ประกาศสำนักงาน ป.ป.ช.
เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
พ.ศ. ๒๕๖๖

โดยที่เป็นการสมควรให้มีแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน ป.ป.ช. เพื่อจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย สำหรับการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบด้วยกฎหมาย และให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งสำนักงาน ป.ป.ช. เป็นนิติบุคคลอันเป็นหน่วยงานของรัฐที่ต้องปฏิบัติให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

อาศัยอำนาจตามพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต พ.ศ. ๒๕๖๑ มาตรา ๑๕๑ (๒) ประกอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๓๗ (๑) ประกอบประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ประกาศ ณ วันที่ ๒๐ มิถุนายน ๒๕๖๕ จึงออกประกาศสำนักงาน ป.ป.ช. ไว้ ดังนี้

๑.วัตถุประสงค์

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เป็นนิติบุคคลอันเป็นหน่วยงานของรัฐที่ต้องปฏิบัติให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยสำนักงาน ป.ป.ช. ได้มีประกาศสำนักงาน ป.ป.ช. เรื่อง นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ พ.ศ. ๒๕๖๕ เพื่อกำหนดหลักเกณฑ์เกี่ยวกับมาตรการกำกับดูแลการให้ความคุ้มครองข้อมูลส่วนบุคคล รวมถึงกำหนดให้มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติเป็นผู้ดำเนินการจัดเก็บนั้น มีมาตรการรักษาความมั่นคงปลอดภัย สำหรับการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบด้วยกฎหมาย ในการนี้ แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลจึงได้จัดทำขึ้นเพื่อกำหนดรายละเอียดต่าง ๆ เพื่อเป็นแนวทางปฏิบัติที่สอดคล้องกับประกาศดังกล่าว โดยมีขอบเขตการบังคับใช้ คำนิยาม ในแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ให้เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน ป.ป.ช.

/๒. บททั่วไป ...

๒. บททั่วไป

สำนักงานต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย สำหรับการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใด โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รวมถึงการดำเนินการเกี่ยวกับความเสี่ยงในการรักษาความมั่นคงปลอดภัย

ทั้งนี้ มาตรการรักษาความปลอดภัยที่เหมาะสม ต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) สภาพพร้อมใช้งาน (Availability) การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย และความเหมาะสมตามระดับความเสี่ยง

๓. มาตรการรักษาความปลอดภัยเชิงองค์กร (Organizational Measures)

มาตรการรักษาความปลอดภัยเชิงองค์กร ประกอบไปด้วยการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญที่มีการพิสูจน์และยืนยันตัวตน การอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็นและการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น โดยกำหนดให้มีมาตรการดังนี้

<u>๓.๑ การควบคุมเข้าถึงข้อมูลส่วนบุคคล (access control)</u>

(๑) สำนักงานต้องกำหนดความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ เปิดเผย การล่วงรู้ไม่ว่าด้วยประการใด ๆ การทำสำเนาข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญโดยไม่ได้รับอนุญาต ปราศจากอำนาจหรือโดยมิชอบด้วยกฎหมาย ตลอดจนเพื่อป้องกันการทำสำเนา การนำอุปกรณ์ที่ใช้สำหรับจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศไปโดยปราศจากมูลเหตุอันจะอ้างกฎหมายได้

(๒) สำนักเทคโนโลยีสารสนเทศต้องบริหารจัดการและกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่อยู่ในระบบสารสนเทศของผู้ใช้งาน (User Responsibilities) ในรูปแบบต่าง ๆ เช่น สิทธิการเข้าถึง การแก้ไข เปิดเผย ล่วงรู้ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและทำลาย รวมทั้งการเข้าถึงพื้นที่ที่สามารถเข้าถึงอุปกรณ์ทั้งหมดที่เกี่ยวข้อง และต้องจัดให้มีการทบทวนปรับปรุงบริหารจัดการและกำหนดสิทธิให้เป็นปัจจุบันอยู่เสมอ

(๓) สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีกระบวนการในการพิสูจน์และยืนยันตัวตน สำหรับการเข้าถึงและใช้งานระบบสารสนเทศที่มีการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ และการเก็บรวบรวมข้อมูลการขอสิทธิในการเข้าถึงและใช้งานระบบสารสนเทศ

(๔) สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีการตรวจสอบยืนยันตัวตนและควบคุมบุคคลภายนอก ที่เข้าปฏิบัติงานในพื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย ตลอดจนพื้นที่อื่นใดที่จัดเก็บอุปกรณ์ที่ใช้สำหรับจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

/<u>๓.๒ การบริการ</u> ...

