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

(เอกสารแนบท้ายประกาศ)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวง

คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

กรกฎาคม พ.ศ. ๒๕๖๘

ประวัติการแก้ไขเอกสาร

ครั้งที่	รายละเอียดการแก้ไข	วันที่มีผลบังคับใช้
๑	ฉบับร่าง	๑๒ มกราคม ๒๕๖๕
๒	ฉบับสมบูรณ์	๑๑ กุมภาพันธ์ ๒๕๖๕
๓	แก้ไขโครงสร้างบริหาร และเพิ่มเติมแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	๑ กันยายน ๒๕๖๖
๔	ปรับปรุงแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ออกจากกัน	๑ สิงหาคม ๒๕๖๗
๕	ปรับปรุง ตาม พระราชบัญญัติ ความมั่นคงปลอดภัยไซเบอร์	๑ กรกฎาคม ๒๕๖๘
๖	-	-
๗	-	-

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๔ ในมาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และ พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒-ที่ให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงานเป็นลายลักษณ์อักษร

การประปานครหลวงได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมทั้งแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของการประปานครหลวงขึ้น เพื่อให้การประปานครหลวงมีแนวทางปฏิบัติในการควบคุมการปฏิบัติงาน และรักษาความปลอดภัยด้านระบบสารสนเทศและไซเบอร์ ตลอดจนสอดคล้องตามพระราชกฤษฎีกาดังกล่าว ซึ่งประกอบด้วย แนวนโยบายและแนวปฏิบัติต่างๆ ซึ่งเป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติ เพื่อให้เกิดความมั่นคงปลอดภัยในการดำเนินงานและการให้บริการต่างๆ ของการประปานครหลวง อีกทั้งยังสร้างความเชื่อมั่นให้กับผู้ใช้บริการ และผู้มีส่วนเกี่ยวข้องทั้งภายในและภายนอกการประปานครหลวง รวมทั้งสร้างความน่าเชื่อถือในการใช้งานระบบสารสนเทศให้การประปานครหลวงต่อไป

การประปานครหลวง

เดือน...กรกฎาคม.....ปี...๒๕๖๘....

สารบัญ

คำนิยาม

“องค์กร”	หมายถึง	การประปานครหลวง
“การรักษาความมั่นคงปลอดภัย”	หมายถึง	การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและไซเบอร์ ของการประปานครหลวง
“มาตรฐาน (Standard)”	หมายถึง	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
“วิธีการปฏิบัติ (Procedure)”	หมายถึง	รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งบรรทัดฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
“ทรัพย์สิน (Asset)”	หมายถึง	ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ อุปกรณ์ ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
“ผู้ใช้งาน”	หมายถึง	บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานระบบสารสนเทศและสินทรัพย์ต่างๆ ขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ตามที่การประปานครหลวง กำหนด ทั้งนี้บุคคลดังกล่าวนี้รวมถึง บุคคลที่ไม่ใช่พนักงาน ลูกจ้าง และผู้บริหารของการประปานครหลวง ด้วย
“ผู้บริหาร”	หมายถึง	ผู้ว่าการ รองผู้ว่าการ ผู้ช่วยผู้ว่าการ ผู้อำนวยการฝ่าย ผู้จัดการสำนักงานประปาสาขา ผู้อำนวยการกอง หัวหน้าส่วน รวมถึงคณะกรรมการบริหารขององค์กร
“ผู้ปฏิบัติงาน”	หมายถึง	พนักงาน และลูกจ้างของการประปานครหลวง (บุคคลที่ได้รับสิทธิการเข้าใช้งานระบบเครือข่ายของการประปานครหลวง)
“บุคคลภายนอก”	หมายถึง	บุคคลที่ได้รับอนุญาตให้สามารถเข้าระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศขององค์กร
“ระบบเทคโนโลยีสารสนเทศ (Information Technology System หรือ IT System)”	หมายถึง	ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารการสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
ระบบเทคโนโลยีปฏิบัติการ (Operational Technology System หรือ OT System)	หมายถึง	ระบบงานของหน่วยงานที่นำเอาระบบคอมพิวเตอร์ ระบบเครือข่าย มาใช้ในการตรวจวัด ควบคุม และบริหารจัดการกระบวนการทางกายภาพในภาคอุตสาหกรรมหรือโครงสร้างพื้นฐานสำคัญ เช่น ระบบควบคุมเครื่องจักรในการผลิต ระบบ

		ควบคุมกระแสไฟฟ้า ระบบควบคุมการผลิต และระบบ Supervisory Control and Data Acquisition (“SCADA”) โดยมีเป้าหมายหลักเพื่อประสิทธิภาพในการดำเนินงาน เพิ่มความน่าเชื่อถือในการทำงาน (Reliability) และความปลอดภัย
“เจ้าของระบบงาน”	หมายถึง	ผู้บริหารของหน่วยงานหรือผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาที่มีความรับผิดชอบโดยรวมต่อระบบเทคโนโลยีสารสนเทศ (IT) หรือระบบเทคโนโลยีปฏิบัติการ (OT) ที่สนับสนุนกระบวนการทางธุรกิจ มีหน้าที่กำหนดความต้องการทางธุรกิจของระบบ ดูแลการใช้ระบบให้สอดคล้องกับวัตถุประสงค์ของการประปานครหลวงและมีอำนาจในการตัดสินใจเรื่องการเปลี่ยนแปลง การควบคุมการเข้าถึง และระดับความมั่นคงปลอดภัยของระบบนั้น
“เจ้าของข้อมูล”	หมายถึง	ผู้บริหารของหน่วยงานหรือผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย ถูกเปลี่ยนแปลงแก้ไขหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต
“ผู้ดูแลระบบงาน (Administrator)”	หมายถึง	ผู้ปฏิบัติงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) หรือระบบเทคโนโลยีปฏิบัติการ (Operational Technology: OT)
“ผู้ดูแลระบบเครือข่าย (Network Administrator)”	หมายถึง	ผู้ปฏิบัติงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่าย
“ผู้ดูแลศูนย์คอมพิวเตอร์”	หมายถึง	ผู้ปฏิบัติงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลศูนย์คอมพิวเตอร์
“ผู้ดูแลศูนย์พื้นที่”	หมายถึง	ผู้ปฏิบัติงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลพื้นที่ติดตั้งระบบคอมพิวเตอร์ที่ไม่ได้อยู่ในศูนย์คอมพิวเตอร์เช่นห้องควบคุมที่มีการติดตั้งอุปกรณ์ SCADA เป็นต้น
“สิทธิของผู้ใช้งาน (User Access Right)”	หมายถึง	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของการประปานครหลวง
“หน่วยงานภายนอก”	หมายถึง	องค์กรภายนอกที่การประปานครหลวงอนุญาต ให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือ สินทรัพย์ต่าง ๆ ของการประปานคร

		หลวง โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบใน การรักษาความลับของข้อมูล
“ผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Third Party Service Provider)”	หมายถึง	บุคคล ห้างหุ้นส่วน หรือบริษัท ที่ให้บริการพัฒนาระบบงาน ออกแบบติดตั้งระบบงานหรือระบบเครือข่าย ให้บริการบำรุงรักษาระบบงาน ผู้ให้บริการ Cloud Computing ผู้ให้บริการการประมวลผล ผู้ให้บริการศูนย์คอมพิวเตอร์ ผู้ให้บริการที่เข้ามาปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หรือผู้ให้บริการอื่น ๆ ที่จัดจ้างเข้ามาเพื่อดำเนินกิจกรรมใด ๆ แทนเจ้าหน้าที่ของการประปานครหลวง
“ข้อมูล (Data)”	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตาม พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔
“สารสนเทศ (Information)”	หมายถึง	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใช้ได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
“ระบบคอมพิวเตอร์”	หมายถึง	อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
“ระบบเครือข่าย (Network System)”	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ขององค์กรได้ได้แก่ ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น
“อุปกรณ์พกพา (Mobile Device)”	หมายถึง	เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเล็ต (Tablet) โดยอุปกรณ์พกพาใช้เพื่อการเข้าถึงการใช้งาน และจัดเก็บสารสนเทศของ การประปานครหลวง
“จดหมายอิเล็กทรอนิกส์ (E-Mail)”	หมายถึง	ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP เป็นต้น

“รหัสผ่าน (Password)”	หมายถึง	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
“ชุดคำสั่งไม่พึงประสงค์”	หมายถึง	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตาม คำสั่งที่กำหนดไว้
“การเข้าถึงหรือควบคุมสารสนเทศ”	หมายถึง	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานการใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตนั้น สำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติ เกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย
“ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์”	หมายถึง	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องด้านครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
“เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์”(Event)	หมายถึง	กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
“สถานการณ์ด้านความมั่นคงปลอดภัยด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security and Cyber Incident)”	หมายถึง	สถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
“ไซเบอร์ (Cyber)”	หมายถึง	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

		(อ้างอิงจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒)
“การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)”	หมายถึง	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคง ทางเศษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
“ภัยคุกคามทางไซเบอร์ (Cyber threat)”	หมายถึง	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้ไซเบอร์คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
“หน่วยงานของรัฐ (Government Agency)”	หมายถึง	ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ
“เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident)”	หมายถึง	เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มิชอบซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
“โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure : CI)”	หมายถึง	บรรดาหน่วยงาน หรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงาน หรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้นมีผลเกี่ยวเนื่อง สำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน
“โครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ (Critical Information Infrastructure)”	หมายถึง	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure Operation)”	หมายถึง	หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มาตร ๔๙ เป็นหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีดังนี้ • ด้านความมั่นคงของรัฐ • ด้านบริการภาครัฐที่สำคัญ • ด้านการเงินการธนาคาร • ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม • ด้านการขนส่งและโลจิสติกส์ • ด้านพลังงานและสาธารณูปโภค • ด้านสาธารณสุข • ด้านอื่นตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนดเพิ่มเติม
“หน่วยงานควบคุมหรือกำกับดูแล (Regulator)”	หมายถึง	หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หมวด ๑
การกำกับดูแลและการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
(Information Security and Cybersecurity Governance and Management)

๑. วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์ให้มีการกำกับดูและการบริหารจัดการ การกำหนดแผนยุทธศาสตร์ การกำกับดูแลการดำเนินงาน การกำหนดแนวทางการบริหารความเสี่ยง และการปรับปรุงอย่างต่อเนื่อง สำหรับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒. ผู้รับผิดชอบ

๒.๑ คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศและไซเบอร์

๒.๒ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๓ คณะทำงานบริหารความเสี่ยงและควบคุมภายใน

๒.๔ ผู้ดูแลระบบงาน

๓. แนวปฏิบัติ

๓.๑ ทำการรวบรวมข้อมูลและวิเคราะห์บริบทขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เพื่อให้เกิดความเข้าใจต่อภารกิจ วัตถุประสงค์และความคาดหวังของผู้มีส่วนได้เสียทั้งภายในและภายนอก เพื่อใช้เป็นแนวทางในการกำหนดแผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์และเป็นแนวทางในการบริหารความเสี่ยง โดยการวิเคราะห์บริบทขององค์กรต้องทำการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยมีวิธีปฏิบัติดังนี้

๓.๑.๑ คณะกรรมการฯ สั่งการคณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๑.๒ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และผู้ปฏิบัติงานที่ได้รับมอบหมายเก็บรวบรวมข้อมูลและจัดการวิเคราะห์บริบทขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ อันประกอบไปด้วย

๓.๑.๒.๑ ภารกิจ วัตถุประสงค์ การดำเนินงานที่สำคัญ คุณสมบัติ และบริการ ขององค์กรและความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่ส่งผลกระทบต่อความสามารถในการบรรลุวัตถุประสงค์ขององค์กร

๓.๑.๒.๒ ความต้องการและความคาดหวังของผู้มีส่วนได้เสียทั้งภายในและภายนอกกับการจัดการความเสี่ยงความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๑.๒.๓ ข้อกำหนดด้านกฎหมาย กฎระเบียบ และสัญญาเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๑.๒.๔ การใช้บริการที่สำคัญจากผู้ให้บริการภายนอกและความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่เกี่ยวข้อง

๓.๑.๓ คณะกรรมการ ฯ พิจารณาอนุมัติ ผลการวิเคราะห์บริบทขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๑.๔ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ สื่อสารผลการวิเคราะห์บริบทขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ให้หน่วยงานที่เกี่ยวข้อง

๓.๒ คณะกรรมการ ฯ ต้องจัดให้มีการจัดทำแผนปฏิบัติการ การรายงานผลเกี่ยวกับ การดำเนินการตามแผนงานโครงการ การปฏิบัติงาน การจัดการความเสี่ยงและเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ โดยมีวิธีการปฏิบัติดังนี้

๓.๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ดูแลระบบงาน จัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ประจำปี โดยพิจารณาจากการวิเคราะห์บริบทขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ อันประกอบไปด้วย

๓.๒.๑.๑ แผนงานโครงการเพิ่มประสิทธิภาพด้านการจัดการความเสี่ยง

๓.๒.๑.๒ แผนการดำเนินงานและกิจกรรมด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๒.๑.๓ แนวทางการวัดผลสัมฤทธิ์ของแผนงานโครงการและแผนการดำเนินงาน

๓.๒.๑.๔ แผนการด้านการบริหารทรัพยากรบุคคลและทรัพยากรเทคโนโลยีสารสนเทศสำหรับการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๒.๑.๕ ผู้ดูแลระบบงาน มีหน้ามีเสนอความเห็นและข้อสังเกตุต่อคณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปในการปรับปรุงประสิทธิภาพของระบบสารสนเทศและการจัดการความเสี่ยง

๓.๒.๒ คณะกรรมการ ฯ พิจารณาอนุมัติจัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๓ คณะกรรมการ ฯ ต้องจัดให้มีการจัดทำและประกาศใช้นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ทั่วทั้งองค์กร โดยคณะทำงานฯและผู้ปฏิบัติงานที่ได้รับมอบหมาย เป็นผู้จัดทำและนำเสนอต่อคณะกรรมการ ฯ เพื่อพิจารณา ทั้งนี้คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ต้องจัดให้มีการทบทวนนโยบายและแนวปฏิบัติ อย่างน้อยปีละ ๑ ครั้ง โดยพิจารณาผลจากการวิเคราะห์บริบทขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ร่วมด้วยเป็นสำคัญ

๓.๔ จัดทำแนวปฏิบัติการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์เพื่อใช้เป็นขั้นตอนแนวทางในการจัดการความเสี่ยง มีวิธีการปฏิบัติ ดังนี้

๓.๔.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ปฏิบัติงานที่ได้รับมอบหมาย จัดทำแนวปฏิบัติด้านการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ โดยต้องประกอบไปด้วยหัวข้อดังต่อไปนี้

๓.๔.๑.๑ ระบุวัตถุประสงค์ของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ โดยสอดคล้องกับการวิเคราะห์บริบทขององค์กรในหัวข้อ ๓.๑

๓.๔.๑.๒ จัดทำคำอธิบายระดับความยอมรับความเสี่ยง (Risk Appetite) และเกณฑ์การยอมรับความเสี่ยงที่สอดคล้องกับการบริหารความเสี่ยงระดับองค์กร

๓.๔.๑.๓ กำหนดแนวทางในการคำนวณค่าความเสี่ยง การระบุระดับค่าความเสี่ยง และการประเมินระดับความเสี่ยง

๓.๔.๑.๔ การระบุแนวทางการตอบสนองต่อความเสี่ยง การจัดลำดับความสำคัญของการจัดการความเสี่ยง

๓.๔.๑.๕ กำหนดวิธีการและรูปแบบการรายงานผลการประเมินความเสี่ยงและแผนการตอบสนองความเสี่ยงต่อผู้เกี่ยวข้อง

๓.๔.๑.๖ รวบรวมและรายงานความเสี่ยงที่เกี่ยวข้องกับโอกาสเชิงกลยุทธ์ขององค์กร

๓.๔.๒ คณะทำงานบริหารความเสี่ยงและควบคุมภายในร่วมพิจารณาให้ความเห็นและให้คำปรึกษาในการจัดทำแนวปฏิบัติด้านการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๔.๓ คณะกรรมการ ฯ พิจารณาอนุมัติ แนวปฏิบัติด้านการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๔.๔ คณะทำงานฯ และผู้ดูแลระบบงานหรือผู้ปฏิบัติงานที่ได้รับมอบหมาย ดำเนินการประเมินความเสี่ยง รายงานความเสี่ยงและจัดทำแผนการตอบสนองความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง หรือคณะกรรมการฯ อาจพิจารณาให้ดำเนินการประเมินความเสี่ยงเพิ่มเติมเมื่อเกิดความเปลี่ยนแปลงที่สำคัญที่ส่งผลกระทบต่อปัจจัยความเสี่ยงเช่น การเริ่มใช้งานเทคโนโลยีใหม่ที่อาจเกิดความเสี่ยงเพิ่มขึ้น หรือหลังการเกิดเหตุการณ์ด้านความปลอดภัยสารสนเทศและไซเบอร์ที่สำคัญ

๓.๔.๕ คณะกรรมการ ฯ พิจารณาอนุมัติผลการประเมินความเสี่ยง

๓.๔.๖ คณะทำงานฯ และผู้ดูแล/ผู้ปฏิบัติงานที่ได้รับมอบหมาย รายงานผลการดำเนินการตามแผนการตอบสนองความเสี่ยงต่อคณะกรรมการ ฯ

๓.๕ คณะกรรมการ ฯ จัดให้มีการประชุม รายงานผล การปฏิบัติงานตามแผนปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ การบริหารความเสี่ยง การปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

หมวด ๒
การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
(Information Security and Cybersecurity Risk Assessment)

๑. วัตถุประสงค์

เพื่อระบุและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่อาจเกิดขึ้นกับการประปานครหลวง เพื่อกำหนดแนวทางควบคุมที่เหมาะสม และสนับสนุนการตัดสินใจเชิงกลยุทธ์ เพื่อป้องกันความเสียหายและรักษาความต่อเนื่องในการดำเนินธุรกิจ อันประกอบด้วยการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินระดับความเสี่ยง การจัดการความเสี่ยง การรายงานและติดตามความเสี่ยง

๒. ผู้ที่เกี่ยวข้อง

๒.๑. คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
๒.๒. คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
๒.๓. คณะทำงานบริหารความเสี่ยงและควบคุมภายใน
๒.๔. ผู้ดูแล/ผู้ปฏิบัติงานที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑. ข้อกำหนดระดับความเสี่ยงที่การประปานครหลวงยอมรับได้ในเชิงกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information Security and Cybersecurity Risk Appetite) ของการประปานครหลวง จัดทำขึ้นเพื่อเป็นกรอบกำหนดระดับความเสี่ยงที่การประปานครหลวงยอมรับได้ในเชิงกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวงให้สอดคล้องกับกลยุทธ์ทางธุรกิจ ระดับความเสี่ยงที่ยอมรับได้ (Risk Acceptant) และข้อกำหนดตามกฎหมายและข้อบังคับการประปานครหลวง ต้องใช้กรอบนี้เป็นแนวทางในการตัดสินใจเรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ ทั้งในระดับยุทธศาสตร์และการดำเนินงาน โดยมีหลักการและแนวทางดังนี้

๓.๑.๑. ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

การประปานครหลวงมีระดับความเสี่ยงที่ยอมรับได้ในเชิงกลยุทธ์ในระดับต่ำ (Low Risk Appetite) ต่อความเสี่ยงที่อาจก่อให้เกิดการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การหยุดชะงักของการดำเนินงาน หรือความเสียหายต่อชื่อเสียงการประปานครหลวง หากไม่สามารถหลีกเลี่ยงความเสี่ยงได้ จะต้องมีการลดระดับความเสี่ยงให้เหลืออยู่ในระดับที่ยอมรับได้

๓.๑.๒. ความเสี่ยงด้านการดำเนินงาน

การประปานครหลวงมีระดับความเสี่ยงที่ยอมรับได้ในเชิงกลยุทธ์ในระดับต่ำมาก (Very Low Risk Appetite) ต่อความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานที่สำคัญ เช่น การโจมตีด้วยแรนซัมแวร์

หรือการโจมตีแบบปฏิเสธการให้บริการ (DDoS) ระบบที่มีความสำคัญจะต้องมีมาตรการควบคุม เหตุการณ์ตอบสนอง และการกู้คืนระบบอย่างชัดเจน

๓.๑.๓. ความเสี่ยงด้านข้อมูล

การประปานครหลวงไม่ยอมรับความเสี่ยงใด ๆ (Zero Tolerance) ที่อาจนำไปสู่การเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินโดยไม่ได้รับอนุญาต ข้อมูลประเภทนี้ต้องมีการเข้ารหัส ควบคุมสิทธิ์เข้าถึง และมีระบบตรวจสอบที่เหมาะสม

๓.๑.๔. ความเสี่ยงจากผู้ให้บริการภายนอก

การประปานครหลวงมีระดับความเสี่ยงที่ยอมรับได้ในเชิงกลยุทธ์ในระดับในระดับปานกลาง (Moderate Risk Appetite) จากการใช้บริการของบุคคลภายนอกในกรณีที่ ผ่านการคัดเลือกและประเมินความมั่นคงปลอดภัยมีขอบเขตการดำเนินงานที่ไม่เกี่ยวข้องกับข้อมูลที่อ่อนไหว มีการควบคุมและติดตามการให้ของผู้ให้บริการ ให้บริการ สำหรับผู้ให้บริการที่มีนัยสำคัญต้องมีข้อตกลงด้านความมั่นคงปลอดภัยในสัญญาและมีการประเมินซ้ำอย่างสม่ำเสมอ

๓.๑.๕. ความเสี่ยงเชิงยุทธศาสตร์

การประปานครหลวงมีระดับความเสี่ยงที่ยอมรับได้ในเชิงกลยุทธ์ในระดับปานกลาง (Moderate Risk Appetite) ในการสนับสนุนนวัตกรรม การเปลี่ยนผ่านสู่ดิจิทัล หรือโอกาสทางธุรกิจที่ชัดเจน โดยต้องมีการระบุความเสี่ยงที่ชัดเจน มีมาตรการควบคุม และอยู่ในระดับที่ยอมรับได้

๓.๑.๖. ความเสี่ยงด้านการตรวจจับและการเฝ้าระวัง

การประปานครหลวงมีระดับความเสี่ยงที่ยอมรับได้ในเชิงกลยุทธ์ในระดับต่ำ (Low Risk Appetite) ต่อจุดอ่อนในการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัย ระบบโครงสร้างพื้นฐานที่สำคัญต้องมีการตรวจจับภัยคุกคาม และบันทึกเหตุการณ์อย่างต่อเนื่อง

๓.๑.๗. ความเสี่ยงจากบุคคลากร

การประปานครหลวงมีระดับความเสี่ยงที่ยอมรับได้ในเชิงกลยุทธ์ในระดับต่ำ (Low Risk Appetite) ต่อความเสี่ยงที่เกิดจากผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคล ภายนอกที่ปฏิบัติงานให้กับการประปานครหลวง ไม่ว่าจะโดยเจตนาหรือไม่ก็ตาม การเข้าถึงระบบหรือข้อมูลจะต้องเป็นไปตามหน้าที่เท่านั้น และต้องจัดให้มีการสร้างความความรู้ ความเข้าใจ ละความตระหนัก ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคล ภายนอกที่ปฏิบัติงานให้กับการประปานครหลวง

๓.๑.๘. ความเสี่ยงด้านการปฏิบัติตามกฎหมาย

การประปานครหลวงไม่ยอมรับความเสี่ยงใด ๆ (Zero Tolerance) ที่เกี่ยวข้องกับการละเมิดกฎหมายหรือข้อกำหนดที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เช่น พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติการกระทำผิดด้านคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) หรือข้อบังคับอุตสาหกรรมอื่น ๆ

๓.๒. คณะกรรมการฯ และคณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ต้องกำหนดให้การการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์นี้ เป็นส่วนหนึ่งของการประเมินความเสี่ยงระดับองค์กร เพื่อให้สามารถบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ในระดับเดียวกับความเสี่ยงอื่น ๆ และสร้างความเข้าใจร่วมกันระหว่างหน่วยงานด้านเทคโนโลยีกับผู้บริหารในเชิงธุรกิจ ด้วยการ

๓.๒.๑. จัดกลุ่มความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ให้สอดคล้องกับประเภทความเสี่ยงของการประปานครหลวง เช่น ด้านปฏิบัติการ การเงิน กฎหมาย

๓.๒.๒. ใช้ทะเบียนความเสี่ยงร่วมกับการบริหารความเสี่ยงระดับองค์กร โดยบันทึกความเสี่ยงไซเบอร์ไว้ในรายการความเสี่ยงระดับองค์กร

๓.๒.๓. ใช้เกณฑ์การประเมินเดียวกันกับการบริหารความเสี่ยงระดับองค์กร เช่น ระดับผลกระทบ/โอกาสเกิด เพื่อเปรียบเทียบความเสี่ยงได้ทุกประเภท

๓.๒.๔. รายงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ร่วมกับความเสี่ยงด้านอื่น โดยนำเสนอรายงานความเสี่ยงไซเบอร์ ในรายงานความเสี่ยงองค์กรรายไตรมาสหรือรายปีต่อผู้บริหารและคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน

๓.๒.๕. เชื่อมโยงความเสี่ยงการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ กับผลกระทบทางธุรกิจ เช่น ภัยคุกคามทางไซเบอร์ นั้นส่งผลกระทบต่อ การให้บริการหรือชื่อเสียง

๓.๒.๖. รวบรวมความเสี่ยงที่ส่งผลหรือเกิดโอกาสในการพัฒนาปรับปรุงหรือส่งผลกระทบในด้านความสามารถในการพัฒนาการประปานครหลวงในอนาคต (Positive Risks) นำเสนอต่อคณะกรรมการฯ เพื่อพิจารณา

๓.๓. คณะกรรมการฯ ต้องจัดให้มีการประเมินความเสี่ยง โดยคณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ดูแลระบบงานที่ได้รับมอบหมาย โดยเริ่มจากการวางแผนและกำหนดขอบเขตของการประเมินความเสี่ยงโดยต้องดำเนินการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง ครอบคลุม ระบบงานสำคัญตามการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) และทรัพย์สินตามรายการทะเบียนทรัพย์สินที่จัดทำไว้

๓.๔. คณะทำงานบริหารความเสี่ยงและควบคุมภายในของหน่วยงานเจ้าของระบบงาน ต้องร่วมดำเนินการประเมินความเสี่ยงโดยร่วมให้ความเห็น ให้คำปรึกษาในการประเมินความเสี่ยง

๓.๕. กระบวนการในการประเมินความเสี่ยงแต่ละขั้นตอนมีรายละเอียดดังนี้

๓.๕.๑. การระบุความเสี่ยง (Risk Identification) เป็นการระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ซึ่งรวมถึงความเสี่ยง จากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการ ปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก ทั้งนี้ความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์มีแนวทางในการพิจารณาลักษณะกลุ่มของความเสี่ยงในเบื้องต้นดังนี้ ทั้งนี้สามารถพิจารณาเพิ่มเติมได้หากพบความเสี่ยงประเภทอื่นในอนาคต

๓.๕.๑.๑. การเข้าถึงระบบโดยไม่ได้รับอนุญาต เช่น ผู้ไม่หวังดีแอบขโมยข้อมูลบัญชีผู้ดูแลระบบผ่านฟิชชิ่ง พนักงานภายในเข้าถึงข้อมูลที่ไม่เกี่ยวข้องกับหน้าที่งาน ผู้บุกรุกเจาะเข้าระบบและขยายสิทธิ์ไปยังระบบอื่น เกิดผลกระทบทำให้ การรั่วไหลของข้อมูล ละเมิดข้อกำหนดทางกฎหมาย ความเสียหายต่อความลับของข้อมูล

๓.๕.๑.๒. มัลแวร์และแรนซัมแวร์ เช่น มีมัลแวร์แฝงตัวมาในอีเมลหรือเว็บไซต์ที่ติดไวรัส แรนซัมแวร์ล็อกไฟล์หรือระบบสำคัญ มัลแวร์มากับซอฟต์แวร์จากผู้ให้บริการภายนอก เกิดผลกระทบทำให้ ระบบไม่สามารถใช้งานได้ ข้อมูลสูญหาย, กระทบต่อการดำเนินธุรกิจ

๓.๕.๑.๓. การโจมตีแบบปฏิเสธการให้บริการ (DoS / DDoS) เช่น เว็บไซต์ถูกโจมตีจนไม่สามารถให้บริการได้ เซิร์ฟเวอร์แอปพลิเคชันล่มจากการถูกใช้งานเกินขีดจำกัด เกิดผลกระทบทำให้ บริการล่ม ลูกค้าเสียความเชื่อมั่น

๓.๕.๑.๔. การรั่วไหลของข้อมูล เช่น การตั้งค่า Cloud Storage ผิดพลาดทำให้ข้อมูลหลุด ส่งอีเมลผิดถึงผู้รับผิดคน แฮกเกอร์แอบขโมยข้อมูลจากฐานข้อมูล เกิดผลกระทบคือทำให้เกิด ข้อมูลลับรั่วไหล โดนค่าปรับจาก ความเสียหายต่อชื่อเสียง

๓.๕.๑.๕. การจัดการตัวตนและสิทธิ์ที่ไม่ปลอดภัย เช่น บัญชีผู้ใช้ที่หมดอายุยังไม่ถูกปิด ใช้รหัสผ่านที่อ่อนแอหรือซ้ำกันในหลายระบบ ไม่มีการใช้การพิสูจน์ตัวตนแบบหลายปัจจัย ทำให้ถูกโจมตีได้ง่าย

๓.๕.๑.๖. ความเสี่ยงจากบุคคลภายนอก / ผู้ให้บริการ เช่น ผู้ให้บริการภายนอกถูกเจาะระบบส่งผลกระทบต่อการประปานครหลวง ระบบที่จ้างภายนอกพัฒนาไม่มีการอัปเดตหรือแพตช์ช่องโหว่ ไม่มีข้อตกลงในการแจ้งเหตุการณ์หรือความมั่นคงปลอดภัยในสัญญา

๓.๕.๑.๗. การโจมตีช่องโหว่ เช่น ระบบที่ยังไม่ได้แพตช์ถูกโจมตีจากระยะไกล ระบบเว็บมีช่องโหว่ (เช่น SQL injection, XSS) อุปกรณ์ ใช้รหัสผ่านเริ่มต้น ทำให้เกิดผลกระทบเช่น ระบบถูกแทรกแซง ความเสียหายต่อความถูกต้องหรือความพร้อมใช้งาน

๓.๕.๑.๘. การหลอกลวงทางสังคม (Social Engineering) เช่น การหลอกให้โอนเงินโดยอ้างเป็นผู้บริหาร (CEO fraud) พนักงานถูกหลอกให้เปิดเผยรหัสผ่าน แอบอ้างเป็นหน่วยงานสายงานเทคโนโลยีดิจิทัล ขอดึงข้อมูลหรือควบคุมระยะไกล ทำให้เกิดผลกระทบเช่น สูญเสียทรัพย์สิน, ข้อมูลรั่วไหล, ความเสียหายชื่อเสียง

๓.๕.๑.๙. ภัยคุกคามจากคนในการประปานครหลวง เช่น พนักงานไม่พอใจองค์กรและนำข้อมูลออกไปเผยแพร่ ติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต (Shadow IT) ใช้สิทธิ์เกินหน้าที่ในการแก้ไข/ลบข้อมูลสำคัญ ทำให้เกิดผลกระทบเสียหายต่อความถูกต้องของข้อมูล

๓.๕.๑.๑๐. ความเสี่ยงทางกายภาพ เช่นการเข้าถึงและทำลายอุปกรณ์คอมพิวเตอร์ การโขมยสื่อบันทึกข้อมูล

๓.๕.๑.๑๑. มีผู้บุกรุกเข้าในห้องเซิร์ฟเวอร์ เช่น ทำให้อุปกรณ์พกพาที่มีข้อมูลสำคัญหาย ภัยธรรมชาติทำลายอุปกรณ์ด้านเทคโนโลยีสารสนเทศโดยไม่มีแผนสำรอง

๓.๕.๑.๑๒. การตั้งค่าระบบผิดพลาด / ความผิดพลาดของมนุษย์ เช่น ตั้งค่าไฟร์วอลล์ผิดเปิดช่องการโจมตีจากอินเทอร์เน็ต สำรองข้อมูลล้มเหลวใช้งานไม่ได้

๓.๕.๑.๑๓. ภัยคุกคามใหม่และซับซ้อน (Advance Persistent Threat: APT) เช่น การโจมตีที่มุ่งเป้าโดยองค์กรภาครัฐของต่างประเทศหรือองค์กรอาชญากรรม ผู้บุกรุกแฝงตัวอยู่ใน

ระบบเป็นเวลานาน การตกเป็นเป้าหมายของโจมตีระบบที่เกี่ยวข้องกับการผลิต ทำให้เกิดผลกระทบเช่น ข้อมูลเชิงกลยุทธ์ถูกขโมย ระบบถูกทำลาย กระทบต่อความมั่นคงของประเทศ

