ประกาศกรมสวัสดิการและคุ้มครองแรงงาน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมสวัสดิการและคุ้มครองแรงงาน

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดเนินการใด ๆ ด้วยวิธีทางการอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับ

กรมสวัสดิการและคุ้มครองแรงงานจึงได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสวัสดิการและคุ้มครองแรงงานเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติตามมาตรการความปลอดภัยที่กำหนด และมีการทบทวนปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในหน่วยงาน โดยมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) เป็นผู้รับผิดชอบต่อนโยบายในฐานะเป็นผู้กำกับ ติดตามและทบทวนนโยบาย โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมสวัสดิการและคุ้มครองแรงงาน เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสวัสดิการและคุ้มครองแรงงาน พ.ศ. ๒๕๖๖” ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๒ นิยาม

๒.๑ “องค์กร” หมายถึง กรมสวัสดิการและคุ้มครองแรงงาน

๒.๒ “คณะทำงาน” หมายถึง คณะทำงานเทคโนโลยีดิจิทัลของกรมสวัสดิการและคุ้มครองแรงงาน

๒.๓ “CEO” หมายถึง อธิบดี

๒.๔ “DCIO” หมายถึง รองอธิบดี หรือผู้ตรวจราชการกรมที่ได้รับมอบหมายให้กำกับดูแลงานราชการของสำนักพัฒนามาตรฐานแรงงาน

๒.๕ “การเข้าถึงการควบคุมการใช้งานสารสนเทศ” หมายถึง การควบคุมการเข้าถึงหรือจำกัดการเข้าถึงข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมสำเร็จรูป โปรแกรมประยุกต์ โปรแกรมอรรถประโยชน์ เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ

๒.๖ “ข้อมูลสารสนเทศ” หมายถึง ข้อมูลที่ถูกประมวลผลโดยระบบสารสนเทศ และสามารถนำไปใช้งานหรือประมวลผลต่อไปได้

๒.๗ “ระบบเครือข่าย” หมายถึง ระบบเครือข่ายคอมพิวเตอร์สำหรับใช้ในการติดต่อสื่อสารหรือรับ-ส่งข้อมูลสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของกรมสวัสดิการและคุ้มครองแรงงาน

๒.๘ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด (Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ความมั่นคงของระ บบสารสนเทศถูกบุกรุก คุกคาม และโจมตี

ข้อ ๓ วัตถุประสงค์

๓.๑ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่ายของกรมสวัสดิการและคุ้มครองแรงงาน มีความมั่นคงปลอดภัยจากสถานการณ์ไม่พึงประสงค์หรือไม่คาดคิดในระบบสารสนเทศ

๓.๒ เพื่อให้มั่นใจได้ว่าการปฏิบัติงานของกรมสวัสดิการและคุ้มครองแรงงานสามารถดำเนินได้อย่างต่อเนื่อง และเมื่อเกิดผลกระทบจากเหตุการณ์ไม่พึงประสงค์สามารถกู้คืนระบบสารสนเทศได้อย่างรวดเร็วและลดความเสียหายที่อาจจะเกิดขึ้น

๓.๓ เพื่อเป็นแนวทางปฏิบัติในการใช้งานระบบสารสนเทศอย่างปลอดภัยสำหรับผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ และบุคคลภายนอก

ข้อ ๔ ขอบเขต

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ กำหนดขึ้นเพื่อสร้างมาตรฐานและแนวทางในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศของกรมสวัสดิการและคุ้มครองแรงงานให้ปลอดภัยจากความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่อาจส่งผลกระทบต่อข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่ายของกรมสวัสดิการและคุ้มครองแรงงาน โดยข้าราชการ พนักงานราชการ ลูกจ้างเหมา และผู้เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานทั้งหมดต้องถือปฏิบัติอย่างเคร่งครัด

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีสาระสำคัญประกอบด้วย

๕.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๕.๒ การมีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและมีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติอย่างต่อเนื่อง

๕.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

องค์กรได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัย โดยมีเนื้อหาสาระสำคัญประกอบด้วย

หมวด ๑ นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ ประกอบด้วยแนวปฏิบัติ ดังนี้

๑. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control)

๑.๑ มีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงการใช้งานและความมั่นคงปลอดภัย โดยกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตการเข้าถึงระบบสารสนเทศต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน

๑.๒ กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงไว้อย่างชัดเจน

๑.๓ ต้องจัดทำแนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศและปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความปลอดภัย

