ประกาศการประปานครหลวง
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
ของการประปานครหลวง (Information and Cyber Security Policy)

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ ประกอบกับตามมาตรา ๔๔ และมาตรา ๔๕ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

อาศัยอำนาจตามความในมาตรา ๓๓ (๒) แห่งพระราชบัญญัติการประปานครหลวง พ.ศ. ๒๕๑๐ จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวงให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ และเพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของการประปานครหลวง จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศการประปานครหลวง เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง (Information and Cyber Security Policy)”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ เป็นต้นไป

ข้อ ๓ ให้ยกเลิก ประกาศการประปานครหลวง เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง ประกาศ ณ วันที่ ๒๖ สิงหาคม ๒๕๖๗

ข้อ ๔ ขอบเขตการดำเนินการ

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง มีขอบเขตครอบคลุมการดำเนินงานตามภารกิจของการประปานครหลวงที่มีการใช้เทคโนโลยีในการสนับสนุนการดำเนินงานอันประกอบไปด้วย ข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ (Information Technology) ระบบเทคโนโลยีเชิงปฏิบัติงาน (Operation Technology) รวมถึงการใช้เทคโนโลยีคอมพิวเตอร์อื่นใดมาสนับสนุนการดำเนินการตามภารกิจ และมีขอบเขตครอบคลุมการกำกับดูแลและบริหารจัดการ การรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ทั่วทั้งองค์กร โดยประกอบไปด้วยการควบคุมเชิงการกำกับดูแลและบริหารงาน การควบคุมด้านกระบวนการ การควบคุมโดยใช้เทคโนโลยี การควบคุมเชิงกายภาพและสิ่งแวดล้อม

และการควบคุมด้านบุคลากร อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework ๒.๐ ของ National Institute of Standards and Technology:NIST)

ข้อ ๕ วัตถุประสงค์

๕.๑ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๕.๒ เพื่อเผยแพร่ให้ผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรได้รับทราบ และผู้ปฏิบัติงานทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๕.๓ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๕.๔ เพื่อกำหนดความรับผิดชอบ ในกรณีที่ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

ข้อ ๖ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง (Information and Cyber Security Policy) มีดังต่อไปนี้

๖.๑ การกำกับดูแลและการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information Security and Cybersecurity Governance and Management) โดยการจัดให้มีคณะกรรมการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์เป็นผู้รับผิดชอบด้านการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศและไซเบอร์เพื่อกำหนดทิศทางและนโยบายด้านความมั่นคงปลอดภัยให้เหมาะสมกับความเสี่ยงและสภาพแวดล้อมของการประปานครหลวง รวมถึงการติดตามการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๖.๒ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information Security and Cybersecurity Risk Assessment) โดยการจัดให้มีการประเมินความเสี่ยงเพื่อการระบุ วิเคราะห์ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ที่อาจเกิดขึ้นกับข้อมูลและระบบสารสนเทศ เพื่อการจัดการความเสี่ยงและจัดทำมาตรการควบคุมที่เหมาะสม

๖.๓ การบริหารองค์กรและทรัพยากรมนุษย์เพื่อการจัดการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Organization and Human Resource Security) โดยการกำหนดแนวทางด้านบุคลากร ประกอบไปด้วยการอบรม การคัดเลือก การจัดทำข้อตกลงการจ้างงานและการบริหารความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๖.๔ การจัดการทรัพย์สินสารสนเทศ (Asset Management) โดยการจัดทำรายการทรัพย์สินสารสนเทศเพื่อระบุ บันทึก และจัดประเภททรัพย์สินสารสนเทศเพื่อให้สามารถควบคุมและปกป้องได้ตามระดับความเสี่ยง

๖.๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) โดยการกำหนดและสื่อสาร ความคาดหวังและแนวปฏิบัติของผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร เพื่อรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๖.๖ การใช้งานอุปกรณ์พกพา (User of Personal Computer and Mobile) โดยการจัดให้มีมาตรการควบคุมความปลอดภัยสำหรับอุปกรณ์พกพาและคอมพิวเตอร์ส่วนบุคคลที่เชื่อมต่อกับระบบขององค์กร