๓.๕.๒. การวิเคราะห์ความเสี่ยง (Risk Analysis) เพื่อ ระบุระดับความเสี่ยงโดยใช้เกณฑ์การประเมินความเสี่ยงในส่วนของ โอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) และทำการประเมินค่าความเสี่ยง (Risk Evaluation) เทียบกับระดับความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยสารสนเทศและไซเบอร์ที่ยอมรับได้ ที่อ้างอิงตามการประเมินความเสี่ยงขององค์กร

๓.๕.๓. พิจารณาแนวทางการตอบสนองต่อความเสี่ยง (Risk Response) โดยมีแนวทางในการตอบสนองดังนี้

๓.๕.๓.๑. ลดความเสี่ยง (Mitigate) ดำเนินการควบคุมเพื่อลดโอกาสหรือผลกระทบของความเสี่ยง ตัวอย่างเช่น ติดตั้ง Firewall, ใช้ MFA, อัปเดต Patch

๓.๕.๓.๒. โอนความเสี่ยง (Transfer) ถ่ายโอนผลกระทบให้บุคคลภายนอก เช่น ผ่านประกันหรือผู้ให้บริการ ตัวอย่างเช่น ทำประกันไซเบอร์, ทำสัญญา SLA กับ Outsource

๓.๕.๓.๓. ยอมรับความเสี่ยง (Accept) ยอมรับความเสี่ยงโดยไม่ดำเนินการใด ๆ เพราะผลกระทบต่ำหรือค่าใช้จ่ายสูงเกิน ตัวอย่างเช่น ไม่พัฒนาระบบงานเพื่อปิดความเสี่ยงบางประเภทเนื่องจาก ไม่คุ้มค่ากับความเสี่ยงที่ประเมินไว้

๓.๕.๓.๔. หลีกเลี่ยงความเสี่ยง (Avoid) หลีกเลี่ยงกิจกรรมที่มีความเสี่ยงสูงโดยตรง ตัวอย่างเช่น ยกเลิกใช้ระบบที่ไม่ปลอดภัย, ไม่ทำโปรเจกต์ที่เสี่ยง

๓.๕.๔. ดำเนินการจัดการความเสี่ยง (Risk Treatment) โดยการจัดให้มีแนวทางจัดการ ควบคุมและป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

๓.๕.๕. กำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้สอดคล้องกับการประเมินความเสี่ยงขององค์กร โดยให้จัดทำดัชนีชี้วัดความเสี่ยงที่สำคัญในส่วนของความเสี่ยงระดับสูงเป็นอย่างน้อย โดยการจัดทำดัชนีชี้วัดความเสี่ยงที่สำคัญนี้ ควรพิจารณาทั้งในส่วนของ ตัวชี้วัดย้อนหลัง (Lagging Indicator) ที่เป็นตัวชี้วัดที่แสดงให้เห็นว่า "ความเสี่ยงเกิดขึ้นแล้ว" หรือมีผลกระทบเกิดขึ้นแล้ว ช่วยให้วิเคราะห์สาเหตุและวางแผนแก้ไข และ ตัวชี้วัดล่วงหน้า (Leading Indicator) ที่เป็นตัวชี้วัดที่ให้ "สัญญาณเตือนล่วงหน้า" ว่าความเสี่ยงอาจเกิดขึ้นในอนาคต ช่วยให้องค์กรสามารถป้องกันหรือเตรียมรับมือได้ก่อน

๓.๖. คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ดูแลระบบงานที่ได้รับมอบหมาย ต้องมีดำเนินการการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ที่ยอมรับได้ที่กำหนดไว้ โดยให้มีการรวบรวมติดตามผลดำเนินการตามแผนจัดการความเสี่ยง (Risk Treatment) หรือการตอบสนองความเสี่ยง รวมถึงทบทวนการประเมิน

ความเสี่ยงอย่างน้อยปีละ ๑ ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ

๓.๗. คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ดูแลระบบงานจัดทำทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ อันประกอบไปด้วยข้อมูลดังนี้

๓.๗.๑.๑. วันที่ระบุความเสี่ยง (Date the Risk is Identified)

๓.๗.๑.๒. คำอธิบายของความเสี่ยง (Description of the Risk)

๓.๗.๑.๓. โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

๓.๗.๑.๔. ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

๓.๗.๑.๕. ระดับของความเสี่ยง (Level of Risk)

๓.๗.๑.๖. การจัดการความเสี่ยง (Risk Treatment)

๓.๗.๑.๗. เจ้าของความเสี่ยง (Risk Owner)

๓.๗.๑.๘. สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

๓.๗.๑.๙. ความเสี่ยงที่เหลือ (Residual Risk)

๓.๗.๑.๑๐. วันที่ทบทวนความเสี่ยง (Date of Risk is Reviewed) (ถ้ามี)

๓.๗.๑.๑๑. ดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) (ถ้ามี)

๓.๘. คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ดูแลระบบงานต้องรายงานผลการประเมินและติดตามความเสี่ยงต่อคณะกรรมการฯ

๓.๙. คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ต้องทำการทบทวนแนวปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

หมวด ๓
การบริหารโครงสร้างองค์กรและทรัพยากรมนุษย์เพื่อการจัดการ
ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
(Organization and Human Resource Security)

๑. วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้กับผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคลภายนอกที่ปฏิบัติงานให้กับการประปานครหลวง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ จนสามารถนำไปปฏิบัติได้ อย่างถูกต้อง รวมถึงเพื่อควบคุมกระบวนการด้านการบริหารทรัพยากรมนุษย์ให้เป็นไปอย่างมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ คณะกรรมการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๓ ฝ่ายบริหารทรัพยากรบุคคล

๒.๔ ฝ่ายพัฒนาทรัพยากรบุคคล

๒.๕ ฝ่ายกฎหมาย

๒.๖ ผู้ดูแลระบบงาน

๓. แนวปฏิบัติ

๓.๑ คณะทำงานฯ จัดให้มีการกำหนดและทบทวนหน้าที่ปฏิบัติงานที่เกี่ยวข้องกับความปลอดภัยสารสนเทศและไซเบอร์ขององค์กร

๓.๑.๑ หน้าที่ปฏิบัติงานต่าง ๆ จะต้องมีการแบ่งแยกหน้าที่ (Segregation of Duties) เพื่อสร้างให้เกิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เช่น การแบ่งแยกผู้พัฒนาระบบหรือผู้ทดสอบระบบ ออกจากผู้ดูแลระบบ

๓.๑.๒ มีการกำหนดช่องทางการติดต่อหน่วยงานผู้มีอำนาจหน้าที่และกลุ่มผู้เชี่ยวชาญที่กับความปลอดภัยสารสนเทศและไซเบอร์ที่ชัดเจนและเข้าถึงได้โดยง่าย

๓.๑.๓ การทบทวนอำนาจหน้าที่จะต้องเป็นไปอย่างสม่ำเสมอ เป็นประจำทุกปีหรือเมื่อมีโครงการ ใหม่ๆ ซึ่งอาจกระทบต่อความปลอดภัยต่อระบบสารสนเทศอย่างมีนัยสำคัญ

๓.๒ การบรรจุ แต่งตั้งบุคลากรเข้าทำงานเป็นไปตามข้อบังคับการประปานครหลวง ว่าด้วย การบริหารงานบุคคล อันประกอบไปด้วยการกำหนดหลักเกณฑ์การคัดเลือก การสอบคัดเลือก ที่สอดคล้องกับข้อบังคับดังกล่าว มีการกำหนดวินัยและการรักษาวินัย อันรวมถึงการปฏิบัติตามข้อบังคับ ระเบียบหลักเกณฑ์และวิธีการปฏิบัติของการประปานครหลวง และการรักษาความลับของราชการและการประปานครหลวง รวมไปถึงการดำเนินการทางวินัยสำหรับพนักงาน ที่กระทำผิดวินัย

๓.๓ คณะทำงานฯ กำหนดกระบวนการควบคุมบุคลากรเพื่อให้การปฏิบัติหน้าที่เป็นไปอย่างมั่นคงปลอดภัยและเป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๓.๑ จัดให้มีการสื่อสารแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์หรือทำคู่มือการใช้งานระบบสารสนเทศอย่างมั่นคงปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของการประปานครหลวง/หน่วยงาน ในระบบ Intranet หรือช่องทางอื่นของการประปานครหลวง ให้กับ ผู้บริหารและพนักงาน

๓.๓.๒ ทำการวางแผนการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ อันประกอบไปด้วยการพัฒนาทักษะการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ให้กับ ผู้ปฏิบัติงาน ผู้ดูแลระบบ ที่เกี่ยวข้อง

๓.๔ การสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๔.๑ คณะทำงานฯ ทำการวางแผนในการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ให้กับผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคลภายนอกที่ปฏิบัติงานให้กับการประปานครหลวง โดยพิจารณาแนวทางการสร้างความตระหนักจากการประเมินความเสี่ยง แนวโน้มความเสี่ยงและภัยคุกคาม หรือเหตุการณ์ด้านความปลอดภัยสารสนเทศและไซเบอร์ที่เคยเกิดขึ้นหรือมีแนวโน้มจะเกิดขึ้น โดยแผนการสร้างความตระหนักควรจัดทำปีละ ๑ ครั้ง ทั้งนี้ให้ฝ่ายพัฒนาทรัพยากรบุคคลทำหน้าที่ให้ความเห็นหรือให้คำปรึกษาในลักษณะและรูปแบบการจัดกิจกรรมเกี่ยวกับ โดยต้องประกอบไปด้วย เนื้อหาดังนี้

๓.๔.๑.๑ วัตถุประสงค์ของการสร้างความตระหนัก เช่น ลดความเสี่ยงจากพฤติกรรมของพนักงาน สร้างวัฒนธรรมความมั่นคงปลอดภัยในองค์กร รองรับการดำเนินการตามกฎหมายหรือข้อกำหนด หรือย้ำเตือนเรื่องการปฏิบัติตามนโยบายและแนวปฏิบัติ

๓.๔.๑.๒ กำหนดกลุ่มเป้าหมายการสร้างความตระหนักในแต่ละกิจกรรม เช่น พนักงานทั่วไป ผู้บริหาร ผู้ดูแลระบบ พนักงานใหม่ หรือผู้ให้บริการภายนอก

๓.๔.๑.๓ หัวข้อหลักที่ควรในการสร้างความตระหนัก เช่น การป้องกัน Email Phishing การตั้งรหัสผ่านที่ปลอดภัย การจัดการข้อมูลส่วนบุคคล การทำงานจากระยะไกลอย่างปลอดภัย การรายงานเหตุการณ์ผิดปกติ ความเสี่ยงจากบุคคลภายใน เป็นต้น

๓.๔.๑.๔ วิธีการอบรมสร้างความตระหนัก โดยพิจารณาตามความเหมาะสมของกลุ่มเป้าหมาย และหัวข้อเป็นหลัก โดยวิธีการฝึกอบรมอาจพิจารณาจัดทำได้ในรูปแบบ ดังนี้ วิดีโอ e-Learning จำลอง Phishing อีเมลข่าวสาร แผ่นภาพ แบบทดสอบ กิจกรรมตอบคำถาม สัมมนาออนไลน์ เป็นต้น

๓.๔.๑.๕ ในการสร้างความตระหนักและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ต้องอ้างอิงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง

๓.๔.๑.๖ กำหนดปฏิทินแผนการสร้างความตระหนักในแต่ละเดือนหรือแต่ละไตรมาสอย่างต่อเนื่อง

๓.๔.๑.๗ กำหนดการวัดผลหรือตัวชี้วัดผลการสร้างความตระหนัก เช่น ร้อยละของพนักงานผ่านการอบรมหรือการทดสอบ อัตราการตกเป็นเหยื่อของ Email Phishing

๓.๔.๒ คณะทำงานฯ เป็นผู้รับผิดชอบในการจัดให้มีกิจกรรมสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ตามแผนการสร้างความตระหนัก ทำการวัดผลการสร้างความตระหนัก

๓.๔.๓ คณะทำงานฯ รายงานผลต่อกรรมการฯ และผู้บริหารหน่วยงานที่เกี่ยวข้อง

๓.๕ คณะทำงานฯ ต้องมั่นใจว่าหลังจากมีการเลิกจ้างบุคลากรหรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบของผู้บริหาร ผู้ปฏิบัติงาน ได้จัดถูกจัดให้มีขั้นตอนปฏิบัติงานดังนี้

๓.๕.๑ เมื่อเกิดการสิ้นสภาพหรือการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของผู้บริหาร ผู้ปฏิบัติงาน ฝ่ายบริหารทรัพยากรบุคคลจะต้องสื่อสารให้แก่สายงานเทคโนโลยีดิจิทัลหรือผู้ดูแลระบบทราบโดยทันที

๓.๕.๒ สายงานเทคโนโลยีดิจิทัลหรือผู้ดูแลระบบงานจะต้องดำเนินการยกเลิกหรือระงับการใช้งานชื่อผู้ใช้ของบุคลากรที่พ้นสภาพหรือเปลี่ยนแปลงหน้าที่ ที่ไม่จำเป็นต้องเข้าถึงระบบงานแล้วออกจากระบบสารสนเทศทุกระบบที่เกี่ยวข้อง

๓.๕.๓ การคืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานระบบสารสนเทศที่เป็นของการประปานครหลวงเช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่การประปานครหลวง ณ วันที่พ้นสภาพพนักงาน

๓.๖ ข้อปฏิบัติของผู้ดูแลระบบงาน

๓.๖.๑ หากผู้ดูแลระบบงานพบว่าผู้ปฏิบัติงานผู้ใดมีพฤติการณ์ส่อไปในทางที่จะละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ผู้ดูแลระบบงานจะต้องรายงานให้คณะกรรมการฯ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่การประปานครหลวง ผู้ดูแลระบบงานมีอำนาจในการระงับการใช้งานระบบสารสนเทศของผู้ปฏิบัติงานดังกล่าวได้ทันที

๓.๖.๒ ผู้ดูแลระบบงานจะต้องตรวจสอบข้อมูลของเจ้าหน้าที่จากภายนอกที่เข้ามาให้คำปรึกษาหรือปฏิบัติงานภายในพื้นที่ควบคุมความปลอดภัย ถ้าหากเจ้าหน้าที่ผู้นั้นต้องการใช้สิทธิของผู้ดูแลระบบในการทำงานกับระบบ ผู้ดูแลระบบงานจะต้องทำการเข้าสู่ระบบให้ด้วยตนเอง หรือติดตามการดำเนินงานอย่างใกล้ชิด

๓.๖.๓ ผู้ดูแลระบบงานจะต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับ หรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่

เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลระบบงานและระบบเครือข่ายคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวเป็นข้อมูล ที่ไม่ควรเปิดเผยให้ผู้หนึ่งผู้ใดทราบ

๓.๖.๔ ผู้ดูแลระบบงานจะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของการประปานครหลวง เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่ผู้บังคับบัญชาในทันทีที่พ้นหน้าที่ และให้คณะกรรมการฯ ดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลระบบงานที่พ้นจากหน้าที่โดยละเอียด

๓.๖.๕ ผู้ดูแลระบบงานที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่ การประปานครหลวงหรือผู้หนึ่งผู้ใด การประปานครหลวงจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลระบบงานนั้น

หมวด ๔
การจัดการทรัพย์สินสารสนเทศ
(Asset Management)

๑. วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรฐานในการจัดทำและบำรุงรักษารายการบัญชีทรัพย์สินสารสนเทศที่เพื่อสนับสนุนการบริหารความเสี่ยงอย่างมีประสิทธิภาพ ให้มั่นใจว่าทรัพย์สินสารสนเทศได้รับการคุ้มครองอย่างเหมาะสมตลอดวงจรชีวิต และสามารถจัดลำดับความสำคัญของการควบคุมด้านความมั่นคงปลอดภัย สารสนเทศและไซเบอร์ได้ตามความสำคัญ

๒. ผู้ที่เกี่ยวข้อง

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๒ ผู้ดูแลระบบงาน

๒.๓ เจ้าของระบบงาน

๓. แนวปฏิบัติ

๓.๑ ผู้ดูแลระบบงานต้องร่วมกับเจ้าของระบบงานจัดทำทะเบียนทรัพย์สินสารสนเทศของระบบงานของหน่วยงาน โดยเจ้าของระบบงานเป็นผู้จัดลำดับความสำคัญของข้อมูลในระบบงานเพื่อระบุระดับความสำคัญของทรัพย์สินสารสนเทศ รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศ ในทะเบียนทรัพย์สิน

๓.๑.๑ ทะเบียนทรัพย์สินด้านสารสนเทศโดยต้องประกอบไปด้วยข้อมูลดังต่อไปนี้

๓.๑.๑.๑ ชื่อและคำอธิบายทรัพย์สิน

๓.๑.๑.๒ ประเภทของทรัพย์สิน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ด้านความมั่นคงปลอดภัย อุปกรณ์สื่อบันทึกข้อมูล

๓.๑.๑.๓ หน้าที่การทำงานของทรัพย์สิน

๓.๑.๑.๔ การระบุและจัดลำดับความสำคัญของทรัพย์สิน โดยให้กำหนดตามลักษณะของข้อมูลสารสนเทศที่มีการประมวลผล จัดเก็บ ส่งผ่าน ทรัพย์สินนั้น ๆ ซึ่งต้องทำการประเมินตามแนวปฏิบัติด้านความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Data Security)

๓.๑.๑.๕ เจ้าของระบบงาน

๓.๑.๑.๖ ผู้ดูแลระบบงาน

๓.๑.๑.๗ ตำแหน่งทางกายภาพ

๓.๑.๑.๘ การขึ้นต่อกันของทรัพย์สินอื่น ๆ หรือ ความสัมพันธ์ในการพึ่งพาระหว่างทรัพย์สิน เพื่อให้สามารถทำงานได้ตามหน้าที่ เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต้องเชื่อมต่อกับอุปกรณ์ระบบเครือข่าย ทั้งนี้อาจพิจารณาอ้างอิงถึงเอกสาร แผนภาพเครือข่าย (Network Diagram) หรือแผนภาพระบบงาน (System Diagram)

๓.๑.๒ ทะเบียนทรัพย์สินด้านสารสนเทศ และปรับปรุงแก้ไขข้อมูลให้มีความถูกต้องอยู่เสมอ

๓.๑.๓ ทรัพย์สินสนเทศที่ถูกติดตั้งใช้งานอยู่ต้องสามารถระบุชื่อ หรือแนวทางอื่นใดที่สามารถระบุตัวทรัพย์สินตามทะเบียนได้

๓.๑.๔ คณะทำงานฯ ต้องจัดให้มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินต้องมีการปรับปรุงทะเบียนทรัพย์สินให้ถูกต้อง

๓.๑.๕ ในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ จะต้องทำการประเมินความเสี่ยงทรัพย์สินที่อยู่ในรายการทะเบียนทรัพย์สิน ให้ครบถ้วน

๓.๒ การบำรุงรักษา แทนที่ และยกเลิกการใช้งานทรัพย์สิน

๓.๒.๑ เจ้าของหรือผู้ดูแลทรัพย์สิน ต้องทำการบำรุงรักษาทรัพย์สินสารสนเทศที่อยู่ภายใต้การดูแลของตนเองดังนี้

๓.๒.๑.๑ ตรวจสอบความเสียหายทางกายภาพ ดูแลรักษาความสะอาดของทรัพย์สิน

๓.๒.๑.๒ ปรับปรุงซอฟแวร์ เฟิร์มแวร์และแพตช์ (Patch) อย่างทันการณ์ตามข้อมูลจากผู้ผลิต ผู้ขาย

๓.๒.๑.๓ ติดตามข้อมูลการสิ้นสุดการสนับสนุนจากผู้ผลิต (End Of Support) เพื่อวางแผนการเปลี่ยนทรัพย์สินสารสนเทศให้เป็นรุ่นใหม่ หรือประเมินความเสี่ยงเพื่อกำหนดการควบคุมทดแทน

๓.๒.๑.๔ เจ้าของหรือผู้ดูแลทรัพย์สิน อาจพิจารณาใช้บริการบำรุงรักษาทรัพย์สิน จากผู้ให้บริการภายนอกโดยต้องกำหนดหน้าที่ความรับผิดชอบการบำรุงรักษาทรัพย์สินให้ครบถ้วนและต้องดำเนินการตามแนวปฏิบัติด้านการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

๓.๒.๒ การยกเลิก/ทดแทน ทรัพย์สิน เจ้าของหรือผู้ดูแลทรัพย์สินต้องมีการดำเนินการลบทำลายข้อมูลตามแนวปฏิบัติด้านความมั่นคงปลอดภัยข้อมูลสารสนเทศและไซเบอร์ (Data Security) ก่อนทำการเลิกใช้

หมวด ๕
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่รับผิดชอบของผู้ใช้งานในป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรโดยไม่รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลอบทำสำเนาข้อมูลสารสนเทศ รวมถึงการสูญหายของข้อมูลและทรัพย์สินสารสนเทศ

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ ผู้ใช่งานต่องยินยอมใช่งานทรัพย์สินสารสนเทศอย่างปลอดภัย โดยใช่งานทรัพย์สินสารสนเทศตามวัตถุประสงค์สำหรับการใช่งานทางธุรกิจของการประปานครหลวงเทานั้น ห้ามมิให่ผู้ใช่งานนำทรัพยสิน และระบบสารสนเทศต่างๆ ไปใช่นอกกิจการที่การประปานครหลวงกำหนดหรือ ใช้นำไปใช้งานที่กอให่เกิดความเสียหายตอการประปานครหลวง หากมีการฝ่าฝืนข้อกำหนดหรืออาจก่อให้เกิดความเสียหายแก่การ ประปานครหลวงหรือผู้หนึ่งผู้ใด การประปานครหลวงจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ปฏิบัติงานที่ฝ่าฝืน

๓.๒ ผู้ใช้งานพึงใช้ทรัพยากรระบบสารสนเทศอย่างมีประสิทธิภาพ

๓.๓ ผู้ใช้งานพึงใช้ข้อความสุภาพและถูกต้องตามธรรมเนียมปฏิบัติในการใช้ระบบสารสนเทศ

๓.๔ ผู้ใช้งานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้ระบบสารสนเทศ โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้ระบบสารสนเทศจากบัญชีผู้ใช้ของตนเอง

๓.๕ ผู้ใช้งานจะต้องไม่ใช้ระบบสารสนเทศ โดยมีวัตถุประสงค์ดังต่อไปนี้

๓.๕.๑ เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๓.๕.๒ เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๓.๕.๓ เพื่อการพาณิชย์

๓.๕.๔ เพื่อการเปิดเผยข้อมูลที่เป็นความลับ ซึ่งได้มาจากการปฏิบัติงานให้แก่การประปานครหลวง

๓.๕.๕ เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของการประปานครหลวงหรือของบุคคลอื่น

๓.๕.๖ เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

๓.๕.๗ เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่การประปานครหลวง

๓.๕.๘ เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของการประปานครหลวงหรือของผู้ใช้งานอื่นของการประปานครหลวง หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของการประปานครหลวงไม่สามารถใช้งานได้ตามปกติ

๓.๕.๙ เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของการประปานครหลวง ไปยังที่อยู่เว็บไซต์ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

๓.๕.๑๐ เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของการประปานครหลวง หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่การประปานครหลวง

๓.๖ ผู้ใช้งานจะต้องระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์

๓.๗ ผู้ใช้งานต้องไม่กระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศ

๓.๘ ผู้ใช้งานต้องไม่กระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศต้องหยุดชะงักจนเป็นเหตุให้การประปานครหลวงเสียหาย

๓.๙ ผู้ใชงานมีสวนร่วมในการดูแลรักษา และรับผิดชอบต่อข่อมูลขององคกร หากเกิดการสูญหาย หรือมีการนำไปใชในทางที่ผิด เช่น การเผยแพรโดยไม่ได้รับอนุญาต ฯลฯ ผู้ใช่งานจะต่อง มีสวนร่วมในการรับผิดชอบต่อความเสียหายนั้น

๓.๑๐ ผู้ใช้งานห้ามเข้าไปในสถานที่ตั้งของระบบสารสนเทศก่อนได้รับอนุญาต

๓.๑๑ ต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบสารสนเทศหรือคณะกรรมการ ด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO๒๗๐๐๑ ในการตรวจสอบระบบความปลอดภัยของระบบข้อมูลและสารสนเทศ รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแลระบบสารสนเทศ หรือคณะทำงาน ฯ

๓.๑๒ การใช้งานรหัสผ่าน (Password Use)

๓.๑๒.๑ ผู้ดูแลต้องกำหนดให้มีการระบุรหัสผ่าน มีความยาวตัวอักษรหรือตัวเลข ไม่น้อยกว่า ๘ ตัวอักษร และเพื่อให้รหัสผ่าน มีความปลอดภัยมากที่สุด รหัสผ่านประกอบด้วย ตัวอักษรตัวเล็กตัวใหญ่ ตัวเลขและอักขระพิเศษ คละรวมกัน

๓.๑๒.๒ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตัวเองใหม่ทุกๆ ๙๐ วัน หรือตามระยะเวลาที่ผู้ดูแลระบบกำหนด หรือมีการใช้การยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication) ในระบบนั้น ๆ

๓.๑๒.๓ ผู้ดูแลระบบต้องกำหนดการเปลี่ยนแปลงรหัสผ่านใหม่ในแต่ละครั้ง จะต้องไม่นำรหัสผ่านที่หมดอายุแล้วมาใช้ซ้ำอีกในครั้งถัดไป

๓.๑๒.๔ ผู้ใช้งานต้องใช้รหัสผ่าน สำหรับแสดงตัวตนทุกครั้งในการเข้าไปปฏิบัติงานในระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตเข้าไปในระบบ ซึ่งอาจเข้าไปใช้งานในทางที่มิชอบหรือทำการลบ ยักย้าย ถ่ายโอน เปลี่ยนแปลง ทำลายระบบสารสนเทศ อันจะเกิดความเสียหายในการดำเนิน ธุรกิจของการประปานครหลวง

๓.๑๒.๕ ผู้ใช้งานจะต้องล็อคหน้าจอทุกครั้งเมื่อไม่ได้ปฏิบัติงานอยู่ที่เครื่องคอมพิวเตอร์และพิสูจน์ตัวตนก่อนใช้งานทุกครั้ง

๓.๑๒.๖ ผู้ใช้งานต้องรับผิดชอบในการเลือก หรือเปลี่ยนแปลงรหัสผ่านที่เหมาะสมและปลอดภัย รวมทั้งปกปิดและรักษารหัสผ่านของตนอย่างดีที่สุดโดย

๓.๑๒.๖.๑ หลีกเลี่ยงการใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน ได้แก่ ชื่อ-สกุล ชื่อสถานที่ปฏิบัติงาน นามแฝง เบอร์โทรศัพท์ ทะเบียนยานพาหนะ หรือข้อมูลอื่นๆ ที่ง่ายต่อการคาดเดา

๓.๑๒.๖.๒ ห้ามจดบันทึกรหัสผ่านในที่ที่สามารถพบเห็นได้โดยง่าย

๓.๑๒.๖.๓ ห้ามเปิดเผยรหัสผ่านให้บุคคลอื่นรับรู้ หากรหัสผ่านถูกเปิดเผยต้องเปลี่ยนใหม่โดยเร็ว

๓.๑๒.๖.๔ ห้ามนำหรือเปิดเผยรหัสผ่านให้แก่บุคคลอื่นที่ไม่ได้รับอนุญาตหรือที่มิได้เกี่ยวข้องแสดงตนเข้าไปใช้ระบบเทคโนโลยีสารสนเทศและระบบข้อมูล หากตรวจสอบพบว่ามีการเปิดเผยหรือนำรหัสผ่านให้แก่บุคคลอื่นที่ไม่ได้รับอนุญาต กระทำการที่ก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการรักษา ความมั่นคงปลอดภัยระบบข้อมูล ผู้ปฏิบัติงานที่ได้รับอนุญาตและได้รับสิทธิให้ใช้ระบบงานนั้นจะต้องรับผิดชอบ ต่อความเสียหายที่เกิดขึ้น

๓.๑๒.๖.๕ หากพบเห็นหรือสงสัยถึงการล่วงละเมิดต่อความปลอดภัยในการใช้งานหรือประเด็นอื่นใดที่เกิดขึ้น เนื่องจากรหัสผ่านถูกนำไปใช้โดยผู้ที่ไม่ใช่เจ้าของจะต้องรายงานการใช้ต่อผู้บังคับบัญชาหรือหน่วยงานที่ดูแลระบบสารสนเทศหรือผู้ดูแลระบบงานทันที เพื่อทำการตรวจสอบและแก้ไขต่อไป

๓.๑๒.๗ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

๓.๑๒.๗.๑ ผู้ดูแลให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ตามระยะเวลาที่กำหนดไว้เมื่อเสร็จสิ้นการทำงาน ทั้งในระบบงาน อุปกรณ์ เครื่องคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์พกพา

๓.๑๒.๗.๒ ผู้ใช้งานล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ดูแลชั่วคราว

๓.๑๒.๗.๓ ผู้ดูแลต้องกำหนดให้มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และหากผู้ใช้งานป้อนรหัสผ่านผิดเกิน ๓ ครั้ง ระบบจะทำการล็อคสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบได้อีก จนกว่าผู้ดูแลจะดำเนินการ ปลดล็อคให้

๓.๑๒.๗.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้ (User Account) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

๓.๑๒.๘ การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen) โดย

๓.๑๒.๘.๑ ผู้ดูแลต้องกำหนดให้มีการพิสูจน์ตัวตนที่เหมาะสม ในการเข้าใช้เครื่องคอมพิวเตอร์และระบบงานขององค์กร

๓.๑๒.๘.๒ ผู้ใช้งานต้องป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศให้อยู่ในสถานที่ที่ไม่เหมาะสม โดยตระหนักป้องกันทรัพย์สินขององค์กร

๓.๑๒.๘.๓ จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับ หรือสื่อบันทึกข้อมูลไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ

๓.๑๒.๘.๔ ผู้ใช้งานออกจากระบบทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน

๓.๑๒.๘.๕ ผู้ดูแล/ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้ทรัพย์สินขององค์กรโดยไม่ได้รับอนุญาต

๓.๑๒.๙ ผู้ใช้สามารถนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๕๔ มีแนวปฏิบัติ ดังนี้

๓.๑๒.๙.๑ การประเมินความเสียงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับ ข้อมูลที่จำเป็นต้องป้องกัน

๓.๑๒.๙.๒ ระบุหลักเกณฑ์ทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล

๓.๑๒.๙.๓ การจัดเก็บรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของระบบสารสนเทศลง ในฐานข้อมูลใดๆ จะต้องทำการเข้ารหัสด้วย MD5 ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

๓.๑๒.๙.๔ มีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล Https สำหรับระบบสารสนเทศแบบ Web Application ที่สำคัญ เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราวเซอร์และเว็บเซิร์ฟเวอร์

๓.๑๒.๙.๕ ระบุช่องทางการรับ-ส่งข้อมูลสำคัญ หรือข้อมูลลับที่เหมาะสมกับองค์กร สำหรับช่องทาง ดังต่อไปนี้

- ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และ Internet
- สามารถใช้สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ จากตัวเครื่องคอมพิวเตอร์ เฉพาะที่ได้รับอนุญาตเท่านั้น

๓.๑๒.๙.๖ ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับ หรือวิธีการรักษาความลับของข้อมูล ดังนี้

- แสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
- ป้องกันไฟล์ข้อมูลความลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่องค์กรกำหนด
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการระบุรหัสผ่านสำหรับไฟล์ที่มีการใช้งาน

๓.๑๒.๙.๗ ผู้ใช้งานห้าม share ไฟล์ข้อมูลลับบนเครือข่ายขององค์กรเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

๓.๑๒.๙.๘ ผู้ใช้งานตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล

๓.๑๒.๙.๙ ผู้ใช้งานตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ (Patch) ในเครื่องตามปกติหรือไม่

๓.๑๒.๙.๑๐ ผู้ใช้งานดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานสม่ำเสมอหรือตามความจำเป็น

๓.๑๓ วิธีปฏิบัติในการป้องกันไวรัสคอมพิวเตอร์

๓.๑๓.๑ ห้ามปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ทุกเครื่อง

๓.๑๓.๒ ห้ามแก้ไขเปลี่ยนแปลงรหัสหมายเลขไอพีประจำเครื่องคอมพิวเตอร์

๓.๑๓.๓ ห้ามนำอุปกรณ์เครือข่ายส่วนตัวมาติดตั้งใช้งานกับเครื่องคอมพิวเตอร์ หากมีความจำเป็นต้องใช้งานต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานระดับผู้อำนวยการฝ่ายขึ้นไป และให้ติดตั้งเฉพาะกับเครื่องที่อยู่นอกระบบเครือข่ายเท่านั้น

๓.๑๓.๔ ห้ามนำโปรแกรมหรือข้อมูลต่าง ๆ ที่ไม่เกี่ยวข้องกับการปฏิบัติงานมาติดตั้ง สำหรับซอฟต์แวร์หรือข้อมูลที่จำเป็นต่อการใช้งาน ก่อนติดตั้งให้ตรวจสอบไวรัสด้วยโปรแกรมป้องกันไวรัสที่ติดตั้งในเครื่องก่อน

