๑) สูงมาก

(๒) สูง

(๓) ปานกลาง

(๔) ต่ำ

(๕) ต่ำมาก

๕.๓ การประเมินความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยของขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคงปลอดภัย ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ X ความรุนแรงของเหตุการณ์ต่าง ๆ

ซึ่งหน่วยงานใช้เกณฑ์ในการจัดแบ่ง ดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑-๓	ต่ำมาก	ยอมรับความเสี่ยง	ขาว
๔-๘	ต่ำ	ยอมรับความเสี่ยง (มีแผนรองรับ)	เหลืองอ่อน
๙-๑๖	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗-๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ส้ม
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยงโดยจัดลำดับจากผลกระทบและความเป็นไปได้ที่จะเกิดขึ้น

ความเสี่ยงปานกลาง - ผลกระทบรุนแรงมาก - โอกาสเกิดน้อย	**ความเสี่ยงสูง** - ผลกระทบรุนแรงมาก - โอกาสเกิดมาก
ความเสี่ยงต่ำ - ผลกระทบน้อย - โอกาสเกิดน้อย	**ความเสี่ยงปานกลาง** - ผลกระทบน้อย - โอกาสเกิดมาก

การประเมินความเสี่ยง

ผลกระทบ							
๕	๕	๑๐	๑๕	๒๐	๒๕	สีแดง	ความเสี่ยงสูงมาก (ถ่ายโอนความเสี่ยง)
๔	๔	๘	๑๒	๑๖	๒๐	สีส้ม	ความเสี่ยงสูง (ควบคุมความเสี่ยง มีแผนควบคุม)
๓	๓	๖	๙	๑๒	๑๕	สีเหลือง	ความเสี่ยงปานกลาง (มีมาตรการติดตาม)
๒	๒	๔	๖	๘	๑๐	สีเหลืองอ่อน	ความเสี่ยงต่ำ (ยอมรับได้ มีแผนรองรับ)
๑	๑	๒	๓	๔	๕	สีขาว	ความเสี่ยงต่ำมาก (ยอมรับได้)
	๑	๒	๓	๔	๕		

โอกาสที่จะเกิด

๕.๔ การบรรเทาความเสี่ยง (Risk Mitigation)

การบรรเทาความเสี่ยงเกี่ยวข้องกับการจัดลำดับ การคำนวณความเสี่ยง และการลงมือควบคุมการลดความเสี่ยงอย่างเหมาะสมตามแนวทางที่มาจากการประเมินความเสี่ยง เนื่องจากการที่จะกำจัดความเสี่ยงในระบบทั้งหมดนั้นเป็นเรื่องที่ทำได้ยาก ผู้บังคับบัญชาของหน่วยงานจะต้องเป็นผู้รับผิดชอบการทำงานนี้ เพื่อให้เกิดประสิทธิภาพสูงสุด และวิธีการควบคุมที่เหมาะสมที่สุดเพื่อลดระดับความเสี่ยงให้อยู่ในระดับยอมรับได้ โดยส่งผลกระทบต่อภารกิจและทรัพยากรของหน่วยงานให้น้อยที่สุด

ทางเลือกเพื่อบรรเทาความเสี่ยง สามารถแบ่งออกเป็น ๕ ประเภท ดังนี้

(๑) การยอมรับความเสี่ยง (Risk Acceptance) คือ การยอมรับความเสี่ยงในระดับที่เป็นอยู่และให้ระบบเทคโนโลยีสารสนเทศดำเนินงานไปตามปกติ ซึ่งเป็นการยอมรับในผลที่อาจตามมา

(๒) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยงความเสี่ยงด้วยการกำจัดสาเหตุของความเสี่ยง เช่น เมื่อพบว่าปัจจุบันหน่วยงาน มีการสำรองข้อมูลเพียง ๑ ชุด และจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจกระทำได้โดย การสำรองข้อมูล ๒ ชุด และแยกเก็บในสถานที่ต่างกันหรือระบบสารสนเทศที่มีชั้นความลับ ลับมาก ต้องห้ามมีการเชื่อมต่อกับอินเทอร์เน็ต เพื่อหลีกเลี่ยงภัยจาก Hacker

