กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

นโยบาย
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(กพร.-IT-SEC-P1)

แก้ไขครั้งที่ ๑
สำเนาที่
วันที่ประกาศใช้

ผู้จัดทำ	ผู้ตรวจ	ผู้อนุมัติ
.....	.....	.....
(นายมานุส มณีนุษย์)	(นายธวัช ผลความดี)	(นายสมเกียรติ ภู่ธงชัยฤทธิ์)
ผอ.ศสท.	รองอธิบดี กพร. (CIO)	อธิบดี กพร.

สารบัญ

ประวัติเอกสาร

เวอร์ชั่น	วันที่	ผู้แก้ไข	หมายเหตุ
๑.๐	๒๑ มีนาคม ๒๕๕๔	นายมานุส มณีนุษย์	สร้างเอกสาร

๑. กำหนดนิยาม

๑.๑. **ผู้ใช้งาน** หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

๑.๒. **สิทธิ์ของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๑.๓. **สินทรัพย์ (asset)** หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

๑.๔. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๑.๕. **ความมั่นคงปลอดภัยด้านสารสนเทศ (information security)** หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

๑.๖. **เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๑.๗. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปอลดภัยถูกคุกคาม

๑.๘. **คำนิยามอื่นๆ**

๑.๘.๑. **กพร.** หมายถึง กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑.๘.๒. **อธิบดี** หมายถึง อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑.๘.๓. CIO หมายถึง รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ที่ได้รับแต่งตั้งให้เป็นผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๘.๔. **ศสท.** หมายถึง ศูนย์สารสนเทศอุตสาหกรรมพื้นฐานและการเหมืองแร่ เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุงบำรุงรักษาระบบสารสนเทศและระบบเครือข่ายภายในองค์กร

๑.๘.๕. **ผอ.ศสท.** หมายถึง ผู้อำนวยการศูนย์สารสนเทศอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑.๘.๖. **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

๒. วัตถุประสงค์และขอบเขต

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ (กพร.) ตระหนักว่าสารสนเทศเป็นสินทรัพย์ที่สำคัญซึ่งจำเป็นต้องมีมาตรการปกป้องสารสนเทศให้มีความมั่นคงปลอดภัย ภายใต้หลักสำคัญที่ทำให้สารสนเทศมีความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีประสิทธิผลจะทำให้การใช้งานสารสนเทศ การปฏิบัติงานตามภารกิจ การให้บริการ หรือการดำเนินการใดๆ ด้วยวิธีการทางอิเล็กรอนิกส์ของ กพร. มีความสะดวกรวดเร็ว มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล

เอกสารนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จัดทำและเผยแพร่เพื่อให้ทั่วทั้งองค์กรหรือผู้เกี่ยวข้องได้รับทราบถึงเจตนารมณ์ ทิศทางการดำเนินการ และการให้การสนับสนุนของผู้บริหาร กพร. ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยมีความสอดคล้องกับภารกิจขององค์กร กฎหมาย และกฎระเบียบที่เกี่ยวข้อง

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะมีการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้มั่นใจได้ว่านโยบายยังคงมีความเหมาะสม มีความเพียงพอ และมีประสิทธิผล ในกรณีที่มีการดำเนินการแก้ไขเปลี่ยนแปลงนโยบาย จะมีการจัดทำและเผยแพร่เอกสารฉบับใหม่เพื่อทดแทน

๓. เจตนารมณ์ของผู้บริหาร กพร.

