ประกาศ สำนักงานกิจการยุติธรรม
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานกิจการยุติธรรม
พ.ศ. ๒๕๖๕

เพื่อให้ข้อมูลข่าวสารสารสนเทศรวมทั้งระบบเทคโนโลยีและการสื่อสารของสำนักงานกิจการยุติธรรม เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สอดคล้องตามหลักมาตรฐานสากล เชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง และเพื่อให้เกิดมาตรการในการป้องกันปัญหาอันอาจเกิดขึ้นจากภัยคุกคามต่างๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่พึงประสงค์ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงานกิจการยุติธรรม และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้องได้

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกาหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และด้วยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ดังต่อไปนี้

๑. ประกาศนี้ เรียกว่า “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานกิจการยุติธรรม พ.ศ. ๒๕๖๕”

๒. ประกาศนี้ให้ใช้ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

๓. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

๔. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้กำหนดขึ้นโดยมีวัตถุประสงค์ดังต่อไปนี้

๔.๑ เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานกิจการยุติธรรม

๔.๒ เพื่อใช้เป็นกรอบมาตรฐาน และแนวปฏิบัติในการปฏิบัติงานด้านสารสนเทศ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับบุคลากรและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานกิจการยุติธรรม

๔.๓ เพื่อสร้างความตระหนัก ความเข้าใจ และมีส่วนรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

๔.๔ เพื่อให้บุคลากรของสำนักงานกิจการยุติธรรม บุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานกิจการยุติธรรม ได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

๔.๕ เพื่อติดตามการดำเนินงานและทบทวนนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับสภาพแวดล้อม และกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานกิจการยุติธรรม มีดังนี้

๕.๑ การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ

๕.๑.๑ การรักษาความมั่นคงปลอดภัยด้านกายภาพ กำหนดให้ต้องควบคุมสภาพแวดล้อมการใช้งานระบบสารสนเทศโดยจำแนกพื้นที่ จัดให้มีการควบคุมสิทธิการเข้า - ออกพื้นที่สารสนเทศ ควบคุมการส่งมอบผลิตภัณฑ์และจัดวางอุปกรณ์ การควบคุมการวางระบบสายไฟ สายสัญญาณต่างๆ การบำรุงรักษาอุปกรณ์ รวมถึงมีมาตรการในการกำกับดูแลหากมีความจำเป็นต้องยืมสินทรัพย์ของสำนักงานกิจการยุติธรรมไปใช้นอกพื้นที่ใช้งาน ควบคุมการนำสินทรัพย์ส่วนตัวเข้ามาใช้กับระบบงาน รวมถึงการกำหนดหลักเกณฑ์การทำลายข้อมูลในอุปกรณ์อิเล็กทรอนิกส์ให้เป็นมาตรฐานสากล

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน กำหนดให้มีการสร้างความรู้ความเข้าใจแก่ผู้ใช้งาน เพื่อให้ตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง การลงทะเบียนผู้ใช้งานให้ผู้ได้รับอนุญาตแล้ว พร้อมทั้งการกำหนดสิทธิการใช้งานสารสนเทศที่สำคัญ การทบทวนสิทธิผู้ใช้งานอย่างสม่ำเสมอ รวมถึงกำหนดขอบเขตการใช้งาน ความรับผิดชอบของผู้ใช้งานต่อการใช้งานระบบสารสนเทศของสำนักงานฯ ไว้ด้วย

๕.๑.๓ การควบคุมการเข้าถึงระบบสารสนเทศ กำหนดการมอบอำนาจ การอนุญาต การควบคุมและกำหนดประเภทข้อมูล ชั้นความลับ ระดับความสำคัญและการรักษาความลับของข้อมูล กำหนดช่องทางการเข้าถึงข้อมูล กำหนดระยะเวลาในการเข้าถึงระบบสารสนเทศ กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ รวมถึงการควบคุมสินทรัพย์สารสนเทศของสำนักงานกิจการยุติธรรม