๓.๑๓.๕ เมื่อพบว่าไม่สามารถกำจัดไวรัสคอมพิวเตอร์ในเครื่องคอมพิวเตอร์ที่ติดตั้งอยู่ในระบบให้แจ้งฝ่ายเทคโนโลยีและสื่อสารโดยด่วน

๓.๑๓.๖ ตรวจสอบข้อมูลที่ได้รับจากภายนอกองค์กรทุกครั้งด้วยโปรแกรมป้องกันไวรัสสำหรับตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ที่การประปานครหลวงจัดให้ และหากตรวจพบไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใด จะต้องรีบทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด

หมวด ๖
การใช้งานอุปกรณ์พกพา
(Use of Personal Computer and Mobile)

๑. วัตถุประสงค์

มาตรฐานการใช้งานอุปกรณ์พกพานี้จัดทำขึ้นเพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานอุปกรณ์พกพาทั้งที่องค์กรจัดเตรียมให้และอุปกรณ์พกพาส่วนบุคคล เพื่อปกป้องข้อมูลขององค์กรในด้านความลับ และรักษาความถูกต้อง เพื่อให้ทรัพยากรมีความพร้อมใช้งานอยู่

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ แนวปฏิบัติทั่วไปในการใช้งานอุปกรณ์พกพาส่วนบุคคล

๓.๑.๑ ผู้ใช้งานที่นำอุปกรณ์พกพามาใช้เพื่อการทำงานภายในองค์กรต้องพิสูจน์ตัวตนด้วยรหัสผู้ใช้งานและรหัสผ่าน เพื่อเข้าใช้งานระบบเครือข่ายไร้สายขององค์กร

๓.๑.๒ ผู้ใช้งานต้องไม่เก็บข้อมูลสำคัญขององค์กรไว้บนอุปกรณ์พกพาส่วนบุคคลและสื่อบันทึกข้อมูลพกพาต่าง ๆ

๓.๑.๓ คณะทำงานฯ ต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์พกพาในที่สาธารณะ ห้องประชุมนอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอกองค์กร

๓.๒ แนวปฏิบัติทั่วไปในการใช้งานอุปกรณ์พกพาที่องค์กรจัดเตรียมให้

๓.๒.๑ โปรแกรมที่ถูกติดตั้งลงบนอุปกรณ์พกพาต้องเป็นโปรแกรมลิขสิทธิ์ถูกต้องตามกฎหมายที่องค์กรจัดหา ดังนั้นห้ามไม่ให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในอุปกรณ์พกพาขององค์กร

๓.๒.๒ ผู้ใช้งานพึงระวังการวางอุปกรณ์พกพาเพื่อป้องกันการสูญหายของอุปกรณ์

๓.๒.๓ อุปกรณ์พกพาประเภทคอมพิวเตอร์แล็ปท็อป จะต้องมีการเข้าร่วมระบบ Active Directory ที่ศูนย์กลางขององค์กร

๓.๓ แนวปฏิบัติการป้องกันโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๓.๓.๑ ผู้ใช้งานทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) และลดความเสี่ยงจากการถูกโจมตี และภัยคุกคามต่างๆ

๓.๓.๒ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนอุปกรณ์พกพาที่องค์กรจัดเตรียมให้

๓.๓.๓ หากผู้ใช้งานพบหรือสงสัยว่าอุปกรณ์พกพาติดโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware) ผู้ใช้งาน ต้องหยุดการเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายขององค์กร เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

๓.๔ แนวปฏิบัติการทั่วไปในการใช้งานอุปกรณ์คอมพิวเตอร์

๓.๔.๑ ผู้ใช้งานระบบสารสนเทศของการประปานครหลวงมีหน้าที่รักษาข้อมูลในระบบสารสนเทศขององค์กรไม่ให้เผยแพร่ หากจำเป็นต้องนำอุปกรณ์คอมพิวเตอร์ซึ่งมีข้อมูลของการประปานครหลวงออกไปภายนอก ต้องจัดหาวิธีป้องกันไม่ให้ข้อมูลเผยแพร่ไปยังภายนอกการประปานครหลวง

๓.๔.๑.๑ การนำเครื่องคอมพิวเตอร์ประจำสำนักงานออกไปซ่อมนอกผู้ใช้งานต้องระมัดระวังข้อมูลที่สำคัญที่เก็บภายในตัวเครื่องไม่ให้ทำสำเนาจากบุคคลภายนอก

๓.๔.๑.๒ เครื่องคอมพิวเตอร์ที่ยกเลิกการใช้งาน ก่อนจะจำหน่าย หน่วยงานเจ้าของเครื่องหรือผู้ใช้งานจะต้องต้องดำเนินการล้างข้อมูลออกทั้งหมดก่อน

หมวด ๗
ความมั่นคงปลอดภัยข้อมูลสารสนเทศ
(Data Security)

๑. วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Data Security) ของข้อมูล เพื่อทำให้สามารถรักษาความมั่นคงปลอดภัยสำหรับข้อมูล โดยการกำหนดการควบคุม ในการจัดเก็บ การส่งข้อมูลผ่านระบบเครือข่าย การใช้งานและการเข้าถึงข้อมูลสารสนเทศไปจนถึงการทำลายข้อมูล เพื่อลดความเสี่ยงที่อาจเกิดขึ้น

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ เจ้าของระบบงาน

๒.๓ เจ้าของข้อมูล

๒.๔ ผู้ดูแลระบบงาน

๒.๕ ผู้ดูแลระบบเครือข่าย

๓. แนวปฏิบัติ

๓.๑ เจ้าของข้อมูลทำการประเมินและจัดลำดับชั้นของข้อมูลสารสนเทศ ในด้าน การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพความพร้อมใช้ (Availability) โดยมีแนวทางดังนี้

๓.๑.๑ การจัดลำดับชั้นของข้อมูลสารสนเทศในด้านการรักษาความลับของข้อมูล (Confidentiality) ให้เป็นไปตามนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) และแนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล ของการประปานครหลวง โดยมีการกำหนดระดับชั้นความลับของข้อมูล ไว้ดังนี้

๓.๑.๑.๑ ระดับที่ ๑ ข้อมูลเปิดเผย (Open) หมายถึง หมายถึง ข้อมูลที่ได้รับการเปิดเผยต่อสาธารณะชน ดังนั้นจึงไม่มีข้อจำกัดในการนำมาใช้ประโยชน์และไม่มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงาน

๓.๑.๑.๒ ระดับที่ ๒ เผยแพร่ภายในองค์กร(Private) หมายถึง ข้อมูลที่ไม่ใช่ประเภทลับ ลับมาก หรือ ลับที่สุด และเป็นข้อมูลเพื่อการใช้งานภายในองค์กรเท่านั้น การเปิดเผยหรือการเข้าถึงข้อมูลในระดับชั้นนี้สามารถเข้าถึงได้โดยบุคคลภายในองค์กรได้แก่ กรรมการ ผู้บริหาร บุคลากร และตัวแทนขององค์กรเท่านั้น ตามหน้าที่ที่ได้รับมอบหมายและสิทธิในการเข้าถึง

๓.๑.๑.๓ ระดับที่ ๓ ข้อมูลลับ (Confidential) หมายถึง ข้อมูลมีความสำคัญต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมการเข้าถึงข้อมูล

เฉพาะผู้มีอำนาจตามที่กำหนดในการเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงาน และห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยคณะกรรมการที่เกี่ยวข้อง หรือหน่วยงานที่เป็นเจ้าของข้อมูลขึ้นไป โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

๓.๑.๑.๔ ระดับที่ ๔ ข้อมูลลับมาก (Secret) หมายถึง ข้อมูลมีความสำคัญต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมอย่างเข้มงวดโดยจำกัดการเข้าถึงข้อมูลเฉพาะผู้มีอำนาจตามที่กำหนดในการเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงาน ซึ่งอาจเป็นกลุ่มคนในหน่วยงานที่เกี่ยวข้องเท่านั้น เพื่อป้องกันการรั่วไหลไปสู่บุคคลที่ไม่เกี่ยวข้อง

๓.๑.๑.๕ ระดับที่ ๕ ข้อมูลลับที่สุด (Top Secret) หมายถึง ข้อมูลมีความสำคัญสูงต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมอย่างเข้มงวดที่สุดโดยต้องจำกัดผู้มีอำนาจในการเข้าถึงข้อมูลให้น้อยที่สุดในระดับบุคคลและตำแหน่งงานเท่านั้น เพื่อป้องกันการรั่วไหลไปสู่บุคคลภายนอก และ/หรือบุคคลที่ไม่เกี่ยวข้อง

๓.๑.๒ การรักษาความถูกต้องครบถ้วน (Integrity) ของข้อมูลนั้นจะประกอบไปด้วยการกำหนดระดับชั้นของข้อมูลสารสนเทศ ในด้านการรักษาความถูกต้องครบถ้วน (Integrity) และแนวทางการประเมินจัดลำดับชั้น

๓.๑.๒.๑ การจัดลำดับชั้นของข้อมูลสารสนเทศในด้านการรักษาความถูกต้องครบถ้วน (Integrity) จะมีการจัดระดับชั้น ๕ ระดับดังนี้

๓.๑.๒.๑.๑ ระดับ ๑ (Minimal) ข้อมูลสามารถผิดพลาดได้โดยไม่ก่อให้เกิดผลกระทบ เช่น ข้อมูลทดสอบหรือข้อมูลที่ไม่มีการใช้งานในเชิงธุรกิจจริงระดับความต้องการต่ำ

๓.๑.๒.๑.๒ ระดับ ๒ (Low) ข้อมูลในระดับนี้ไม่ได้มีความจำเป็นต้องถูกต้องมาก ความผิดพลาดเล็กน้อยสามารถยอมรับได้ โดยไม่ส่งผลกระทบต่อประสิทธิภาพงานหรือธุรกิจ

๓.๑.๒.๑.๓ ระดับ ๓ (Moderate) ข้อมูลควรมีความถูกต้องในระดับที่เหมาะสม สามารถยอมรับความคลาดเคลื่อนเพียงเล็กน้อยได้ โดยไม่ส่งผลกระทบโดยตรงต่อการดำเนินงานหลัก

๓.๑.๒.๑.๔ ระดับ ๔ (High) ข้อมูลต้องมีความถูกต้องสูง โดยอาจยอมให้มีการตรวจสอบหรือแก้ไขผ่านระบบควบคุมภายในได้บ้าง ความผิดพลาดอาจมีผลกระทบต่อการปฏิบัติตามข้อกำหนดหรือการตัดสินใจเชิงธุรกิจสำคัญ

๓.๑.๒.๑.๕ ระดับ ๕ (Critical) ข้อมูลต้องมีความถูกต้องสมบูรณ์ 100% ห้ามมีความผิดพลาดหรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตโดยเด็ดขาด เพราะอาจก่อให้เกิดผลกระทบร้ายแรงทางกฎหมาย ความปลอดภัย หรือการดำเนินธุรกิจ

๓.๑.๒.๒ สำหรับการประเมินลักษณะของข้อมูลเพื่อกำหนดระดับชั้นของการรักษาความถูกต้องครบถ้วน (Integrity) ของข้อมูลมีแนวทางการประเมินในด้านต่าง ๆ ตามเกณฑ์

ด้านล่างนี้ ทั้งนี้ให้ ถือเอาระดับชั้นสูงสุด จากการประเมินในแต่ละด้านเป็นตัวกำหนดระดับชั้น

ด้าน	ระดับชั้นของการรักษาความถูกต้องครบถ้วน (Integrity)	ลักษณะของผลกระทบเมื่อสูญเสียความถูกต้องครบถ้วน (Integrity)
ด้านธุรกิจและการดำเนินงาน	ระดับ ๑ (Minimal)	มีผลกระทบต่อกระบวนการดำเนินงานทำให้การดำเนินงานหยุดชะงักไม่เกิน 6 ชม
	ระดับ ๒ (Low)	มีผลกระทบต่อกระบวนการดำเนินงาน ทำให้ การดำเนินงานหยุดชะงักมากกว่า 6 ชม. แต่ไม่เกิน 12 ชม.
	ระดับ ๓ Moderate)	มีผลกระทบต่อกระบวนการดำเนินงานทำให้การดำเนินงานหยุดชะงักมากกว่า 12 ชม. แต่ไม่เกิน 24 ชม.
	ระดับ ๔ (High)	มีผลกระทบต่อกระบวน การดำเนินงานทำให้การดำเนินงานหยุดชะงักมากกว่า 24 ชม. แต่ไม่เกิน 48 ชม.
	ระดับ ๕ (Critical)	มีผลกระทบต่อกระบวนการดำเนินงานทำให้การดำเนินงานหยุดชะงักมากกว่า48 ชม.
ด้านการเงิน	ระดับ ๑ (Minimal)	สูญเสียหรือมีโอกาสสูญเสียทางการเงินน้อยกว่า / เท่ากับ 5 ล้านบาท
	ระดับ ๒ (Low)	สูญเสียหรือมีโอกาสสูญเสียทางการเงินมากกว่า 5 ล้านบาท แต่ไม่เกิน 10 ล้านบาท
	ระดับ ๓ (Moderate)	สูญเสียหรือมีโอกาสสูญเสียทางการเงินมากกว่า 10 ล้านบาท แต่ไม่เกิน 100 ล้านบาท
	ระดับ ๔ (High)	สูญเสียหรือมีโอกาสสูญเสียทางการเงินมากกว่า 100 ล้านบาท แต่ไม่เกิน 300 ล้านบาท
	ระดับ ๕ (Critical)	สูญเสียหรือมีโอกาสสูญเสียทางการเงิน 300 ล้านบาทขึ้นไป
ด้านชื่อเสียง	ระดับ ๑ (Minimal)	ส่งผลให้มีการเผยแพร่ข่าวในวงจำกัดภายในองค์กร
	ระดับ ๒ (Low)	ส่งผลให้มีการเผยแพร่ข่าวในวงกว้าง ทั่วทั้งองค์กร
	ระดับ ๓ (Moderate)	ส่งผลให้มีการเผยแพร่ข่าวในวงกว้างตามสื่อสาธารณะต่าง ๆ ซึ่งสามารถชี้แจงหรือแก้ไขได้ภายใน 3-6 ชม.
	ระดับ ๔ (High)	ส่งผลให้มีการเผยแพร่ข่าวในวงกว้างตามสื่อสาธารณะต่าง ๆ อย่างต่อเนื่อง ซึ่งสามารถชี้แจงหรือแก้ไขได้ภายใน 6-12 ชม.
	ระดับ ๕ (Critical)	ส่งผลให้มีการมีการพาดหัวข่าวที่รุนแรงตามสื่อ สาธารณะ ต่าง ๆ อย่างต่อเนื่อง ซึ่งสามารถชี้แจงหรือแก้ไขได้เกินกว่า 12 ชม.

ด้าน	ระดับชั้นของการรักษาความถูกต้องครบถ้วน (Integrity)	ลักษณะของผลกระทบเมื่อสูญเสียความถูกต้องครบถ้วน (Integrity)
ด้านการปฏิบัติตามกฎหมายหรือข้อกำหนด	ระดับ ๑ (Minimal)	ไม่มีผลกระทบหรือมีผลกระทบในระดับต่ำมากต่อการปฏิบัติตามกฎหมายหรือข้อกำหนด ข้อมูลไม่สำคัญต่อการรายงานตามกฎหมาย
	ระดับ ๒ (Low)	ส่งผลกระทบเล็กน้อยต่อความสามารถในการปฏิบัติตามข้อกำหนด แต่ยังสามารถดำเนินการแก้ไขได้ทันเวลาโดยไม่มีผลทางกฎหมาย
	ระดับ ๓ (Moderate)	มีความเสี่ยงต่อการไม่ปฏิบัติตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง ส่งผลให้ต้องมีการชี้แจงกับหน่วยงานกำกับดูแล หรืออาจมีคำแนะนำ/เตือนเบื้องต้น
	ระดับ ๔ (High)	มีผลกระทบอย่างมีนัยสำคัญ ทำให้ไม่สามารถปฏิบัติตามข้อกำหนดหรือกฎหมายที่สำคัญ อาจนำไปสู่การปรับเงิน การสอบสวน หรือการถูกสั่งระงับการดำเนินงานชั่วคราว
	ระดับ ๕ (Critical)	ส่งผลกระทบร้ายแรงต่อการปฏิบัติตามกฎหมายหรือข้อกำหนดที่เป็นสาระสำคัญ ทำให้เกิดคดีความทางกฎหมาย การฟ้องร้อง และความเสียหายต่อชื่อเสียงอย่างรุนแรง

๓.๑.๓ การประเมินและจัดลำดับชั้นของข้อมูลสารสนเทศ ในด้านการรักษาสภาพความพร้อมใช้ (Availability) จะประกอบไปด้วยการกำหนดระดับชั้นของข้อมูลสารสนเทศ การรักษาสภาพความพร้อมใช้ (Availability) และแนวทางการประเมินจัดลำดับชั้น

๓.๑.๓.๑ จัดลำดับชั้นของข้อมูลสารสนเทศในด้านการรักษาสภาพความพร้อมใช้ (Availability) จะมีการจัดระดับชั้น ๕ ระดับดังนี้

๓.๑.๓.๑.๑ ระดับ ๑ – ไม่เกี่ยวข้องโดยตรงกับธุรกิจ (Non-Business-Critical) หมายถึง ข้อมูลที่ไม่มีความสัมพันธ์โดยตรงกับกระบวนการทางธุรกิจในปัจจุบัน และไม่มีความจำเป็นต้องเข้าถึงบ่อยครั้ง อาจเป็นข้อมูลที่เก็บไว้เพื่อการอ้างอิง การตรวจสอบย้อนหลัง หรือข้อมูลที่หมดอายุแล้ว ตัวอย่างเช่น รายงานย้อนหลังมากกว่า 5 ปี, ข้อมูลระบบทดสอบ, หรือไฟล์ที่เก็บถาวรในคลังข้อมูล

๓.๑.๓.๑.๒ ระดับ ๒ – ใช้เฉพาะกิจหรือกรณีพิเศษ (Occasional or Non-Core Use) หมายถึงข้อมูลที่ใช้เฉพาะในบางโอกาส หรือใช้ในหน่วยงานสนับสนุน ซึ่งสามารถรอการเข้าถึงได้โดยไม่ส่งผลกระทบต่อกระบวนการหลักของธุรกิจ ตัวอย่างเช่น ระบบประเมินผลการอบรม, ระบบการจัดเก็บข้อเสนอจาก ซัพพลายเออร์, หรือฐานข้อมูลโครงการที่ปรับใช้แล้วเสร็จ

๓.๑.๓.๑.๓ ระดับ ๓ – สนับสนุนการบริหารจัดการ (Management Support) หมายถึง ข้อมูลที่ใช้ในกระบวนการบริหารจัดการทั่วไป หากไม่สามารถใช้งานได้ จะทำให้เกิดความล่าช้าในงานเอกสาร การอนุมัติ หรือการตัดสินใจเชิงบริหาร แต่ไม่ส่งผลกระทบต่อกระบวนการหลักทันที ตัวอย่างเช่น ระบบจัดการทรัพยากรบุคคล (HRIS) ระบบเวิร์กโฟลว์การอนุมัติ หรือระบบรายงานภายใน

๓.๑.๓.๑.๔ ระดับ ๔ – สนับสนุนกระบวนการหลัก (Critical Business Enabler) หมายถึง ข้อมูลของระบบที่มีความสำคัญอย่างมากต่อการดำเนินงาน แม้ไม่ใช่ส่วนที่ทำให้ธุรกิจหยุดโดยตรง แต่หากไม่สามารถใช้งานได้จะส่งผลให้รายได้ การบริการลูกค้าหรือความต่อเนื่องในการดำเนินงานได้รับผลกระทบ ตัวอย่างเช่น ระบบ Point of Sale (POS) หรือระบบบริการลูกค้า (CRM)

๓.๑.๓.๑.๕ ระดับ ๕ – จำเป็นต่อความอยู่รอดของธุรกิจ (Vital for Business Survival) หมายถึงข้อมูลของระบบในระดับนี้มีความจำเป็นอย่างยิ่งต่อการดำเนินงานหลักขององค์กร หากไม่สามารถเข้าถึงได้จะส่งผลให้ธุรกิจหยุดชะงักทันที อาจส่งผลถึงความปลอดภัย ชีวิต ทรัพย์สิน หรือความเสียหายทางการเงินอย่างรุนแรง เช่น ข้อมูลควบคุมระบบการผลิต (SCADA), ระบบบริหารจัดการเหตุฉุกเฉิน, หรือระบบการเงินแบบเรียลไทม์

๓.๑.๓.๒ สำหรับการประเมินลักษณะของข้อมูลเพื่อกำหนดระดับชั้นของการรักษาสภาพความพร้อมใช้ (Availability) ของข้อมูลมีแนวทางการประเมินในด้านต่าง ๆ ตามเกณฑ์ด้านล่างนี้ ทั้งนี้ให้ ถือเอาระดับชั้นสูงสุด จากการประเมินในแต่ละด้านเป็นตัวกำหนดระดับชั้น

ด้าน	ระดับชั้นของการรักษาสภาพความพร้อมใช้ (Availability)	ลักษณะของผลกระทบเมื่อสูญเสียสภาพความพร้อมใช้ (Availability)
ด้านธุรกิจและการดำเนินงาน	ระดับ ๑ ไม่เกี่ยวข้องโดยตรงกับธุรกิจ	มีผลกระทบต่อกระบวนการดำเนินงานทำให้การดำเนินงานหยุดชะงักไม่เกิน 6 ชม
	ระดับ ๒ – ใช้เฉพาะกิจหรือกรณีพิเศษ	มีผลกระทบต่อกระบวนการดำเนินงาน ทำให้ การดำเนินงานหยุดชะงักมากกว่า 6 ชม. แต่ไม่เกิน 12 ชม.
	ระดับ ๓ – สนับสนุนการบริหารจัดการ	มีผลกระทบต่อกระบวนการดำเนินงานทำให้การดำเนินงานหยุดชะงักมากกว่า 12 ชม. แต่ไม่เกิน 24 ชม.
	ระดับ ๔ – สนับสนุนกระบวนการหลัก	มีผลกระทบต่อกระบวน การดำเนินงานทำให้การดำเนินงานหยุดชะงักมากกว่า 24 ชม. แต่ไม่เกิน 48 ชม.
	ระดับ ๕ – จำเป็นต่อความอยู่รอดของธุรกิจ	มีผลกระทบต่อกระบวนการดำเนินงานทำให้การดำเนินงานหยุดชะงักมากกว่า48 ชม.
ด้านการเงิน	ระดับ ๑ ไม่เกี่ยวข้องโดยตรงกับธุรกิจ	สูญเสียหรือมีโอกาสสูญเสียทางการเงินน้อยกว่า / เท่ากับ 5 ล้านบาท
	ระดับ ๒ – ใช้เฉพาะกิจหรือกรณีพิเศษ	สูญเสียหรือมีโอกาสสูญเสียทางการเงินมากกว่า 5 ล้านบาท แต่ไม่เกิน 10 ล้านบาท
	ระดับ ๓ – สนับสนุนการบริหารจัดการ	สูญเสียหรือมีโอกาสสูญเสียทางการเงินมากกว่า 10 ล้านบาท แต่ไม่เกิน 100 ล้านบาท
	ระดับ ๔ – สนับสนุนกระบวนการหลัก	สูญเสียหรือมีโอกาสสูญเสียทางการเงินมากกว่า 100 ล้านบาท แต่ไม่เกิน 300 ล้านบาท

ด้าน	ระดับชั้นของการรักษาสภาพความพร้อมใช้ (Availability)	ลักษณะของผลกระทบเมื่อสูญเสียสภาพความพร้อมใช้ (Availability)
	ระดับ ๕ – จำเป็นต่อความอยู่รอดของธุรกิจ	สูญเสียหรือมีโอกาสสูญเสียทางการเงิน 300 ล้านบาทขึ้นไป
ด้านชื่อเสียง	ระดับ ๑ ไม่เกี่ยวข้องโดยตรงกับธุรกิจ	ส่งผลให้มีการเผยแพร่ข่าวในวงจำกัดภายในองค์กร
	ระดับ ๒ – ใช้เฉพาะกิจหรือกรณีพิเศษ	ส่งผลให้มีการเผยแพร่ข่าวในวงกว้าง ทั่วทั้งองค์กร
	ระดับ ๓ – สนับสนุนการบริหารจัดการ	ส่งผลให้มีการเผยแพร่ข่าวในวงกว้างตามสื่อสาธารณะต่าง ๆ ซึ่งสามารถชี้แจงหรือแก้ไขได้ภายใน 3-6 ชม.
	ระดับ ๔ – สนับสนุนกระบวนการหลัก	ส่งผลให้มีการเผยแพร่ข่าวในวงกว้างตามสื่อสาธารณะต่าง ๆ อย่างต่อเนื่อง ซึ่งสามารถชี้แจงหรือแก้ไขได้ภายใน 6-12 ชม.
	ระดับ ๕ – จำเป็นต่อความอยู่รอดของธุรกิจ	ส่งผลให้มีการมีการพาดหัวข่าวที่รุนแรงตามสื่อ สาธารณะ ต่าง ๆ อย่างต่อเนื่อง ซึ่งสามารถชี้แจงหรือแก้ไขได้เกินกว่า 12 ชม.
ด้านการปฏิบัติตามกฎหมายหรือข้อกำหนด	ระดับ ๑ ไม่เกี่ยวข้องโดยตรงกับธุรกิจ	ไม่มีผลกระทบหรือมีผลกระทบในระดับต่ำมากต่อการปฏิบัติตามกฎหมายหรือข้อกำหนด ข้อมูลไม่สำคัญต่อการรายงานตามกฎหมาย
	ระดับ ๒ – ใช้เฉพาะกิจหรือกรณีพิเศษ	ส่งผลกระทบเล็กน้อยต่อความสามารถในการปฏิบัติตามข้อกำหนด แต่ยังสามารถดำเนินการแก้ไขได้ทันเวลาโดยไม่มีผลทางกฎหมาย
	ระดับ ๓ – สนับสนุนการบริหารจัดการ	มีความเสี่ยงต่อการไม่ปฏิบัติตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง ส่งผลให้ต้องมีการชี้แจงกับหน่วยงานกำกับดูแล หรืออาจมีคำแนะนำ/เตือนเบื้องต้น
	ระดับ ๔ – สนับสนุนกระบวนการหลัก	มีผลกระทบอย่างมีนัยสำคัญ ทำให้ไม่สามารถปฏิบัติตามข้อกำหนดหรือกฎหมายที่สำคัญ อาจนำไปสู่การปรับเงิน การสอบสวน หรือการถูกสั่งระงับการดำเนินงานชั่วคราว
	ระดับ ๕ – จำเป็นต่อความอยู่รอดของธุรกิจ	ส่งผลกระทบร้ายแรงต่อการปฏิบัติตามกฎหมายหรือข้อกำหนดที่เป็นสาระสำคัญ ทำให้เกิดคดีความทางกฎหมาย การฟ้องร้อง และความเสียหายต่อชื่อเสียงอย่างรุนแรง

๓.๒ เจ้าของระบบงาน ต้องกำหนดให้มีการออกแบบระบบงานตามประเมินและจัดลำดับชั้นของข้อมูลสารสนเทศ โดยต้องคำนึงถึงทั้งข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest) ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit) ข้อมูลที่กำลังถูกใช้งาน (Data in Use) และการลบข้อมูล

๓.๒.๑ การควบคุมตามระดับชั้นความลับของข้อมูล (Confidentiality) ที่ต้องพิจารณาดำเนินการ

ระดับชั้นความลับของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)	การลบข้อมูล
ระดับที่ ๑ ข้อมูลเปิดเผย (Open)	จัดเก็บในสื่อบันทึกทั่วไป	ส่งผ่านในเครือข่ายทั่วไป	ไม่มีการควบคุมเฉพาะ	ไม่มีการควบคุมเฉพาะ
ระดับที่ ๒ เผยแพร่ภายในองค์กร(Private)	จัดเก็บในสื่อบันทึกทั่วไป	ส่งผ่านในเครือข่ายภายในทั่วหรือเครือข่ายภายนอกที่มีการใช้ Protocol ในการส่งที่มีความมั่นปลอดภัยเช่น HTTPS, FTPS เป็นต้น	ผู้ใช้งานระมัดระวังการเปิดเผยข้อมูลความลับเมื่อปฏิบัติงานนอกสถานที่ตามแนวปฏิบัติการใช้งานอุปกรณ์พกพา(Use of Personal Computer and Mobile)	ทำลายสื่อบันทึกข้อมูลด้วยเครื่องมือในการลบข้อมูลทำงานตามมาตรฐาน NIST SP 800-88 Rev. 1 – Guidelines for Media Sanitization หรือ DoD 5220.22-M ยกตัวอย่างเครื่องมือของระบบปฏิบัติการดังนี้ Microsoft Windows: sdelete Linux:shred

ระดับชั้นความลับของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)	การลบข้อมูล
				หรือเครื่องมืออื่นที่ได้รับการรับรองตามมาตรฐานของ NIST หรือ DoD หรือหากมีการใช้บริการผู้ให้บริการภายนอกในการลบทำลายสื่อบันทึกข้อมูลต้องกำหนดให้มีการจัดทำรายงาน และการยืนยันการลบทำลายดังกล่าวด้วย สำหรับข้อมูลประเภทเอกสารตีพิมพ์ ให้ทำลายโดยเครื่องทำลายเอกสาร
ระดับที่ ๓ ข้อมูลลับ (Confidential)	- จัดเก็บในสื่อบันทึกทั่วไปที่มีการควบคุมสิทธิ์การเข้าถึงโดยการพิสูจน์ตัวตนและการกำหนด	ดำเนินการตามการควบคุมสำหรับข้อมูลเผยแพร่ภายในองค์กร	ผู้ใช้งานระมัดระวังการเปิดเผยข้อมูลความลับเมื่อปฏิบัติงานนอกสถานที่ตามแนวปฏิบัติการใช้งาน	ดำเนินการตามการควบคุมสำหรับข้อมูลเผยแพร่ภายในองค์กร

ระดับชั้นความลับของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)	การลบข้อมูล
	สิทธิ์ตามแนวปฏิบัติที่กำหนดไว้ - จัดให้มี full-disk encryption สำหรับเครื่องคอมพิวเตอร์แบบพกพา (Laptop Computer) - ใช้ระบบฐานข้อมูลที่มีเทคโนโลยีการเข้ารหัส - จัดให้มีระบบการป้องกันข้อมูลรั่วไหล (Data Leakage Prevention)		อุปกรณ์พกพา(Use of Personal Computer and Mobile)	
ระดับที่ ๔ ข้อมูลลับมาก (Secret)	ดำเนินการตามการควบคุมสำหรับข้อมูลลับ และเข้ารหัสข้อมูลไฟล์ข้อมูลด้วย Advanced Encryption Standard (AES) 256 Bit ขึ้นไป	ดำเนินการตามการควบคุมสำหรับข้อมูลเผยแพร่ภายในองค์กร และทำการเข้ารหัสข้อมูลก่อนส่งผ่านระบบเครือข่าย	ไม่ควรเข้าถึงใช้งานข้อมูลลับมากในการปฏิบัติงานนอกสถานที่	ดำเนินการตามการควบคุมสำหรับข้อมูลเผยแพร่ภายในองค์กร

ระดับชั้นความลับของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)	การลบข้อมูล
ระดับที่ ๕ ข้อมูลลับที่สุด (Top Secret)	ดำเนินการตามการควบคุมสำหรับข้อมูลลับ และเข้ารหัสข้อมูลไฟล์ข้อมูลด้วย Advanced Encryption Standard (AES) 256 Bit ขึ้นไป	ดำเนินการตามการควบคุมสำหรับข้อมูลเผยแพร่ภายในองค์กร และทำการเข้ารหัสข้อมูลก่อนส่งผ่านระบบเครือข่าย	ไม่ควรเข้าถึงใช้งานข้อมูลลับที่สุดในการปฏิบัติงานนอกสถานที่	ดำเนินการตามการควบคุมสำหรับข้อมูลเผยแพร่ภายในองค์กร

๓.๒.๒ การควบคุมตามระดับการรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) ที่ต้องพิจารณาดำเนินการ

ระดับการรักษาความถูกต้องครบถ้วนของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)
ระดับ ๑ (Minimal)	จัดเก็บในสื่อบันทึกทั่วไปที่มีการควบคุมสิทธิ์การเข้าถึงโดยการพิสูจน์ตัวตนและการกำหนดสิทธิ์ตามแนวปฏิบัติที่กำหนดไว้	ไม่มีการควบคุมเฉพาะ	ไม่มีการควบคุมเฉพาะ
ระดับ ๒ (Low)	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๑ และ สำรองข้อมูลเป็นระยะ (เช่น รายเดือน)	ส่งผ่านในเครือข่ายภายในหรือเครือข่ายภายนอกที่มีการใช้ Protocol	มีการตรวจสอบค่าข้อมูลเบื้องต้นในการนำเข้าหรือเปลี่ยนแปลง (Input