๒. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ได้กำหนดแนวทาง ดังนี้

๓.๑ สร้างความรู้ ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงข้อกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓.๒ การลงทะเบียนผู้ใช้งาน (User Registration) กำหนดไว้เป็นขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๓.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม และใช้งานอย่างปลอดภัย

๓.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) สม่ำเสมอมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ต้องมีแนวทางอย่างน้อย ดังนี้

๔.๑ การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีความปลอดภัย

๔.๒ มีการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานต้องกำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๔.๓ กำหนดให้การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น ไฟล์ สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

๕.๑ การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ได้กำหนดหนดแนวทางปฏิบัติ ดังนี้

๖.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๖.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และกำหนดขั้นตอนทางเทคนิคการยืนยันตัวตนอย่างเหมาะสมเพื่อรองรับการกล่าวอ้างว่าผู้ใช้งานที่ระบุถึง

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System) จัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๖.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ได้จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๖.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๗.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) โดยกำหนดแนวปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

๘. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) โดยผู้ใช้งานจะต้องลงทะเบียนใช้งานกับผู้ดูแลระบบ และนำอุปกรณ์มาขึ้นทะเบียนเพื่อให้สามารถเข้าใช้งานกับเครือข่ายที่ลงทะเบียนได้

๙. การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเตอร์เน็ตอย่างปลอดภัย

๙.๑ กำหนดการใช้เส้นทางเชื่อมต่อระบบอินเทอร์เน็ตที่ปลอดภัยที่องค์กรจัดไว้ให้เท่านั้น ได้แก่ Proxy, Firewall, IPS-IDS ห้ามมิให้ผู้ใช้งานเชื่อต่อผ่าน Dial-up Modem

๙.๒ การรับส่งข้อมูลผ่านอินเทอร์เน็ต ต้องมีการทดสอบไวรัส (Virus Scanning) ก่อนรับส่งข้อมูล

๙.๓ การดาวน์โหลดข้อมูล หรือโปรแกรมใด ๆ จากอินเทอร์เน็ต ต้องไม่เป็นการละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๙.๔ ต้องใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นไปตามที่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดยคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตผู้ใช้ระบบสารสนเทศใช้งาน เป็นทรัพย์สินของหน่วยงานที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๑๑. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook) โดยเครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย อยู่ในสภาพพร้อมใช้งาน และใช้งานได้อย่างปลอดภัย

๑๒. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) ผู้ดูแลระบบจะต้องควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Sever) และควบคุมการเปลี่ยนแปลงต่าง ๆ ที่อาจส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน รวมถึงความมั่นคงปลอดภัยของข้อมูล

๑๓. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) โดยจัดแบ่งพื้นที่ในการควบคุมตามระดับความสำคัญทางสารสนเทศ ควบคุมการเข้าถึงพื้นที่อย่างปลอดภัย รวมถึงการจัดให้มีการบำรุงรักษาอุปกรณ์สารสนเทศให้พร้อมใช้เสมอ

๑๔. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail: e-Mail) การลงทะเบียนผู้ใช้งาน และการใช้งานจดหมายอิเล็กทรอนิกส์อย่างปลอดภัย

๑๕. การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) อย่างปลอดภัยไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล ประกอบด้วยแนวปฏิบัติที่สำคัญ ดังนี้

๑. การสำรองระบบและสำรองข้อมูล

๑.๑ การจัดลำดับความสำคัญของระบบ เพื่อวางแผนในการจัดทำระบบสำรอง

๑.๒ กำหนดประเภทของข้อมูลที่ต้องการสำรอง

๑.๓ การจัดเก็บระบบและข้อมูลสำรองไว้อย่างปลอดภัย และทดสอบ (Restore) สม่ำเสมอ

๒. การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน และเตรียมความพร้อมโดยการทดสอบแผนสม่ำเสมอ เพื่อให้มั่นใจได้ว่าเมื่อเกิดเหตุฉุกเฉินสามารถกู้คืน (Recover) กลับมาได้ตามเป้าหมาย

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑. จัดให้มีการประเมินความเสี่ยงสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง โดยประเมินจัดระดับความสำคัญของความเสี่ยงแต่ละรายการ และวางแผนการจัดการความเสี่ยงอย่างเหมาะสม

๒. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) โดยดำเนินการตามความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

หมวด ๔ หน้าที่รับผิดชอบด้านสารสนเทศ

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๒๕ เมษายน ๒๕๖๖

(นายนิยม สองแก้ว)
อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน