ประกาศกรมส่งเสริมอุตสาหกรรม
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ข้อ ๑ ในประกาศนี้

"นโยบาย" หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมอุตสาหกรรม ซึ่งกรมประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของกรมที่ต้องเกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

"แนวปฏิบัติ" หมายถึง ขั้นตอนวิธีการที่กรมส่งเสริมอุตสาหกรรมได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของกรมที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

"ผู้ใช้งาน" หมายความว่า ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างตามสัญญาจ้างของกรม ผู้ดูแลระบบของกรมส่งเสริมอุตสาหกรรม ผู้บริหารองค์กร ผู้รับบริการ ผู้รับจ้างทำของ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของกรม

"บัญชีผู้ใช้งาน" หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรม

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของกรม

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"สินทรัพย์ (asset)" หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

"สินทรัพย์คอมพิวเตอร์" หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"สารสนเทศ" หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ต่างๆ ตามภารกิจของกรมฯ

"เครือข่าย" หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

"ความมั่นคงปลอดภัยด้านสารสนเทศ" (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)" หมายความว่า

กรณีที่ ๑ คือ เหตุการณ์ที่เกิดขึ้นแล้วกับระบบคอมพิวเตอร์และเครือข่ายของกรมฯ

กรณีที่ ๒ คือ เหตุการณ์ที่เป็นจุดอ่อนหรือสงสัยว่าจะเป็นจุดอ่อน

ทั้งสองกรณีสามารถสร้างความเสียหายให้กับองค์กรได้ในลักษณะใดลักษณะหนึ่ง ซึ่งอาจส่งผลให้

- เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของกรมฯ
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กรมฯ กำหนดไว้
- เกิดภาพลักษณ์ที่ไม่ดีต่อกรมฯ หรือทำให้สูญเสียชื่อเสียง (เช่น การไปโพสต์ข้อความพาดพิงถึงกรมฯ ในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของกรมฯ)

ตัวอย่างของเหตุการณ์ที่เกิดขึ้นแล้ว ได้แก่

- การพบการแพร่ระบาดของโปรแกรมไม่ประสงค์ดีในเครือข่ายของกรมฯ
- การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน
- การแจ้งเตือนของระบบป้องกันการบุกรุกตามที่กรมฯ ได้กำหนดไว้
- ระบบสารสนเทศซึ่งให้บริการแก่ประชาชนถูกบุกรุกทางเครือข่าย
- ข้อมูลสำคัญบนระบบที่ให้บริการประชาชนถูกเปลี่ยนแปลง หรือสูญหาย
- หน้าเว็บไซต์ของกรมฯ และบนระบบฯ ถูกเปลี่ยนแปลง
- ระบบถูกโจมตีจนไม่สามารถให้บริการได้
- ระบบ อุปกรณ์ ฮาร์ดแวร์ หรือทรัพย์สินสารสนเทศอื่นๆ ถูกขโมย
- พนักงานที่ลาออกแล้วยังใช้สิทธิ์ของระบบได้อยู่

ตัวอย่างของเหตุการณ์ที่เป็นจุดอ่อน ได้แก่

- ประตูเข้า-ออกศูนย์คอมพิวเตอร์ไม่สามารถล็อกได้กรณีที่ไฟดับมากกว่า ๑ ชั่วโมง
- บุคคลภายนอกเดินตามพนักงานเข้าห้องสำนักงานโดยไม่มีการแลกบัตร
- พนักงานไม่มีการระบุตัวตนก่อนที่จะเข้าถึงห้องสำนักงาน

ทั้งเหตุการณ์ที่เกิดขึ้นแล้วหรือเหตุการณ์ที่เป็นจุดอ่อน จำเป็นต้องได้รับรายงานจากผู้ใช้งานที่พบเหตุ เพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสม ได้ผล และทันกาล

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

(unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"หน่วยงาน" หมายความว่า สำนัก ส่วน หรือที่เรียกชื่อเป็นอย่างอื่นในสังกัดกรมส่งเสริมอุตสาหกรรม

"ผู้มีอำนาจ" หมายความว่า หัวหน้าหน่วยงานที่มีคอมพิวเตอร์ของกรมฯ อยู่ในความครอบครอง และให้หมายความรวมถึงผู้ซึ่งได้รับมอบหมายจากบุคคลดังกล่าวด้วย

"ผู้บริหารระดับสูง" หมายความว่า อธิบดีหรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรม

"กรม" หมายความว่า กรมส่งเสริมอุตสาหกรรม

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม แบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ นโยบาย

ส่วนที่ ๒ แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ โดยมีการควบคุมการใช้งานระบบสารสนเทศ การเข้าถึงระบบเครือข่าย การเข้าถึงระบบปฏิบัติการ และการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น ให้เป็นไปตามที่ผู้ดูแลระบบกำหนด

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมให้เป็นไปตามที่กำหนดไว้ใน **แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมส่งเสริมอุตสาหกรรม พ.ศ.๒๕๕๕**

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบการอนุญาตการให้เข้าถึงและควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมอย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายในหน่วยงาน เจ้าของระบบงาน หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) ให้นำผลการตรวจประเมินมาปรับปรุงให้สอดคล้องกับนโยบาย

ข้อ ๕ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานของกรม เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์ภายในกรมฯ ให้แก่ผู้ใช้งานสามารถเข้าถึงได้

(๒) จัดอบรมหรือให้ข้อมูลความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๖ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พ.ร.บ.ข้อมูลข่าวสารของ ทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรือข้อกำหนดอื่นๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๗ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูง เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๘ ให้หน่วยงานที่ดูแลระบบสารสนเทศของกรมฯ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๘ เดือน พ.ค. พ.ศ. ๒๕๕๔

(นายพสุ โลหารชุน)
อธิบดีกรมส่งเสริมอุตสาหกรรม