(๓) การจำกัดความเสี่ยง (Risk Limitation) คือ การทำระบบควบคุมเพื่อให้เกิดผลกระทบจากการถูกคุกคามระบบหรือจากความไม่มั่นคงของระบบให้น้อยที่สุด เช่น การใช้ Firewall ป้องกันระบบจากภัยคุกคามในอินเทอร์เน็ต

(๔) การวิจัยและการรับรู้ความเสี่ยง (Research and Acknowledgement) คือ การลดความสูญเสียที่เกิดจากความเสี่ยงโดยการตรวจสอบเพื่อรับทราบความอ่อนแอของระบบและค้นคว้าวิจัยให้ได้วิธีการควบคุมเพื่อเสริมความมั่นคงให้แก่ระบบ

(๕) การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การถ่ายโอนความเสี่ยงด้วยการหาทางเลือกอื่นเพื่อชดเชยความสูญเสีย เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน หน่วยงานอาจเลือกซื้อประกัน หรือสัญญาการซ่อมบำรุง เป็นต้น

๕.๕ การควบคุมความเสี่ยง (Risk Control)

เมื่อต้องมีการควบคุมเกิดขึ้นสิ่งที่ต้องปฏิบัติ คือ ระบุความเสี่ยงที่เกิดขึ้นให้มากที่สุด แล้วพยายามหาวิธีลดความเสี่ยงด้วยวิธีที่มีต้นทุนต่ำและส่งผลกระทบต่อภารกิจอื่น ๆ ของหน่วยงานให้น้อยที่สุด กระบวนการในการควบคุมความเสี่ยงสรุปได้ ดังนี้

(๑) จัดลำดับความสำคัญของการปฏิบัติงาน (Prioritize Actions) จากผลการจัดลำดับความเสี่ยงในกระบวนการประเมินความเสี่ยง นำไปสู่การจัดลำดับการลงมือปฏิบัติงานด้วย ภายใต้ทรัพยากรที่มีอยู่ลำดับแรกสุดควรจะเลือกลงมือกับความเสี่ยงที่มีระดับความเสี่ยงสูง ซึ่งต้องการการแก้ไขในทันทีเพื่อปกป้องภารกิจของหน่วยงาน ผลลัพธ์ที่ได้ คือ ลำดับการลงมือจัดการความเสี่ยง

(๒) ประเมินทางเลือกในการควบคุม (Evaluate Recommended Control Options) วิธีการควบคุมที่ถูกเสนอในกระบวนการประเมินความเสี่ยงอาจไม่ใช่วิธีที่เหมาะสมที่สุด หรือเป็นทางเลือกที่เป็นไปได้ที่สุดสำหรับแต่ละหน่วยงาน ขั้นตอนนี้จึงเป็นการเลือกวิธีการที่มีความเป็นไปได้มากที่สุดที่จะสามารถบรรเทาความเสี่ยงได้ ผลลัพธ์ที่ได้ คือ รายชื่อของวิธีการควบคุม

(๓) วิเคราะห์ผลประโยชน์ที่ได้รับ (Conduct Cost-Benefit Analysis) การวิเคราะห์ผลประโยชน์จะช่วยให้ผู้บังคับบัญชาสามารถตัดสินใจ และเลือกวิธีการควบคุมที่มีประสิทธิภาพ

(๔) เลือกวิธีการควบคุม (Select Control) จากพื้นฐานผลลัพธ์ที่ได้จากการวิเคราะห์ผลประโยชน์ ผู้บังคับบัญชาสามารถตรวจสอบวิธีการควบคุมทั้งหมด และเลือกวิธีที่ครอบคลุมทั้งการควบคุมเชิงเทคนิค เชิงปฏิบัติการ และเชิงบริหารเพื่อให้มั่นใจความเพียงพอต่อความต้องการความปลอดภัยของระบบและหน่วยงาน

