ประกาศการประปานครหลวง
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์
ของการประปานครหลวง (Information and Cyber Security Policy)

โดยที่เป็นการสมควรปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวง ให้สอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๔๓ และที่แก้ไขเพิ่ม รวมทั้งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

อาศัยอำนาจตามความในมาตรา ๓๓ (๒) แห่งพระราชบัญญัติการประปานครหลวง พ.ศ. ๒๕๑๐ ประกอบกับมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๔๓ และที่แก้ไขเพิ่ม และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จึงกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวงให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยความเห็นชอบของคณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO ๒๗๐๐๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของการประปานครหลวง จึงออกประกาศดังต่อไปนี้

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

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิก ประกาศการประปานครหลวง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการประปานครหลวง ประกาศ ณ วันที่ ๓๐ กันยายน ๒๕๖๕

ข้อ ๔ ในประกาศนี้

“องค์กร” หมายถึง การประปานครหลวง

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของการประปานครหลวง

“มาตรฐาน (Standard)” หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

วิธีการ...

"วิธีการปฏิบัติ (Procedure)" หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งบรรทัดฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

"แนวทางปฏิบัติ (Guideline)" หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

"ผู้ใช้งาน" หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานระบบเครือข่าย หรือระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ดังนี้

(๑) "ผู้บริหาร" หมายถึง ผู้ว่าการ รองผู้ว่าการ ผู้ช่วยผู้ว่าการ ผู้อำนวยการฝ่าย ผู้จัดการสำนักงานประปาสาขา ผู้อำนวยการกอง หัวหน้าส่วน ซึ่งรวมถึงคณะกรรมการบริหาร

(๒) "ผู้ปฏิบัติงาน" หมายถึง พนักงาน และลูกจ้างเอกชนของการประปานครหลวง

(๓) "บุคคลภายนอก" หมายถึง บุคคล หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ สามารถเข้าระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศขององค์กร

"ผู้ดูแล (Administrator)" หมายถึง ผู้ปฏิบัติงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ

"สิทธิของผู้ใช้งาน (User Access Right)" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานหรือการประปานครหลวง

"หน่วยงานภายนอก" หมายถึง องค์กรหรือหน่วยงานภายนอกที่การประปานครหลวงอนุญาต ให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของการประปานครหลวง โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

"ข้อมูลคอมพิวเตอร์ (Data)" หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความ รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

"สารสนเทศ (Information)" หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใช้ได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย (Network System)" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ขององค์กรได้ ได้แก่ ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น

"ระบบเทคโนโลยีสารสนเทศ (Information Technology System)" หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้...

"พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace)" หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

(๑) พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

(๒) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

(๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)

(๔) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

(๕) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"เจ้าของระบบงาน" หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลระบบงานที่พัฒนา ซึ่งสามารถกำหนดการใช้งานระบบงานให้กับผู้ใช้งานได้

"สินทรัพย์" หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ อุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เป็นต้น

"อุปกรณ์พกพา (Mobile Device)" หมายถึง เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเล็ต (Tablet) โดยอุปกรณ์พกพาใช้เพื่อการเข้าถึงการใช้งานและจัดเก็บสารสนเทศของการประปานครหลวง

"จดหมายอิเล็กทรอนิกส์ (E-Mail)" หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP เป็นต้น

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"ชุดคำสั่งไม่พึงประสงค์" หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตนั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

"ไซเบอร์ (Cyber)" หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป (อ้างอิงจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒)

"ความมั่นคง...

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information Security incident)" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๕ ขอบเขตการดำเนินการ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวง มีขอบเขตครอบคลุมการบริหารจัดการ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบเครื่องแม่ข่าย การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา การใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ การป้องกัน ระบบเครือข่ายและตรวจจับการบุกรุก การสำรองและกู้คืนข้อมูลการสอบทานการปฏิบัติตามนโยบาย รวมถึงการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ข้อ ๖ วัตถุประสงค์

๖.๑ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรตระหนักถึงความสำคัญ ของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๖.๒ เพื่อเผยแพร่ให้ผู้ปฏิบัติงานทุกระดับในองค์กรได้รับทราบ และผู้ปฏิบัติงานทุกคนต้องถือปฏิบัติ ตามนโยบายนี้อย่างเคร่งครัด

๖.๓ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๖.๔ เพื่อกำหนดความรับผิดชอบ ในกรณีที่ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารซึ่งดำรงตำแหน่งผู้บริหารสูงสุดขององค์กร เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๗ แนวทางการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๗.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๗.๑.๑ ผู้บริหาร ผู้ปฏิบัติงานด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการจัดทำนโยบาย

๗.๑.๒ นโยบาย...