ระดับการรักษาความถูกต้องครบถ้วนของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)
		ในการส่งที่มีความมั่นคงปลอดภัย เช่น HTTPS, FTPS เป็นต้น	Validation) เช่น ประเภทข้อมูล หรือค่าคงที่
ระดับ ๓ (Moderate)	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๑ และ - จัดให้มีการบันทึก Log การเข้าถึง - ใช้ระบบจัดเก็บที่รองรับการควบคุมเวอร์ชัน (Version Control)	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๒	- ตรวจสอบค่าข้อมูลตามกฎทางธุรกิจ (Business Rules) - มีการบันทึกประวัติการเปลี่ยนแปลง (Audit Log)
ระดับ ๔ (High)	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๑ และ - ใช้กลไกตรวจสอบความสมบูรณ์ของไฟล์ เช่น Checksum หรือ Hash - สำรองข้อมูลแบบ Daily และเก็บในหลายสถานที่ (Offsite/Cloud) - มีการตรวจสอบการเปลี่ยนแปลงไฟล์อัตโนมัติ (File Integrity Monitoring)	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๒	- บันทึกการเปลี่ยนแปลงพร้อมระบุวันเวลาและผู้กระทำ - ใช้กระบวนการอนุมัติหลายขั้นตอนก่อนการแก้ไข - จัดให้มีระบบติดตามเวอร์ชันข้อมูล (Version History)

ระดับการรักษาความถูกต้องครบถ้วนของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)
ระดับ ๕ (Critical)	- ใช้การสำรองแบบ Real-time replication หรือ High Availability Storage - ใช้ระบบเก็บ Log ที่ไม่สามารถแก้ไขได้ (Immutable Logs) - ตรวจสอบความถูกต้องของข้อมูลด้วยระบบอัตโนมัติและรายงานสม่ำเสมอ - ใช้ลายเซ็นดิจิทัลหรือกลไกตรวจสอบความถูกต้องด้วย Hash	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๒	- แบ่งหน้าที่ผู้ปฏิบัติงาน (Segregation of Duties) - แจ้งเตือนทันทีเมื่อมีการเปลี่ยนแปลงผิดปกติ - มีการทบทวนและกระทบยอดข้อมูลอย่างสม่ำเสมอ

๓.๒.๓ การควบคุมตามระดับความพร้อมใช้ของข้อมูล (Availability) ที่ต้องพิจารณาดำเนินการ

ระดับการรักษาความถูกต้องครบถ้วนของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)
ระดับ ๑ ไม่เกี่ยวข้องโดยตรงกับธุรกิจ (Non-Business-Critical)	ไม่มีการควบคุมเฉพาะ	ไม่มีการควบคุมเฉพาะ	ไม่มีการควบคุมเฉพาะ
ระดับ ๒ ใช้เฉพาะกิจหรือกรณีพิเศษ (Occasional or Non-Core Use)	สำรองข้อมูลเป็นรอบระยะเวลาที่ตกลงกับเจ้าของข้อมูล	ไม่มีการควบคุมเฉพาะ	ไม่มีการควบคุมเฉพาะ
ระดับ ๓ สนับสนุนการบริหารจัดการ (Management Support)	- มีการสำรองข้อมูลตาม Recovery Point Objective (RPO) และ Recovery Time Objective (RTO) ที่ได้กำหนดโดยเจ้าของระบบงาน	จัดให้มีระบบเครือข่ายที่มี Service Level Agreement ด้าน Availability ไม่ต่ำกว่า 99.5%	มีระบบการแจ้งเตือนเมื่อระบบประมวลผลไม่พร้อมใช้งานเพื่อแก้ปัญหาได้ทันท่วงที

ระดับการรักษาความถูกต้องครบถ้วนของข้อมูล	ข้อมูลที่ถูกจัดเก็บไว้ (Data at Rest)	ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data in Transit)	ข้อมูลที่กำลังถูกใช้งาน (Data in Use)
ระดับ ๔ สนับสนุนกระบวนการหลัก (Critical Business Enabler)	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๓ และ - มีระบบ Redundant หรือ DR site - ทำการสำรองข้อมูลอย่างน้อย ๒ ชุด (เมื่อรวมกับข้อมูลในระบบงานจะทำให้มีข้อมูลสามชุด) - เลือกสื่อบันทึกข้อมูลที่มีความแตกต่างกัน เช่นสำรองข้อมูลใน Disk และ บน Cloud หรือใน Tape Backup - ต้องมีสำรองข้อมูลแยกสถานที่กับศูนย์คอมพิวเตอร์หลัก-	จัดให้มีระบบเครือข่ายที่มี Service Level Agreement ด้าน Availability ไม่ต่ำกว่า 99.9%	มีระบบงานสำรองเพื่อการประมวลผล เช่น DR Site หรือ Redundant System ที่สามารถใช้งานได้ตาม Recovery Time Objective (RTO)
ระดับ ๕ จำเป็นต่อความอยู่รอดของธุรกิจ (Vital for Business Survival)	ดำเนินการตามการควบคุมสำหรับข้อมูลระดับ ๔ และ - เก็บข้อมูลในระบบที่มี High Availability หรือ Data Replication - สำรองข้อฒชมูลแบบ Real-time และตรวจสอบความครบถ้วนอัตโนมัติ	จัดให้มีระบบเครือข่ายที่มี Service Level Agreement ด้าน Availability ไม่ต่ำกว่า 99.9%	มีระบบงานสำรองเพื่อการประมวลผลที่สามารถใช้งานได้อย่างต่อเนื่องเมื่อระบบหลักไม่สามารถใช้งานได้เช่น ระบบ Failover หรือ Load Balancer

๓.๓ ผู้ดูแลระบบงาน และ ผู้ดูแลระบบเครือข่าย เป็นผู้สนับสนุนทางด้านเทคนิคต่อเจ้าของระบบงานในการควบคุมหรือดำเนินการในการออกแบบ ติดตั้งและบำรุงรักษาระบบงาน

๓.๔ คณะทำงานฯ ต้องตรวจสอบให้มั่นใจว่าข้อมูลและระบบงาน ได้รับการจัดการการควบคุมตามแนวทางการควบคุมในแต่ชนิดและคุณสมบัติของข้อมูล

๓.๕ ช่องทางการเข้าถึงข้อมูล ที่องค์กรได้จัดเตรียมไว้ ได้แก่

- ๓.๕.๑ เครือข่ายอินเทอร์เน็ต
- ๓.๕.๒ เครือข่ายอินทราเน็ต
- ๓.๕.๓ ระบบเอ็กซ์ทราเน็ต
- ๓.๕.๔ เครือข่ายไร้สาย

๓.๖ ผู้ดูแลระบบงาน มีหน้าที่ในการตรวจสอบการอนุมัติและระบุสิทธิในการเข้าถึงข้อมูลสารสนเทศให้แก่ผู้ใช้งาน ในการขออนุญาตเข้าถึงข้อมูลสารสนเทศนั้น ต้องมีการทำเป็นเอกสารเพื่อขอข้อมูลสารสนเทศ และให้มีการลงนาม อนุมัติเอกสารดังกล่าว และมีการจัดเก็บไว้เป็นหลักฐาน

หมวด ๘
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน ป้องกันมิให้ผู้ไม่มีสิทธิหรือผู้ที่ไม่ได้รับอนุญาตสามารถใช้งานบริการทางด้านเทคโนโลยีสารสนเทศ รวมทั้งสามารถระบุสิทธิ ยืนยันและตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งาน

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบงาน

๒.๒ ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ แนวปฏิบัติการลงทะเบียนผู้ใช้งาน (User Registration)

๓.๑.๑ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานระบบ และได้รับการอนุมัติ

๓.๑.๒ ผู้ดูแลระบบงานตรวจสอบบัญชีผู้ใช้งาน โดยเฉพาะผู้ที่ไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๓.๑.๓ ผู้ดูแลระบบงานตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๓.๑.๔ ผู้ดูแลระบบงานมีการแจกเอกสารหรือสิ่งที่แสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนาม รับทราบด้วย

๓.๑.๕ ผู้ดูแลระบบงาน มีการถอดถอนสิทธิการเข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนผู้ใช้งาน เมื่อมี การลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓.๑.๖ การลงทะเบียนผู้ใช้งานผู้ดูแลระบบงาน ทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการ เข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๓.๒ แนวปฏิบัติการบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๓.๒.๑ ผู้ดูแลระบบงาน ระบุสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตาม ความจำเป็นในการใช้งาน และทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๒.๒ ผู้ดูแลระบบงาน มอบหมายสิทธิ ให้สอดคล้องตามนโยบายควบคุมการเข้าถึง

๓.๒.๓ ผู้ดูแลระบบงาน ทำการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิแก่ผู้ใช้งาน

๓.๒.๔ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยให้มีการระบุระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการระบุสิทธิ์พิเศษที่ได้รับด้วยว่า การเข้าถึงได้นั้น สามารถเข้าถึงได้ในระดับใดบ้าง และให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๒.๕ การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๒.๕.๑ หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลในแบบฟอร์ม และยื่นคำขอกับสายงานเทคโนโลยีสารสนเทศ

๓.๒.๕.๒ ผู้ดูแลระบบงานยกเลิกสิทธิการใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจาก ระบบงานที่เกี่ยวข้องทั้งหมด

๓.๒.๕.๓ ระบุสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยให้สิทธิเฉพาะที่เกี่ยวกับการ ปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบจากผู้ดูแลระบบงานเป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๓ แนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๓.๓.๑ ผู้ดูแลระบบงานระบุการตั้งหรือเปลี่ยนรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย โดยมีความยาวตัวอักษรและหรือตัวเลข ไม่น้อยกว่า ๘ ตัวอักษร และ ประกอบด้วย ตัวอักษรตัวเล็ก ตัวใหญ่ ตัวเลขและอักขระพิเศษ

๓.๓.๒ ผู้ดูแลระบบงานจัดส่งรายชื่อผู้ใช้และรหัสผ่านแยกจากกันอย่างปลอดภัย โดยจัดส่งรายชื่อผู้ใช้ผ่านทางระบบอีเมล และจัดส่งรหัสผ่านทางอีเมลหรือโทรแจ้งผู้ใช้งานให้รับทราบโดยตรง

๓.๓.๓ ผู้ปฏิบัติงานใช้รหัสผ่าน สำหรับแสดงตัวตนทุกครั้งในการเข้าไปปฏิบัติงานในระบบเทคโนโลยีสารสนเทศขององค์กร

๓.๓.๔ ผู้บังคับบัญชาหน่วยงานเจ้าของระบบงานระดับผู้อำนวยการฝ่ายขึ้นไป เป็นผู้อนุมัติให้ผู้ปฏิบัติงานใช้ระบบเทคโนโลยีสารสนเทศ พร้อมกับแจ้งหน่วยงานที่ดูแลระบบสารสนเทศเพื่อรหัสผ่าน

หมวด ๙
การออกแบบระบบเครือข่ายและการควบคุมการเข้าถึงระบบเครือข่าย
(Secured Network Design and Network Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกันการเข้าถึงการบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยมีการกำหนด กระบวนการการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันตามกลุ่มของเครือข่าย

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบเครือข่าย

๒.๒ ผู้ใช้งานระบบเครือข่าย

๓. แนวปฏิบัติ

๓.๑ การใช้งานบริการเครือข่าย

๓.๑.๑ ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของการประปานครหลวง

๓.๑.๒ การประปานครหลวงไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย ได้แก่ การประกาศแจ้งความต้องการซื้อ หรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓.๑.๓ ผู้ใช้งานระบบเครือข่ายต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่ไม่ใช่ของตนเองโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว การประปานครหลวงไม่มีส่วน ร่วมรับผิดชอบความเสียหายดังกล่าว

๓.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามบุกรุกล้ำเขตหวงห้ามของการประปานครหลวง

๓.๑.๕ ผู้ดูแลระบุบัญชีผู้ใช้งานเป็นรายบุคคลสำหรับผู้ใช้งานแต่ละคน โดยให้สามารถเข้าใช้งานระบบเครือข่าย (LAN) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ได้

๓.๑.๖ บัญชีผู้ใช้งาน (User Account) ที่การประปานครหลวงให้ผู้ใช้งานนั้น ผู้ใช้งานจะเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๑.๗ ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๑.๘ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง

๓.๒ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks)

๓.๒.๑ ผู้ดูแลระบบเครือข่ายต้องควบคุมป้องกันการเชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาตเข้าสู่ระบบเครือข่ายโดยการปิดกั้นการเชื่อมต่อหรือใช้เครื่องมือในการปิดกั้นการเชื่อมต่อ

๓.๒.๒ ผู้ดูแลระบบเครือข่ายต้องเก็บบัญชีการเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่อง คอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง ด้วยระบบบริหารจัดการ IP Address (IP Address Management)

๓.๒.๓ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องทำการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

๓.๒.๔ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๓.๒.๕ ผู้ขอใช้บริการทำหนังสือเป็นลายลักษณ์อักษรถึงผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล เรื่อง “การขอเชื่อมต่อเครือข่าย” และได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับขั้น

๓.๓ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่นอกหน่วยงาน (User authentication for external Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของการประปานครหลวง ดังนี้

๓.๓.๑ ผู้ขอใช้บริการกรอกแบบฟอร์มเพื่อขอใช้ระบบจากเครือข่ายภายนอกการประปานครหลวง พร้อมทั้ง ระบุระบบสารสนเทศที่ต้องการใช้ และได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับขั้น

๓.๓.๒ ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) เพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานด้วยรายชื่อผู้ใช้ (username) ทุกครั้ง

๓.๓.๓ ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยมีวิธีการยืนยันตัวบุคคล (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้รหัสผ่าน (password) และการใช้ token ที่มีความสามารถ PKI

๓.๓.๔ ผู้ใช้งานที่ทำการเชื่อมต่อจากภายนอกการประปานครหลวงต้องทำการเข้ารหัสข้อมูลในการเข้าถึงระบบ พิสูจน์ตัวตนจากระยะไกลผ่านระบบที่การประปานครหลวงได้จัดไว้เท่านั้น

๓.๓.๕ การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งาน และเก็บ Log การเข้าใช้งานด้วย

๓.๔ ผู้ดูแลระบบเครือข่ายต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

๓.๔.๑ ดำเนินการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบ เครือข่ายได้รับการควบคุมผ่านกระบวนการควบคุมการเปลี่ยนแปลง (Change Management)

๓.๔.๒ ยกเลิกหรือปิดพอร์ต และบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้

๓.๔.๓ ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการบริหารจัดการระบบเครือข่ายทั้งทางกายภาพและโดยการล็อกอินเข้ามาใช้งาน

๓.๔.๔ ล็อคอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า Configuration ด้วยกุญแจเพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์ และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๓.๔.๕ ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๓.๕ การแบ่งแยกเครือข่าย (Segregation in networks)

๓.๕.๑ การประปานครหลวงแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคาร สำนักงานประปาสาขา โรงสูบจ่ายน้ำ เพื่อควบคุมการเข้าถึงเครือข่ายโดยมิได้รับอนุญาต

๓.๕.๒ ผู้ดูแลระบบเครือข่ายต้องป้องกันไม่ให้มีการเชื่อมต่อเครือข่ายภายในหรือเครือข่ายกลุ่มต่าง ๆ เข้าหากันโดยไม่ได้มีการประเมินความเสี่ยงและกำหนดการควบคุม

๓.๕.๓ การประปานครหลวงจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยหน่วยงานต่างๆ สามารถใช้งานระบบผ่านเครือข่ายภายในและภายนอกได้ เมื่อปฏิบัติงานอยู่ในพื้นที่ปฏิบัติงานของการประปานครหลวง

๓.๕.๔ ใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย

๓.๕.๕ กรองและจำกัดการไหลของข้อมูลระหว่างเครือข่าย

๓.๕.๖ ใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอก ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของการประปานครหลวง

๓.๕.๗ แยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ

๓.๕.๘ แยกกลุ่มเครือข่ายเป็น ๔ ประเภท ได้แก่

- ระบบเครือข่ายภายใน
- ระบบเครือข่ายที่ ให้บริการภายนอก (DMZ : Demilitarized Zone)
- ระบบเครือข่ายสำหรับ Application
- ระบบเครือข่ายสำหรับการเข้าถึงระยะไกล (Remote Zone)

๓.๕.๙ จัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยทำการปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๓.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ผู้ดูแลระบบเครือข่ายต้องควบคุมการเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติควบคุมการเข้าถึง ดังนี้

๓.๖.๑ ตรวจสอบการเชื่อมต่อเครือข่าย

๓.๖.๒ จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๓.๖.๓ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๓.๖.๔ ติดตั้งระบบการตรวจจับผู้บุกรุกทั้งระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

๓.๖.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๓.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing Control) ผู้ดูแลระบบเครือข่ายต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ด้วยระบบ Network Management and Monitoring ดังนี้

๓.๗.๑ ควบคุมมิให้มีการเปิดเผยแผนผังการใช้งานหมายเลขเครือข่าย (network diagram พร้อม IP Address)

๓.๗.๒ ให้เปลี่ยนแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓.๗.๓ มีมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๓.๗.๔ ติดตั้งอุปกรณ์เกตเวย์หรืออุปกรณ์บนเครือข่ายเพื่อตรวจสอบหมายเลขเครือข่าย

๓.๗.๕ มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก

๓.๘ จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้เท่านั้น

หมวด ๑๐
นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความ ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. ผู้ที่รับผิดชอบ

๒.๑ ผู้ดูแลระบบงาน

๒.๒ ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๓.๑.๑ ผู้ใช้งานระบุรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓.๑.๒ ผู้ใช้งานตั้งค่าการพักหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๓.๑.๓ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง (หากเป็นเครื่องคอมพิวเตอร์ในระบบเครือข่ายภายในให้ใช้รหัส Active Directory)

๓.๑.๔ ผู้ใช้งานไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้า ใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๑.๕ ผู้ใช้งานทำการออกจากระบบ (Log out) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓.๑.๖ ซอฟต์แวร์ลิขสิทธิ์ขององค์กร ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๓.๑.๗ ซอฟต์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

๓.๑.๘ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นขององค์กรเพื่อประโยชน์ทางการค้าส่วนบุคคล

๓.๑.๙ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม ขัดต่อศีลธรรม

๓.๑.๑๐ ห้ามผู้ใช้ระบบสารสนเทศขององค์กร เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดย ไม่ได้รับอนุญาตจากผู้มีอำนาจ

๓.๒ แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authorization)

ผู้ดูแลระบบงานต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิค ในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ด้วยระบบ Active Directory Management , Internet Web Authentication และ Mail User Authentication โดยมีแนวปฏิบัติดังนี้

๓.๒.๑ ผู้ใช้งานมีรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๓.๒.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านลิขสิทธิ์หรือด้านเทคนิค

๓.๒.๓ ผู้ใช้งานที่เป็นเจ้าของชื่อผู้ใช้งาน (Username) เป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากใช้ชื่อ ผู้ใช้งาน (Username) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

๓.๓ แนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management System) จัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการ ทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการระบุรหัสผ่านที่มีคุณภาพ โดยมีแนวทางปฏิบัติดังนี้

๓.๓.๑ ระบบสารสนเทศขององค์กรทุกระบบมีการจัดการรหัสผ่าน โดยแยกเป็นรายบุคคลเพื่อให้สามารถ ติดตามการใช้งานและให้เป็นความรับผิดชอบของแต่ละคนได้

๓.๓.๒ ให้ผู้ใช้งานระบุรหัสผ่านที่ยากต่อการคาดเดา (Strong Password)

๓.๓.๓ ให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อครบ ๙๐ วัน และแจ้งให้ผู้ใช้งานเปลี่ยนโดยอัตโนมัติ

๓.๓.๔ เมื่อดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยอัตโนมัติ

๓.๔ แนวปฏิบัติการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

ให้ผู้ดูแลระบบงานจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยง มาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว โดยมีแนวทางปฏิบัติ ดังนี้

๓.๔.๑ จัดทำบัญชีรายชื่อโปรแกรมประเภทอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น

๓.๔.๒ จำกัดผู้ที่สามารถใช้งานโปรแกรมอรรถประโยชน์ และไม่อนุญาตให้ผู้ใช้งานทั่วไปใช้งานได้

๓.๔.๓ แยกจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน โดยแยกไว้ในไดเรกทอรี่ต่างหาก เพื่อให้ง่ายในการควบคุมและจัดการโปรแกรมเหล่านี้

๓.๔.๔ ถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๓.๕ แนวปฏิบัติเมื่อว่างเว้นจากการใช้งานระบบสารสนเทศ (Session Time-Out)

๓.๕.๑ ระบบเทคโนโลยีสารสนเทศ มีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๓๐ นาที

๓.๕.๒ ให้ล็อกหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๓.๕.๓ ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูงหรือความสำคัญสูง ทางด้านระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๕.๔ มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

๓.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

จำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือ โปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง โดยมีแนวทางปฏิบัติ ดังนี้

๓.๖.๑ ระบุระยะเวลาการเชื่อมต่อระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง และให้ใช้งานได้เฉพาะช่วงเวลาทำงานของหน่วยงานตามปกติเท่านั้น

๓.๖.๒ ช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความ เสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๓.๖.๓ ระบบสารสนเทศที่เป็นระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

หมวด ๑๑
นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
(Application and Information Access Control Policy)

๑. วัตถุประสงค์

เพื่อมีมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร และ ป้องกันการบุกรุกผ่านระบบเครือข่าย จากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัว บุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบงาน

๒.๒ ผู้ใช้งาน

๒.๓ เจ้าของระบบงาน

๓. แนวปฏิบัติ

๓.๑ แนวปฏิบัติการลงทะเบียนผู้ใช้งาน (User Registration)

๓.๑.๑ ผู้ดูแลระบบงานสร้างบัญชีผู้ใช้งาน (User Account) สำหรับผู้ใช้งานแต่ละคน ตามสิทธิเฉพาะที่ตนปฏิบัติงาน ในหน้าที่ และได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๑.๒ ผู้ดูแลระบบงานสร้างบัญชีผู้ใช้งาน (User Account) สำหรับผู้ใช้งานที่เป็น Outsource กรณีที่มีการจ้างเหมา ดำเนินการเกี่ยวกับระบบสารสนเทศของหน่วยงาน ตามสิทธิเฉพาะที่ตนปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบจากการประปานครหลวงเป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิทุก ๓ เดือน

๓.๑.๓ ผู้ดูแลระบบงานบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

๓.๑.๓.๑ การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๓.๑.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๓.๑.๓.๓ ให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

๓.๑.๓.๔ ให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๑.๓.๕ บัญชีผู้ใช้งาน (User Account) หรือรายชื่อผู้ใช้ (User name) ต้องไม่ซ้ำกัน

๓.๑.๓.๖ ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการระบุระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อ พ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการระบุสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดได้บ้าง และให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

๓.๑.๓.๗ กำหนดให้มีการระงับบัญชีชื่อผู้ใช้ที่มีการยืนยันตัวตนผิดพลาดเป็นจำนวน ๕ ครั้งติดต่อกัน

๓.๑.๓.๘ ตั้งค่าระบบให้ไม่อนุญาตให้มีการเข้าถึงระบบจากชื่อผู้ใช้งานเดียวกันมากกว่า ๑ session พร้อม ๆ กัน

๓.๑.๔ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ องค์กรมีช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยให้เข้าถึงผ่านระบบเครือข่ายภายในเท่านั้น และมีการตรวจสอบการผ่านเข้า ออกพื้นที่ควบคุม (Restriction Area Access Control) และมีเครือข่ายเฉพาะ (VLAN) สำหรับ Outsource

๓.๑.๕ เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ได้แก่ ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๓.๑.๖ ผู้ดูแลระบบงานจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยมีวิธีปฏิบัติ ดังนี้

๓.๑.๖.๑ ผู้ดูแลระบบงานป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงโดยไม่ได้รับอนุญาต

๓.๑.๖.๒ ผู้ดูแลระบบงานควบคุมการเข้าถึงระบบ โดยมีขั้นตอนและแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ใช้บริการ เหตุผลในการขอใช้ระยะเวลาในการใช้บริการ

๓.๑.๖.๓ เจ้าของระบบงานมีรายการข้อมูลสำหรับการให้บริการประกอบด้วย รายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ระดับขั้นของการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง เป็นต้น

๓.๑.๖.๔ เจ้าของระบบงานบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับสำหรับข้อมูลสำคัญ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- มีรายชื่อผู้ใช้บริการและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ ข้อมูลในแต่ละชั้นความลับข้อมูล

- มีระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ มีการเข้ารหัส (Encryption) ที่เป็นสากล
- เปลี่ยนรหัสผ่านของข้อมูลหรือระบบที่มีลำดับความสำคัญตามระยะเวลาที่กำหนด

๓.๑.๖.๕ ลงทะเบียนผู้ใช้งาน เพื่อควบคุม จำกัด หรือให้สิทธิการเข้าถึงข้อมูลและฟังก์ชั่นต่างๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

๓.๑.๖.๖ ควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงาน เพื่อให้สามารถเข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้อง และจำเป็นสำหรับการนำไปใช้งานเท่านั้น

๓.๑.๖.๗ แสดงเฉพาะข้อมูลพื้นฐาน เพื่อให้ผู้ใช้งานได้รับทราบข้อมูลที่จำเป็นเท่านั้น

๓.๑.๖.๘ แสดงรายละเอียดเท่าที่จำเป็นสำหรับแต่ละผู้ใช้งาน หลังจากที่ล็อกอินเสร็จแล้ว

๓.๑.๖.๙ แสดงข้อความแสดงเตือน ห้ามผู้ไม่มีสิทธิเข้าถึงระบบงาน

๓.๑.๖.๑๐ ตรวจสอบข้อมูลการล็อกอิน หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว

๓.๑.๗ จำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งาน ในลักษณะที่เปิดเผยข้อมูลภายในของระบบงาน

๓.๑.๘ จำกัดจำนวนครั้งที่ผู้ใช้งานใส่ข้อมูลการล็อกอินผิด

๓.๑.๙ ส่งข้อความเตือนไปยังผู้ดูแลให้ทราบว่ามีผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดเป็นจำนวนหลายครั้ง

๓.๑.๑๐ บันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

๓.๑.๑๑ จำกัดช่วงระยะเวลาที่นานที่สุดที่ผู้ใช้งานจะล็อกอินเข้าใช้งานให้สำเร็จ

๓.๒ แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน (Sensitive System Isolation)

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร คือระบบควบคุมการผลิตน้ำประปา ต้องดำเนินการดังนี้

๓.๒.๑ ระบุระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อองค์กร

๓.๒.๒ แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบงานอื่นๆ และแสดงให้เห็นถึงผลกระทบและ ระดับความสำคัญต่อองค์กร หรือแยกเครือข่ายโดยใช้วิธีการทางเทคนิค VLAN

๓.๒.๓ ทำการติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์แม่ข่ายต่างหาก

๓.๒.๔ ควบคุมอุปกรณ์คอมพิวเตอร์สำหรับการสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile Computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว โดยไม่อนุญาตให้นำอุปกรณ์ส่วนตัว หรืออุปกรณ์จากภายนอกเข้ามาเชื่อมต่อ หากจำเป็นต้องใช้ในการปฏิบัติงาน ให้มีการลงทะเบียนอุปกรณ์ พร้อมทั้งตรวจสอบความพร้อมด้านความปลอดภัยของอุปกรณ์ ได้แก่ ติดตั้ง Antivirus Personal Firewall ตามที่การประปานครหลวงกำหนด

๓.๒.๕ ทำการควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall

๓.๒.๖ การเข้าถึงระบบแอปพลิเคชันซึ่งไวต่อการรบกวน จะต้องได้รับการปกป้องจากอุปกรณ์ Firewall ที่สามารถปกป้องได้ในระดับ Application เช่น Web Application Firewall เสมอ

๓.๓ แนวปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ผู้ดูแลระบบงานกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกล รวมถึงการเตรียมการระบบ เทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ โดยมีแนวทางปฏิบัติดังนี้

๓.๓.๑ มีแผนการปฏิบัติงานสำหรับผู้ใช้งานที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอก หรือจากระยะไกล

๓.๓.๒ ผู้ใช้งานระบบจากระยะไกล ได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานอย่างเป็นทางการ ผู้ใช้งานต้องใช้งานตามขั้นตอนและตามระยะเวลาที่กำหนดไว้

๓.๓.๓ ผู้ใช้งานที่ต้องการยกเลิกการปฏิบัติงานจากระยะไกล ต้องคืนอุปกรณ์ที่ใช้งาน

๓.๓.๔ ผู้ใช้งานระบบจากระยะไกลทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๓.๓.๕ ระบุข้อกำหนดเฉพาะสำหรับการปฏิบัติงานจากระยะไกล ดังนี้

๓.๓.๕.๑ ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล

๓.๓.๕.๒ ระบบงานหรือบริการต่างๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล

๓.๓.๕.๓ ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน

๓.๓.๕.๔ ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

๓.๓.๖ ทำการป้องกันข้อมูลสำหรับการสื่อสารระหว่างสถานที่ที่จะมีการปฏิบัติงานระยะไกลกับระบบงาน ต่างๆ ภายในองค์กร

๓.๓.๗ ควบคุมการใช้งานเครือข่ายจากบ้านเพื่อเข้าสู่ระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกล เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๓.๘ ติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็นในอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร

๓.๓.๙ ผู้ดูแลระบบงานทำการทบทวนสิทธิของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๓.๓.๑๐ สำหรับผู้ใช้งานทั่วไปเข้าใช้งานระบบงานทั่วไปให้ผ่านระบบ Extranet ที่จัดไว้ให้เท่านั้น โดยจะสามารถเข้าใช้ระบบงานผ่านระบบ VPN (Virtual Private Network) ของ องค์กร ซึ่งได้รับการอนุมัติจากผู้บังคับบัญชา และเข้าใช้งานได้เฉพาะระบบงานที่มีความจำเป็นกับหน้าที่ของ ผู้ใช้งานนั้นๆ เท่านั้น

๓.๔ สำหรับผู้ดูแลระบบงาน (System Administrator) ใช้อุปกรณ์ Security Token Key เพื่อเข้าใช้งาน ในระดับผู้ดูแล กรณีที่ต้องตรวจสอบหรือแก้ไขค่า Configuration จากระยะไกล

หมวด ๑๒
การทำให้ระบบมีความแข็งแกร่ง
(System Hardening)

๑. วัตถุประสงค์

เพื่อกำหนดแนวทางการตั้งค่าระบบให้มีความแข็งแกร่ง เพื่อช่วยลดความเสี่ยงจากการถูกโจมตี ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลหรือระบบได้ง่ายและช่วยให้ระบบทำงานได้อย่างมั่นคงปลอดภัย เป็นไปตามแนวทางของมาตรฐานด้านความมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ดูแลระบบเครือข่าย

๓. แนวปฏิบัติ

๓.๑ คณะทำงานฯ กำหนดให้ผู้ดูแลระบบงาน/ผู้ดูแลระบบเครือข่าย กำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) โดยมาตรฐานตามการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

๓.๑.๑ สิทธิในการเข้าถึงน้อยที่สุด (Least Access Privilege) เช่น บัญชีผู้ใช้ทุกประเภท ต้องได้รับสิทธิ์ขั้นต่ำสุดที่จำเป็นต่อหน้าที่ ห้ามใช้บัญชี Administrator หรือ Root สำหรับงานทั่วไป มีการบันทึกและอนุมัติการขอสิทธิ์พิเศษ (High Privilege User) เป็นกรณีชั่วคราวเท่านั้น

๓.๑.๒ การแบ่งแยกหน้าที่ (Separation of Duties) เช่น แยกบทบาทของผู้ดูแลระบบ ออกจากผู้พัฒนา ผู้ทดสอบ และผู้ตรวจสอบ ระบบควรมีการแบ่ง environment ชัดเจน เช่น Dev/Test/Production

๓.๑.๓ การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน ให้เป็นไปตามมาตรฐานของการประปานครหลวง

๓.๑.๔ การลบบัญชีที่ไม่ได้ใช้

๓.๑.๕ การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๓.๑.๖ การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งานโดยปิดพอร์ตที่ไม่จำเป็นผ่าน firewall หรือ system-level configuration ใช้หลักการ “Deny by default, Allow by exception

๓.๑.๗ การป้องกันมัลแวร์ (Malware) โดยการติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์อย่างสม่ำเสมอ เปิดใช้งาน Real-time Scanning และ Scheduled Scan เชื่อมต่อกับระบบ Threat Intelligence

๓.๑.๘ การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่าง ทันการณ์และเหมาะสม

๓.๒ ผู้ดูแลระบบงาน/ผู้ดูแลระบบเครือข่ายควรพิจารณาใช้เอกสารแนวทางจากแหล่งมาตรฐาน เช่น CIS Benchmarks, หรือ ข้อแนะนำจากผู้ผลิตหรือ ผู้ขาย ประกอบการจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย

๓.๓ ผู้ดูแลระบบงาน/ผู้ดูแลระบบเครือข่ายต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุง

๓.๔ ในโครงการจัดหาระบบงานหรือระบบเครือข่ายจากผู้ขายหรือผู้ให้บริการภายนอก ผู้ดูแลระบบงาน/ผู้ดูแลระบบเครือข่าย ต้องระบุในเอกสารขอบเขตงานส่งมอบให้ผู้ขายหรือผู้ให้บริการภายนอก ต้องนำเสนอมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของอุปกรณ์ที่จำการติดตั้งในโครงการให้เป็นไปตามแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ดีของ อุปกรณ์หรือระบบงานดังกล่าว

๓.๕ การตั้งค่าตามมาตรฐานขั้นต่ำหรือการปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ ต้องดำเนินการผ่านกระบวนการจัดการการเปลี่ยนแปลง (Change Management Process) IT.PCD.001

หมวด ๑๓
การประเมินช่องโหว่และการทดสอบระบบ
(Vulnerability Assessment and Penetration Testing)

๑. วัตถุประสงค์

เพื่อเป็นแนวทางในการประเมินและจัดการกับช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของบริการที่สำคัญขององค์กร รวมถึงการทดสอบเจาะระบบอย่างมีประสิทธิภาพ เพื่อระบุจุดอ่อน ลดความเสี่ยงจากการโจมตีทางไซเบอร์ เพื่อใช้เป็นข้อมูลในการวางแผนปรับปรุงระบบ และสนับสนุนการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. ผู้รับผิดขอบ

๒.๑ คณะกรรมการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๓ เจ้าของระบบงาน

๒.๔ ผู้ดูแลระบบงาน

๓. แนวปฏิบัติ

๓.๑ การประเมินช่องโหว่ (Vulnerability Assessment)เป็นกระบวนการในการตรวจสอบ วิเคราะห์และระบุจุดอ่อนหรือช่องโหว่ด้านความมั่นคงปลอดภัยในระบบสารสนเทศและไซเบอร์ โดยมีขั้นตอนดังนี้

๓.๑.๑ คณะทำงานฯ วางแผนการประเมินช่องโหว่ โดยระบุระบบงานที่อยู่ในขอบเขตการประเมิน ทั้งนี้ระบบของการประปานครหลวงนั้นจะต้องวางแผนให้ครอบคลุมระบบสารสนเทศที่สำคัญตามการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) และครอบคลุมส่วนต่าง ๆ ต่อไปนี้

๓.๑.๑.๑ การประเมินในส่วนของเครื่องคอมพิวเตอร์ (Host Security Assessment) ซึ่งประกอบไปด้วยระบบปฏิบัติการ (Operating System) และการให้บริการด้านเครือข่าย

๓.๑.๑.๒ การประเมินในส่วนของเครือข่าย (Network Security Assessment) ซึ่งประกอบไปด้วยอุปกรณ์ระบบเครือข่ายและอุปกรณ์ด้านความมั่นคงปลอดภัย

๓.๑.๑.๓ การตรวจสอบสถาปัตยกรรมของระบบสารสนเทศ (Architecture Security Assessment) เพื่อวิเคราะห์และประเมิน โครงสร้างภาพรวมของระบบสารสนเทศ ว่ามีการออกแบบที่สอดคล้องกับหลักความมั่นคงปลอดภัยทางไซเบอร์หรือไม่ โดยมุ่งเน้น

ไปที่การลดความเสี่ยงเชิงโครงสร้าง (Structural Risk) และความเปราะบาง (Systemic Weakness) ที่อาจนำไปสู่การโจมตีที่รุนแรงได้

๓.๑.๒ การประเมินช่องโหว่นี้ต้องวางแผนให้มีการดำเนินการอย่างน้อย ปีละ ๑ ครั้ง และ ในช่วงของการทำระบบใหม่เชื่อมต่อกับระบบหลัก หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเช่น การปรับปรุงระบบ หรือการเปลี่ยนเทคโนโลยี หรือเมื่อทราบข้อมูลภัยคุกคามใหม่ ๆ (Threat Intelligence) ที่อาจมีช่องโหว่ที่เกี่ยวข้องในระบบของการประปานครหลวง

๓.๒ การทดสอบเจาะระบบ (Penetration Testing) คือกระบวนการทดสอบความมั่นคงปลอดภัยของระบบ เพื่อค้นหาช่องโหว่หรือจุดอ่อนที่สามารถถูกใช้โจมตีจริงได้และประเมินความสามารถของระบบในการป้องกันและตรวจจับภัยคุกคาม โดยต้องดำเนินการดังนี้

๓.๒.๑ คณะทำงานฯ ทำการวางแผนการทดสอบเจาะระบบโดยกำหนดให้ดำเนินการในระบบที่มีความเสี่ยงสูงโดยเฉพาะระบบที่เชื่อมต่อกับอินเทอร์เน็ตต้องได้รับการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยขอบเขตของการทดสอบเจาะระบบนี้ครอบคลุมทั้ง ระบบงาน เครื่องคอมพิวเตอร์ และระบบเครือข่ายที่เกี่ยวข้อง

๓.๒.๒ การดำเนินการทดสอบเจาะระบบต้องวางแผนทำงานร่วมกับเจ้าของระบบ เพื่อหลีกเลี่ยงผลกระทบต่อระบบปฏิบัติงานจริง โดยต้องมีขั้นตอนการประเมินความเสี่ยง การขออนุมัติจากเจ้าของระบบและการควบคุมก่อนการดำเนินการดังนี้

๓.๒.๒.๑ การประเมินความเสี่ยงก่อนการทดสอบ โดยผู้ทดสอบ เจ้าของระบบและผู้ดูแลระบบงานต้องดำเนินการประเมินความเสี่ยงจากการทดสอบ โดยพิจารณา

- ความสำคัญของระบบและข้อมูลที่เกี่ยวข้อง
- ความเป็นไปได้ของผลกระทบต่อการให้บริการ
- ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์จากการเปิดเผยข้อมูล หรือการหยุดชะงักของบริการ
- ข้อกำหนดตามกฎหมายและข้อบังคับที่เกี่ยวข้อง

๓.๒.๒.๒ ขออนุมัติการทดสอบ โดยผู้ทดสอบต้องขออนุญาตทดสอบเจาะระบบจากเจ้าของระบบ ซึ่งต้องประกอบด้วยรายละเอียดดังนี้

- วัตถุประสงค์ของการทดสอบ
- ขอบเขตของระบบหรือทรัพยากรที่จะทดสอบ
- ช่วงเวลาที่ดำเนินการทดสอบ
- ผู้ให้บริการภายนอก (ชื่อบริษัท/ชื่อผู้เชี่ยวชาญ)
- แผนการควบคุมผลกระทบและแผนตอบสนองฉุกเฉินหากเกิดปัญหา

๓.๒.๒.๓ จัดทำเอกสารข้อตกลง (Rules of Engagement) ก่อนเริ่มการทดสอบ ต้องจัดทำและ ลงนามในเอกสาร “Rules of Engagement” ระหว่างเจ้าของระบบ และผู้ทดสอบ โดยต้องระบุเงื่อนไขต่อไปนี้ที่ชัดเจน

๓.๒.๒.๓.๑ ขอบเขตและวิธีการที่อนุญาตให้ใช้

๓.๒.๒.๓.๒ เวลาที่ทำการทดสอบ

๓.๒.๒.๓.๓ การแจ้งเตือนเหตุการณ์ผิดปกติ

๓.๒.๒.๓.๔ ข้อจำกัดด้านกฎหมาย เช่น ห้ามเข้าถึงข้อมูลส่วนบุคคล หรือข้อมูลสำคัญของลูกค้า

๓.๒.๒.๔ ผู้ดูแลเจ้าของระบบบวข้องต้องได้รับแจ้งล่วงหน้าก่อนเริ่มทดสอบ พร้อมทั้งเตรียมการรองรับผลกระทบที่อาจเกิดขึ้น

๓.๒.๒.๕ เอกสารทั้งหมดที่เกี่ยวข้องกับการอนุมัติและการทดสอบต้องจัดเก็บเป็นหลักฐานเพื่อการตรวจสอบ

๓.๒.๓ การทดสอบการเจาะระบบต้องดำเนินการโดยผู้เชี่ยวชาญที่มีใบรับรองความรู้ความสามารถอันเป็นที่ยอมรับ อาทิเช่น

- ประกาศนียบัตรการรับรองจากสถาบัน Council for Registered Ethical Security Testers (CREST) เช่น CREST Registered Penetration Tester, CREST Certified Web Application Tester, CREST Certified Infrastructure Tester
- ประกาศนียบัตรการรับรองจากสถาบัน Offensive Security เช่น Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), Offensive Security Certified Expert (OSCE), Offensive Security Exploitation Expert (OSEE) และ Offensive Security Web Expert (OSWE)
- ประกาศนียบัตรการรับรองจากสถาบัน Global Information Assurance Certification (GIAC) เช่น GIAC Certified Incident Handler (GCIH), GIAC Mobile Device Security Analyst (GMOB), GIAC penetration tester (GPEN), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC Assessing and Auditing Wireless Networks (GAWN) และ GIAC Web Application Penetration Tester (GWAPT)

๓.๓ หากเป็นการว่าจ้างผู้ให้บริการภายนอกเข้ามาดำเนินการประเมินช่องโหว่หรือทดสอบเจาะระบบ จะต้องดำเนินการตามแนวปฏิบัติด้านการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management) อย่างเคร่งครัด และต้องจัดให้มีการควบคุมดูแลการปฏิบัติที่เหมาะสม

๓.๔ ช่องโหว่หรือจุดอ่อนที่ตรวจพบทั้งจากการประเมินช่องโหว่หรือทดสอบเจาะระบบต้องมีการบริหารจัดการดังต่อไปนี้

๓.๔.๑ ช่องโหว่หรือจุดอ่อนที่ตรวจพบต้องถูกระบุความรุนแรงของช่องโหว่โดยอาจพิจารณาใช้ Common Vulnerability Scoring System (CVSS Score) ซึ่งเป็นระบบให้คะแนนความรุนแรงของช่องโหว่ทางความมั่นคงปลอดภัยไซเบอร์ โดยเป็นมาตรฐานกลางที่ใช้กันทั่วโลก เพื่อช่วยให้องค์กรสามารถประเมินความเสี่ยงและจัดลำดับความสำคัญในการจัดการช่องโหว่ได้อย่างมีประสิทธิภาพ โดย CVSS จะมีคะแนนตั้งแต่ 0.0 – 10.0 ดังนี้

คะแนน (Score)	**ระดับความรุนแรง (Severity Level)**
0.0	None (ไม่เป็นอันตราย)
0.1 – 3.9	Low (ความเสี่ยงต่ำ)
4.0 – 6.9	Medium (ความเสี่ยงปานกลาง)
7.0 – 8.9	High (ความเสี่ยงสูง)
9.0 – 10.0	Critical (ความเสี่ยงวิกฤต)

๓.๔.๒ วิเคราะห์ผลกระทบของช่องโหว่ที่ตรวจสอบตามบริบทขององค์กรและข้อมูลความเสี่ยงด้านอื่น ๆ ดังนี้

๓.๔.๒.๑ ระบบหรือข้อมูลที่ได้รับผลกระทบมีความสำคัญในระดับใด โดยพิจารณาจากข้อมูลการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) และการประเมินระดับความสำคัญของข้อมูลตามแนวปฏิบัติความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Data Security)

๓.๔.๒.๒ ช่องโหว่นั้นถูกเปิดเผยสู่ภายนอกหรือเชื่อมต่ออินเทอร์เน็ต หรือไม่

๓.๔.๒.๓ ช่องโหว่มีโค้ดหรือเครื่องมือสาธารณะที่สามารถใช้ในการโจมตี (Exploit Available) หรือไม่

๓.๔.๒.๔ มีการตรวจพบว่ามี การโจมตีเกิดขึ้นในองค์กรอื่นแล้วหรือยัง (Threat Intelligence)

๓.๔.๓ จากข้อมูล CVSS และวิเคราะห์ผลกระทบของช่องโหว่ที่ตรวจสอบตามบริบทขององค์กรและข้อมูลความเสี่ยงด้านอื่น ๆ ให้ดำเนินการประเมินความเสี่ยงตามแนวทางที่กำหนดไว้ในแนวปฏิบัติการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information Security and Cybersecurity Risk Assessment) เพื่อพิจารณาถึงโอกาสที่จะถูกโจมตีและผลกระทบ และจัดลำดับความสำคัญของช่องโหว่ที่ตรวจพบเพื่อวางแผนการแก้ไข ปิดช่องโหว่ดังกล่าว

๓.๔.๔ จัดทำแผนการแก้ไขช่องโหว่โดยระบุแนวทางการแก้ไข ผู้รับผิดชอบและระยะเวลา รวมถึงกำหนดให้มีการทดสอบซ้ำเพื่อยืนยันการปิดช่องโหว่ ทั้งนี้หากไม่สามารถแก้ไขช่องโหว่ได้โดยตรงหรือไม่สามารถดำเนินการได้ตามเวลา ผู้ดูแล/ผู้ปฏิบัติงานที่ได้รับมอบหมาย ต้องกำหนดแผนการควบคุมทดแทนที่สามารถบริหารความเสี่ยงได้

๓.๔.๕ จัดทำรายงานการประเมินช่องโหว่หรือทดสอบเจาะระบบ โดยต้องประกอบไปด้วย

๓.๔.๕.๑ รายละเอียดระบบที่ทดสอบ

๓.๔.๕.๒ เทคนิคที่ใช้ในการทดสอบ

๓.๔.๕.๓ รายการช่องโหว่ที่พบ พร้อมระดับความรุนแรง

๓.๔.๕.๔ ข้อเสนอแนะในการแก้ไข

๓.๔.๕.๕ แผนการดำเนินการแก้ไขหรือแผนการควบคุมทดแทนที่สามารถบริหารความเสี่ยงได้

๓.๔.๕.๖ ผลการทดสอบซ้ำ (ถ้ามี)

๓.๕ คณะทำงานฯ ต้องติดตามผลการจัดการช่องโหว่และรายงานต่อ คณะกรรมการฯ เพื่อทราบถึงรายงานถึงผลการประเมินช่องโหว่หรือทดสอบเจาะระบบและการจัดการ

๓.๖ หากได้รับการร้องขอจาก คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม). หรือ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) การประปานครหลวงต้องส่งสำเนารายงานสรุปผลการทดสอบการเจาะระบบ ไปยัง สกมช. ในกำหนด ๓๐ วัน นับแต่วันที่ได้รับหนังสือด้วย

หมวด ๑๔
การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and Environmental Control)

๑. วัตถุประสงค์

เพื่อสร้างแนวทางและมาตรการที่ชัดเจนในการควบคุมและป้องกันความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ อาคารสถานที่ อุปกรณ์ฮาร์ดแวร์ เซิร์ฟเวอร์ ระบบเครือข่าย และทรัพย์สินทางเทคโนโลยีสารสนเทศอื่น ๆ ของการประปานครหลวง ไม่ให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงหรือใช้งานได้ทางกายภาพ (Physical Access) รวมถึงการป้องกันภัยจากสิ่งแวดล้อม เช่น ไฟไหม้ ไฟฟ้าดับ แผ่นดินไหว อุณหภูมิที่สูงเกินไป หรือความชื้นที่ไม่เหมาะสม ซึ่งอาจทำให้เกิดความเสียหายต่ออุปกรณ์หรือระบบงานสำคัญของการประปานครหลวงและส่งผลต่อความมั่นคงปลอดภัยและความต่อเนื่องในการดำเนินธุรกิจ

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ดูแลระบบเครือข่าย

๒.๔ ผู้ดูแลศูนย์คอมพิวเตอร์

๓. แนวปฏิบัติ

๓.๑ คณะทำงานฯ ผู้ดูแลระบบงาน ผู้ดูแลระบบเครือข่าย และผู้ดูแลศูนย์คอมพิวเตอร์ ต้องจัดให้มีมาตรการรักษาความมั่นคงทางกายภาพ (Physical Security) ดังนี้

๓.๑.๑ กำหนดเขตพื้นที่อย่างชัดเจน พร้อมติดตั้งสิ่งกีดขวาง เช่น รั้ว ผนัง หรือประตูรั้ว เพื่อป้องกันการบุกรุกจากบุคคลภายนอก อาจมีระบบประตูอัตโนมัติหรือจุดตรวจเพื่อควบคุมการเข้าออกพื้นที่

๓.๑.๒ กำหนดให้มีระบบควบคุมการเข้าออก เช่น บัตรพนักงาน, เครื่องสแกนลายนิ้วมือ หรือสแกนใบหน้า เพื่อให้เฉพาะบุคคลที่ได้รับอนุญาตสามารถเข้าถึงพื้นที่ที่มีข้อมูลหรืออุปกรณ์สำคัญได้ และต้องกำหนดสิทธิ์การเข้าแต่ละพื้นที่ตามหน้าที่รับผิดชอบของบุคลากร

๓.๑.๓ กำหนดพื้นที่ที่มีความสำคัญสูง เช่น ห้องควบคุมระบบ ห้องเซิร์ฟเวอร์ หรือพื้นที่ที่เก็บข้อมูลสำคัญ ให้มีระบบควบคุมเฉพาะและการควบคุมการเข้าถึงที่เข้มงวดกว่าพื้นที่ทั่วไป

๓.๑.๔ กำนดให้มีระบบกล้องวงจรปิด (CCTV) และระบบสัญญาณเตือนภัยในจุดสำคัญ เพื่อบันทึกและตรวจสอบเหตุการณ์ย้อนหลัง

๓.๑.๕ ติดตั้งอุปกรณ์ให้มั่นคง แข็งแรง และอยู่ในตำแหน่งที่ปลอดภัย เช่น การติดตั้งเครื่องเซิร์ฟเวอร์ หรืออุปกรณ์เครือข่ายกับตู้แร็ค รวมถึงการจัดเก็บอุปกรณ์ที่ไม่ได้ใช้งานไว้ในที่ปลอดภัย

๓.๒ คณะทำงานฯ ผู้ดูแลระบบงาน ผู้ดูแลระบบเครือข่าย และผู้ดูแลศูนย์คอมพิวเตอร์ ต้องจัดให้มีมาตรการรักษาความมั่นคงด้านสิ่งแวดล้อม (Environmental Control) สำหรับระบบเทคโนโลยีสารสนเทศดังนี้

๓.๒.๑ ติดตั้งระบบไฟฟ้าสำรอง เช่น เครื่องสำรองไฟฟ้า (UPS) เพื่อให้ระบบสารสนเทศสามารถทำงานต่อได้อย่างต่อเนื่องในกรณีเกิดไฟฟ้าดับ ลดความเสี่ยงที่ระบบจะไม่สามารถทำงานได้ หรือข้อมูลเสียหายจากการตัดไฟกะทันหัน

๓.๒.๒ ติดตั้งอุปกรณ์ตรวจจับควันและความร้อน เช่น เครื่องตรวจจับควัน และอุปกรณ์ดับเพลิงอัตโนมัติภายในห้องที่มีอุปกรณ์เทคโนโลยีสารสนเทศ โดยเลือกชนิดของสารดับเพลิงให้เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์

๓.๒.๓ ประสานงานกับกองอาคารในการกำหนดให้มีเครื่องดับเพลิงแบบมือถือประจำแต่ละจุด และจัดฝึกซ้อมอพยพหนีไฟเป็นประจำ

๓.๒.๔ ห้องที่ติดตั้งอุปกรณ์คอมพิวเตอร์สำคัญควรมีระบบควบคุมอุณหภูมิและความชื้นให้คงที่อยู่ในระดับที่ปลอดภัยต่อการทำงานของอุปกรณ์ เพื่อป้องกันความร้อนสะสมเกินกว่าที่อุปกรณ์จะรับได้ และลดโอกาสเกิดการกัดกร่อนจากความชื้น

๓.๒.๕ พิจารณาติดตั้งระบบตรวจจับน้ำรั่วในบริเวณที่มีความเสี่ยง เช่น ใต้พื้นห้องเซิร์ฟเวอร์ ห้องเครื่อง หรือใกล้ท่อน้ำ พร้อมทั้งยกระดับอุปกรณ์สำคัญให้อยู่สูงจากพื้น เพื่อป้องกันความเสียหายกรณีน้ำรั่ว

๓.๒.๖ ใช้ระบบตรวจสอบและบันทึกสภาพแวดล้อม เช่น อุณหภูมิ ความชื้น หรือสภาพอากาศภายในห้องควบคุมหรือห้องอุปกรณ์ เพื่อให้สามารถแจ้งเตือนเมื่อมีค่าผิดปกติและดำเนินการแก้ไขได้ทันที

หมวด ๑๕
การควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์และพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์
(Data Center and Secure Area Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกัน มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมเข้า-ออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความ จำเป็นต้องเข้า-ออกศูนย์คอมพิวเตอร์และพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ดูแลระบบเครือข่าย

๒.๔ ผู้ดูแลศูนย์คอมพิวเตอร์

๒.๕ ผู้ดูแลพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์

๓. แนวปฏิบัติ

๓.๑ คณะทำงานฯ ต้องกำหนดให้ศูนย์คอมพิวเตอร์ ห้องคอมพิวเตอร์ของสำนักงานประปาสาขาและพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์ที่สำคัญ ทำการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) เพื่อควบคุมการเข้าออก โดยใช้เทคโนโลยีระบบ Biometric Finger Scan หรือ การใช้รหัสผ่านตัวเลข (PIN Code) และ Key Card รวถึงมีการติดตั้งระบบกล้องวงจรปิดเพื่อเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้น

๓.๒ ผู้ปฏิบัติงานในพื้นที่ต้องมีบัตรผ่าน (Key Card) และ/หรือ การพิสูจน์ตัวตนด้วยลายนิ้วมือ (Finger Scan) หรือ ภาพใบหน้า (Facial Scan) เพื่อใช้ในควบคุมการเข้า – ออกศูนย์คอมพิวเตอร์ หรือพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์

๓.๓ ระบุสิทธิเฉพาะผู้ปฏิบัติงานที่มีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ประกอบด้วย

๓.๓.๑ จัดทำ “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๓.๓.๒ ระบุผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้า-ออก” ระบุผู้ปฏิบัติงานทำหน้าที่ตรวจสอบประวัติการเข้า-ออก ศูนย์คอมพิวเตอร์

หรือพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์เป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ ปีละ ๑ ครั้ง เป็นอย่างน้อย

๓.๔ ผู้ดูแลพื้นที่ ซึ่งหมายถึงผู้ดูแลศูนย์คอมพิวเตอร์หรือผู้ดูแลพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์ มีแนวทางปฏิบัติ ดังนี้

๓.๔.๑ ผู้ดูแลพื้นที่จัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วน โดยแบ่งส่วนระบบ เครือข่าย (Network Zone) และส่วนเครื่องแม่ข่าย (Server Zone) เพื่อสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากยิ่งขึ้น

๓.๔.๒ ผู้ดูแลพื้นที่ ทำการระบุสิทธิบุคคลในการเข้า-ออกศูนย์คอมพิวเตอร์ โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่” ไม่ว่าจะเป็นผู้ปฏิบัติงานด้านคอมพิวเตอร์ Computer Operator) ผู้ดูแลระบบ (System Administrator) ผู้ดูแลระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ (Network and Security Administrator)

๓.๔.๓ สิทธิในการเข้า-ออกศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ ของผู้ปฏิบัติงานแต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงาน

๓.๔.๔ ผู้ปฏิบัติงานทุกคนต้องได้รับอนุญาตทำบัตรผ่าน (Key Card) และการพิสูจน์ตัวตนด้วยลายนิ้วมือ (Finger Scan) หรือ ภาพใบหน้า (Facial Scan) เพื่อใช้ในการเข้า-ออกศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ

๓.๔.๕ จัดทำระบบเก็บบันทึกการเข้า-ออกศูนย์คอมพิวเตอร์ตามกระบวนการที่ระบุไว้ใน เอกสาร “บันทึกการเข้า-ออก”

๓.๔.๖ กรณีผู้ปฏิบัติงานที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นเข้า-ออกศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์ต้องได้รับอนุญาตและมีการควบคุมอย่างรัดกุม

๓.๔.๗ การเข้าถึงศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์ มีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออก” และ ตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า-ออกทุกคน กรอกแบบฟอร์มดังกล่าวให้ครบถ้วน

๓.๔.๘ กรณีผู้ติดต่อจากหน่วยงานภายนอก ที่มาปฏิบัติงานในศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์จะต้องลงชื่อในแบบฟอร์มขอเข้าปฏิบัติงานและต้องบันทึกลงในแบบฟอร์มบันทึกเข้า-ออกศูนย์คอมพิวเตอร์ ผู้ปฏิบัติงานที่รับผิดชอบจะเป็นผู้นำพาเข้าไปและคอยควบคุมกำกับดูแลตลอดการปฏิบัติงาน

๓.๕ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๓.๕.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกอาคาร” ทุกครั้งก่อนเข้าอาคาร

๓.๕.๒ ผู้ติดต่อจากหน่วยงานภายนอกต้องติดต่อผู้ปฏิบัติงานที่รับผิดชอบเพื่อลงชื่อตามแบบฟอร์มการขอเข้า-ออก เพื่อปฏิบัติงานในศูนย์คอมพิวเตอร์และรับบัตรการผ่านเข้า-ออกบริเวณพื้นที่ศูนย์คอมพิวเตอร์กับผู้ดูแลพื้นที่

๓.๕.๓ กรณีที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้ามาภายในศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มขอเข้าปฏิบัติงานให้ถูกต้องชัดเจน

๓.๕.๔ ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลา ที่อยู่ในศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ

๓.๕.๕ สามารถเข้าพื้นที่ได้ตามที่ระบุไว้ในแบบฟอร์มขอเข้าปฏิบัติงานในศูนย์คอมพิวเตอร์หรือพื้นที่ติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศและจะต้องมีผู้ปฏิบัติงานภายในคอยควบคุมดูแลตลอดเวลา

๓.๕.๖ ต้องคืนบัตรผู้ติดต่อกับผู้ดูแล เมื่อปฏิบัติงานภายในศูนย์คอมพิวเตอร์เสร็จแล้วและผู้ดูแลตรวจสอบการคืนบัตร และตรวจสอบบันทึกเข้า-ออก

๓.๕.๗ ผู้ดูแลพื้นที่ตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มขอเข้าปฏิบัติงานและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

๓.๕.๘ ผู้ปฏิบัติงานตรวจสอบความถูกต้องของข้อมูลในแบบฟอร์มบันทึกเข้า-ออก และแบบฟอร์มขอเข้าปฏิบัติงานกับผู้ดูพื้นที่แลทุกครั้ง

๓.๕.๙ เมื่อปฏิบัติงานภายในอาคารเสร็จแล้วต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย แล้วทำการลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกอาคาร”

๓.๖ ในกรณีที่มีการใช้บริการจากผู้ให้บริการภายนอกสำหรับให้บริการศูนย์คอมพิวเตอร์และพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์ หน่วยงานที่ทำการจัดจ้างต้องตรวจสอบให้มั่นใจว่าผู้ให้บริการภายนอก มีการควบคุมด้านความมั่นคงปลอดภัยเชิงกายภาพและมีวิธีปฏิบัติในการควบคุมการเข้าถึงสอดคล้องกับแนวปฏิบัตินี้ และการคัดเลือก การเริ่มใช้บริการ การควบคุมระหว่างการใช้บริการจนถึงภายหลังการเสร็จสิ้นสัญญาการใช้บริการ ต้องเป็นไปตามแนวปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

หมวด ๑๖
การเข้ารหัสข้อมูลสารสนเทศ
(Cryptography)

๑. วัตถุประสงค์

เพื่อให้มีการเข้ารหัสข้อมูลสารสนเทศอย่างเหมาะสม มีประสิทธิผลในการป้องกันข้อมูลชั้นความลับ การปลอมแปลง หรือความถูกต้องของข้อมูลสารสนเทศ ไม่ให้มีการรั่วไหลออกไปสู่บุคคลภายนอกที่ไม่ได้เกี่ยวข้องหรือมีสิทธิในการเข้าถึงข้อมูล

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบงาน

๒.๒ ผู้ใช้งาน

๒.๓ เจ้าของระบบงาน

๓. แนวปฏิบัติ

๓.๑ มาตรการการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

๓.๑.๑ ในการจัดเก็บข้อมูล ผู้ดูแลระบบงานต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานสากลที่ไม่มีความเสี่ยงในระดับกลางถึงระดับสูง โดยเทียบเคียงกับมาตรฐาน NIST SP 800-171 encryption และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศเพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

๓.๑.๒ ต้องใช้เฉพาะ เทคโนโลยีและอัลกอริธึมการเข้ารหัสที่ได้รับอนุมัติ เท่านั้น

๓.๑.๓ ห้ามใช้อัลกอริธึมหรือเทคโนโลยีที่ล้าสมัยหรือไม่ปลอดภัยโดยเด็ดขาด

๓.๑.๔ การเข้ารหัสข้อมูลต้องสอดคล้องกับกฎหมายและข้อบังคับที่เกี่ยวข้อง (เช่น PDPA, GDPR, PCI DSS)

๓.๑.๕ เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานของคีย์ที่เข้ารหัสในทุก ๆ ปีเพื่อให้สอดคล้องกับความปลอดภัยและประสิทธิภาพของการดำเนิน

๓.๑.๖ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ องค์กรมีช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยให้เข้าถึงผ่านระบบเครือข่ายภายในเท่านั้น และมีการตรวจสอบการผ่านเข้า ออกพื้นที่ควบคุม (Restriction Area Access Control) และมีเครือข่ายเฉพาะ (VLAN) สำหรับ Outsource

๓.๒ เทคโนโลยีและอัลกอริธึมที่ได้รับอนุมัติ

๓.๒.๑ ข้อมูลขณะจัดเก็บ (Data at Rest)

๓.๒.๑.๑ ใช้ AES (Advanced Encryption Standard) ที่มีขนาดกุญแจ 256 บิต (ขั้นต่ำ 128 บิต)

๓.๒.๑.๒ สำหรับการลงลายมือชื่อดิจิทัล อนุญาตให้ใช้ RSA ที่มีขนาดกุญแจ 2048 บิต หรือสูงกว่า

๓.๒.๑.๓ ใช้โซลูชันการเข้ารหัสระดับไฟล์หรือดิสก์ เช่น BitLocker, LUKS, dm-crypt, Veracrypt ตามแนวปฏิบัติที่ดีที่สุดของผู้ผลิต

๓.๒.๒ ข้อมูลขณะส่งผ่าน (Data in Motion)

๓.๒.๒.๑ ใช้ TLS (Transport Layer Security) เวอร์ชัน 1.3 เป็นหลัก หรือ 1.2 (ในกรณีที่ยังจำเป็น)

๓.๒.๒.๒ เว็บไซต์หรือเว็บแอปพลิเคชันต้องใช้ HTTPS ที่มีการบังคับใช้ TLS เวอร์ชันดังกล่าว

๓.๒.๒.๓ VPN ต้องใช้ IPsec หรือ SSL VPN ที่มี AES-256 พร้อม SHA-2 HMAC

๓.๒.๒.๔ สำหรับอีเมลที่ต้องเข้ารหัส ใช้ S/MIME หรือ PGP โดยใช้ RSA-2048 หรือ ECC P-256

๓.๒.๓ ข้อมูลขณะประมวลผล (Data in Use)

๓.๒.๓.๑ ใช้การ ปกปิดข้อมูล (Data Masking) ระดับแอปพลิเคชันตามการจัดประเภทข้อมูล

๓.๒.๓.๒ สำหรับการจัดการข้อมูลที่สำคัญ ใช้เทคนิค Tokenization ที่ปลอดภัยและสอดคล้องกับมาตรฐาน (เช่น NIST SP 800-38G)

๓.๓ การบริหารจัดการกุญแจ (Key Management)

๓.๓.๑ ข้อมูลที่มีการเข้ารหัสต้องจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพโดยการดำเนินการเกี่ยวกับกุญแจทุกประเภท เช่น การสร้าง การจัดเก็บ การจัดส่งและการเปลี่ยนควรกระทำอย่างปลอดภัยและมีการควบคุมที่เหมาะสม

๓.๓.๒ กุญแจส่วนตัวที่ใช้ในการเข้ารหัสข้อมูลต้องถูกจัดเก็บให้เป็นความลับและจัดเก็บอย่างมั่นคงปลอดภัยเสมอ

๓.๓.๓ การส่งกุญแจถึงผู้รับกุญแจต้องส่งผ่านในช่องทางที่มีความมั่นคงปลอดภัยเสมอ

๓.๓.๔ กุญแจต้องได้รับการเพิกถอนทันทีเมื่อทราบว่ากุญแจมีความเสี่ยงที่จะก่อให้เกิดการล่วงละเมิดทางด้านความมั่นคงปลอดภัย เช่น เมื่อกุญแจส่วนตัว (private key) รั่วไหลไปยังบุคคลอื่น เป็นต้น

๓.๓.๕ การเพิกถอนการใช้งานกุญแจต้องมีการแจ้งให้ผู้เกี่ยวข้องกับกุญแจหรือผู้ที่ใช้งานกุญแจทราบ โดยต้องรวมถึงรหัสกุญแจเหตุผลของการเพิกถอนวันที่และเวลาที่กุญแจถูกเพิกถอน