(๕) มอบหมายความรับผิดชอบ (Assign Responsibility) คือ การเลือกบุคคลที่เหมาะสม ซึ่งมีความเชี่ยวชาญและมีทักษะในการลงมือควบคุม พร้อมมอบหมายหน้าที่รับผิดชอบ

(๖) พัฒนาแผนการปฏิบัติงานเพื่อการป้องกัน (Develop a Safeguard Implementation Plan) อย่างน้อยที่สุด แผนงานควรจะประกอบด้วยข้อมูล ดังต่อไปนี้

๑) ความเสี่ยงและระดับความเสี่ยง
๒) วิธีการควบคุมที่ได้รับการแนะนำ
๓) การปฏิบัติงานที่ได้รับการจัดลำดับไว้
๔) การเลือกวิธีการควบคุม
๕) ทรัพยากรที่ต้องการใช้ในการลงมือควบคุม
๖) รายชื่อผู้มีหน้าที่รับผิดชอบ
๗) กำหนดวันที่เริ่มลงมือปฏิบัติ
๘) กำหนดวันเสร็จสิ้นการปฏิบัติ
๙) รายละเอียดการดูแลรักษาระบบ

(๗) ลงมือปฏิบัติตามวิธีการควบคุมที่เลือก (Implement Selected Control) ขึ้นอยู่กับแต่ละสถานการณ์ บางครั้งการควบคุมอาจจะลดความเสี่ยงได้ แต่ไม่สามารถกำจัดความเสี่ยงนั้นออกจากระบบหรือหน่วยงานได้ ซึ่งอาจทำให้มีความเสี่ยงที่ยังเหลืออยู่แต่เป็นความเสี่ยงที่หน่วยงานสามารถยอมรับได้

แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์
กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑. หลักการและเหตุผล

เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทที่สำคัญต่อกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ และถูกนำมาใช้เป็นเครื่องมือในการจัดการข้อมูล การบริการต่าง ๆ ให้มีคุณภาพเพื่อใช้ในการปฏิบัติงาน การตัดสินใจและการสื่อสารให้มีประสิทธิภาพและประสิทธิผล ดังนั้น การบริหารจัดการเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยจากปัจจัยเสี่ยงต่าง ๆ จึงเป็นสิ่งที่จำเป็นอย่างยิ่งต่อการดำเนินงานขององค์กร

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ของหน่วยงาน แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ฉบับนี้ จึงได้จัดทำขึ้นมาเพื่อใช้เป็นแนวทางปฏิบัติประกอบการบริหารความเสี่ยงเพื่อช่วยลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อกระบวนการบริหารงานของหน่วยงาน

๒. วัตถุประสงค์

(๑) เพื่อเป็นแนวทางในการบริหารเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานให้มีความมั่นคงปลอดภัยมากขึ้น

(๒) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศและการสื่อสาร

(๓) เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงและความปลอดภัยทางไซเบอร์

(๔) เพื่อให้ผู้ปฏิบัติงานได้รับทราบและเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ การเผยแพร่ความรู้เกี่ยวกับความเสี่ยงและความปลอดภัยทางไซเบอร์ของหน่วยงาน

(๕) เพื่อให้มีการปฏิบัติตามกระบวนการบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง

๓. การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ของหน่วยงานสามารถแยกประเภทความเสี่ยงออกเป็น ๔ ประเภท ดังนี้

(๑) ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์อาจถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะระบบ ทำลายระบบจาก Cracker เป็นต้น

(๒) ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

(๓) ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

(๔) ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๔. การระบุความเสี่ยง (Risk Identification)

