ประกาศกรมการจัดหางาน

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนด หลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ อธิบดีกรมการจัดหางาน จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศกรมการจัดหางาน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ"

ข้อ ๒ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๓ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีวัตถุประสงค์ดังต่อไปนี้

๓.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของกรมการจัดหางาน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๓.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานของกรมการจัดหางานได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริการ ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมการจัดหางาน ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของกรมการจัดหางาน ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการจัดหางาน กำหนดตามประกาศมี ๒ ส่วน ดังต่อไปนี้

๔.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๔.๑.๑ กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) กรมการจัดหางาน เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการจัดหางาน

๔.๑.๒ กำหนดให้ผู้อำนวยการศูนย์บริหารคอมพิวเตอร์ เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

๔.๑.๓ ผู้บริหาร เจ้าหน้าที่ที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย และกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๔.๑.๔ นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางระบบของกรมการจัดหางาน

๔.๑.๕ จัดให้มีการทบทวนและปรับปรุง อย่างน้อยปีละ ๑ ครั้ง

๔.๒ ส่วนที่ว่าด้วยรายละเอียดของแนวปฏิบัติ

๔.๒.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๔.๒.๒ การบริหารจัดการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๔.๒.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่กรมการจัดหางานจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๔.๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการเพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน และจำกัดระยะเวลา ในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์ และป้องกันโปรแกรมไม่ประสงค์ดีต่างๆ

๔.๒.๕ การควบคุมเข้าถึงโปรแกรมประยุกต์และแอพพลิเคชั่น ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอพพลิเคชั่นต่างๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) และระบบงานต่างๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๕ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

๕.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๕.๒ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ และระบบสำรอง

๕.๓ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถดำเนินงานได้ตามปกติอย่างต่อเนื่องโดยต้องปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการงานตามภารกิจ

๕.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ ปีละ ๑ ครั้ง

๕.๕ มีการปฏิบัติและทบทวนแนวทางในการจัดทำระบบสำรอง ปีละ ๑ ครั้ง

ข้อ ๖ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๗ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจ ถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ ดังนี้

๗.๑ เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์ของกรมการจัดหางาน ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

๗.๒ จัดอบรมหรือจัดทำคู่มือที่ให้มีความรู้ความเข้าใจแก่ผู้ใช้งานเกี่ยวกับเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๘ องค์ประกอบของนโยบายนั้นจัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมการจัดหางาน โดยอ้างอิงรายละเอียด “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการจัดหางาน พ.ศ. ๒๕๕๘” เพื่อใช้เป็นแนวทางในการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย และเป็นไปตามกฎระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่กรมการจัดหางาน ต้องถือปฏิบัติอย่างเคร่งครัด

ข้อ ๙ กรณีคอมพิวเตอร์หรือข้อมูลข่าวสารสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์การหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๐ ให้ศูนย์บริหารคอมพิวเตอร์ของกรมการจัดหางาน เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ โดยให้มีการทบทวนและพิจารณาแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๑๑ พฤศจิกายน พ.ศ. ๒๕๕๘

(นายอารักษ์ พรหมณี)
อธิบดีกรมการจัดหางาน