๗.๑.๒ นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านเว็บไซต์ของการประปานครหลวง

๗.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจนมีการทบทวน และปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๗.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๗.๒.๑ การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง สะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่ถูกเปิดเผย

๗.๒.๒ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๗.๒.๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๗.๒.๔ การสร้างความรู้ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่ การใช้งานระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๘ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวง (Information and Cyber Security Policy) มีดังต่อไปนี้

๘.๑ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ (Information and Cyber Security Risk Assessment Policy)

๘.๑.๑ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ที่อาจเกิดขึ้นกับระบบสารสนเทศและไซเบอร์ (Information and cyber security audit and assessment) ปีละ ๑ ครั้ง

๘.๑.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศขององค์กร (Internal IT Auditor) และหน่วยงานตรวจสอบภายใน (Internal Auditing unit) เพื่อให้องค์กรทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

๘.๒ นโยบายการบริหารองค์กรและทรัพยากรมนุษย์เพื่อการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Organization and Human Resource Security)

๘.๒.๑ มีการฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ

๘.๒.๒ ให้ความรู้เกี่ยวกับแนวปฏิบัติ โดยการจัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงานในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๘.๒.๓ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผลและสำรวจความต้องการของผู้ใช้บริการ

๘.๒.๔ มีการ...

๘.๒.๔ มีการทบทวนหน้าที่รับผิดชอบที่เกี่ยวกับความปลอดภัยสารสนเทศที่ได้มอบหมายไปอย่างสม่ำเสมอ

๘.๒.๕ มีกระบวนการบริหารจัดการด้านทรัพยากรมนุษย์อย่างปลอดภัย ตั้งแต่กระบวนการควบคุมระหว่างพิจารณารับบุคลากร กระบวนการควบคุมบุคลากรระหว่างการปฏิบัติหน้าที่ และกระบวนการควบคุมหลังจากที่มีการเลิกจ้างบุคลากร

๘.๓ นโยบายด้านการจัดการทรัพย์สินสารสนเทศ (Asset Management)

๘.๓.๑ มีการจัดทำบัญชีทรัพย์สินสารสนเทศ โดยจะต้องมีการระบุเจ้าของทรัพย์สินผู้รับผิดชอบไว้อย่างชัดเจน

๘.๓.๒ มีการจัดเก็บทะเบียนทรัพย์สินสารสนเทศเพื่อใช้สนับสนุนการรับมือเหตุการณ์ภัยคุกคามด้านไซเบอร์

๘.๓.๓ ทรัพย์สินสารสนเทศต่าง ๆ จะต้องมีการแบ่งระดับชั้นความลับของข้อมูลโดยที่ระดับชั้นความลับสามารถแบ่งออกเป็น ๕ ระดับ ได้แก่ ลับที่สุด ลับมาก ลับ ภายใน และทั่วไป

๘.๓.๔ จะต้องมีการบริหารจัดการสื่อบันทึกข้อมูล (Media) อย่างปลอดภัยตั้งแต่การลงทะเบียนเริ่มใช้งาน ตลอดไปจนถึงการทำลายเมื่อเลิกใช้แล้ว

๘.๔ นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy)

๘.๔.๑ ผู้ใช้งานต้องยินยอมใช้งานทรัพย์สินสารสนเทศอย่างปลอดภัยโดยใช้งานทรัพย์สินสารสนเทศ ที่จัดเตรียมไว้ให้ใช้งาน ตามวัตถุประสงค์สำหรับการใช้งานทางธุรกิจขององค์กรเท่านั้น ดังนั้นจึงห้ามมิให้ผู้ใช้งานนำทรัพย์สิน และระบบสารสนเทศต่าง ๆ ไป ใช้นอกกิจการที่องค์กรกำหนดหรือก่อให้เกิดความเสียหายต่อองค์กร