การระบุถึงความเสี่ยงพื้นฐานที่สำคัญที่จำเป็นต้องจัดการจากการศึกษาสถานภาพปัจจุบันของการบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ พบว่ามีความเสี่ยงด้านต่าง ๆ ทั้งสิ้น ๑๑ ความเสี่ยง (R01-R11) ตามตารางแสดงรายละเอียดความเสี่ยง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงในการให้ผู้อื่นเข้าถึงข้อมูลของตนเองโดยไม่มีสิทธิ (R01)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้งานระบบสารสนเทศ เช่น มอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ (R02)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อกับระบบเครือข่ายหน่วยงาน โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าความปลอดภัยให้ถูกต้อง	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - ระบบเครือข่าย
๓. ความเสี่ยงจากเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ (R03)	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้ ได้แก่ Web Server, Mail Server, File Server, Database Server	- การตั้งค่าอุปกรณ์ผิดพลาด - การทำงานผิดพลาดของอุปกรณ์ - อุปกรณ์เครื่องแม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดต - ความเสี่ยงจากไวรัสคอมพิวเตอร์ - ความเสี่ยงจากการโจมตีของผู้ไม่ประสงค์ดี	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - ระบบเครือข่าย - อุปกรณ์เครือข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๔. ความเสี่ยงจากระบบเครือข่าย (R04)	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์มีการทำงานผิดพลาดของอุปกรณ์เครือข่ายหลัก ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ - ความเสี่ยงจากการโจมตีของผู้ไม่ประสงค์ดี - ความเสี่ยงจากไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - ระบบเครือข่าย - อุปกรณ์เครือข่าย
๕. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์ (R05)	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถทำงานได้ - มัลแวร์ทำให้เกิดช่องโหว่ให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมคอมพิวเตอร์ โจรกรรมข้อมูล - Ransomware ทำให้เครื่องคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - ระบบเครือข่าย - อุปกรณ์เครือข่าย
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker (R06)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (DoS, DDoS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้าย หรือไฟล์ Auto Run - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ - ไฟล์ที่ผู้ใช้บริการ Download มีการฝังไวรัสคอมพิวเตอร์ คำสั่งอันตราย อันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี - การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การตั้งค่าความปลอดภัยอุปกรณ์เครือข่ายไม่รัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Load Balance - ระบบปฏิบัติการไม่อัพเดตทำให้มีช่องโหว่	- ระบบสารสนเทศ - ระบบฐานข้อมูล - ระบบเครือข่าย - อุปกรณ์เครือข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๗. ความเสี่ยงจากการทำงานโปรแกรมประยุกต์ทำงานผิดพลาดเป็นช่องโหว่ของโปรแกรม (R07)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดจากโปรแกรมประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรมหรือช่องโหว่ของโปรแกรม	- การทำงานผิดพลาดของโปรแกรม - ช่องโหว่ของโปรแกรม เกิดจากไม่มีการอัพเดตระบบอย่างสม่ำเสมอ - โปรแกรมประยุกต์ติดต่อฐานข้อมูลไม่ได้ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์อาจเกิดการติดไวรัส มัลแวร์ หรือเกิดช่องโหว่ที่นำไปสู่ความไม่ปลอดภัยทางไซเบอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - ระบบเครือข่าย
๘. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้ (R08)	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์เครือข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตทำให้มีช่องโหว่ - ความเสี่ยงจากไวรัสคอมพิวเตอร์ - ความเสี่ยงจากการโจมตีของผู้ไม่ประสงค์ดี - อุปกรณ์ในระบบเครือข่ายชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
๙. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ (R09)	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑๐. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ (R10)	ความเสี่ยงจากการปฏิบัติงาน	การใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์อาจทำให้เกิดโอกาสการโจมตีได้สูง และเป็นการดำเนินงานที่ผิดกฎหมาย	- การอำพรางหรือสวมรอยผู้ใช้ - การโจมตีจากผู้บุกรุกมีโอกาสสูง - ละเมิดลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ภาพลักษณ์ขององค์กร - ระบบเครือข่าย - ระบบสารสนเทศ
๑๑. ความเสี่ยงจากการขาดแคลนบุคลากรที่เชี่ยวชาญด้านไซเบอร์ (R11)	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านไซเบอร์ทำให้การทำงานหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบการพัฒนาและควบคุมดูแลระบบ	- บุคลากรที่เชียวชาญด้านไซเบอร์มีจำนวนไม่เพียงพอ - หลักสูตรฝึกอบรมความรู้ด้านไซเบอร์มีราคาสูง - ความรู้ความเข้าใจด้านไซเบอร์มีซับซ้อนและความยาก	- ผู้ดูแลระบบ - ระบบเครือข่าย - ระบบสารสนเทศ - องค์กร