๕.๑.๔ การควบคุมการเข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายต้องควบคุมตรวจสอบ กำกับ ดูแลผู้ใช้งาน และบุคคลภายนอกในการอนุญาตให้เข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย การป้องกันการเข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายโดยไม่ได้รับอนุญาต รวมถึงกำหนดให้เจ้าหน้าที่บันทึกการปฏิบัติงานเมื่อเข้าใช้งานในห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายทุกครั้ง

๕.๑.๕ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย ต้องมีการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายโดยผู้ไม่มีสิทธิอย่างรัดกุม ปลอดภัย ควบคุมการพัฒนาระบบสารสนเทศ รวมถึงการควบคุมทางด้านเทคนิคที่รัดกุมเพียงพอ

๕.๑.๖ การควบคุมการเข้าถึงเครือข่าย ต้องควบคุม ป้องกัน การเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยกำหนดสิทธิในการเข้าถึงเครือข่ายให้ผู้ใช้งานต้องพิสูจน์ยืนยันตัวตนก่อนเข้าใช้งาน การกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานเครือข่าย โดยผ่านระบบการรักความมั่นคงปลอดภัยที่สำนักงานกิจการยุติธรรมได้ติดตั้งไว้ การจัดเก็บข้อมูลอุปกรณ์บนเครือข่าย จัดให้มีการควบคุมการเชื่อมต่อเครือข่ายผ่านอุปกรณ์ที่ปลอดภัย และจัดให้มีการแบ่งระบบ

เครือข่ายแบบแบ่งโซนการใช้งาน (Demilitarized Zone) เพื่อให้สามารถควบคุมและป้องกันภัยคุกคามอย่างมีประสิทธิภาพ

๕.๑.๗ การควบคุมการเข้าถึงระบบปฏิบัติการ กำหนดให้มีการป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตโดยผู้ใช้งาน ต้องพิสูจน์ตัวตนก่อนเข้าใช้งานอย่างถูกต้อง มีการกำหนดระยะเวลาการยุติการใช้งานเมื่อเว้นว่างจากการใช้งาน การจำกัดเวลา การเชื่อมต่อระบบสารสนเทศ ตลอดจนการควบคุมการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ เพื่อป้องกันโปรแกรมไม่ประสงค์ดี

๕.๑.๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น ต้องกำหนดสิทธิการเข้าถึงและทบทวนสิทธิการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นให้สอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งานการกำหนดแนวทางการบริหารจัดการระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและสำคัญสูงต่อสำนักงานกิจการยุติธรรม การควบคุม และป้องกันอุปกรณ์สื่อสารเคลื่อนที่ในการเข้าถึงสารสนเทศ ตลอดจนถึงการควบคุมการเข้าใช้งานระบบสารสนเทศของสำนักงานกิจการยุติธรรมจากระยะไกล

๕.๑.๙ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ ต้องควบคุมการเข้าถึงจดหมายอิเล็กทรอนิกส์จากผู้ซึ่งไม่ได้รับอนุญาต ควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ของสำนักงานกิจการยุติธรรม เพื่อภารกิจ ของสำนักงานฯ เท่านั้น

๕.๑.๑๐ การควบคุมตรวจจับการบุกรุก ต้องจัดให้มีอุปกรณ์หรือเครื่องมือ IDS/IPS Firewall เพื่อตรวจสอบการเข้าถึงสารสนเทศของสำนักงานกิจการยุติธรรมจากทุกช่องทาง เพื่อสอดส่องพฤติกรรมการเข้าใช้งานระบบของผู้ใช้งาน การกำหนดการยุติการให้บริการสำหรับผู้ใช้งานที่มีพฤติกรรมเสี่ยง การตรวจสอบการบุกรุกโจมตีระบบ