๘.๔.๒ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษา และรับผิดชอบต่อข้อมูลขององค์กรหากเกิดการสูญหาย หรือมีการนำไปใช้ในทางที่ผิด ได้แก่ การเผยแพร่โดยไม่ได้รับอนุญาต ฯลฯ ผู้ใช้งานจะต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้น

๘.๔.๓ การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๘.๔.๔ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๘.๔.๕ การปฏิบัตินโยบายการควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy) โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึง โดยผู้ซึ่งไม่มีสิทธิและต้องให้ผู้ใช้งานออกจากระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน

๘.๔.๖ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบ ว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๘

๘.๕ นโยบายการใช้งานอุปกรณ์พกพา (User of Personal Computer and Mobile Policy)

๘.๕.๑ ต้องใช้อุปกรณ์พกพาที่องค์กรจัดเตรียมให้ หรืออุปกรณ์พกพาส่วนตัวของผู้ปฏิบัติงานที่ได้รับอนุญาตเท่านั้น

๘.๕.๒ ผู้ใช้งานอุปกรณ์พกพาที่องค์กรจัดเตรียมให้หรืออุปกรณ์พกพาส่วนตัวที่ได้รับอนุญาต ต้องดูแลและตรวจสอบไวรัสของเครื่องอย่างสม่ำเสมอ เมื่อนำมาใช้งานในระบบเครือข่ายขององค์กร

๘.๕.๓ องค์กร...

๘.๕.๓ องค์กรต้องควบคุมการใช้งานอุปกรณ์พกพาในการเข้าสู่ระบบสารสนเทศขององค์กร โดยต้องมีมาตรการควบคุมการเข้าถึงระบบเครือข่ายขององค์กร ได้แก่ การลงทะเบียนเครื่องด้วย MAC Address และสามารถใช้ระบบงานเฉพาะตามสิทธิที่ได้รับเท่านั้น

๘.๕.๔ องค์กรต้องควบคุมการใช้งานอุปกรณ์พกพาที่ลงทะเบียนเครื่องด้วย MAC Address และสามารถเข้าใช้งานเครือข่ายโดยไม่ต้องพิสูจน์ตัวตนด้วยรหัสผู้ใช้งานและรหัสผ่าน ให้สามารถเข้าใช้งานระบบอินเทอร์เน็ตและระบบงานเฉพาะตามสิทธิที่ได้รับเท่านั้น และต้องเป็นผู้บริหารระดับสูง

๘.๕.๕ ผู้ใช้งานต้องรับผิดชอบต่อการใช้งานอุปกรณ์พกพาที่ตนเองใช้งาน และผลกระทบที่จะเกิดขึ้น โดยต้องไม่ใช้กระทำความผิดอันขัดต่อระเบียบ นโยบาย ข้อบังคับ กฎหมายที่มีประกาศใช้งาน

๘.๕.๖ ผู้ดูแลต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร เพื่อให้สิทธิต่าง ๆ ในการใช้งานตามความจำเป็น

๘.๕.๗ ผู้ดูแลต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๘.๕.๘ ต้องมีการจำกัดระยะเวลาในการเชื่อมต่อระบบโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ รวมถึงมีการพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงเวลาที่กำหนดไว้ทุก ๆ ๑ ชั่วโมง

๘.๕.๙ การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ ที่พัฒนาในรูปแบบ Web-based Application มีการให้เข้าถึงเฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายภายใน

๘.๕.๑๐ ผู้ดูแลให้ผู้พัฒนาระบบจัดทำคำขออนุมัติการขอพัฒนาระบบใหม่ หรือปรับปรุง ระบบเดิม พัฒนาโดยปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย

๘.๖ นโยบายการควบคุมการเข้าถึงข้อมูลสารสนเทศ (Data Access Control Policy)

๘.๖.๑ ต้องมีการกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ปฏิบัติงานใหม่เพื่อให้มีสิทธิต่าง ๆ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

๘.๖.๒ ผู้ดูแลต้องตรวจสอบการอนุมัติการกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ ทุก ๕ เดือนเป็นอย่างน้อย

๘.๖.๓ ผู้ดูแลต้องบริหารจัดการสิทธิและการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control) ของผู้ใช้งาน การทบทวนสิทธิการใช้งาน และตรวจสอบการละเมิดความปลอดภัย

๘.๖.๔ เจ้าของข้อมูล และเจ้าของระบบงาน ต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น และการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

๘.๖.๕ การควบคุมการเข้าใช้งานระบบจากภายนอกสายงานเทคโนโลยีดิจิทัล ผู้ดูแลต้องมีการควบคุมการใช้งานระบบจากภายนอก กรณีผู้ใช้งานเข้าสู่ระบบจากระยะไกล (Remote Access) โดยการกำหนดสิทธิ การควบคุมพอร์ต (Port) และพิสูจน์ยืนยันตัวตน (Authentication) โดยการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบความถูกต้อง

๘.๗ นโยบาย...