ผู้บริหาร กพร. ตระหนักถึงความสำคัญของการดำเนินการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จึงมีเจตจำนงที่จะให้การสนับสนุนทั้งในเชิงนโยบาย การผลักดันและส่งเสริมกิจกรรมต่างๆ รวมถึงให้การสนับสนุนในการจัดหางบประมาณเพื่อใช้ในการดำเนินงานใดๆ ไม่ว่าจะเป็นการจัดทำนโยบาย ข้อปฏิบัติ การจัดหาฮาร์ดแวร์ การจัดหาซอร์ฟแวร์ การจัดจ้างที่ปรึกษา การสร้างความตระหนักให้กับบุคลากร หรือกิจกรรมอื่นใดที่จะทำให้การรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีมาตรฐานเชื่อถือได้ มีความสอดคล้องกับวิสัยทัศน์ พันธกิจ ภารกิจ และข้อกฎหมาย

การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ กพร. จะมีการดำเนินงานภายใต้กรอบของประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๓ และจะมีการประยุกต์ใช้มาตรฐาน ISO/IEC 27001

๔. ผู้รับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ บทบาทและหน้าที่

๔.๑. **การบริหารนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ**

ผอ.ศสท. มีหน้าที่รับผิดชอบในการจัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ทบทวนนโยบาย ภายใต้การกำกับของรองอธิบดี (CIO ของ กพร.) นำเสนอนโยบายให้ที่ประชุมผู้บริหารพิจารณาให้ความเห็นชอบ และนำเสนออธิบดี เพื่อลงนามอนุมัติก่อนประกาศใช้

ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอยู่ภายใต้กำกับของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ให้อยู่ในความดูแลของ ผอ.ศสท. โดย

๔.๑.๑. จัดทำข้อเสนอแนะ และกำหนดข้อปฏิบัติที่ทำให้เกิดความร่วมมือระหว่างผู้ใช้และผู้กำกับดูแลซึ่งช่วยให้มั่นใจว่าสารสนเทศมีความมั่นคงปลอดภัย

๔.๑.๒. ทบทวน และปรับปรุงข้อปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑.๓. จัดให้มีระบบการตรวจสอบและควบคุมที่มีประสิทธิภาพสำหรับข้อมูลที่มีความสำคัญยิ่งยวด

๔.๑.๔. นำเสนอ CIO เพื่อลงนามอนุมัติข้อปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศที่จะประกาศใช้อย่างเป็นทางการโดยต้องผ่านความเห็นชอบจากที่ประชุมผู้บริหาร

๔.๒. **ผู้กำกับดูแลความมั่นคงปลอดภัยด้านสารสนเทศ**

ผู้กำกับดูแลความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนราชการหรือบุคคลที่ได้รับมอบหมายให้ทำหน้าที่ควบคุมการเข้าถึงทรัพยากรสารสนเทศ จัดหาหรือจัดให้มีระบบป้องกันภัย ตลอดจนเฝ้าระวัง ตรวจจับ วิเคราะห์ สืบสวน และจัดทำรายงานที่เกี่ยวกับการฝ่าฝืนระบบรักษาความมั่นคงปลอดภัยที่อาจเกิดกับสารสนเทศในความดูแลของ กพร. กำหนดให้มีผู้กำกับดูแลดังนี้

๔.๒.๑. ศสท. ทำหน้าที่เป็นผู้กำกับดูแลระบบสารสนเทศของ กพร.

๔.๒.๒. กลุ่มพัฒนาระบบเครือข่ายและการสื่อสาร ทำหน้าที่เป็นผู้กำกับดูแลระบบเครือข่ายและการสื่อสารของ กพร.

๔.๒.๓. กลุ่มพัฒนาระบบสำนักงานรัฐอิเล็กทรอนิกส์ ทำหน้าที่กำกับดูแลงานสารสนเทศส่วนกลาง ยกเว้นระบบงานสารสนเทศเฉพาะเรื่องที่อยู่ภายใต้การดูแลโดยสำนัก/กอง/กลุ่มงาน

๔.๒.๔. สำนัก/กอง/กลุ่มงาน เป็นผู้กำกับดูแลระบบงานสารสนเทศตลอดจนระบบคอมพิวเตอร์ที่ส่วนราชการนั้นรับผิดชอบโดยตรง