๕. การประมาณค่าความเสี่ยง (Risk Estimation)

หลักเกณฑ์การประมาณที่จะใช้ในการประมาณระดับความเสี่ยง ซึ่งเป็นการวิเคราะห์โอกาสที่จะเกิดความเสี่ยงและระดับความรุนแรงของผลกระทบที่เกิดจากเหตุการณ์กรณีที่ความเสี่ยงนั้นเกิดขึ้นจริง โดยหน่วยงานใช้เกณฑ์ระดับความเสี่ยง ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	๑๕ ครั้งขึ้นไปต่อปี หรือโอกาสที่จะเกิดสูงมาก
๔	สูง	ไม่เกิน ๑๕ ครั้งต่อปี หรือโอกาสที่จะเกิดสูง
๓	ปานกลาง	ไม่เกิน ๑๐ ครั้งต่อปี หรือโอกาสที่จะเกิดปานกลาง
๒	น้อย	ไม่เกิน ๕ ครั้งต่อปี หรือโอกาสที่จะเกิดน้อย
๑	น้อยมาก	ไม่เกิน ๑ ครั้งต่อปี หรือโอกาสที่จะเกิดน้อยมาก

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	เกิดความสูญเสียต่อระบบที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	ระบบที่สำคัญมีปัญหา และส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	เกิดเหตุร้ายที่ค่อนข้างมีความสำคัญ
๑	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

การประมาณค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับโอกาสที่เกิด	ระดับความรุนแรง
๑. ความเสี่ยงในการให้ผู้อื่นเข้าถึงข้อมูลของตนเองโดยไม่มีสิทธิ (R01)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้งานระบบสารสนเทศ เช่น มอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๓	๒
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ (R02)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อกับระบบเครือข่ายหน่วยงาน โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าความปลอดภัยให้ถูกต้อง	๒	๔
๓. ความเสี่ยงจากเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ (R03)	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้ ได้แก่ Web Server, Mail Server, File Server, Database Server	๒	๔
๔. ความเสี่ยงจากระบบเครือข่าย (R04)	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์มีการทำงานผิดพลาดของอุปกรณ์เครือข่ายหลัก ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	๑	๕

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับโอกาสที่เกิด	ระดับความรุนแรง
๕. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์ (R05)	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถทำงานได้ - มัลแวร์ทำให้เกิดช่องโหวให้ผู้ไม่หวังดีเข้ามาควบคุมคอมพิวเตอร์ โจรกรรมข้อมูล - Ransomware ทำให้เครื่องคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	๒	๔
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker (R06)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (DoS,DDoS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้าย หรือไฟล์ Auto Run - มีการฝั่งโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่างๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ - ไฟล์ที่ผู้ใช้บริการ Download มีการฝังไวรัสคอมพิวเตอร์ คำสั่งอันตราย อันก่อให้เกิดช่องโหวให้ Hacker เข้ามาโจมตี	๓	๔
๗. ความเสี่ยงจากการทำงานโปรแกรมประยุกต์ทำงานผิดพลาดเป็นช่องโหว่ของโปรแกรม (R07)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดจากโปรแกรประยุกต์ต่างๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรมหรือช่องโหว่ของโปรแกรม	๒	๒
๘. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้ (R08)	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	๒	๓
๙. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ (R09)	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	๑	๕