๘.๗ นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Control Policy)

๘.๗.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยคุกคามและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงมีมาตรการเชิงป้องกันตามความเหมาะสม

๘.๗.๒ การลงทะเบียนผู้ใช้งาน (User registration) ต้องมีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๘.๗.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User management) ต้องจัดให้มีการควบคุม และจำกัดสิทธิเพื่อเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๘.๗.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๘.๗.๕ การทบทวนสิทธิการถึงของผู้ใช้งาน (Review of user access right) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

๘.๘ นโยบายการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control Policy)

๘.๘.๑ ผู้ดูแลต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๘.๘.๒ การเข้าสู่ระบบเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตหรืออินทราเน็ต ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของสายงานเทคโนโลยีดิจิทัล ก่อนที่จะสามารถใช้งานได้ทุกกรณี

๘.๘.๓ ผู้ดูแลต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๘.๘.๔ ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กรต้องเชื่อมต่อผ่าน Firewall หรือ Hardware อื่น ๆ ที่มีคุณสมบัติป้องกันการบุกรุก หรือการทำ Packet Filtering

๘.๘.๕ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๘.๘.๖ การเข้าสู่ระบบเครือข่ายภายในองค์กรผ่านทางอินเทอร์เน็ต ต้องมีการ Login และมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๘.๘.๗ ผู้ใช้งานต้องรับผิดชอบระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งผู้ใช้งานต้องไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่าย หรือเข้าถึงระบบสารสนเทศจากบัญชีผู้ใช้งานของตนเอง

๘.๘.๘ IP Address ภายในของระบบเครือข่ายภายในองค์กร ต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๘.๘.๙ การติดตั้ง...

๘.๘.๙ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ปฏิบัติงานสายงานเทคโนโลยีดิจิทัลเท่านั้น

๘.๙ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Policy)

๘.๙.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๘.๙.๒ ก่อนการใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้งและต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๘.๙.๓ ผู้ใช้งานต้องออกจากระบบ (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๘.๙.๔ ระบบเทคโนโลยีสารสนเทศ ระบบงาน อุปกรณ์เครือข่ายมีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

๘.๙.๕ ระบบเทคโนโลยีสารสนเทศมีการล้างหน้าจอหลังจากไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๘.๙.๖ ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบงานเกี่ยวกับงบประมาณและการเงิน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘.๑๐ นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control Policy)

๘.๑๐.๑ ผู้ดูแลต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร เพื่อให้สิทธิต่าง ๆ ในการใช้งานตามความจำเป็น

๘.๑๐.๒ ผู้ดูแลต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๘.๑๐.๓ ต้องมีการจำกัดระยะเวลาในการเชื่อมต่อระบบโปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ รวมถึงมีการพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงเวลาที่กำหนดไว้ ทุก ๆ ๑ ชั่วโมง

๘.๑๐.๔ การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่พัฒนาในรูปแบบ Web-based Application มีการให้เข้าถึงเฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายภายใน

๘.๑๐.๕ ผู้ดูแลให้ผู้พัฒนาระบบจัดทำคำขออนุมัติการขอพัฒนาระบบใหม่ หรือปรับปรุง ระบบเดิม พัฒนาโดยปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย

๘.๑๑ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical Entry Control Policy)

๘.๑๑.๑ กำหนดมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง กับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

๘.๑๑.๒ จัดให้มี...