๓.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีมาตรการในการลงทะเบียนและการถอนสิทธิผู้ใช้งาน ตลอดจนการจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ เพื่อควบคุมการเข้าถึง เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบและทำลายข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๓.๓ มาตรการรักษาความมั่นคงปลอดภัยตามกฎหมาย (Legal Measures for Private Security)

กรณีที่มีกฎหมายอื่นกำหนดให้สำนักงานต้องกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลนั้น ให้สำนักงานดำเนินการตามที่กฎหมายอื่นกำหนดแต่ต้องมีมาตรฐานไม่ต่ำกว่ากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๔. มาตรการรักษาความปลอดภัยเชิงเทคนิค (Technical measures)

มาตรการรักษาความปลอดภัยเชิงเทคนิค สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ที่ครอบคลุมส่วนประกอบของระบบสารสนเทศที่เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) ที่ประกอบด้วยมาตรการป้องกันหลายชั้น (Multiple - Layered of Security Controls) เพื่อลดความเสี่ยงในบางสถานการณ์ โดยกำหนดให้มีมาตรการดังนี้

๔.๑ สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีวิธีการเพื่อสามารถตรวจสอบย้อนกลับเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๔.๒ สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีกระบวนการบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึง เปลี่ยนแปลง แก้ไข เปิดเผย ล่วงรู้ ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและทำลายข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๔.๓ สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบสารสนเทศหรือบริการต่าง ๆ ยังดำเนินการได้อย่างต่อเนื่อง

๕. มาตรการรักษาความปลอดภัยเชิงกายภาพ (Physical Safeguards)

มาตรการรักษาความปลอดภัยเชิงกายภาพ สำหรับป้องกันข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ตลอดจน อาคาร อุปกรณ์ที่เกี่ยวข้องให้ได้รับความปลอดภัยจากการถูกทำลายทั้งจากภัยทางธรรมชาติและการกระทำโดยมิชอบด้วยกฎหมาย ที่ประกอบด้วยมาตรการการควบคุมการเข้าถึงสิ่งปลูกสร้าง อาคาร พื้นที่ปฏิบัติงาน ความมั่นคงปลอดภัยของพื้นที่ปฏิบัติงาน และการควบคุมการใช้อุปกรณ์และส่วนประกอบของระบบสารสนเทศ โดยกำหนดให้มีมาตรการดังนี้

๕.๑ หน่วยงานภายในสังกัดสำนักงาน ที่เก็บรวบรวมข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศในทุกรูปแบบ ทั้งข้อมูลเอกสารและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น การจัดทำบันทึกการเข้าออกพื้นที่สำหรับบุคคลที่ไม่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ติดตั้งระบบกล้องวงจรปิด จัดให้มี

/ทางเข้าออก ...

ทางเข้าออกด้วยระบบที่สามารถตรวจสอบกำหนดสิทธิเฉพาะบุคคลในการผ่านเข้าออกโดยใช้บัตรผ่าน ลายนิ้วมือ หรือวิธีการอื่นใดในการยืนยันตัวตน เป็นต้น เพื่อตรวจสอบผู้มีสิทธิเข้าออกหรือตรวจสอบและเฝ้าระวังผู้เข้าออกพื้นที่ และการเก็บข้อมูลส่วนบุคคลที่เป็นเอกสารในที่เก็บที่ควบคุมการเข้าถึงได้

ทั้งนี้ ให้กำหนดแต่เฉพาะผู้ที่เกี่ยวข้องเท่านั้น ที่เป็นผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๕.๒ สำนักเทคโนโลยีสารสนเทศ ต้องจัดให้มีการบันทึกข้อมูลการเข้าออกพื้นที่ปฏิบัติงานที่มีการจัดเก็บและเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศสำหรับบุคคลอื่นใดที่ไม่มีสิทธิเข้าพื้นที่ดังกล่าว และต้องกำหนดให้ตรวจสอบรายชื่อผู้มีสิทธิเข้าพื้นที่ปฏิบัติงานที่มีการจัดเก็บและเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ตลอดจนอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล ให้เหมาะสมกับระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น เพื่อเป็นข้อมูลประกอบการดำเนินการ หากมีการกระทำที่เป็นการละเมิดข้อมูลส่วนบุคคล หรือการกระทำอื่นใดโดยมิชอบด้วยกฎหมาย