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับโอกาสที่เกิด	ระดับความรุนแรง
๑๐. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ (R10)	ความเสี่ยงจากการปฏิบัติงาน	การใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์อาจทำให้เกิดโอกาสการโจมตีได้สูงและเป็นการดำเนินงานที่ผิดกฎหมาย	๓	๔
๑๑. ความเสี่ยงจากการขาดแคลนบุคลากรที่เชี่ยวชาญด้านไซเบอร์ (R11)	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านไซเบอร์ ทำให้การทำงานหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบการพัฒนาและควบคุมดูแลระบบ	๓	๔

๖. การประเมินค่าความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยงพิจารณาจากปัจจัยของโอกาสที่ภัยคุกคามที่เกิดขึ้น ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ โดยเกณฑ์การประเมินระดับความรุนแรงของความเสี่ยงของหน่วยงาน มีดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ X ความรุนแรงของเหตุการณ์ต่างๆ

ระดับความเสี่ยง	ค่าความเสี่ยง (โอกาส x ผลกระทบ)	เกณฑ์การประเมิน
สูงมาก	๒๕	อยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งรัดจัดการความเสี่ยงให้ลดลงและอยู่ในระดับที่ยอมรับได้ (ถ่ายโอนความเสี่ยง)
สูง	๑๗ – ๒๔	อยู่ในระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (มีแผนควบคุมความเสี่ยง)
ปานกลาง	๙ – ๑๖	อยู่ในระดับที่ยอมรับได้ สามารถดำเนินการควบคุมโดยกระบวนการควบคุมภายใน (มีมาตรการติดตาม)
ต่ำ	๔ – ๘	อยู่ในระดับที่ยอมรับได้ แต่ต้องควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยง (มีแผนรองรับ)
ต่ำมาก	๑ - ๓	อยู่ในระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง

การประเมินค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับโอกาสที่เกิด	ระดับความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงในการให้ผู้อื่นเข้าถึงข้อมูลของตนเองโดยไม่มีสิทธิ (R01)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้งานระบบสารสนเทศ เช่น มอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๕	๒	๑๐
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ (R02)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อกับระบบเครือข่ายหน่วยงาน โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าความปลอดภัยให้ถูกต้อง	๒	๔	๘
๓. ความเสี่ยงจากเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ (R03)	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้ ได้แก่ Web Server, Mail Server, File Server, Database Server	๔	๕	๒๐
๔. ความเสี่ยงจากระบบเครือข่าย (R04)	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์มีการทำงานผิดพลาดของอุปกรณ์เครือข่ายหลัก ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	๔	๕	๒๐
๕. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์ (R05)	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถทำงานได้ -มัลแวร์ทำให้เกิดช่องโหว่ให้ผู้ไม่หวังดีเข้ามาควบคุมคอมพิวเตอร์ โจรกรรมข้อมูล - Ransomware ทำให้เครื่องคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้ และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	๔	๕	๒๐
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker (R06)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (DoS, DDoS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้าย หรือไฟล์ Auto Run - มีการฝังโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่างๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ - ไฟล์ที่ผู้ใช้บริการ Download มีการฝังไวรัสคอมพิวเตอร์ คำสั่งอันตราย อันก่อให้เกิดช่องโหว่ให้ Hacker เข้ามาโจมตี	๔	๕	๒๐

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับโอกาสที่เกิด	ระดับความรุนแรง	ระดับคะแนน
๗. ความเสี่ยงจากการทำงานโปรแกรมประยุกต์ทำงานผิดพลาดเป็นช่องโหว่ของโปรแกรม (R07)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดจากโปรแกรประยุกต์ต่างๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรมหรือช่องโหว่ของโปรแกรม	๓	๕	๑๕
๘. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้ (R08)	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	๔	๕	๒๐
๙. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ (R09)	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	๑	๕	๕
๑๐. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ (R10)	ความเสี่ยงจากการปฏิบัติงาน	การใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์อาจทำให้เกิดโอกาสการโจมตีได้สูงและเป็นการดำเนินงานที่ผิดกฎหมาย	๒	๕	๑๐
๑๑. ความเสี่ยงจากการขาดแคลนบุคลากรที่เชี่ยวชาญด้านไซเบอร์ (R11)	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านไซเบอร์ ทำให้การทำงานหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบการพัฒนาและควบคุมดูแลระบบ	๔	๔	๑๖