๓.๓.๖ การทำ Archive กุญแจเมื่อไม่มีการใช้งานกุญแจเป็นระยะเวลานาน ต้องใช้วิธีการ Archive ที่มีความมั่นคงปลอดภัยโดยต้องมีการเข้ารหัสกุญแจที่ถูก Archive ด้วยเสมอ

๓.๓.๗ การทำลายกุญแจต้องทำด้วยความระมัดระวังเป็นพิเศษโดยต้องทำลายด้วยวิธีการทำลายกุญแจแบบมั่นคงปลอดภัย (Secure Deletion) และต้องแน่ใจว่ากุญแจนั้นจะไม่มีความต้องการในการใช้งานถอดรหัสข้อมูลอีกในอนาคต

๓.๓.๘ การกระทำใด ๆ ที่เกี่ยวข้องกับกุญแจต้องได้รับการจัดเก็บบันทึกอย่างมั่นคงปลอดภัยเสมอเพื่อให้สามารถตรวจสอบได้ภายหลัง

๓.๔ ห้ามใช้อัลกอริธึมดังต่อไปนี้ในการเข้ารหัส

๓.๔.๑ DES, 3DES (Triple DES)

๓.๔.๒ MD5, SHA-1 (ยกเว้นกรณีจำเป็นต่อการรองรับระบบภายนอก)

๓.๔.๓ SSL ทุกเวอร์ชัน และ TLS 1.0 / 1.1

๓.๔.๔ RC4, RC2, Blowfish และอัลกอริธึมที่พัฒนาขึ้นเองโดยไม่ได้รับการตรวจสอบความปลอดภัย

๓.๕ มีวิธีการในการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัสข้อมูล ดังนี้

๓.๕.๑ การสร้างและจัดเก็บกุญแจ

๓.๕.๑.๑ กุญแจต้องถูกสร้างโดยอุปกรณ์หรือระบบที่มีความปลอดภัย เช่น Hardware Security Module (HSM) หรือระบบที่ได้รับการรับรองมาตรฐาน

๓.๕.๑.๒ กุญแจต้องถูกจัดเก็บในรูปแบบที่เข้ารหัสและมีระบบควบคุมการเข้าถึงที่เหมาะสม

๓.๕.๑.๓ ห้ามจัดเก็บกุญแจร่วมกับข้อมูลที่ถูกเข้ารหัสในสถานที่เดียวกันโดยไม่มีมาตรการแยกส่วนที่ชัดเจน

๓.๕.๒ การแจกจ่ายและใช้งานกุญแจ

๓.๕.๒.๑ การแจกจ่ายกุญแจต้องดำเนินการผ่านช่องทางที่ปลอดภัย เช่น การใช้ช่องทางที่เข้ารหัส หรือการส่งมอบผ่าน HSM

๓.๕.๒.๒ บุคคลที่ได้รับสิทธิ์ในการใช้งานกุญแจต้องผ่านการรับรองตัวตนที่เหมาะสม และได้รับอนุญาตอย่างชัดเจน

๓.๕.๒.๓ การใช้งานกุญแจต้องเป็นไปตามวัตถุประสงค์ที่กำหนดไว้เท่านั้น ห้ามนำไปใช้ผิดวัตถุประสงค์

๓.๕.๓ การเปลี่ยนและทำลายกุญแจ

๓.๕.๓.๑ กำหนดรอบระยะเวลาการเปลี่ยนกุญแจตามระดับความเสี่ยงและมาตรฐานที่เกี่ยวข้อง เช่น ทุก 1 ปี หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

๓.๕.๓.๒ กุญแจที่หมดอายุหรือไม่ได้ใช้งานต้องถูกทำลายอย่างปลอดภัย โดยใช้วิธีที่ไม่สามารถกู้คืนได้ เช่น การลบทิ้งจาก HSM หรือการใช้ซอฟต์แวร์ทำลายข้อมูล

๓.๕.๔ วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้ เสียหาย

๓.๕.๔.๑ การสำรองกุญแจ (Key Backup)

๓.๕.๔.๑.๑ ต้องมีการสำรองกุญแจเข้ารหัสที่สำคัญไว้ในรูปแบบที่ปลอดภัย เช่น การจัดเก็บใน Hardware Security Module (HSM) หรืออุปกรณ์จัดเก็บกุญแจที่ได้รับการรับรองมาตรฐาน

๓.๕.๔.๑.๒ การสำรองกุญแจต้องดำเนินการโดยบุคคลที่ได้รับมอบหมายและมีอำนาจเท่านั้น (Key Custodian)

๓.๕.๔.๑.๓ กุญแจสำรองต้องได้รับการป้องกันด้วยมาตรการควบคุมการเข้าถึงที่เข้มงวด และต้องเข้ารหัสเพิ่มเติมหากจัดเก็บในรูปแบบดิจิทัล

๓.๕.๔.๒ การกู้คืนกุญแจจากข้อมูลสำรอง

๓.๕.๔.๒.๑ ในกรณีที่กุญแจหลักสูญหายหรือเสียหาย ให้ดำเนินการกู้คืนกุญแจจากชุดสำรองโดยคณะทำงานฯ เป็นผู้อนุมัติ

๓.๕.๔.๒.๒ กระบวนการกู้คืนต้องดำเนินการในสภาพแวดล้อมที่ปลอดภัย เช่น ภายในห้อง Data Center ที่ควบคุมการเข้าถึง

๓.๕.๔.๒.๓ ต้องมีการบันทึกหลักฐานการกู้คืนกุญแจอย่างครบถ้วน เช่น วันเวลา ผู้ดำเนินการ และเหตุผลในการกู้คืน

๓.๕.๔.๓ การกู้คืนข้อมูลกรณีไม่สามารถกู้คืนกุญแจได้

หากไม่สามารถกู้คืนกุญแจจากชุดสำรองได้ องค์กรต้องดำเนินการดังนี้

๓.๕.๔.๓.๑ ตรวจสอบว่ามีข้อมูลต้นฉบับ (Unencrypted Data) ที่ไม่ได้เข้ารหัสหรือข้อมูลสำรองที่ไม่ได้เข้ารหัสหรือไม่

๓.๕.๔.๓.๒ หากมีข้อมูลสำรอง ให้ทำการกู้คืนข้อมูลจากชุดสำรองดังกล่าว

๓.๕.๔.๓.๓ หากไม่มีข้อมูลสำรองหรือข้อมูลต้นฉบับ องค์กรต้องยอมรับว่าข้อมูลที่ถูกเข้ารหัสจะไม่สามารถกู้คืนได้ และดำเนินการตามแผนบริหารเหตุการณ์และแผนรองรับเหตุการณ์ที่เกี่ยวข้อง เช่น แจ้งผู้มีส่วนได้เสียและดำเนินการตามข้อกำหนดทางกฎหมาย

หมวด ๑๗

การสำรองและกู้คืนข้อมูล

(Backup and Recovery)

๑. วัตถุประสงค์

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุก รุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่สูญหายหรือถูกแก้ไขอย่างไม่ถูกต้องกลับมาใช้งานได้

๒. ผู้ที่รับผิดชอบ

๒.๑ เจ้าของข้อมูล

๒.๒ ผู้ดูแลระบบงาน

๒.๓ คณะทำงานความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓. แนวปฏิบัติ

๓.๑ ผู้ดูแลระบบงานจะต้องกำหนดแนวทางการจัดทำระบบสำรองข้อมูลที่ ชัดเจนเพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้อยู่เสมอ โดยมีวิธีปฏิบัติ ดังนี้

๓.๑.๑ เจ้าของข้อมูล และผู้ดูแลระบบงานระบุหน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน ซึ่งดูแลรับผิดชอบในการสำรองข้อมูล

๓.๑.๒ ผู้ดูแลระบบงานจัดให้มีการสำรองและกำหนแนวทางการทดสอบหรือยืนยันความถูกต้องสมบูรณ์ของข้อมูลที่สำรองเก็บไว้

๓.๑.๓ ผู้ดูแลระบบงาน/ผู้ปฏิบัติงานที่ได้รับมอบหมายหารือกับเจ้าของข้อมูลเพื่อระบุข้อมูลที่จำเป็นต้องจัดทำระบบสำรองและลักษณะความต้องการการสำรองข้อมูล อันประกอบไปด้วยข้อมูลเหล่านี้ เป็นต้น

๓.๑.๓.๑ ผลการประเมินลักษณะของข้อมูลตาม แนวปฏิบัติเรื่องความมั่นคงปลอดภัยของข้อมูล (Data Security) ในส่วนของระดับความพร้อมใช้

๓.๑.๓.๒ Recovery Point Objective (RPO) หรือ ระยะเวลาสูงสุดของข้อมูลที่สามารถยอมรับการสูญหายได้ในกรณีที่เกิดเหตุการณ์ที่ทำให้ระบบหยุดชะงักหรือข้อมูลสูญหาย

๓.๑.๓.๓ Recovery Time Objective (RTO) หรือระยะเวลาสูงสุดที่ยอมให้ระบบหยุดชะงักก่อนที่จะต้องกลับมาให้บริการได้ตามปกติ

๓.๑.๓.๔ ส่วนประกอบข้อมูลที่ต้องการให้สำรอง เช่น การสำรองข้อมูลระบบงาน ต้องประกอบไปด้วย ฐานข้อมูล ไฟล์เอกสาร การตั้งค่าของระบบงาน ข้อมูลอ้างอิงของระบบงาน (Master Data) หรือ Virtual Machine Image

๓.๑.๓.๕ ปริมาณของข้อมูลที่ต้องการสำรอง

๓.๑.๓.๖ ลักษณะการสำรองข้อมูลเช่น เป็นแบบ Snapshot หรือเก็บแบบ Increament

๓.๑.๓.๗ ระยะเวลาการเก็บข้อมูลสำรอง

๓.๑.๓.๘ ต้องมีการเข้ารหัสข้อมูลที่สำรองไว้หรือไม่

๓.๑.๓.๙ ความต้องการในการทดสอบข้อมูล

๓.๑.๔ ผู้ดูแลระบบงาน ออกแบบระบบและกำหนดขั้นตอนการสำรองข้อมูลตามความต้องการของเจ้าของข้อมูล ที่ได้มีการหารือตกลงกัน โดยจัดทำแผนการสำรองที่สอดคล้องกับความต้องการของหน่วยงานเจ้าของระบบงานโดยจะระบุ ข้อมูลดังนี้

๓.๑.๔.๑ ระบบงานและระบบข้อมูลสารสนเทศที่จะทำสำรอง

๓.๑.๔.๒ เวลาเริ่มต้นและระยะเวลาในการทำสำรองระบบข้อมูลแต่ละระบบงาน

๓.๑.๔.๓ ความถี่ในการสำรองระบบข้อมูล

๓.๑.๔.๔ ระยะเวลาที่ต้องการจัดเก็บของข้อมูลสารสนเทศแต่ละระบบ

๓.๑.๔.๕ ลักษณะของการสำรองข้อมูล

๓.๑.๔.๖ สถานที่เก็บข้อมูลสำรอง

๓.๑.๔.๗ เงื่อนไขและข้อจำกัดต่าง ๆ

๓.๑.๔.๘ กำหนดสื่อที่ใช้ในการสำรองระบบข้อมูลสารสนเทศ จัดทำสารบบสำหรับเทปหรือดิสก์ที่จัดเก็บไว้ทั้งหมด

๓.๑.๔.๙ กำหนดบุคคลผู้จัดเก็บรักษาสื่อ โดยให้ผู้ปฏิบัติงานผู้ซึ่งมีหน้าที่รับผิดชอบนำสื่อสำรองระบบข้อมูลไปเก็บยังพื้นที่ควบคุมความปลอดภัย และอนุญาตให้เข้าถึงได้เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น

๓.๑.๕ ผู้ดูแลระบบงาน ดำเนินการตามกระบวนการสำรองข้อมูล สำหรับแต่ละระบบ และจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชนิดของข้อมูลที่บันทึก โดยมีระยะเวลาการเก็บสมุดบันทึก ไม่น้อยกว่า ๑ ปี และมีการตรวจสอบ

๓.๑.๖ สื่อบันทึกข้อมูลสำรองต้องมีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้ในการเก็บข้อมูล

๓.๑.๗ หากเกิดความผิดพลาดของการสำรองข้อมูลผู้ดูแลระบบงานต้องรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไข ต่อผู้บังคับบัญชาและเจ้าของข้อมูล

๓.๒ แนวปฏิบัติทั่วไปเกี่ยวกับการสำรองข้อมูล มีวิธีการปฏิบัติ ดังนี้

๓.๒.๑ ผู้ดูแลระบบงาน ตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเอง โดยจะใช้วิธีสำรองข้อมูลแบบ Full Backup ตามความถี่ ที่ได้ตกลงกับเจ้าของข้อมูลหรือตามแนวทางดังนี้

๓.๒.๑.๑ Web Servers: สำรองข้อมูลเผยแพร่บนเว็บไซต์ ๑ ครั้งต่อเดือน

๓.๒.๑.๒ Database Servers: สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ ๑ ครั้งต่อเดือน

๓.๒.๑.๓ Firewall Servers: สำรองข้อมูล Rule ของ Firewall ๑ ครั้งต่อเดือน

๓.๒.๑.๔ Server อื่น ๆ: สำรองข้อมูลบนเซิร์ฟเวอร์อื่นๆ ได้แก่ ระบบงานต่างๆ ๑ ครั้งต่อเดือน

๓.๒.๑.๕ ผู้ดูแลระบบงาน ตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้น ถูกต้องสมบูรณ์หรือไม่

๓.๓ ผู้ดูแลระบบงานต้องกำหนดแผนการทดสอบกู้คืนข้อมูลหรือการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง เพื่อให้มั่นใจว่าข้อมูลสำรองสามารถนำมาใช้งานได้เมื่อ ข้อมูลหลักหรือระบบสารสนเทศเกิดความเสียหายขึ้น อย่างน้อยปีละ ๑ ครั้ง โดยมีขั้นตอนดังนี้

๓.๓.๑ สำหรับการทดสอบข้อมูลสำรองผู้ดูแลระบบงานต้องกำหนดแผนการทดสอบกู้คืนข้อมูลโดย นำข้อมูลจากสื่อบันทึกข้อมูลมากู้คืนและทดสอบความครบถ้วนของข้อมูล โดยการทดสอบต้องสามารถยืนยันได้ว่าข้อมูลที่สำรองไว้สามารถนำมาใช้งานได้ โดยสามารถพิจารณาแนวทางการทดสอบได้ดังนี้

๓.๓.๑.๑ ทำการกู้คืนข้อมูลในระบบงานทดสอบ (Test Environment) และทำการทดสอบการใช้งานระบบงาน

๓.๓.๑.๒ สำหรับระบบงานที่มีการทำการสำรองข้อมูลอัตโนมัติไปที่ศูนย์คอมพิวเตอร์สำรอง (DR-Site) สามารถกำหนดการทดสอบโดยการให้ผู้ใช้ ไปทดสอบใช้งานที่ระบบงานในศูนย์คอมพิวเตอร์สำรอง (DR-Site) ได้ ทั้งนี้ต้องวางแผนและควบคุมไม่ให้การทดสอบดังกล่าวส่งผลกระทบต่อการทำงานและข้อมูลของระบบงานในศูนย์คอมพิวเตอร์หลัก

๓.๓.๑.๓ ทำการกู้คืนข้อมูลในสื่อบันทึกข้อมูล อื่นใดและใช้เครื่องมือในการประเมินความครบถ้วนสมบูรณ์ของการสำรองข้อมูลเช่น การใช้โปรแกรมในการตรวจสอบเปรียบเทียบข้อมูล การนับ record ของข้อมูล ทั้งนี้ขึ้นอยู่กับลักษณะของข้อมูลที่ทำการสำรองไว้

๓.๓.๒ หากผู้ดูแลระบบงาน ไม่สามารถทำการทดสอบข้อมูลสำรองได้โดยการกู้ข้อมูลที่สำรองไว้ออกมาทดสอบได้ สามารถพิจารณาแนวทางดังต่อไปนี้ เพื่อตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรองได้ดังนี้

๓.๓.๒.๑ ใช้ซอฟต์แวร์สำรองข้อมูลที่สามารถตรวจสอบความถูกต้องของข้อมูลได้โดยอัตโนมัติ เช่น การใช้ค่า checksum/hash เพื่อยืนยันว่าข้อมูลไม่ได้เสียหายระหว่างการสำรอง เช่น Veeam Backup & Replication, Veritas NetBackup เป็นต้น

๓.๓.๒.๒ กำหนดให้การสำรองข้อมูลมีการสำรองบางแฟ้มข้อมูลในระบบงานแยกออกมาโดยใช้เครื่องมือ และความถี่ในการสำรองแบบเดียวกันเพื่อ ให้ผู้ดูแล

ระบบงาน สามารถทำการทดสอบการสำรองข้อมูลจากแฟ้มข้อมูลที่ถูกสำรองแยกออกมานั้นเพื่อลดขั้นตอนและเวลาในการทดสอบ

๓.๓.๒.๓ ตรวจสอบรายงานผลการสำรองข้อมูลจากซอฟต์แวร์สำรองข้อมูล เพื่อตรวจสอบความครบถ้วนสมบูรณ์ของการสำรองข้อมูล

๓.๓.๓ ผู้ดูแลระบบงานต้องนำเสนอแผนการทดสอบและข้อจำกัดในการทดสอบข้อมูลสำรองและแผนการในการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรองและความเสี่ยงที่อาจเกิดขึ้นกับการไม่สามารถทดสอบข้อมูลสำรองทั้งหมดให้กับคณะทำงานฯ เพื่อรับทราบและพิจารณาบริหารจัดการความเสี่ยง

๓.๔ แนวปฏิบัติเกี่ยวกับการกู้คืนข้อมูล

เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการประมวลผลโปรแกรมหยุดทำงาน (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ หรือการประมวลผลของ คอมพิวเตอร์หยุดทำงานอย่างกะทันหัน หรือเปลี่ยนการทำงานไปจากเดิม ทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลา หรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติมีมาตรการในการกู้คืนข้อมูล ดังนี้

๓.๔.๑ ผู้ดูแลระบบงานจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย

๓.๔.๒ การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

๓.๔.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้งานระบบ ให้แจ้งผู้ใช้งานระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

หมวด ๑๘
การควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์
(Internet and E-Mail Control)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์ (E-mail) ให้มีการป้องกันการเข้าถึงหรือการเปลี่ยนแปลงแก้ไขข้อความใน E-mail โดยไม่ได้รับอนุญาต และการรักษาข้อมูลและทรัพยากรต่าง ๆ ของการประปานครหลวง ให้มีความมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบงาน

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

๓.๑.๑ ผู้ดูแลระบบเครือข่ายระบุเส้นทางเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่เชื่อมต่อผ่านระบบ รักษาความปลอดภัยที่องค์กรจัดสรรไว้ ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุความจำเป็นและทำการขออนุญาตจากผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล เป็นลายลักษณ์อักษรพร้อมทั้งระบุแนวทางจัดการความเสี่ยงประกอบการขออนุมัติแล้ว

๓.๑.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่าน เว็บเบราเซอร์ (Web Browser) ต้องทำการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของ ระบบปฏิบัติการที่เว็บเบราเซอร์ติดตั้งอยู่

๓.๑.๓ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อ ชาติ ศาสนา พระมหากษัตริย์

๓.๑.๔ ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

๓.๑.๕ ผู้ใช้งานไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๓.๑.๖ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๓.๑.๗ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่ หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๓.๑.๘ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกเกลียดชัง หรือได้รับความอับอาย

๓.๑.๙ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๓.๑.๑๐ ผู้ใช้งานระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๓.๑.๑๑ ในการเสนอความคิดเห็นผ่านสื่อสังคมออนไลน์ (Social Media) ผู้ใช้งานไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กรและไม่ใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับพนักงานของหน่วยงานอื่นๆ

๓.๑.๑๒ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเวบเบราเซอร์และ ออกจากระบบ (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๓.๒ แนวปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

๓.๒.๑ ผู้ใช้งานที่ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กรเพื่อการทำงานขององค์กรเท่านั้น

๓.๒.๒ ผู้ใช้งานระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสื่อมเสียและความเสียหายต่อองค์กร หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

๓.๒.๓ ผู้ใช้งานไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๓.๒.๔ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ต้องรักษารหัสผ่าน (Password) ส่วนบุคคล หรือหน่วยงาน ของจดหมายอิเล็กทรอนิกส์ไว้เป็นความลับ

๓.๒.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก ๓ เดือน

๓.๒.๖ ที่อยู่จดหมายอิเล็กทรอนิกส์ และรหัสผ่าน (Password) ของหน่วยงานหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับ หากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องยากแก่การคาดเดา (Strong Password)

๓.๒.๗ ผู้ใช้งานต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านโดยอัตโนมัติ (Save Password)

๓.๒.๘ ผู้ใช้งานไม่เปิด หรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๒.๙ ผู้ใช้งานไม่ใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร

๓.๒.๑๐ ผู้ใช้งานตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองอย่างสม่ำเสมอและจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด รวมทั้งไม่จัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๓.๒.๑๑ ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๓.๒.๑๒ ผู้ใช้งานทำการตรวจสอบเอกสารแนบ จากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File

๓.๒.๑๓ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ให้ออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๓.๒.๑๔ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ขององค์กรได้อย่างถูกต้อง

๓.๒.๑๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใด ๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์

๓.๒.๑๖ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กรในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใดๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่องค์กรกำหนด

๓.๒.๑๗ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อเผยแพร่ข้อมูลข่าวสาร หรือภาพเสียง ข้อความ ที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๒.๑๘ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือองค์กร

๓.๒.๑๙ ห้ามทำการปลอมแปลงที่อยู่จดหมายอิเล็กทรอนิกส์เป็นบุคคลอื่น (Impersonation)

๓.๒.๒๐ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ ได้แก่

๓.๒.๒๐.๑ การสร้างจดหมายลูกโซ่ (Chain Mail)

๓.๒.๒๐.๒ การสร้างจดหมายจำนวนมาก (Spam Mail)

๓.๒.๒๐.๓ การส่งจดหมายต่อเนื่อง (Letter Bomb)

๓.๒.๒๐.๔ การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๓.๒.๒๑ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับขององค์กรให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับองค์กร

๓.๒.๒๒ การส่งข้อมูลข่าวสารที่เป็นความลับขององค์กรให้กับบุคคลหรือหน่วยงานภายนอก จะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่องค์กรกำหนด

๓.๒.๒๓ ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กรให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งทบทวนสิทธิการเข้าใช้อย่างสม่ำเสมอ ได้แก่ การลาออก เป็นต้น

๓.๒.๒๔ ผู้ดูแลระบบกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อตรวจสอบ ตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

๓.๒.๒๕ การใส่รหัสผ่านของระบบจดหมายอิเล็กทรอนิกส์ครั้งแรก (Default Password) ในการผ่านเข้า ระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๓.๒.๒๖ เมื่อกรอกรหัสผ่านในระบบจดหมายอิเล็กทรอนิกส์ต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่แสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษร

๓.๒.๒๗ กรณีผู้ใช้งานกรอกรหัสผ่านในระบบจดหมายอิเล็กทรอนิกส์ไม่ถูกต้องในช่วงระยะเวลาหนึ่ง จะต้องทำการยืนยันตัวตน

๓.๒.๒๘ กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิที่จะทำการยกเลิก หรือระงับบริการแก่ผู้ใช้งานนั้น ๆ เป็นการชั่วคราวเพื่อทำการสอบสวน และตรวจสอบ หาสาเหตุของมูลเหตุนั้นๆ โดยไม่จำเป็นต้องแจ้งล่วงหน้า

หมวด ๑๙
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการ กำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งต้อง ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจาก ผู้ดูแล เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบงาน

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ ผู้ใช้งานที่มีบัญชีผู้ใช้งานระบบเครือข่ายขององค์กร จึงจะสามารถใช้งานระบบเครือข่ายไร้สายได้

๓.๒ ผู้ดูแลระบบเครือข่าย ต้องระบุตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ-ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้ และเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและสำรวจว่าสัญญาณรั่วไหลออกไปภายนอก

๓.๓ ผู้ดูแลระบบเครือข่าย ต้องไม่ใช้โปรโตคอลในการเข้าถึงระบบเครือข่ายไร้สายที่ไม่มีความมั่นคงปลอดภัยเช่น WEP (Wired Equivalent Protocol) หรือ WPA (Wi-Fi Protected Access) โดยต้องเลือกใช้โปรโตคอลที่มีความมั่นคงปลอดภัยเช่น WPA3, WPA2-AES เป็นต้น

๓.๔ ผู้ดูแลระบบเครือข่าย ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๓.๕ ผู้ดูแลระบบเครือข่าย เปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบเลือกใช้ชื่อ Login และรหัสผ่านที่มีการคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๓.๖ ผู้ดูแลระบบเครือข่าย ต้องตั้งค่าในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น

๓.๗ ผู้ดูแลระบบเครือข่าย ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

๓.๘ ในการใช้งานเครือข่ายไร้สายผู้ใช้งานต้องปฏิบัติตามนโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด องค์กรสงวนสิทธิ์ในการยกเลิกสิทธิในการเข้าใช้เครือข่ายไร้สาย โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

หมวด ๒๐
ความปลอดภัยของกระบวนการจัดหา พัฒนาและบำรุงดูแลระบบสารสนเทศ
(System acquisition, development and maintenance)

๑. วัตถุประสงค์

เพื่อควบคุมกระบวนการจัดหา พัฒนา และบำรุงดูแลระบบสารสนเทศขององค์กร ให้เป็นไปตามมาตรฐานด้านการพัฒนาระบบสารสนเทศอย่างปลอดภัยตลอดทั้งวงจรของการพัฒนา (Secure System Development Life Cycle)

๒. ผู้รับผิดชอบ

๒.๑ หน่วยงานที่ทำหน้าที่ควบคุมดูแล กระบวนการจัดหา พัฒนาและบำรุงดูแลระบบ

๒.๒ เจ้าของระบบงาน

๓. แนวปฏิบัติ

๓.๑ ในกระบวนการจัดหาระบบสารสนเทศเจ้าของระบบงาน และหน่วยงานที่ทำหน้าที่ควบคุมดูแลกระบวนการจัดหา พัฒนาและบำรุงดูแลระบบต้องดำเนินการดังนี้

๓.๑.๑ โครงการในกระบวนการจัดซื้อจัดจ้างระบบสารสนเทศใด ๆ ต้องนำเอาข้อกำหนดต่าง ๆ ในนโยบายและแนวปฏิบัติฉบับนี้ ไปเป็นข้อกำหนดขั้นพื้นฐานด้านความปลอดภัยสารสนเทศ

๓.๑.๒ สัญญาจ้างในการพัฒนาหรือติดตั้งระบบสารสนเทศ จะต้องกำหนดให้ผู้รับจ้างปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง

๓.๒ การพัฒนาระบบเทคโนโลยีสารสนเทศและเทคโนโลยีปฏิบัติการอย่างมั่นคงปลอดภัยควรดำเนินการอย่างเป็นระบบ ครอบคลุมทุกขั้นตอนของวงจรการพัฒนา (System Development Life Cyc;e) ตั้งแต่การวางแผนไปจนถึงการบำรุงรักษา โดยมีรายละเอียดในแต่ละขั้นตอนดังนี้

๓.๒.๑ การวางแผนและวิเคราะห์ความต้องการ (Planning & Requirements Analysis)

๓.๒.๑.๑ เก็บรวบรวมความต้องการทั้งด้านฟังก์ชัน (Functional Requirement) ซึ่งหมายถึงการทำงานของระบบที่ผู้ใช้ต้องการและความต้องการด้านความมั่นคงปลอดภัย(Security Requirement) ซึ่งหมายถึง การพิสูจน์ตัวตน (Authentication) การควบคุมสิทธิ์การเข้าถึง (Authorization and Access Control) การเข้ารหัสข้อมูล (Encryption) ความต้องการด้านความปลอดภัยของข้อมูลส่วนบุคคล (Data Privacy) การบันทึกและติดตาม (Logging & Monitoring) เป็นต้น

๓.๒.๑.๒ พิจารณาข้อกำหนดด้านกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติว่า

ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพื่อกำหนดการทำงานของระบบ ให้เป็นไปตามข้อกำหนดด้านกฎหมายที่เกี่ยวข้อง

๓.๒.๒ การออกแบบระบบให้มีความมั่นคงปลอดภัย (Secure System Design) และมีความทนทาน (Resilient System Design)

๓.๒.๒.๑ ใช้หลัก การออกแบบที่มีความมั่นคงปลอดภัย (Secure Architecture) โดยอาจพิจารณาหลักการดังนี้

- Least Privilege (สิทธิ์ขั้นต่ำที่จำเป็น) ให้ผู้ใช้หรือระบบเข้าถึงเฉพาะข้อมูลหรือทรัพยากรที่จำเป็นเท่านั้น เพื่อจำกัดผลกระทบหากเกิดเหตุไม่พึงประสงค์
- Defense in Depth (การป้องกันแบบหลายชั้น) ออกแบบระบบให้มีมาตรการควบคุมด้านความมั่นคงปลอดภัยหลายระดับ เช่น Firewall Anti-virus Access Control และ Encryption เพื่อเสริมความแข็งแกร่ง
- Fail-Safe Defaults (การตั้งค่าเริ่มต้นแบบปลอดภัย) การตั้งค่าระบบเริ่มต้นควรอยู่ในระดับที่ปลอดภัย เช่น การปิดสิทธิ์การเข้าถึงเมื่อกลับไปทำงานที่การตั้งค่าเริ่มต้น และให้สิทธิ์เฉพาะที่จำเป็นเท่านั้น
- Separation of Duties (การแยกหน้าที่) กระจายหน้าที่การทำงานออกจากกัน เพื่อป้องกันไม่ให้บุคคลใดบุคคลหนึ่งควบคุมกระบวนการทั้งหมด เช่น แยกผู้พัฒนาออกจากผู้อนุมัติการนำระบบขึ้นใช้งาน
- Security by Design (ความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบ) พิจารณาเรื่องความมั่นคงปลอดภัยตั้งแต่ต้น ไม่ใช่เพิ่มเติมในภายหลัง เช่น การเลือกใช้ Framework ที่มีมาตรฐานความปลอดภัย
- Redundancy and Failover (มีระบบสำรองและทำงานต่อเนื่อง) เช่น การเตรียมระบบสำรองไว้รองรับเมื่อระบบหลักล้มเหลว
- Fail Secure / Graceful Degradation (ระบบยังคงทำงานได้ในระดับที่ยอมรับได้ แม้จะเกิดปัญหาหรือความล้มเหลว) เมื่อระบบล้มเหลว ต้องล้มเหลวในลักษณะที่ไม่เปิดช่องโหว่ เช่น หยุดการให้บริการโดยไม่เปิดข้อมูลสำคัญ
- Minimization (การลดความซับซ้อนและลดพื้นผิวการโจมตี) ติดตั้งและเปิดใช้งานเฉพาะฟังก์ชันที่จำเป็นเพื่อลดช่องโหว่ที่อาจถูกโจมตี เช่น ปิดพอร์ตที่ไม่ใช้งาน
- Auditability (การสามารถตรวจสอบย้อนหลังได้) ระบบต้องสามารถบันทึกและติดตามกิจกรรมที่สำคัญ เช่น Log การเข้าถึง การเปลี่ยนแปลงข้อมูล เพื่อใช้ในการตรวจสอบเหตุการณ์
- Monitoring and Detection (ตรวจจับและเฝ้าระวัง) ระบบต้องถูกออกแบบให้สามารถเฝ้าดูพฤติกรรมผิดปกติ และแจ้งเตือนทันที
- Secure Defaults (ตั้งค่าระบบให้ปลอดภัยตั้งแต่แรก)เช่น การตั้งค่ารหัสผ่านที่มีความซับซ้อน และบังคับใช้การเปลี่ยนรหัสผ่านตามรอบเวลา

- Secure Identity assertions (การยืนยันตัวตนต้องได้รับการป้องกัน) เช่นการกำหนดให้ใช้มาตรฐานในการตรวจสอบและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย SAML 2.0 OAuth 2.0 หรือ OpenID Connect
- Zero Trust Principle (หลักการความปลอดภัยที่เน้นการตรวจสอบและยืนยันความถูกต้องของทุกการเข้าถึง) ทุกการเข้าถึงต้องได้รับการยืนยันตัวตน และตรวจสอบความถูกต้อง โดยไม่อนุญาตตามความเชื่อใจที่มีอยู่เดิม

๓.๒.๒.๒ ระบุจุดที่มีข้อมูลสำคัญหรือข้อมูลส่วนบุคคล

๓.๒.๒.๓ ดำเนินการสร้างแบบจำลองภัยคุกคาม (Threat Modeling) เพื่อคาดการณ์วิธีการโจมตีและวางมาตรการป้องกันไว้ล่วงหน้า

๓.๒.๓ การพัฒนาโปรแกรมอย่างมั่นคงปลอดภัย(Secure Coding) เพื่อป้องกันผู้บุกรุกสามารถใช้ช่องโหว่หรือความผิดพลาดในการเขียนโปรแกรมเพื่อโจมตีระบบ