๕.๑.๑๑ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ต้องกำหนดให้มีการเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log) พฤติกรรมการใช้งานของผู้ใช้งาน การป้องกันการเข้าถึงข้อมูลจราจรคอมพิวเตอร์จากผู้ที่ไม่เกี่ยวข้องอย่างน้อย ๙๐ วัน รวมถึงให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๕.๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

๕.๒.๑ การรักษาความปลอดภัยฐานข้อมูล ต้องควบคุมโดยจัดทำบัญชีระบบสารสนเทศโดยจำแนกตามกลุ่มทรัพยากรและการทำงาน กำหนดรายละเอียดของการสำรองข้อมูลและหน้าที่รับผิดชอบของผู้ดูแลระบบสำรองข้อมูล รวมถึงกำหนดเกณฑ์การใช้ฐานข้อมูลร่วมกันระหว่างสำนักงานกิจการยุติธรรมและหน่วยงานอื่น

๕.๒.๒ การสำรองข้อมูล ต้องควบคุมระบบสารสนเทศให้มีสภาพพร้อมใช้งานอยู่ตลอดเวลา โดยกำหนดความถี่การสำรองข้อมูล หน้าที่ความรับผิดชอบของผู้ดูแลระบบการสำรองข้อมูล รวมถึงกำหนดความสำคัญและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินไว้รับมือกับสถานการณ์ไม่พึงประสงค์หรือไม่อาจคาดคิด พร้อมทั้งต้องจัดให้มีการทบทวนแผนเตรียมความพร้อมฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๕.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยให้มีการตรวจสอบและควบคุมประสิทธิภาพของระบบ

สารสนเทศ และตรวจสอบประเมินความมั่นคงปลอดภัยด้านระบบสารสนเทศของสำนักงานกิจการยุติธรรม โดยผู้ตรวจสอบภายในอย่างน้อยปีละ ๑ ครั้ง หรือโดยผู้ตรวจสอบอิสระจากภายนอกอย่างน้อย ๒ ปี/ครั้ง

๕.๔ การสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๔.๑ การทบทวนนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องดำเนินการทบทวนและปรับปรุงให้เป็นปัจจุบัน ทันเหตุการณ์อยู่เสมอ โดยกลุ่มเทคโนโลยีสารสนเทศและการสื่อสารกระบวนการยุติธรรม อย่างน้อยปีละ ๑ ครั้ง

๕.๔.๒ การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้ใช้งาน กำหนดให้มีการจัดหลักสูตรการฝึกอบรม การจัดทำและเผยแพร่ความรู้ ข้อควรระมัดระวัง และการใช้งานเทคโนโลยีสารสนเทศอย่างถูกวิธี ในลักษณะเกร็ดความรู้ที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย จัดทำคู่มือสำหรับผู้ใช้งาน และคู่มือสำหรับผู้ดูแลระบบ แนะนำการแก้ปัญหาและการป้องกันเบื้องต้นแก่ผู้ใช้งานเมื่อพบภัยคุกคามจากโปรแกรมไม่พึงประสงค์ รวมถึงการสร้างการมีส่วนร่วมของผู้ใช้งานในการพัฒนาระบบสารสนเทศในอนาคต

๖. การกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่นที่ได้ประกาศใช้ทดแทน

๗. กำหนดให้หัวหน้ากลุ่มเทคโนโลยีสารสนเทศและการสื่อสารกระบวนการยุติธรรม ซึ่งเป็นผู้ดูแลและกำกับกลุ่มเทคโนโลยีสารสนเทศฯ เป็นผู้รับผิดชอบในการกำกับดูแลให้เป็นไปตามประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๘. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่สำนักงานกิจการยุติธรรม หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้อำนวยการสำนักงานกิจการยุติธรรมเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๙. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๓ เดือน สิงหาคม พ.ศ. ๒๕๖๕

พันตำรวจโท

(พงษ์ธร ธัญญสิริ)

ผู้อำนวยการสำนักงานกิจการยุติธรรม