๗. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk Reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศและไซเบอร์ในการบริหารจัดการได้อย่างมีประสิทธิภาพ ดังนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับคะแนน
๓. ความเสี่ยงจากเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ (R03)	ความเสี่ยงด้านเทคนิค	ไม่สามารถใช้งานผ่านเครื่องคอมพิวเตอร์แม่ข่ายได้ ได้แก่ Web Server, Mail Server, File Server, Database Server	๒๐
๔. ความเสี่ยงจากระบบเครือข่าย (R04)	ความเสี่ยงด้านเทคนิค	ระบบเครือข่ายคอมพิวเตอร์มีการทำงานผิดพลาดของอุปกรณ์เครือข่ายหลัก ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต, Domain Server, DNS Server, Firewall, Core Switch	๒๐
๕. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์ (R05)	ความเสี่ยงด้านเทคนิค	- ไวรัสคอมพิวเตอร์ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง ไม่สามารถทำงานได้ -มัลแวร์ทำให้เกิดช่องโหวให้ผู้ไม่หวังดีเข้ามาควบคุมคอมพิวเตอร์ โจรกรรมข้อมูล - Ransomware ทำให้เครื่องคอมพิวเตอร์ถูกเข้ารหัสข้อมูล ทำให้ไม่สามารถใช้งานได้และถูกเรียกค่าไถ่ในการถอดรหัสข้อมูล	๒๐
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker (R06)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	- ระบบเครือข่ายโดนโจมตีโดย Hacker - การโจมตีการให้บริการ (DoS, DDoS) - การดักจับข้อมูลผ่านระบบเครือข่าย - คำสั่งเจตนาร้าย หรือไฟล์ Auto Run - มีการฝั่งโค้ด หรือคำสั่งต่าง ๆ ในระบบเครือข่าย - ระบบต่าง ๆ ทำงานผิดพลาดโดยไม่รู้สาเหตุ - ไฟล์ที่ผู้ใช้บริการ Download มีการฝังไวรัสคอมพิวเตอร์ คำสั่งอันตราย อันก่อให้เกิดช่องโหวให้ Hacker เข้ามาโจมตี	๒๐
๘. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้ (R08)	ความเสี่ยงด้านเทคนิค	ระบบสำรองข้อมูลไม่สามารถทำงานได้ตามปกติ ทำให้การสำรองข้อมูลไม่เป็นไปอย่างต่อเนื่อง	๒๐

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับคะแนน
๑๑. ความเสี่ยงจากการขาดแคลนบุคลากรที่เชี่ยวชาญด้านไซเบอร์ (R11)	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านไซเบอร์ ทำให้การทำงานหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบการพัฒนาและควบคุมดูแลระบบ	๑๖
๗. ความเสี่ยงจากการทำงานโปรแกรมประยุกต์ทำงานผิดพลาดเป็นช่องโหว่ของโปรแกรม (R07)	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากการปฏิบัติงาน	ความเสี่ยงที่เกิดจากโปรแกรประยุกต์ต่าง ๆ ไม่ว่าจะเป็นการทำงานผิดพลาดของโปรแกรมหรือช่องโหว่ของโปรแกรม	๑๕
๑. ความเสี่ยงในการให้ผู้อื่นเข้าถึงข้อมูลของตนเองโดยไม่มีสิทธิ (R01)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้งานระบบสารสนเทศ เช่น มอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๑๐
๑๐. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ (R10)	ความเสี่ยงจากการปฏิบัติงาน	การใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์อาจทำให้เกิดโอกาสการโจมตีได้สูงและเป็นการดำเนินงานที่ผิดกฎหมาย	๑๐
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ (R02)	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อกับระบบเครือข่ายหน่วยงาน โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าความปลอดภัยให้ถูกต้อง	๘
๙. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ (R09)	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ ทำให้ระบบงานที่อยู่ภายในเครื่องคอมพิวเตอร์เสมือนไม่สามารถให้บริการได้	๕