๖.๗ ความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Data Security) โดยการกำหนดให้มีวิธีการปกป้องข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการทำลายโดยมิชอบ ทั้งในระหว่างการจัดเก็บ การสื่อสาร และการใช้งาน

๖.๘ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Control) โดยการกำหนดการควบคุมการเข้าถึงระบบสารสนเทศตามสิทธิ์ที่เหมาะสมกับบทบาทหน้าที่ของผู้ใช้งาน

๖.๙ การออกแบบระบบเครือข่ายและการควบคุมการเข้าถึงระบบเครือข่าย (Secured Network Design and Network Access Control) โดยการกำหนดมาตรการในการออกแบบเครือข่ายและการควบคุมการเข้าถึงเพื่อป้องกันภัยคุกคาม

๖.๑๐ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) โดยการกำหนดการจัดการสิทธิ์การเข้าถึงระบบปฏิบัติการให้มีความมั่นคงปลอดภัย

๖.๑๑ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยการกำหนดสิทธิ์การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและข้อมูลสำคัญให้มีความมั่นคงปลอดภัย

๖.๑๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) โดยการกำหนดการควบคุมเชิงเทคนิคในการลดช่องโหว่ทางเทคนิคโดยการตั้งค่าระบบและอุปกรณ์ให้มีความมั่นคงปลอดภัยตามแนวปฏิบัติที่ดี

๖.๑๓ การประเมินช่องโหว่และการทดสอบระบบ (Vulnerability Assessment and Penetration Testing) โดยการจัดให้มีการตรวจหาช่องโหว่ในระบบและทดสอบด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์เพื่อประเมินความเสี่ยงและการจัดการความเสี่ยงจากช่องโหว่ทางด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๖.๑๔ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Control) โดยการจัดให้มีมาตรการป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาตในเชิงกายภาพและควบคุมด้านสภาพแวดล้อมการประมวลผลของอุปกรณ์คอมพิวเตอร์เพื่อป้องกันความเสี่ยงจากปัจจัยสิ่งแวดล้อม

๖.๑๕ การควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์และพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์ (Data Center and Secure Area Access Control) โดยการควบคุมและตรวจสอบการเข้าออกของบุคคลในพื้นที่ที่มีอุปกรณ์สำคัญของระบบ

๖.๑๖ การเข้ารหัสข้อมูลสารสนเทศ (Cryptography) โดยการกำหนดแนวทางการใช้เทคโนโลยีการเข้ารหัสเพื่อปกป้องความลับและความถูกต้องของข้อมูล

๖.๑๗ การสำรองและกู้คืนข้อมูล (Backup and Recovery) โดยการวางแผนและดำเนินการสำรองข้อมูลทำให้เกิดความพร้อมในการกู้คืนเมื่อเกิดเหตุผิดปกติ

๖.๑๘ การควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (Internet and E-Mail) โดยการควบคุมเชิงเทคนิคและการกำหนดวิธีการใช้งานอินเทอร์เน็ตและอีเมลของพนักงานอย่างมั่นคงปลอดภัย

๖.๑๙ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Network Security) โดยการกำหนดมาตรการในการปกป้องระบบเครือข่ายไร้สายจากการบุกรุกหรือใช้งานโดยไม่ได้รับอนุญาต

๖.๒๐ ควบคุมความปลอดภัยของกระบวนการจัดหา พัฒนา และบำรุง ดูแลระบบสารสนเทศ (System acquisition, development and maintenance) โดยการกำหนดมาตรการพัฒนาระบบงานอย่างมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ

๖.๒๑ การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management) โดยการกำหนดแนวทางการบริหารจัดการผู้ให้บริการภายนอกด้านความมั่นคงปลอดภัยตั้งแต่การคัดเลือก การเริ่มใช้บริการ ระหว่างการใช้บริการ จนถึงภายหลังการเสร็จสิ้นสัญญาการใช้บริการ

๖.๒๒ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cybersecurity Detection and Monitoring) โดยการจัดให้มีระบบและขั้นตอนการปฏิบัติงานในการตรวจจับและติดตามภัยคุกคามทางความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๖.๒๓ การบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศและไซเบอร์ (Information Security and Cybersecurity Incident Management) โดยการกำหนดขั้นตอนการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยอย่างเป็นระบบและทันท่วงที