๖. มาตรการเสริมสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Measures to Enhance Understanding of Personal Data Security)

สำนักงานต้องส่งเสริมให้บุคลากร พนักงาน ลูกจ้าง บุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือบุคคลอื่นใดที่เกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ ล่วงรู้ไม่ว่าด้วยการประการใด ๆ หรือเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ให้มีความรู้ความเข้าใจและตระหนักรู้ในการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้แก่ผู้เกี่ยวข้องทั้งหมด ตลอดจนสำนักงานต้องแจ้งให้บุคคลดังกล่าวทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติและมาตรการที่เกี่ยวข้องทั้งหมด โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

๗. มาตรการจัดการความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล (Risk Management Measures in Personal Data Protection)

สำนักเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรการจัดการความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล โดยดำเนินการระบุความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคลอันประกอบไปด้วยความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ (Information Assets) ที่สำคัญ เพื่อการป้องกันความเสี่ยงที่สำคัญที่อาจเกิดขึ้น เพื่อการตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคล เมื่อมีการตรวจพบเหตุอันเป็นภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ตลอดจนการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุแห่งการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสมและเป็นไปได้ตามประเภทและระดับความเสี่ยง และให้ดำเนินการแจ้งให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือบุคคลอื่นใดที่เกี่ยวข้องทราบ และดำเนินการตามมาตรการอย่างเคร่งครัด

๘. การทบทวนมาตรการรักษาความมั่นคงปลอดภัย (Review of Security Measures)

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประกาศฉบับนี้ ต้องจัดให้มีการทบทวนอยู่เสมอ และในกรณีเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม

/มาตรฐาน ...

มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ที่มีลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน โดยกำหนดให้ต้องมีการทบทวนมาตรการรักษาความมั่นคงปลอดภัย ดังนี้

๘.๑ เมื่อมีเหตุละเมิดหรือกระทำการโดยมิชอบด้วยกฎหมาย ต่อข้อมูลส่วนบุคคล ให้ถือว่าสำนักงานมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย เว้นแต่เหตุหรือการกระทำนั้นไม่มีความเสี่ยงในการเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๘.๒ เมื่อสำนักเทคโนโลยีสารสนเทศเห็นว่ามีการเปลี่ยนแปลงที่มีนัยสำคัญทางเทคโนโลยีสารสนเทศที่มีความจำเป็นต้องทบทวนมาตรการในการรักษาความมั่นคงปลอดภัย

๘.๓ สำนักเทคโนโลยีสารสนเทศต้องเสนอให้สำนักงานทบทวนมาตรการในการรักษาความมั่นคงปลอดภัย อย่างน้อยปีละ ๑ ครั้ง

๙. มาตรการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processors Controlling Measures)

สำนักงานต้องจัดให้มีมาตรการในการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ หรือการกระทำที่มิชอบด้วยกฎหมาย และต้องปฏิบัติตามประกาศฉบับนี้ โดยกำหนดให้มีมาตรการ ดังนี้

๙.๑ สำนักงาน ต้องควบคุมบุคคลหรือนิติบุคคลที่เป็นผู้ให้บริการด้านการจัดเก็บข้อมูล ผู้พัฒนาระบบสารสนเทศ ผู้รับจ้างบันทึกข้อมูล หรือผู้เกี่ยวข้องภายนอก ที่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ รวมถึงผู้ใช้งานข้อมูลส่วนบุคคลที่สำนักงานเป็นผู้ควบคุมข้อมูลส่วนบุคคล ให้เป็นไปตามมาตรการรักษาความปลอดภัยเชิงกายภาพ

๙.๒ สำนักงาน ต้องจัดให้มีข้อตกลงระหว่างสำนักงานและผู้ประมวลข้อมูลเป็นลายลักษณ์อักษร โดยต้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งให้สำนักงานทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และกำหนดให้ต้องปฏิบัติตามประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ ตลอดจนกฎหมาย ระเบียบ หลักเกณฑ์ วิธีการ หรือเงื่อนไขเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศซึ่งใช้บังคับ ณ ปัจจุบัน รวมถึงที่ได้มีการแก้ไขในอนาคต

ประกาศ ณ วันที่ ๑๔ มีนาคม ๒๕๖๖

(นายนิวัติไชย เกษมมงคล)
เลขาธิการคณะกรรมการ ป.ป.ช.