๘. การจัดการความเสี่ยง

หน่วยงานกำหนดให้ระดับความเสี่ยงที่อยู่ในระดับยอมรับได้ต่ำกว่า ๑๖ ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ ส่วนความเสี่ยงที่จำเป็นต้องมาดำเนินการบริหารจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๖ ขึ้นไป การบริหารจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ชื่อความเสี่ยง	ระดับคะแนน	การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	หน่วยงานรับผิดชอบ
๓. ความเสี่ยงจากเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้ตามปกติ (R03)	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่อง ระบบสำรองข้อมูลอย่างสม่ำเสมอ	ศสท. (กค.)
๔. ความเสี่ยงจากระบบเครือข่าย (R04)	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน เพื่อสามารถปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องและอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	ศสท. (กค.)
๕. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์ (R05)	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ติดตั้งระบบป้องกันไวรัส และมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - อัพเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ	ศสท. (กค. กอ.)
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker (R06)	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- นำระบบที่สำคัญเข้าสู่ระบบ VM เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการสำรองข้อมูล และการแยกส่วนเป็นเครือข่ายย่อย - ตรวจสอบและปรับปรุงการตั้งค่าของ Firewall อย่างสม่ำเสมอ	ศสท. (กค. กอ.)

ชื่อความเสี่ยง	ระดับคะแนน	การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	หน่วยงานรับผิดชอบ
๘. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้ (R08)	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ปรับปรุงระบบคอมพิวเตอร์แม่ข่าย - จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์อย่างสม่ำเสมอ	ศสท. (กค.)
๑๑. ความเสี่ยงจากการขาดแคลนบุคลากรที่เชี่ยวชาญด้านไซเบอร์ (R11)	๑๖	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้	ศสท. สล.
๗. ความเสี่ยงจากการทำงานโปรแกรมประยุกต์ทำงานผิดพลาดเป็นช่องโหว่ของโปรแกรม (R07)	๑๕	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ - ตรวจสอบการทำงานของโปรแกรมอย่างละเอียด	ศสท. (กค. กอ.)
๑. ความเสี่ยงในการให้ผู้อื่นเข้าถึงข้อมูลของตนเองโดยไม่มีสิทธิ (R01)	๑๐	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	ทุกหน่วยงานภายใน กพร.
๑๐. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ (R10)	๑๐	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- กำหนดและสื่อสารนโยบายการบริหารจัดการลิขสิทธิ์ของหน่วยงานให้ทั่วถึง - จัดทำบันทึกรายการซอฟต์แวร์ลิขสิทธิ์ - สุ่มตรวจสอบซอฟต์แวร์ลิขสิทธิ์บนเครื่องคอมพิวเตอร์ที่เกี่ยวข้อง	ศสท. (กค. กอ.)

ชื่อความเสี่ยง	ระดับคะแนน	การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	หน่วยงานรับผิดชอบ
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ (R02)	๘	ยอมรับความเสี่ยง (มีแผนรองรับ)	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างจริงจัง - ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิการเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย	ทุกหน่วยงานภายใน กพร.
๙. ความเสี่ยงด้านเครื่องคอมพิวเตอร์เสมือนไม่สามารถทำงานได้ตามปกติ (R09)	๕	ยอมรับความเสี่ยง (มีแผนรองรับ)	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทน - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย	ศสท. (กค.)

แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการข้อมูลข่าวสารและความมั่นคงปลอดภัยข้อมูลข่าวสาร กพร. เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ ต่อไป

ลงชื่อ .....

(นายอดิทัต วะสีนนท์)

อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

...../...../.....