๖.๒๔ การบริหารความต่อเนื่องและพร้อมใช้ของระบบสารสนเทศอย่างปลอดภัย (Information security aspects of business continuity management) โดยการวางแผนและทดสอบความต่อเนื่องของระบบงานสำคัญเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดสถานการณ์ด้านความปลอดภัยสารสนเทศและไซเบอร์ที่ส่งผลกระทบต่อการดำเนินงาน

๖.๒๕ การใช้เทคโนโลยี Generative AI ที่ยอมรับได้ (Acceptable Use Policy: Generative AI) โดยการกำหนดแนวทางการใช้เทคโนโลยี Generative AI อย่างถูกต้องเหมาะสมมีความรับผิดชอบและให้สามารถนำเทคโนโลยีดังกล่าวไปรังสรรค์งานได้อย่างปลอดภัย มีประสิทธิภาพ ตลอดจนป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานที่ไม่เหมาะสม

๖.๒๖ การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Audit) โดยการกำหนดแนวทางการปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๖.๒๗ การปฏิบัติตามข้อบังคับ (Compliance) โดยการกำหนดขั้นตอนในการบริหารจัดการให้การดำเนินงานเป็นไปตามกฎหมาย มาตรฐาน หรือข้อบังคับที่เกี่ยวข้อง

ข้อ ๗ คณะกรรมการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์จัดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่สนับสนุนการดำเนินงานตามนโยบายนี้ โดยให้แต่งตั้งคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขึ้นทำหน้าที่หลักในการดำเนินการ ทั้งนี้ คณะกรรมการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เป็นผู้อนุมัติ และประกาศใช้แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ นี้

ข้อ ๘ บุคลากรของการประปานครหลวงต้องปฏิบัติตามกฎหมาย นโยบาย ระเบียบ คำสั่ง ขั้นตอนและแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง หากผู้ใช้งานฝ่าฝืนและก่อหรืออาจก่อให้เกิดความเสียหายแก่การประปานครหลวงหรือผู้หนึ่งผู้ใด การประปานครหลวง จะพิจารณาดำเนินการทางวินัยและทางกฎหมาย

ข้อ ๙ ให้มีการทบทวน/ปรับปรุง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง รวมทั้งแนวปฏิบัติที่เกี่ยวข้อง อย่างน้อย ปีละ ๑ ครั้ง

ข้อ ๑๐ ให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์หรือข้อมูลเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ โดยผู้บริหารระดับสูงสุดมีหน้าที่กำกับดูแลรับผิดชอบให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

ข้อ ๑๑ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ถือเป็นมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและไซเบอร์ขององค์กร โดยให้อ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยเชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรต้องถือปฏิบัติตามอย่างเคร่งครัด

ข้อ ๑๒ กฎหมาย ระเบียบข้อบังคับ และประกาศที่เกี่ยวข้อง

๑๒.๑ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่ประกาศใช้งาน

๑๒.๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ประกาศใช้งาน

๑๒.๓ พระราชบัญญัติข้อมูลข่าวสารของราชการ ที่ประกาศใช้งาน

๑๒.๔ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ที่ประกาศใช้งาน

๑๒.๕ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ที่ประกาศใช้งาน

๑๒.๖ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ ที่ประกาศใช้งาน

๑๒.๗ ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ ที่ประกาศใช้งาน

๑๒.๘ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย ที่ประกาศใช้งาน

๑๒.๙ ระเบียบว่าด้วยการรักษาความลับของทางราชการ ที่ประกาศใช้งาน

๑๒.๑๐ ระเบียบการประปานครหลวง ว่าด้วยข้อมูลข่าวสารของการประปานครหลวง ที่ประกาศใช้งาน

๑๒.๑๑ ระเบียบการประปานครหลวง ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑ สิงหาคม พ.ศ. ๒๕๖๘

(นางสาวสุวรา ทวิชศรี)
ผู้ว่าการการประปานครหลวง

ที่ กกล.ว ๑๗๕/๒๕๖๘
เรียน หน่วยงานต่าง ๆ
เพื่อโปรดทราบ

(นางสาวขนิสถา พัฒน์เชียร)
ผู้อำนวยการกองกลาง