๓.๒.๓.๑ ใช้ภาษาหรือกรอบการพัฒนาระบบงาน (Framework) ที่ได้รับการสนับสนุนและมีการปรับปรุงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๓.๒.๓.๒ ปฏิบัติตามแนวทางการการเขียนโค้ดที่มั่นคงปลอดภัย Secure Coding เพื่อป้องกันผู้บุกรุกสามารถใช้ช่องโหว่หรือความผิดพลาดในการเขียนโปรแกรมเพื่อโจมตีระบบ เช่น OWASP Top 10, SEI CERT Guidelines เป็นต้น

๓.๒.๓.๓ หลีกเลี่ยงการฝังข้อมูลลับโดยตรงใน Source code (Hardcoded credentials) การแทรกคำสั่ง SQL แอบแฝงลงในโปรแกรม เพื่อควบคุมหรือเจาะข้อมูลจากฐานข้อมูล(SQL Injection) การตรวจสอบการนำเข้า (Input Control) ที่ไม่เหมาะสม

๓.๒.๓.๔ ใช้ระบบจัดเก็บซอร์สโค้ดที่มีการควบคุมสิทธิ์การเข้าถึงและมีการควบคุมเวอร์ชั่น

๓.๒.๓.๕ ต้องมีการแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงออกจากกัน ทั้งในส่วนของระบบเครือข่ายและเครื่องแม่ข่าย โดยกำหนดให้สภาพแวดล้อมของการพัฒนาสามารถเข้าถึงได้เฉพาะกลุ่มนักพัฒนาระบบที่เกี่ยวข้องเท่านั้น

๓.๒.๓.๖ ชุดข้อมูลที่ใช้สำหรับการทดสอบระบบ (Test Data) จะต้องมีการควบคุมการเข้าถึงให้เฉพาะกลุ่มนักพัฒนาและติดตั้งระบบเข้าถึงได้เท่านั้น เมื่อสิ้นสุดกระบวนการพัฒนา จะต้องดำเนินการทำลายข้อมูลอย่างปลอดภัย เสมือนข้อมูลจริง

๓.๒.๔ การตรวจสอบโค้ดและวิเคราะห์ช่องโหว่ (Code Review & Static Analysis)

๓.๒.๔.๑ จัดให้มีกระบวนการที่ให้ เพื่อนร่วมงาน หรือผู้เชี่ยวชาญในระดับเดียวกันตรวจสอบผลงาน เพื่อให้แน่ใจว่าถูกต้อง มีคุณภาพ และเป็นไปตามมาตรฐานก่อนเผยแพร่หรือใช้งานจริง (Peer Review) หรืออาจพิจารณาใช้

เครื่องมือ Static Application Security Testing (SAST) เพื่อค้นหาช่องโหว่โดยอัตโนมัติ

๓.๒.๔.๒ จัดทำบันทึกผลการตรวจสอบ และวิเคราะห์ความเสี่ยงของข้อผิดพลาดที่พบ

๓.๒.๔.๓ ดำเนินการแก้ไขก่อนเข้าสู่ขั้นตอนการทดสอบระบบ

๓.๒.๕ การทดสอบความมั่นคงปลอดภัย (Security Testing)

๓.๒.๕.๑ ทดสอบการเจาะระบบ (Penetration Testing) โดยเครื่องมือของการประปานครหลวงหรือผู้เชี่ยวชาญจากภายนอก

๓.๒.๕.๒ ตรวจสอบช่องโหว่ (Vulnerability Assessment)

๓.๒.๕.๓ ทดสอบความสามารถของระบบในการตรวจจับและป้องกันการโจมตี

๓.๒.๕.๔ จัดลำดับความสำคัญของช่องโหว่ที่พบ พร้อมแผนการแก้ไขและยืนยันผลการแก้ไข

๓.๒.๖ การเริ่มใช้งานระบบ (Release & Deployment)

๓.๒.๖.๑ ตรวจสอบความพร้อมด้านความปลอดภัยให้อยู่ในระดับที่ยอมรับได้ หรือระดับต่ำ

๓.๒.๖.๒ จัดทำเอกสารรายละเอียดของเวอร์ชันของซอฟต์แวร์ และข้อมูลเกี่ยวกับซอฟต์แวร์เวอร์ชั่นนี้ ประกอบด้วย หมายเลขเวอร์ชัน (Version Number) วันที่ออกเวอร์ชัน (Release Date) ประเภทของการอัปเดต เช่น Major, Minor, Patch, Hotfix คำอธิบายโดยรวมของเวอร์ชันนี้ว่ามีการเปลี่ยนแปลงอะไรสำคัญ หรือเน้นอะไรเป็นพิเศษ

๓.๒.๖.๓ อาจพิจารณาใช้เทคนิค Canary Release โดยการปล่อยเวอร์ชั่นใหม่ให้กับผู้ใช้กลุ่มเล็กๆ การติดตามผล และหากพบปัญหากับเวอร์ชั่นใหม่ การเผยแพร่สามารถย้อนกลับและใช้เวอร์ชั่นเก่าได้ทันที เพื่อลดความเสี่ยงในการเผยแพร่เวอร์ชั่นใหม่

๓.๓ การบำรุงรักษาและอัปเดต (Maintenance & Updates)

๓.๓.๑ ติดตามช่องโหว่ของซอฟต์แวร์หรือไลบรารีที่ใช้งานอย่างสม่ำเสมอ

๓.๓.๒ ดำเนินการอัปเดต Patch ทันทีเมื่อพบช่องโหว่ความรุนแรง ในระดับความเสี่ยงสูงและความเสี่ยงวิกฤติ ตาม Common Vulnerability Scoring System (CVSS Score) ตามที่ระบุในแนวปฏิบัติด้านการประเมินช่องโหว่และการทดสอบระบบ (Vulnerability Assessment and Penetration Testing) หมวด ๑๐

๓.๓.๓ มีขั้นตอนการตรวจสอบผลกระทบก่อนการอัปเดตระบบ

๓.๓.๔ การแก้ไขเปลี่ยนแปลงใด ๆ ของระบบสารสนเทศในช่วงการพัฒนา จะต้องมีการจดบันทึกและผ่านกระบวนการควบคุมการแก้ไขเปลี่ยนแปลงระบบ โดยได้รับการอนุมัติจากเจ้าของระบบนั้น ๆ ก่อนดำเนินการจริงเสมอ

หมวด ๒๑
การบริหารจัดการผู้ให้บริการภายนอก
(Third Party Management)

๑. วัตถุประสงค์

เพื่อกำหนดแนวทางการประเมิน ควบคุม และติดตามความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์จากบุคคลภายนอก (Third Parties) เช่น ผู้ให้บริการภายนอก คู่ค้า ผู้ขาย และผู้พัฒนาระบบที่เกี่ยวข้องกับข้อมูลหรือระบบ รวมถึงการกำหนดมาตรการควบคุมและป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศ สามารถลดโอกาสการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยที่มีต้นตอมาจากบุคคลภายนอก และสามารถตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๒ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอก

๒.๓ ผู้ดูแลระบบงาน

๒.๔ ผู้ดูแลศูนย์คอมพิวเตอร์

๓. แนวปฏิบัติ

๓.๑ หน่วยงานของการประปานครหลวงที่ต้องการจะจัดให้มีการใช้บริการผู้ให้บริการภายนอก ต้องพิจารณาวัตถุประสงค์เพื่อเสริมศักยภาพในการดำเนินธุรกิจ โดยช่วยเติมเต็มความเชี่ยวชาญเฉพาะทางที่อาจไม่มีภายใน ลดต้นทุนและความเสี่ยงจากการลงทุนในเทคโนโลยี เพิ่มความยืดหยุ่นในการขยายบริการ รองรับการดำเนินโครงการได้อย่างรวดเร็ว สนับสนุนการปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง รวมถึงช่วยให้สามารถมุ่งเน้นทรัพยากรไปยังกิจกรรมหลัก (Core Business) ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยหน่วยงานของการประปานครหลวงที่จัดให้มีผู้ให้บริการภายนอก จะต้องเป็นผู้ประเมินความเสี่ยงจากการใช้บริการ กำหนดมาตรการควบคุม เช่น การจัดทำสัญญาการให้บริการ รวมถึงติดตามตรวจสอบการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยเทคโนโลยีและไซเบอร์ของบุคคลภายนอกในระหว่างที่มีสัญญา รวมถึงการยกเลิกสัญญา

๓.๒ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอก ต้องสื่อสารหน้าที่รับผิดชอบต่อความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ กับผู้ให้บริการภายนอก ตามแต่ขอบเขตการทำงานและความเสี่ยง ซึ่งต้องระบุไปในสัญญาการให้บริการและมีการสื่อสารให้รับทราบก่อนเริ่มปฏิบัติงานตามสัญญา

๓.๓ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกต้องทำการประเมินความเสี่ยงและจัดการความเสี่ยงของการใช้บริการผู้ให้บริการภายนอกตามแนวปฏิบัติเรื่องการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ (Information Security and Cybersecurity Risk Assessment)

๓.๔ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องมอบหมายให้หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกจัดทำรายชื่อผู้ให้บริการภายนอกที่ใช้บริการ รวมถึงอธิบายขอบเขตการใช้บริการให้ครบถ้วนและประเมินระดับความสำคัญของผู้ให้บริการและแนวทางการควบคุมแต่ละระดับดังนี้

ระดับความสำคัญ	ลักษณะผู้ให้บริการที่เข้าข่าย	แนวทางการควบคุมขั้นต่ำ
สูง (Critical)	มีสิทธิ์เข้าถึงหรือเป็นบริการที่เกี่ยวข้องกับระบบงานหลักตาม BIA หรือเข้าถึงข้อมูลส่วนบุคคล	● จัดทำสัญญาที่มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ● มีการประเมินความเสี่ยงก่อนการใช้บริการและประเมินความเสี่ยงระหว่างใช้บริการ ● มีการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์รายปี ● มีการติดตามผลการดำเนินงานและทบทวนผลการปฏิบัติงานอย่างสม่ำเสมอ
กลาง (Moderate)	เข้าถึงระบบบางส่วน หรือข้อมูลทั่วไปหรือให้บริการสนับสนุนบางระบบงาน	● จัดทำสัญญาที่มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ● มีการประเมินความเสี่ยงก่อนการใช้บริการ ● มีการประเมินด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ประจำปี

ต่ำ (Low)	ไม่มีสิทธิ์เข้าระบบหรือข้อมูลหรือระบบงาน	● มีการประเมินความเสี่ยงก่อนการใช้บริการ

๓.๕ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกต้อง จัดทำสัญญาการให้บริการโดยระบุข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและข้อตกลงระดับการให้บริการให้ชัดเจน โดยข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์จะต้องประกอบไปด้วยหัวข้อต่อไปนี้เป็นอย่างน้อย

๓.๕.๑ ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก

๓.๕.๒ บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกและการประปานครหลวง

๓.๕.๓ มาตรฐานขั้นต่ำในการปฏิบัติงานของบุคคลภายนอก เช่น การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศการรักษาความลับของข้อมูล และการไม่นำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ เป็นต้น

๓.๕.๔ ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) สำหรับการใช้บริการจากบุคคลภายนอก

๓.๕.๕ การติดตาม รายงานผลการปฏิบัติงานของบุคคลภายนอก ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือปัญหาที่สำคัญ การรายงานเหตุการณ์ผิดปกติอย่างทันการณ์ และการบริหารจัดการการเปลี่ยนแปลง

๓.๕.๖ รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๓.๕.๗ การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก

๓.๕.๘ เงื่อนไขหรือสิทธิของผู้ประกอบธุรกิจในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลงกับบุคคลภายนอก เช่น กรณีที่บุคคลภายนอกมีการละเมิดสัญญาหรือข้อตกลง เป็นต้น

๓.๕.๙ การจัดให้มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT contingency plan) ที่สอดคล้องกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของการประปานครหลวง

๓.๕.๑๐ การรายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมถึงการมีส่วนร่วมในแผนการรับมือเหตุการณ์ผิดปกติ

๓.๕.๑๑ ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้

๓.๖ ก่อนการเลือกใช้บริการผู้ให้บริการภายนอก หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกต้องดำเนินการตรวจสอบก่อนทำสัญญา (Third Party Due Diligence) เพื่อพิจารณาความเหมาะสมที่จะใช้บริการและระบุความเสี่ยงของผู้ให้บริการในหัวข้อดังนี้

๓.๖.๑ ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ ความสามารถในการให้บริการในช่วงที่ผ่านมา และระบบการบริหารงานภายใน

๓.๖.๒ การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน

๓.๖.๓ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ เช่น มีนโยบายหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยหรือไม่

๓.๖.๔ การบริหารจัดการผู้ให้บริการช่วง (Subcontractor หรือ Third Party Chain)

๓.๖.๕ การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ

๓.๖.๖ การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการตรวจสอบประวัติด้านการกระทำความผิด เป็นต้น

๓.๖.๗ การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เช่น การตรวจสอบเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยการรับรองการปฏิบัติตามมาตรฐานสากล หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกควรพิจารณาว่า บุคคลภายนอกได้รับการรับรองในส่วนระบบที่สำคัญ หรือระบบที่ผู้ประกอบธุรกิจใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูล หรือได้รับการรับรองครอบคลุมทั้งองค์กร

๓.๖.๘ การใช้เทคโนโลยีสารสนเทศ แบบเปิด (Open Technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (Interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยีสารสนเทศ ผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

๓.๗ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกต้องมีการติดตามผลการปฏิบัติงานตามสัญญาและทำการทบทวนการประเมินการความเสี่ยงจากการใช้บริการ อย่างน้อยปีละ ๑ ครั้ง

๓.๘ เมื่อสิ้นสุดสัญญาการใช้บริการหน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกต้องดำเนินการถอนสิทธิ์การเข้าถึงระบบงานหรือข้อมูลของผู้ให้บริการทั้งหมด กำหนดให้ผู้ให้บริการลบหรือส่งคืนข้อมูลของการประปานครหลวงทั้งหมด ผู้ให้บริการต้องส่งมอบทรัพย์สินที่เกี่ยวข้องกลับคืน หากมีข้อมูลสำคัญอาจพิจารณาให้ผู้ให้บริการต้องทำรายงานใบรับรองการทำลายข้อมูล (Data Destruction Certificate) ให้กับการประปานครหลวงด้วย

๓.๙ การระบุสัญญาเพื่อควบคุมการเข้าใช้งานของหน่วยงานภายนอก

๓.๙.๑ หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของการประปานครหลวง จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้บังคับบัญชาเจ้าของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าว

๓.๙.๒ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกต้องทำการแจ้งเป็นลายลักษณ์อักษรให้หน่วยงานภายนอกทราบถึงความสำคัญที่มีต่อความมั่นคงปลอดภัยข้อมูลสารสนเทศของข้อมูลสารสนเทศ ซึ่งหน่วยงานภายนอกจะต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของการประปานครหลวง โดยเอกสารดังกล่าวจะถูกจัดเก็บไว้เป็นหลักฐาน

๓.๙.๓ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้เฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๓.๙.๔ หน่วยงานภายนอก มีหน้าที่ต้องแจ้งให้กับหน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกทราบทันทีที่พบว่ามีการคุกคามที่มีผลต่อความมั่นคงปลอดภัยในลักษณะใดๆ ก็ตาม รวมถึงการเข้าถึงข้อมูล โดยผู้ไม่มีสิทธิ หรือการผ่อนปรน หรือละเว้นไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวงนอกจากนั้น ผู้ดูแลระบบของการประปานครหลวง ผู้ซึ่งรับทราบถึงเหตุการณ์คุกคามด้านความปลอดภัยซึ่งเกิดจากหน่วยงานภายนอก ต้องแจ้งให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ ทราบทันทีตามกระบวนการ แนวปฏิบัติการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

๓.๙.๕ สัญญาการใช้งานระบบสารสนเทศทั้งหมดที่มีการจัดทำขึ้นต้องระบุถึง “สิทธิในการตรวจสอบ” เพื่อให้มั่นใจได้ว่าการประปานครหลวง สามารถเข้าไปประเมินสภาพแวดล้อมของการควบคุมภายในทั้งทางกายภาพ (Physical) และทาง Logical ของคู่สัญญาหรือหน่วยงานภายนอกได้

๓.๙.๖ การประเมินเรื่องชีวอนามัย หรือ ข้อกำหนดอื่น ๆ ในการใช้บริการผู้ให้บริการภายนอกของ การประปานครหลวง

๓.๑๐ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

๓.๑๑ หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายขององค์กร เพื่อใช้งานระบบอินเทอร์เน็ต ทำเรื่องแจ้งรายชื่อขออนุญาตเป็นลายลักษณ์อักษรและแนบเอกสารสำเนาบัตร

ประชาชนเป็นรายบุคคล เพื่อขออนุมัติจากหน่วยงานภายในที่ทำงานร่วมกันและผู้อำนวยการฝ่ายขึ้นไป และแจ้งผู้ดูแลระบบเครือข่ายล่วงหน้าก่อนการดำเนินงาน ในกรณีที่มีการเปลี่ยนแปลงรายชื่อ หน่วยงานภายนอกจะต้องแจ้งล่วงหน้าก่อนทุกครั้ง

๓.๑๒ หน่วยงานภายนอกของโครงการพัฒนาระบบแอปพลิเคชัน หากต้องการสิทธิในการเข้าถึงการใช้งาน ระบบขององค์กร ต้องทำเรื่องแจ้งรายชื่อขออนุญาตเป็นลายลักษณ์อักษรและแนบเอกสารสำเนาบัตรประชาชนเป็นรายบุคคล โดยแจ้งเหตุผลในการขอ โครงการที่เกี่ยวข้อง และระบบแอปพลิเคชันที่ต้องการเข้าใช้ เพื่อขออนุมัติจากหน่วยงานภายในที่ทำงานร่วมกันและผู้อำนวยการฝ่ายขึ้นไป และแจ้งผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายล่วงหน้าก่อนการดำเนินงาน โดยหน่วยงานภายนอกสามารถเข้าระบบแอปพลิเคชันได้เฉพาะตามโครงการ และตามความจำเป็นในหน้าที่ ในกรณีที่มีการเปลี่ยนแปลงรายชื่อ หน่วยงานภายนอกจะต้องแจ้งล่วงหน้าก่อนทุกครั้ง

๓.๑๓ ในการเข้าปฏิบัติงานภายในศูนย์คอมพิวเตอร์ขององค์กร หน่วยงานภายนอกจะต้องบันทึกรายละเอียดตามเอกสารแบบฟอร์มที่องค์กรจัดไว้ให้โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยี สารสนเทศ ซึ่งมีรายละเอียดอย่างน้อย ดังนี้

- ๓.๑๓.๑ เหตุผลในการขอใช้งาน
- ๓.๑๓.๒ ระยะเวลาในการใช้งาน
- ๓.๑๓.๓ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- ๓.๑๓.๔ การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
- ๓.๑๓.๕ การป้องกันในเรื่องการเปิดเผยข้อมูล

๓.๑๔ หน่วยงานภายนอกที่ทำงานให้กับองค์กร / หน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓.๑๕ หน่วยงานที่จัดให้มีการใช้บริการผู้ให้บริการภายนอกซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องระบุ การเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๓.๑๖ การประปามีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่า สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๓.๑๗ หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

๓.๑๘ ทุกครั้งที่จะทำการแก้ไขค่า Configuration ของอุปกรณ์ทุกชนิดภายในศูนย์คอมพิวเตอร์ของการประปานครหลวง หน่วยงานภายนอกจะต้องทำการสำรองค่า Configuration เดิมไว้ก่อน

รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้น ไม่สามารถใช้งานได้ตามต้องการ จะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมาให้สามารถใช้งานได้ตามสภาพเดิม

๓.๑๙ ทุกครั้งที่มีการแก้ไขหรือเปลี่ยนแปลงค่า Configuration ระบบงานสารสนเทศหรือเปลี่ยนแปลงโครงสร้างของฐานข้อมูล หน่วยงานภายนอกจะต้องทำการสำรองโปรแกรม/ โมดูล หรือฐานข้อมูลเดิมที่มีการแก้ไข รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้นไม่สามารถใช้งานได้ตามต้องการ จะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมา ให้สามารถใช้งานได้ตามสภาพเดิม

๓.๒๐ ในกรณีที่หน่วยงานภายนอกจะเข้ามาปฏิบัติงานที่ศูนย์คอมพิวเตอร์ขององค์กร ในวันหยุดหรือนอกเวลาราชการ จะต้องขอความเห็นชอบหรือผู้ดูแลล่วงหน้าก่อนทุกครั้ง และการดำเนินงานทุกครั้งจะต้องอยู่ในความดูแลของผู้รับผิดชอบหรือผู้ดูแล

๓.๒๑ ในกรณีที่ผู้ปฏิบัติงานของหน่วยงานภายนอกประมาท ทำให้อุปกรณ์และระบบสารสนเทศขององค์กรได้รับความเสียหายหรือสูญเสีย หน่วยงานภายนอก จะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม

หมวด ๒๒
การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
(Cybersecurity Detection and Monitoring)

๑. วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงเวลาที่เหมาะสม และกำหนดแนวทางในการเฝ้าระวัง ตรวจจับ และวิเคราะห์เหตุการณ์ทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบสารสนเทศและระบบควบคุมขององค์กร โดยให้สามารถตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที ลดความเสียหายจากเหตุการณ์ที่ไม่พึงประสงค์

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ดูแลระบบเครือข่าย

๒.๔ ทุกหน่วยงาน

๒.๕ ผู้ปฏิบัติงานศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์

๓. แนวปฏิบัติ

๓.๑ ผู้ดูแลระบบงานและผู้ดูแลระบบเครือข่ายต้องจัดให้มีการจัดเก็บบันทึก Log เพื่อการเฝ้าระวังตรวจจับ เหตุการณ์ผิดปกติทางไซเบอร์ดังนี้

๓.๑.๑ ระบบสารสนเทศที่จำเป็นต้องมีการเก็บบันทึก Log ได้แก่ระบบต่าง ๆ ดังนี้

๓.๑.๑.๑ อุปกรณ์เครือข่ายและอุปกรณ์ความมั่นคงปลอดภัย

๓.๑.๑.๒ เครื่องแม่ข่ายและระบบแอปพลิเคชันที่เข้าถึงได้จากอินเทอร์เน็ต

๓.๑.๑.๓ เครื่องแม่ข่ายและระบบแอปพลิเคชันที่ให้บริการแก่ผู้ใช้งานภายนอก

๓.๑.๒ ระบบสารสนเทศ ที่จำเป็นจะต้องมีการเก็บบันทึก Log จะต้องมีการพิจารณาเก็บบันทึก Log ต่าง ๆ ดังนี้

๓.๑.๒.๑ Log จากระบบ Web Application (แหล่งที่มา: Web Server, Application Server, API Gateway)

- Access Log – บันทึกการเข้าใช้งานของผู้ใช้ IP ต้นทาง รายละเอียดคำขอ (เช่น Apache/Nginx logs)
- Error Log – แสดงข้อผิดพลาดของแอปพลิเคชัน ซึ่งอาจบ่งบอกถึงช่องโหว่
- Authentication Log – บันทึกความพยายามเข้าสู่ระบบ สำเร็จ/ล้มเหลว
- Database Log – ตรวจสอบคำสั่ง SQL ที่ถูกเรียกใช้ การเข้าถึงฐานข้อมูลที่ไม่ได้รับอนุญาต การโจมตี SQL Injection

- Web Application Firewall (WAF) Log – ตรวจจับการโจมตีที่เกี่ยวข้องกับเว็บ เช่น XSS SQL Injection

๓.๑.๒.๒ Log จากเซิร์ฟเวอร์ UNIX (แหล่งที่มา: Syslog , Security Logs, Application Logs)

- System Log (/var/log/syslog, /var/log/messages) – บันทึกเหตุการณ์ระดับระบบปฏิบัติการ
- Authentication Log (/var/log/auth.log, /var/log/secure) – ติดตามความพยายามเข้าสู่ระบบ SSH การใช้คำสั่ง sudo การยกระดับสิทธิ์
- Kernel Log (/var/log/kern.log, /var/log/dmesg) – ตรวจจับกิจกรรมระดับ Kernel เช่น Rootkit
- Audit Log (/var/log/audit/audit.log) – ติดตามการเปลี่ยนแปลงที่สำคัญของระบบ การแก้ไขไฟล์
- Process Monitoring Log – ตรวจจับกระบวนการ (Process) ที่ผิดปกติหรือไม่ได้รับอนุญาต

๓.๑.๒.๓ Log จาก จากเซิร์ฟเวอร์ Microsoft Windows (แหล่งที่มา: Windows Event Viewer)

- Security Logs ประกอบไปด้วย Event ID 4624 สำหรับการเข้าสู่ระบบที่สำเร็จ Event ID 4625 สำหรับการเข้าสู่ระบบที่ล้มเหลว Event ID 4771 สำหรับการตรวจสอบล่วงหน้าของ Kerberos ที่ล้มเหลว Event ID 4768 สำหรับการขอตั๋วการตรวจสอบสิทธิ์ Kerberos (TGT) Event ID 4769 สำหรับการขอตั๋วบริการ Kerberos และ Event ID 4776 สำหรับการพยายามตรวจสอบสิทธิ์ของบัญชีผู้ใช้.
- Event Logs ประกอบด้วย: Event ID 6005 สำหรับการเริ่มต้นบริการบันทึกเหตุการณ์ Event ID 6006 สำหรับการหยุดบริการบันทึกเหตุการณ์ และ Event ID 6008 สำหรับการปิดระบบที่ไม่คาดคิด.
- Application Logs ประกอบด้วยบันทึกจากแอปพลิเคชันและบริการที่สำคัญที่ทำงานบนเซิร์ฟเวอร์ เช่น SQL Server IIS เป็นต้น
- PowerShell Logs ประกอบไปด้วย Module Logging: คำสั่งที่ถูกเรียกใช้ Script Block Logging: สคริปต์ทั้งหมดที่ถูกเรียกใช้ Transcription: การบันทึกการทำงานของคอนโซลทั้งหมด
- Directory Service Logs ประกอบด้วย: Event ID 2886 สำหรับการไม่ต้องการการลงชื่อ LDAP (LDAP signing is not required.) Event ID 2887 สำหรับจำนวนการเชื่อมต่อ LDAP ที่ไม่ได้ลงชื่อ (Number of unsigned LDAP binds)

- DNS Server Logs ประกอบด้วย: Event ID 4000 สำหรับการเริ่มต้นเซิร์ฟเวอร์ DNS Event ID 4004 สำหรับการไม่สามารถทำการสำรวจบริการไดเรกทอรีของโซนได้
- File Replication Service Logs ประกอบด้วย: Event ID 13508 สำหรับปัญหาในการเปิดใช้งานการ Replica Event ID 13568 สำหรับการตรวจพบว่า Replica file อยู่ในสถานะข้อผิดพลาด

๓.๑.๒.๔ Log จาก Firewall และอุปกรณ์เครือข่าย (แหล่งที่มา: Firewall, IDS/IPS, Load Balancers, Routers, Switches)

- Firewall Log – บันทึกทราฟฟิก แพ็กเก็ตที่ถูกบล็อก การเชื่อมต่อที่ได้รับอนุญาต
- VPN Log – ติดตามการเข้าถึงระยะไกล ความพยายามล็อกอินที่ล้มเหลว
- Intrusion Detection/Prevention System (IDS/IPS) Log – ตรวจจับกิจกรรมที่เป็นอันตรายในเครือข่าย
- DNS Log – ตรวจสอบโดเมนที่ถูกเรียกใช้ การเชื่อมต่อไปยังเซิร์ฟเวอร์ควบคุมมัลแวร์
- NetFlow/Packet Capture Log – วิเคราะห์รูปแบบทราฟฟิกที่ผิดปกติ

๓.๑.๓ บันทึก Log จะต้องถูกจัดเก็บและวิเคราะห์ อยู่ในระบบบริหารจัดการข้อมูล Log แบบรวมศูนย์ (Centralized Log Management System)

๓.๑.๔ ระบบที่ใช้บันทึก Log จะต้องมีทรัพยากรที่เพียงพอต่อการเก็บบันทึก Log ได้ไม่ต่ำกว่า ๙๐ วันหรือตามที่กฎหมายกำหนด

๓.๑.๕ ระบบที่ใช้บันทึก Log จะต้องป้องกันมิให้มีแก้ไขเปลี่ยนแปลงหรือลบบันทึกได้

๓.๑.๖ ระบบที่บันทึก Log จะต้องควบคุมการเข้าถึงให้เข้าถึงได้เฉพาะพนักงานเจ้าหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศดังกล่าวเท่านั้น

๓.๒ กระบวนการเฝ้าระวังและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยสารสนเทศ

๓.๒.๑ ต้องจัดให้มีศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามด้านสารสนเทศและไซเบอร์ ซึ่งทำหน้าที่ในการเฝ้าระวังเหตุการณ์ด้านความปลอดภัยสารสนเทศและไซเบอร์ โดยต้องสามารถเฝ้าระวังระวังภัยคุกคามด้านสารสนเทศและไซเบอร์ในส่วนต่าง ๆ ดังนี้

๓.๒.๑.๑ ตรวจสอบภัยคุกคามบนระบบเครือข่ายหรือบริการบนระบบเครือข่าย

๓.๒.๑.๒ ตรวจสอบกิจกรรมของบุคลากรและการใช้งานเทคโนโลยี

๓.๒.๑.๓ ตรวจสอบกิจกรรมและบริการของผู้ให้บริการภายนอก

๓.๒.๑.๔ ตรวจสอบระบบฮาร์ดแวร์ ซอฟต์แวร์ การทำงานของระบบงาน และข้อมูล

๓.๒.๒ การเฝ้าระวังภัยคุกคามด้านสารสนเทศและไซเบอร์ต้องสามารถรวบรวมเอาเหตุการณ์ต่าง ๆ จากอุปกรณ์หลาย ๆ อุปกรณ์เพื่อทำการวิเคราะห์เหตุการณ์ได้ (Event Correlated) และสามารถรายงานผลอัตโนมัติต่อ ผู้ปฏิบัติงานศูนย์ปฏิบัติการเฝ้าระวังได้

๓.๒.๓ ศูนย์ปฏิบัติการเฝ้าระวังต้องสามารถวิเคราะห์เพื่อระบุลักษณะของเหตุการณ์และตรวจจับเหตุการณ์ทางไซเบอร์ โดยระบุ ความผิดปกติ ตัวบ่งชี้การถูกยึดครอง (Indicator of Compromise) และเหตุการณ์ที่อาจเป็นอันตราย

๓.๒.๔ ศูนย์ปฏิบัติการเฝ้าระวังต้องดำเนินการวิเคราะห์ผลกระทบและขอบเขตของเหตุการณ์ที่อาจเป็นอันตราย และต้องรายงานข้อมูลเกี่ยวกับเหตุการณ์ที่อาจเป็นอันตราย ตามขั้นตอนในแผนรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response) อย่างทันท่วงที

๓.๒.๕ ข้อมูลเทคนิควิธีการในการเฝ้าระวัง รวมถึงข้อมูลเกี่ยวกับภัยคุกคาม (Threat intelligence) ต้องมีการปรับปรุงอยู่เสมอตลอดเวลา

หมวด ๒๓
การบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศไซเบอร์
(Information Security and Cybersecurity Incident Management)

๑. วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างเป็นระบบ ครอบคลุมตั้งแต่การระบุ การรายงาน การประเมิน การตอบสนอง และการกู้คืนระบบ โดยมีเป้าหมายเพื่อลดผลกระทบจากเหตุการณ์ รักษาความต่อเนื่องในการดำเนินงาน และสนับสนุนการปฏิบัติตามข้อกำหนดทางกฎหมายและระเบียบที่เกี่ยวข้อง ทั้งนี้ในแนวปฏิบัตินี้มีขอบเขตที่การรับมือภัยคุกคามทางไซเบอร์ตามประกาศเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเท่านั้นส่วนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอื่น ๆ จะมีการดำเนินการตามขั้นตอนปฏิบัติการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ปฏิบัติงานที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ คณะทำงานฯ และ ผู้ปฏิบัติงานที่ได้รับมอบหมาย จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่ต้องมีรายละเอียดดังนี้

๓.๑.๑ โครงสร้างและบทบาทและความรับผิดชอบของทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

๓.๑.๒ ลักษณะรูปแบบการรายงานเหตุการณ์ทั้งภายในและภายนอกองค์กร

๓.๑.๓ เกณฑ์การวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และขั้นตอนการเริ่มใช้แผนการรับมือภัยคุกคามทางไซเบอร์

๓.๑.๔ ขั้นตอนการวิเคราะห์ลักษณะการโจมตีโดยจะทำการระบุรายละเอียดของการโจมตีเพื่อระบุตัวบ่งชี้การถูกโจมตี (Indicator of Compromise: IOC)

๓.๑.๕ ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๑.๖ ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

๓.๑.๗ ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence)

๓.๑.๘ ขั้นตอนการการกำจัดเหตุภัยคุกคามทางไซเบอร์ (Eradication)

๓.๑.๙ ขั้นตอนการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Recovery)