๔.๓. **บุคลากรในสังกัด กพร.**

บุคลากรในสังกัด กพร. ซึ่งได้แก่ ข้าราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และพนักงานราชการ มีสิทธิ์ใช้ทรัพยากรสารสนเทศภายใต้ข้อกำหนด ดังนี้

๔.๓.๑. บุคลากรต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศฉบับนี้

๔.๓.๒. บุคลากรต้องใช้ทรัพยากรสารสนเทศตามนโยบายที่อนุญาตให้ใช้งาน โดยต้องลงนามรับทราบและยินดีปฏิบัติตาม

๔.๓.๓. บุคลากรมีหน้าที่ตรวจสอบข้อมูลอย่างสม่ำเสมอเพื่อมั่นใจว่าข้อมูลสำคัญในเครื่องคอมพิวเตอร์ภายใต้ความรับผิดชอบตามภารกิจงานที่ได้รับมอบหมาย มีชุดข้อมูลสำรองพร้อมอยู่ เพื่อป้องกันข้อมูลสูญหาย

๔.๓.๔. บุคลากรมีหน้าที่รับผิดชอบดูแลคอมพิวเตอร์ที่ใช้งานและอยู่ภายใต้ความรับผิดชอบให้มีความมั่นคงปลอดภัย

๔.๓.๕. บุคลากรต้องปฏิบัติตามคำแนะนำด้านความมั่นคงปลอดภัยสำหรับคอมพิวเตอร์ที่อยู่ภายใต้ความรับผิดชอบ ได้แก่ การปรับปรุงช่องโหว่ของระบบปฏิบัติการและซอฟต์แวร์ การป้องกันกำจัดไวรัส เวิร์ม และสปายแวร์ ทั้งนี้บุคลากรต้องรับผิดชอบต่อเหตุการณ์ความมั่นคงปลอดภัยที่เกิดขึ้นจากคอมพิวเตอร์ที่อยู่ภายใต้ความรับผิดชอบ

๔.๔. **บุคคลภายนอก**

๔.๔.๑. บุคคลภายนอกทั่วไปไม่ได้รับสิทธิ์เข้าใช้ทรัพยากรสารสนเทศ ยกเว้นกรณีที่มีข้อตกลงระหว่าง กพร. และหน่วยงานที่บุคคลนั้นสังกัด หรือได้รับอนุญาตเป็นกรณีเฉพาะภายใต้ระเบียบของ กพร. โดยจะต้องได้รับการอนุมัติโดยผู้บริหาร กพร./สำนัก/กอง/กลุ่มงาน

๔.๔.๒. การพัฒนาซอฟต์แวร์โดยการว่าจ้างหน่วยงานภายนอกและจำเป็นต้องมีผู้ปฏิบัติงานจากหน่วยงานภายนอกให้อยู่ภายใต้ข้อกำหนดของนโยบายนี้เช่นกัน

๕. นโยบายการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศ

ความเสี่ยงในด้านต่างๆ ที่มีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของ กพร. จะต้องได้รับการตรวจพิเคราะห์อย่างเป็นระบบและสอดคล้องกับข้อกำหนดในการดำเนินการบริหารความเสี่ยงของ กพร. ความเสี่ยงจะต้องได้รับการประเมินระดับความเสี่ยงและเลือกวิธีจัดการกับความเสี่ยงนั้น ไม่ว่าจะเป็นการพัฒนากระบวนการควบคุมเพื่อลดความเสี่ยง ยอมรับความเสี่ยงโดยมีเหตุผลอันสมควร หรือถ่ายโอนความเสี่ยง

การบริหารความเสี่ยงด้านสารสนเทศ จะต้องได้รับการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลง เพิ่มเติม ที่มีผลกระทบอย่างมีนัยสำคัญ

๖. นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศของ กพร. จะต้องตั้งอยู่บนพื้นที่ฐานที่การเข้าใช้งานสารสนเทศใดๆ ต้องสามารถตรวจสอบได้ สามารถป้องกันการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต และจะต้องใช้เพื่อภารกิจงานของ กพร. เท่านั้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศต้องมีการดำเนินการ บริหารจัดการการเข้าถึงหรือควบคุมในส่วนต่างๆ ดังนี้ การบริหารจัดการการเข้าถึงของผู้ใช้งาน หน้าที่ความรับผิดชอบผู้ใช้งาน การควบคุมการเข้าถึงระบบเครือข่าย การควบคุมการเข้าถึงระบบปฏิบัติการ การควบคุมการเข้าถึงแอปพลิเคชั่นและสารสนเทศ และการควบคุมอุปกรณ์แบบพกพาและการปฏิบัติงานจากภายนอกองค์กร

๗. นโยบายการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

สารสนเทศของ กพร. จะต้องมีสภาพพร้อมใช้งานอยู่เสมอ พร้อมทั้งต้องมีการสำรองข้อมูลที่เชื่อถือได้ มีการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมออย่างน้อยเดือนละหนึ่งครั้ง หรือในกรอบระยะเวลาที่เหมาะสมเพื่อให้มั่นใจได้ว่าข้อมูลที่สำรองไว้นั้นสามารถนำมาใช้งานได้จริง

กพร. จะต้องมีความพร้อมในการรับมือกับภัยพิบัติใดๆ ที่จะเกิดขึ้นกับระบบสารสนเทศขององค์กร รวมถึงจะต้องมีขีดความสามารถในการกู้คืนระบบสารสนเทศที่เป็นส่วนสำคัญต่อการดำเนินงานขององค์กรในระยะเวลาที่เหมาะสมภายหลังจากการเกิดภัยพิบัติ โดยต้องมีแผนการดำเนินงานในการป้องกัน การดำเนินงานขณะเกิดกรณีภัยพิบัติ และการฟื้นคืนระบบภายหลังจากการเกิดภัยพิบัติ ซึ่งแผนการดำเนินงานเหล่านี้จะต้องได้รับการทบทวนและการซักซ้อมแผนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบอย่างมีนัยสำคัญต่อการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

๘. นโยบายการปฏิบัติตามกฎหมาย และกฎระเบียบที่เกี่ยวข้อง

บรรดากฎหมายใดๆ ที่ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของ กพร. ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้นหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าวถือว่าเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

๙. มาตรการดำเนินการการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

๙.๑. หากตรวจพบว่ามีการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ดูแลระบบรายงานเหตุการณ์การฝ่าฝืนนั้นกับ ผอ.ศสท. โดยเร็ว

๙.๒. ผู้ดูแลระบบมีอำนาจในการตัดการเชื่อมต่อ เพิกถอนสิทธิ์ของผู้ใช้ หรือเครื่องคอมพิวเตอร์ที่ถูกตรวจพบว่าเป็นต้นเหตุของการละเมิดมาตรการความมั่นคงปลอดภัย หรือตรวจพบว่าเป็นจุดเสี่ยงของความมั่นคงปลอดภัยต่อระบบสารสนเทศของ กพร.

๙.๓. รายงานการละเมิดใดๆ ให้แจ้งต่อผู้บริหารของหน่วยราชการระดับสำนัก/กอง/กลุ่มงาน ที่เกิดกรณีเหตุการณ์นั้น

๙.๔. การละเมิดนโยบาย และข้อปฏิบัติที่ออกภายใต้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ อันก่อให้เกิดความเสียหายแก่บุคคลอื่น หรือ กพร. ให้ ผอ.ศสท. ทำรายงานเสนอ CIO เพื่อแต่งตั้งคณะกรรมการสอบสวนเพื่อพิจารณาโทษทางวินัยหรือทางกฎหมาย

๙.๕. กพร. จะไม่รับผิดชอบต่อผลของการกระทำความผิดใดๆ อันเกิดจากการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ กพร. ถือว่าความผิดทางกฎหมายที่เกิดจากการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นความผิดส่วนบุคคล ผู้ละเมิดจะต้องเป็นผู้รับผิดชอบผลของการกระทำความผิดนั้น