๓.๑.๑๐ วิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ กับผู้เชี่ยวชาญเฉพาะทางด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

๓.๑.๑๑ กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๓.๒ คณะทำงานฯ จะต้องมีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญ

๓.๓ คณะทำงานฯ จะต้องสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในกระบวนการการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๓.๔ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ปฏิบัติงานที่ได้รับมอบหมายจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) อันประกอบไปด้วย

๓.๔.๑ ทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต โดยรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๓.๔.๒ กำหนดแผนการดำเนินการสำหรับการสื่อสารในภาวะวิกฤตสำหรับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้

๓.๔.๓ ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียจากสถานการณ์ที่อาจเกิดขึ้นเพื่อวางแผนการสื่อสาร

๓.๔.๔ ระบุผู้มีหน้าที่แถลงข่าวกับสื่อมวลชนทั้งส่วนของโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิค

๓.๔.๕ ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๓.๔.๖ ต้องมีการติดต่อประสานงานระหว่างทีมตอบสนองต่อภัยคุกคาม ไปยังผู้รับผิดชอบด้านสื่อสารองค์กร เมื่อมีเหตุการณ์ซึ่งมีผลกระทบต่อชื่อเสียงขององค์กร

๓.๔.๗ องค์กรต้องมีการกำหนดแนวทางในการสื่อสารกับสาธารณชน เมื่อเกิดเหตุการณ์ที่กระทบต่อชื่อเสียงขององค์กร

๓.๔.๘ จัดให้มีการกำหนดเงื่อนไขในการรายงานไปยังผู้บริหารในแต่ละระดับชั้นอย่างเหมาะสม (Incident Escalation)

๓.๔.๙ ขั้นตอนการการประสานงานกับผู้มีส่วนได้ส่วนเสีย

๓.๔.๑๐ กำหนดแนวทางและรูปแบบข้อมูลในการสื่อสารไปยังกลุ่มธุรกิจในอุตสาหกรรมเดียวกัน เพื่อแจ้งเตือนถึงเหตุการณ์ภัยคุกคามที่อาจมีผลกระทบถึงกัน

๓.๕ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และผู้ดูและหรือผู้ปฏิบัติงานที่ได้รับมอบหมาย จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของประปานครหลวง สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนขององค์กร

๓.๖ คณะทำงานฯ จะต้องจัดให้มีการฝึกซ้อม แผนการรับมือภัยคุกคามทางไซเบอร์ แผน BCP ในสถานการณ์ภัยคุกคามด้านไซเบอร์ แผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละ ๑ ครั้ง

๓.๗ หากการประปานครหลวงได้รับคำสั่งเป็นลายลักษณ์อักษรจาก คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้เข้าร่วมในการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน จะต้องสั่งการให้บุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๓.๘ คณะทำงานฯ มีหน้าที่ในการให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญการประปานครหลวง เพื่อวัตถุประสงค์ในการวางแผนและ ดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) อาจร้องขอ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ แผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้น และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของการประปานครหลวง

๓.๙ คณะทำงานฯ ต้องจัดให้มีการทบทวน แผนการรับมือภัยคุกคามทางไซเบอร์ แผน BCP ในสถานการณ์ภัยคุกคามด้านไซเบอร์ แผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละ ๑ ครั้ง หรือมีการระบุความเสี่ยงใหม่ ๆ ที่สำคัญ หรือหลังจากมีการตรวจจับเหตุการณ์ภัยคุกคามประเภทใหม่ที่มีผลกระทบต่อระบบ

หมวด ๒๔
การบริหารความต่อเนื่องและพร้อมใช้ของระบบสารสนเทศอย่างปลอดภัย
(Information security aspects of business continuity management)

๑. วัตถุประสงค์

เพื่อบริหารความต่อเนื่องและพร้อมใช้ของระบบสารสนเทศอย่างมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบงาน

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ใช้งาน

๓. แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยปรับปรุงแผนเตรียมความพร้อมกรณี ฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๓.๑ ระบุหน้าที่ และความรับผิดชอบของผู้เกี่ยวข้องทั้งหมด

๓.๒ ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญและกำหนดมาตรการเพื่อลดความเสี่ยง ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การถูกโจมตีทางไซเบอร์ การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๓.๓ ระบุขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๓.๔ ระบุขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๓.๕ ระบุช่องทางในการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๓.๖ การสร้างความตระหนัก หรือให้ความรู้แก่ผู้ปฏิบัติงานผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๓.๗ ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓.๘ มีแผนรองรับการดำเนินการธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) และมีการซ้อมปฏิบัติการตามแผนดังกล่าว อย่างน้อยปีละ ๑ ครั้ง

หมวด ๒๕
การใช้เทคโนโลยี Generative AI ที่ยอมรับได้
(Acceptable Use Policy: Generative AI)

๑. วัตถุประสงค์

เพื่อกำหนดแนวทางการใช้เทคโนโลยี Generative AI .ให้พนักงานทราบถึงผลกระทบของการไม่ปฏิบัติตามนโยบาย และตัวอย่างพฤติกรรมที่ควรทำและไม่ควรทำของการใช้งานเทคโนโลยี Generative AI ที่การประปานครหลวงแนะนำ เพื่อให้สามารถนำเทคโนโลยี Generative AI ไปใช้งานได้อย่างถูกต้องเหมาะสมมีความรับผิดชอบและสามารถนำเทคโนโลยีดังกล่าวไปรังสรรค์งานได้อย่างปลอดภัย มีประสิทธิภาพ ตลอดจนป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานที่ไม่เหมาะส

๒. ผู้รับผิดชอบ

๒.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ การใช้เทคโนโลยี Generative AI ที่ยอมรับได้ สำหรับการดำเนินงานตามภารกิจของการประปานครหลวง

๓.๑.๑ ผู้ใช้งานต้องทำการศึกษาข้อมูลเทคโนโลยี Generative AI แต่ละประเภทเพื่อสร้างความเข้าใจเกี่ยวกับข้อมูลพื้นฐาน ศักยภาพ ประโยชน์ ความเสี่ยง และข้อจำกัด เพื่อให้ผู้ใช้งานสามารถประยุกต์ใช้เทคโนโลยี Generative AI ได้อย่างเหมาะสม มีประสิทธิภาพและสอดคล้องกับเป้าหมายของงานแต่ละประเภทที่ได้รับมอบหมาย

๓.๑.๒ ผู้ใช้งานต้องประยุกต์ใช้เทคโนโลยี Generative AI เพื่อช่วยสนับสนุนในการดำเนินงานในบริบทที่กำหนด ดังต่อไปนี้

๓.๑.๒.๑ การวิเคราะห์ข้อมูลและสร้างรายงาน

๓.๑.๒.๒ การเขียนชุดคำสั่งหรือโปรแกรม

๓.๑.๒.๓ การจัดทำร่างหนังสือหรือเอกสารต่าง ๆ เช่น บันทึกข้อความ นโยบาย หรือคำแนะนำ เป็นต้น

๓.๑.๒.๔ การให้คำแนะนำหรือแนวทางเบื้องต้นในการแก้ปัญหาด้านต่าง ๆ

๓.๑.๒.๕ การสร้างเนื้อหาสำหรับการสื่อสารภายในองค์กร

๓.๑.๒.๖ การสร้างสื่อประชาสัมพันธ์

๓.๑.๒.๗ ดำเนินงานอื่น ๆ ที่ได้รับมอบหมายจากผู้บังคับบัญชา

ทั้งนี้ การประยุกต์ใช้เทคโนโลยี Generative AI ต้องเป็นไปตามภารกิจและเพื่อประโยชน์ของการประปานครหลวง เท่านั้น

๓.๑.๓ ผู้ใช้งานต้องใช้เทคโนโลยี Generative AI อย่างมีธรรมาภิบาล เหมาะสมมีความมั่นคงปลอดภัย และสอดคล้องกับกฎหมาย ข้อบังคับ ระเบียบ ประกาศ หรือคำสั่งของการประปานครหลวงหรืออื่น ๆ ที่เกี่ยวข้อง

๓.๒ ข้อห้ามในการใช้เทคโนโลยี Generative AI

แม้ว่าเทคโนโลยี Generative AI จะเป็นเครื่องมือที่ช่วยสนับสนุนและเพิ่มประสิทธิภาพในการดำเนินงานให้แก่ผู้ใช้งานอยู่หลายประการ แต่อย่างไรก็ตาม การใช้เทคโนโลยี Generative AI จำต้องอยู่ในขอบเขตที่เหมาะสมและไม่ก่อให้เกิดความเสียหายใด ๆ ต่อบุคคล การประปานครหลวง สังคม หรือประเทศชาติ ในการนี้ การประปานครหลวงจึงกำหนดข้อห้ามสำหรับผู้ใช้งานเทคโนโลยี Generative AI ไว้ดังนี้

๓.๒.๑ ห้ามใช้แทนการตัดสินใจของผู้ใช้งานในกรณีที่มีความเสี่ยงสูง เช่น การตัดสินใจ ทางกฎหมาย ทางการแพทย์ ทางการเงิน หรือการตัดสินใจที่อาจส่งผลกระทบต่อชีวิต ทรัพย์สินและสิทธิของบุคคล

๓.๒.๒ ห้ามใช้เพื่อสร้างข้อมูลอันเป็นเท็จ หรือสร้างเนื้อหาที่อาจก่อให้เกิดความเสียหายต่อบุคคล การประปานครหลวง หรือสังคม อันอาจนำไปสู่ความเข้าใจผิด หรือสร้างความขัดแย้งในสังคม

๓.๒.๓ ห้ามใช้หรือเปิดเผยข้อมูลที่เป็นความลับของการประปานครหลวง รวมถึงข้อมูลภายในเอกสารสำคัญ หรือข้อมูลที่อาจส่งผลกระทบต่อการดำเนินงานของสำนักงาน

๓.๒.๔ ห้ามใช้ข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือใช้ข้อมูลที่อาจเป็นความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๓.๒.๕ ห้ามใช้ในทางที่ขัดต่อหลักธรรมาภิบาล คุณธรรม จริยธรรม ศีลธรรม หรือมีเจตนาแอบแฝงโดยไม่สุจริต

๓.๒.๖ ห้ามใช้เพื่อสร้างเนื้อหาที่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา รวมถึงการทำซ้ำ คัดลอก หรือ ดัดแปลงซึ่งเนื้อหาที่เป็นของบุคคลหรือหน่วยงานอื่นโดยไม่ได้รับอนุญาต

๓.๒.๗ ห้ามใช้เพื่อสร้างเนื้อหาที่ส่งเสริมการเหยียดเชื้อชาติ ศาสนา เพศ วัย ความพิการ หรือสถานะทางสังคม ซึ่งอาจขัดต่อกฎหมายและหลักสิทธิมนุษยชน

๓.๒.๘ ห้ามใช้ในการดำเนินการใด ๆ ที่อาจเป็นการกระทำความผิดตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ คำสั่ง หลักเกณฑ์ หรืออื่น ๆ ที่เกี่ยวข้อง

๓.๓ การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล

การใช้งานเทคโนโลยี Generative AI โดยเฉพาะอย่างยิ่งที่มีการให้บริการแบบไม่มีค่าใช้จ่าย อาจมีความเสี่ยงที่ข้อมูลที่ผู้ใช้งานระบุหรือโต้ตอบกับระบบ จะถูกเข้าถึงหรือบันทึกและนำไปใช้ในการฝึกสอนโมเดล Generative AI เพื่อปรับปรุงและพัฒนาประสิทธิภาพการทำงานของระบบ ดังนั้น เพื่อเป็นการป้องกันมิให้เกิดการรั่วไหลของข้อมูล การละเมิดสิทธิของบุคคล หรือก่อให้เกิดความเสียหายต่อการประปานครหลวง หน่วยงานภายนอก หรือบุคคลที่เกี่ยวข้อง ผู้ใช้งานจึงต้องมีความระมัดระวังและต้องปฏิบัติดังนี้

๓.๓.๑ ห้ามนำข้อมูลภายในการประปานครหลวง และข้อมูลที่มีชั้นความลับ (เช่น รหัสผ่าน เอกสารสัญญา เอกสารหรือหนังสือที่ประทับข้อความลับ เอกสารหรือข้อมูลเกี่ยวกับโครงการภายในการประปานครหลวง เป็นต้น)ไปใช้งานร่วมกับเทคโนโลยี Generative AI

๓.๓.๒ ในกรณีที่ต้องใช้เทคโนโลยี Generative AI ร่วมกับข้อมูลภายในองค์กรข้อมูลที่มีชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลที่อ่อนไหว ผู้ใช้งานจะต้องใช้เทคโนโลยี Generative AI ที่การประปานครหลวงประกาศกำหนดเท่านั้น และผู้ใช้งานต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อนนำมาใช้งานทุกกรณี

๓.๓.๓ ในกรณีที่มีข้อสงสัยเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลหรือข้อกำหนดตามกฎหมาย ผู้ใช้งานต้องปรึกษา หารือกับผู้บังคับบัญชาหรือเจ้าหน้าที่ที่เกี่ยวข้องก่อนดำเนินการใด ๆ

๓.๔ การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีนำเทคโนโลยี Generative AI มาใช้งาน

๓.๔.๑ ห้ามนำข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ(เช่น รหัสผ่าน ข้อมูล API Key รายละเอียดการตั้งค่าของระบบ เป็นต้น) ไปใช้งานร่วมกับเทคโนโลยี Generative AI

๓.๔.๒ ต้องตรวจสอบซอร์สโค้ดที่สร้างโดยเทคโนโลยี Generative AI ก่อนนำมาใช้งานโดยพิจารณาถึงความถูกต้อง และการตรวจสอบช่องโหว่อย่างถี่ถ้วน

๓.๔.๓ หากพบเหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดจากการประยุกต์ใช้เทคโนโลยี Generative AI ผู้ใช้งานต้องแจ้งให้บังคับบัญชาตามลำดับชั้นทราบ และต้องปฏิบัติตามขั้นตอนการปฏิบัติงานเกี่ยวกับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยโดยทันที

๓.๔.๔ การใช้งานเทคโนโลยี Generative AI ผู้ใช้งานต้องดำเนินการให้มีความมั่นคงปลอดภัยไซเบอร์ ความมั่นคงปลอดภัยของระบบสารสนเทศ ความมั่นคงปลอดภัยของข้อมูล และความมั่นคงปลอดภัยในด้านอื่น ๆ ที่เกี่ยวข้อง

๓.๔.๕ การประปานครหลวงจะมีการตรวจสอบการใช้เทคโนโลยีสารสนเทศ Generative AI ของผู้ใช้งานอย่างต่อเนื่องเพื่อเป็นการรักษาความมั่นคงปลอดภัยของการประปานครหลวง

๓.๕ การลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination) ต่อบุคคลหรือกลุ่มบุคคล

ด้วยผลลัพธ์จากการประยุกต์ใช้เทคโนโลยี Generative AI มีโอกาสที่จะสร้างเนื้อหาที่มีความคิดเชิงลบ อคติ หรือแบ่งแยก อันอาจถูกเผยแพร่เป็นวงกว้างและไม่สามารถควบคุมการแพร่กระจายได้โดยง่าย อาจก่อให้เกิดความเสียหายแก่ชื่อเสียง จิตใจของบุคคล เกิดอคติ หรือการเลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล ดังนั้น ผู้ใช้งานจึงต้องมีความระมัดระวังและปฏิบัติ ดังนี้

๓.๕.๑ ต้องตรวจสอบเนื้อหาที่สร้างโดยเทคโนโลยี Generative AI ก่อนนำไปใช้งานหรือเผยแพร่ต่อสาธารณะ เพื่อลดหรือหลีกเลี่ยงการเกิดอคติหรือการเลือกปฏิบัติอย่างไม่เป็นธรรม

๓.๕.๒ ระมัดระวังการใช้งานเทคโนโลยี Generative AI ในการดำเนินงานที่อาจกระทบต่อสิทธิของบุคคลหรือกลุ่มบุคคล หรือมีผลกระทบต่อหลักความเสมอภาค และมาตรฐานด้านสิทธิมนุษยชน

๓.๖ หน้าที่และความรับผิดชอบ

การนำเนื้อหาที่สร้างโดยเทคโนโลยี Generative AI มาใช้งาน อาจส่งผลกระทบเชิงลบต่อบุคคล หน่วยงาน สังคม และประเทศชาติ ทั้งโดยเจตนาหรือไม่เจตนา ซึ่งการประปานครหลวงและผู้ใช้งานไม่อาจปฏิเสธความรับผิดชอบต่อผลที่เกิดขึ้นจากการกระทำดังกล่าวได้ ดังนั้น ผู้ใช้งานและบุคคลที่เกี่ยวข้องกับการประยุกต์ใช้เทคโนโลยี Generative AI จึงมีหน้าที่และความรับผิดชอบ ดังนี้

๓.๖.๑ ผู้ใช้งานต้องแจ้งผู้บังคับบัญชาเกี่ยวกับวัตถุประสงค์ ขอบเขตและลักษณะของการทำงานร่วมกันระหว่างผู้ใช้งานกับเทคโนโลยี Generative AI (AI-Human Involvement) และเมื่อมีใช้เทคโนโลยี Generative AI ในการปฏิบัติงาน

๓.๖.๒ ผู้ใช้งานต้องปฏิบัติตามหลักเกณฑ์และวิธีการใช้งานเทคโนโลยี Generative AIตามที่กำหนดในแนวปฏิบัตินี้ และตรวจสอบเนื้อหาที่สร้างโดยเทคโนโลยี Generative AI ก่อนนำไปใช้งานหรือเผยแพร่ และต้องมีการตรวจสอบอย่างเคร่งครัด โดยเฉพาะเนื้อหาที่เกี่ยวข้องกับกฎหมาย ข้อมูลด้านการเงิน ข้อมูลอ่อนไหว ซึ่งผู้ใช้งานจำเป็นต้องพิจารณาในประเด็นดังตอไปนี้ ประกอบด้วย

๓.๖.๒.๑ ความถูกต้องของเนื้อหา

๓.๖.๒.๒ ผลการใช้งานหรือเผยแพร่เนื้อหาที่นำไปสู่การกระทำผิดทางกฎหมาย

๓.๖.๒.๓ รวมถึงการละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือทรัพย์สินทางปัญญาอื่น ๆ

๓.๖.๒.๔ ความเท่าเทียมและการไม่เลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล

๓.๖.๒.๕ การรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล

๓.๖.๒.๖ ผลกระทบต่อความมั่นคงปลอดภัยและความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน

๓.๖.๒.๗ ผลกระทบเชิงลบอื่น ๆ ที่อาจเกิดขึ้นต่อบุคคล การประปานครหลวง สังคม และประเทศชาติ

๓.๖.๓ ผู้ใช้งานต้องรายงานให้ผู้บังคับบัญชารับทราบโดยทันที ในกรณีที่การประยุกต์ใช้ Generative AI เกิดความผิดพลาดหรือพบประเด็นปัญหา ทั้งกรณีการนำเข้าข้อมูลและแสดงผลลัพธ์ที่อาจส่งผลกระทบเชิงลบต่อบุคคล การประปานครหลวง สังคม และประเทศชาติ เพื่อให้สามารถดำเนินมาตรการแก้ไขได้โดยเร็ว

๓.๖.๔ ผู้บังคับบัญชาและผู้ใช้งานต้องมีการติดตาม ทบทวน และประเมินประสิทธิภาพประสิทธิผลของการใช้งานเทคโนโลยี Generative AI อย่างต่อเนื่อง เพื่อปรับปรุงวิธีการทำงานและการเลือกใช้เทคโนโลยี Generative AI ที่เหมาะสมกับการปฏิบัติงาน

๓.๖.๕ การนำเนื้อหาที่สร้างจากเทคโนโลยี Generative AI มาใช้งาน ต้องมีการระบุว่า “เนื้อหานี้ได้รับความช่วยเหลือจากเทคโนโลยี Generative AI” ตามความเหมาะสม เพื่อให้เกิดความโปร่งใส และป้องกันความเข้าใจผิดของผู้รับข้อมูล

๓.๖.๖ คณะทำงานฯ มีหน้าที่ในการพิจารณาตรวจสอบและนำเสนอ คณะกรรมการฯ ถึงรายการแอปพลิเคชัน หรือบริการ Generative AI ที่ใช้งานภายในการประปานครหลวง ตามความเหมาะสมของระดับการใช้งาน

๓.๗ การเคารพสิทธิในทรัพย์สินทางปัญญา

๓.๗.๑ การนำเนื้อหาที่สร้างโดยเทคโนโลยี Generative AI ไปใช้งานหรือเผยแพร่ต่อสาธารณะ ผู้ใช้งานต้องใช้แอปพลิเคชันหรือบริการของเทคโนโลยี Generative AI ที่การประปานครหลวงประกาศกำหนดเท่านั้น

๓.๗.๒ การประยุกต์ใช้เทคโนโลยี Generative AI ผู้ใช้งานต้องมีความระมัดระวังไม่ให้เกิดการละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือสิทธิในทรัพย์สินทางปัญญาอื่น ๆ โดยการตรวจสอบให้แน่ใจว่าเนื้อหาที่สร้างขึ้นไม่เป็นการทำซ้ำ คัดลอก ดัดแปลง หรือใช้ประโยชน์จากผลงานที่มีเจ้าของโดยไม่ได้รับอนุญาต เพื่อป้องกันการละเมิดกฎหมายและข้อพิพาทที่อาจเกิดขึ้น

หมวด ๒๖
การปฏิบัติตามข้อบังคับ
(Compliance)

๔. วัตถุประสงค์

การปฏิบัติตามข้อบังคับด้านกฎหมาย เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมายที่เกี่ยวข้องกับการดำเนินงานขององค์กร การที่องค์กรทราบถึงข้อกำหนดต่างๆ ที่เกี่ยวข้อง จะทำให้ผู้ปฏิบัติงานมี ความตระหนักถึงความเสี่ยงที่เกิดขึ้นรวมทั้งวางมาตรการควบคุมที่เหมาะสมได้ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการละเมิดดังกล่าว

๕. ผู้รับผิดชอบ

๕.๑ คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๕.๒ ผู้ดูแลระบบงาน

๕.๓ ผู้ใช้งาน

๖. แนวปฏิบัติ

๖.๑ การปฏิบัติตามข้อบังคับด้านกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานคอมพิวเตอร์จะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานคอมพิวเตอร์กระทำผิดตามกฎหมายดังกล่าว องค์กรถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล

๖.๒ คณะทำงานฯ มีหน้าที่ในการติดตามกฎหมาย ข้อบังคับ ประกาศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และศึกษาผลกระทบต่อการดำเนินงานขององค์กร พิจารณาแนวทางในการดำเนินการตามกฎหมาย ข้อบังคับ ประกาศ นั้นซึ่งอาจผ่านการ ปรับปรุงหรือจัดทำนโยบายและ/หรือแนวปฏิบัติ การจัดให้เกิดความตระหนักหรือความความรู้แก่บุคคลากรในองค์กร หรือการจัดให้มีอุปกรณ์เครื่องมือ กลไกทางเทคโนโลยีเพื่อให้องค์กรสามารถปฏิบัติตามข้อบังคับดังกล่าวได้

๖.๓ ผู้บังคับบัญชา ผู้บริหารของแต่ละหน่วยงานมีหน้ามี่ควบคุมดูแลให้บุคคลการภายใต้การดูแลปฏิบัติตามกฎหมาย ข้อบังคับ ประกาศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๖.๔ หากพบการไม่ปฏิบัติตามกฎหมาย ข้อบังคับ ประกาศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ไม่ว่าโดย บุคลากรขององค์กร ผู้ดูแลระบบงาน ผู้ดูแลระบบเครือข่าย หรือผู้บริหาร จะต้องทำการแจ้งเหตุการณ์ไม่ปฏิบัติตามกฎหมาย ข้อบังคับ ประกาศ นั้นต่อคณะทำงาน ฯ เพื่อหาแนวทางลดความเสี่ยง จำกัดผลกระทบของเหตุการณ์และดำเนินการเพื่อป้องกันไม่ให้

เกิดขึ้นซ้ำในอนาคต และคณะทำงานฯ ต้องติดตามแผนการดำเนินการนั้นเพื่อให้มั่นใจว่ามีประสิทธิผล

๖.๕ การปกป้องข้อมูลส่วนบุคคล

๖.๕.๑ ข้อมูลรายละเอียดที่เกี่ยวกับการดำเนินงานขององค์กรถือว่าเป็นข้อมูลสำคัญเฉพาะผู้ปฏิบัติงานที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บริหารเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวได้

๖.๕.๒ ข้อมูลส่วนตัวของผู้ปฏิบัติงานถือว่าเป็นข้อมูลลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิได้แก่ ผู้ปฏิบัติงานเอง หรือผู้ทำงานที่มีความเกี่ยวข้องเท่านั้น อย่างไรก็ดี องค์กรสงวนสิทธิ์ในการเข้าถึงข้อมูลทั้งหมดที่สร้างและเก็บอยู่ในระบบสารสนเทศขององค์กร

๖.๖ ลิขสิทธิ์ซอฟต์แวร์

๖.๖.๑ ห้ามมิให้ผู้ปฏิบัติงานนำซอฟต์แวร์ภายนอกมาใช้ในระบบประมวลผลขององค์กร โดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในหน่วยงาน ทั้งนี้ผู้บังคับบัญชาต้องสอบทานกับฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ในเรื่องลิขสิทธิ์ขององค์กรและความเสี่ยงด้านความปลอดภัยสารสนเทศในการนำซอฟต์แวร์ดังกล่าว มาใช้ตามลำดับ

๖.๖.๒ ผู้ปฏิบัติงานไม่ทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งานยกเว้นการทำสำเนานั้นเพียงเพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

๖.๖.๓ ซอฟต์แวร์ที่พัฒนาภายในองค์กร ทั้งโดยบุคคลอื่นหรือผู้ปฏิบัติงานขององค์กรถือเป็นเป็นทรัพย์สินขององค์กรไม่อนุญาตให้ผู้ปฏิบัติงานทำสำเนาหรือเผยแพร่ซอฟต์แวร์ ที่เป็นทรัพย์สินขององค์กรโดยไม่ได้รับการอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร

๖.๖.๔ ผู้ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรทั้งหมด ยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

๖.๖.๕ ซอฟต์แวร์ที่ได้จัดซื้อจากภายนอกอาจมีเงื่อนไขในเรื่องลิขสิทธิ์ด้านการใช้งานที่แตกต่างกัน หน่วยงานที่รับผิดชอบด้านการจัดซื้อ รับผิดชอบในการศึกษาเงื่อนไขดังกล่าว และสร้างความตระหนักถึง ผู้ใช้งานซอฟต์แวร์ดังกล่าวได้ทราบถึงเงื่อนไข ต่าง ๆ และข้อห้ามที่เกี่ยวข้อง

๖.๖.๖ การจัดซื้อหรือใช้ซอฟต์แวร์ของบุคคลอื่นต้องปฏิบัติให้สอดคล้องกับข้อตกลงด้านลิขสิทธิ์ ห้ามนำซอฟต์แวร์ที่ซื้อไปติดตั้งที่คอมพิวเตอร์เครื่องอื่นนอกเหนือจากเครื่องที่ได้มีการติดตั้งแล้วตามข้อตกลงเรื่อง ลิขสิทธิ์ซอฟต์แวร์

๖.๖.๗ ทำการตรวจสอบการใช้งานคอมพิวเตอร์ขององค์กรอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์คอมพิวเตอร์ทุกชนิดเป็นไปตามข้อตกลงด้านลิขสิทธิ์ซอฟต์แวร์

๖.๖.๘ ผู้ปฏิบัติงานที่ฝ่าฝืนละเมิดข้อตกลงด้านลิขสิทธิ์ของเจ้าของซอฟต์แวร์ถือว่าเป็นการละเมิดนโยบายความปลอดภัยสารสนเทศขององค์กร ถึงแม้การละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานขององค์กร ผู้ปฏิบัติงานต้องรับผิดชอบผลเสียหายทั้งหมด

๖.๖.๙ ในกรณีที่หน่วยงานใดมีความจำเป็นต้องใช้โปรแกรมคอมพิวเตอร์นอกเหนือจากที่เจ้าหน้าที่ของหน่วยงานที่ทำหน้าที่ดูแลระบบสารสนเทศติดตั้งให้ และยังไม่มีใบอนุญาตลิขสิทธิ์การใช้งานจาก ผู้ผลิตแล้ว ให้หน่วยงานดังกล่าวดำเนินการดังนี้

๖.๖.๙.๑ ดำเนินการจัดหาใบอนุญาตลิขสิทธิ์การใช้งานจากผู้ผลิตให้ถูกต้อง

๖.๖.๙.๒ ในกรณีที่ไม่อาจดำเนินการตามข้อ ๓.๖.๙.๑ ได้ ให้หน่วยงานดังกล่าวดำเนินการลบโปรแกรมคอมพิวเตอร์ออกจากเครื่องคอมพิวเตอร์โดยเร็ว

๖.๖.๙.๓ หากผู้ดูแลระบบสารสนเทศตรวจสอบได้ว่ามีการติดตั้งโปรแกรมคอมพิวเตอร์เกินความจำเป็นของการใช้ของระบบงาน สามารถดำเนินการลบโปรแกรมคอมพิวเตอร์ออกจากเครื่องคอมพิวเตอร์นั้นได้

๖.๖.๑๐ ห้ามทุกหน่วยงานติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์

๖.๖.๑๑ ห้ามทุกหน่วยงานติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้นหรือเครือข่ายคอมพิวเตอร์ของการประปานครหลวงได้

หมวด ๒๗
การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Audit)

๑. วัตถุประสงค์

เพื่อจัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่ ซึ่งเป็นกระบวนการสำคัญในการสนับสนุนให้การบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทาง ไซเบอร์ตาม พระราชบัญญัติ ารรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นไปอย่างยั่งยืน และมีการพัฒนาอย่างต่อเนื่อง

๒. ผู้ที่เกี่ยวข้อง

๒.๑ หน่วยงานตรวจสอบภายใน

๓. แนวปฏิบัติ

๓.๑ หน่วยงานตรวจสอบภายในจะต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งดำเนินการโดยผู้ที่มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง โดยมีเนื้อหาในการตรวจสอบครอบคลุมเนื้อหาเหล่านี้เป็นอย่างน้อย

๓.๑.๑ กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ซึ่งเกิดจากภัยคุกคามทางไซเบอร์

๓.๑.๒ มาตรการในการรักษาความมั่นคงปลอดภัยของบริการที่สำคัญองค์กร ซึ่งเป็นผลจากการวิเคราะห์ในข้อ ๓.๑.๑

๓.๑.๓ ระดับของการปฏิบัติตามกฎหมายพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒ การดำเนินการตรวจสอบภายในจะต้องพิจารณาถึงข้อกำหนดทางกฎหมายที่องค์กรต้องปฏิบัติตามและความรับผิดทางกฎหมาย ซึ่งเกี่ยวข้องกับความปลอดภัยทางไซเบอร์

๓.๓ ผู้ตรวจสอบภายในด้านการบริหารความเสี่ยงด้านไซเบอร์ มีหน้าที่ในการจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งดำเนินการตามข้อที่ ๓.๑ ต่อสำนักงานภายในกำหนด ๓๐ วัน นับแต่วันที่ดำเนินการแล้วเสร็จ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๓.๔ ในกรณีที่ผลจากการตรวจสอบตามข้อที่ ๓.๒ พบความไม่สอดคล้องในการปฏิบัติตามกฎหมายฯ ผู้ตรวจสอบภายในด้านการบริหารความเสี่ยงด้านไซเบอร์ ต้องจัดทำแผนในการดำเนินการแก้ไขภายในกำหนด ๓๐ วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

๓.๔.๑ รายละเอียดการดำเนินการแก้ไขเพื่อจัดการกับการไม่ปฏิบัติตาม

๓.๔.๒ กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้

๓.๕ ผู้ตรวจสอบภายในด้านการบริหารความเสี่ยงด้านไซเบอร์ ต้องติดตามให้มีการดำเนินการแก้ไขตามแผนในข้อ ๓.๓ ซึ่งได้รับความเห็นชอบจาก กกม.แล้ว ภายในกรอบระยะเวลาที่ระบุไว้ในแผน เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

ผู้จัดทำ	
ชื่อ นายสุรบดี แก้วพ่วงเสก ตำแหน่ง ผอ.กขม.ฝคท วันที่ 24 ก.ค. 2568	ลงชื่อ ..... ((นายสุรบดี แก้วพ่วงเสก) ผอ.กขม.ฝคท.)
ผู้สอบทาน	
ชื่อ นายภาคภูมิ พิระชัย ตำแหน่ง ผอ.ฝคท. วันที่ 24 ก.ค. 2568	ลงชื่อ ..... ((นายภาคภูมิ พิระชัย) ผอ.ฝคท.)
ผู้อนุมัติ	
ชื่อ นายปริพรรห์ พิณสุรงค์ ตำแหน่ง รวก.(ท) วันที่ 25 ก.ค. 2568	ลงชื่อ ..... ((นายปริพรรห์ พิณสุรงค์) รวก.(ท))