๘.๑๑.๒ จัดให้มีเวรยามรักษาอาคาร ซึ่งเป็นที่ตั้งของศูนย์คอมพิวเตอร์และอุปกรณ์เครือข่าย ภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายใน เพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูล และระบบเครือข่าย

๘.๑๑.๓ การเข้าถึงอาคารของหน่วยงานภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ ได้แก่ บัตรประจำตัว ประชาชน ใบอนุญาตขับขี่ ผู้มาติดต่อ เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในเอกสาร “บันทึกการเข้า - ออกพื้นที่”

๘.๑๒ นโยบายการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ (Data Center Policy)

๘.๑๒.๑ ผู้ดูแลศูนย์คอมพิวเตอร์ต้องกำหนดสิทธิบุคคลในการเข้า – ออก ศูนย์คอมพิวเตอร์ มีการบันทึก “ทะเบียนผู้มีสิทธิเข้า – ออกพื้นที่”

๘.๑๒.๒ ผู้ดูแลศูนย์คอมพิวเตอร์และผู้ปฏิบัติงานที่เกี่ยวข้องต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้า - ออกศูนย์คอมพิวเตอร์

๘.๑๒.๓ การเข้าถึงศูนย์คอมพิวเตอร์ ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า – ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า – ออกทุกคนต้องกรอกแบบฟอร์มดังกล่าวทุกครั้ง

๘.๑๒.๔ ผู้ติดต่อจากหน่วยงานภายนอกต้องแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า – ออกพื้นที่” และในการเข้าศูนย์คอมพิวเตอร์ ผู้ดูแลต้องเป็นผู้นำพาเข้าไป และคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน

๘.๑๓ นโยบายการเข้ารหัสข้อมูลสารสนเทศ (Cryptography Policy)

๘.๑๓.๑ มีการเข้ารหัสข้อมูลในการรับ-ส่งข้อมูลผ่านระบบเครือข่าย และปฏิบัติตามแนวปฏิบัติการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๘.๑๓.๒ การเข้ารหัสข้อมูลต้องกำหนดวิธีการทางเทคโนโลยีและวิธีการเก็บรักษากุญแจในการเข้ารหัสที่เหมาะสม

๘.๑๔ นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

๘.๑๔.๑ ผู้ดูแลต้องสำรองข้อมูลขององค์กรให้อยู่ในสภาพพร้อมใช้งาน โดยเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร และจัดเก็บไว้ในสถานที่ที่เหมาะสม และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ผู้ดูแลต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือสำรองข้อมูลของระบบที่อยู่ในความรับผิดชอบตามความเหมาะสมของแต่ละแบบ ไม่ต่ำกว่า ๑ ครั้ง ต่อเดือน

๘.๑๔.๒ ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป ต้องสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนตามความเหมาะสม ไม่ต่ำกว่า ๓ เดือน/ครั้ง

๘.๑๔.๓ ผู้ดูแลต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ / ซอฟท์แวร์ เพื่อให้สามารถฟื้นฟู ระบบ/ข้อมูลจากความเสียหาย ที่อาจเกิดขึ้นจากการหยุดทำงานในการประมวลผลของโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ

๘.๑๕ นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (Internet and E-Mail Policy)

๘.๑๕.๑ ผู้ดูแลต้องมีการกำหนดสิทธิการเข้าถึงระบบอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ เฉพาะบัญชีผู้ใช้ที่มีสิทธิเท่านั้น (User Authentication)

๘.๑๕.๒ ผู้ดูแล...

๘.๑๕.๒ ผู้ดูแลต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้ ได้แก่ Proxy Firewall IPS/IDS เป็นต้น

๘.๑๕.๓ กำหนดแนวทางปฏิบัติการใช้งานระบบอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ที่ถูกต้อง โดยผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๘.๑๕.๔ ต้องมีการเก็บข้อมูลการเข้าถึงระบบ (Log File) และข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data)

๘.๑๖ นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

๘.๑๖.๑ ผู้ดูแลจะต้องกำหนดบัญชีผู้ใช้ รหัสผ่าน และสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN)

๘.๑๖.๒ กรณีองค์กรมีนโยบายใช้ชื่อผู้ใช้กลาง ให้ผู้ใช้งานติดต่อผู้ปฏิบัติงานของฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล เพื่อรับค่า SSID (Service Set Identifier) และ Network Key ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่ายไร้สาย

๘.๑๖.๓ ผู้ดูแลต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมและลงทะเบียนอุปกรณ์ไร้สายทุกเครื่อง เพื่อควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งานและป้องกันไม่ให้ผู้โจมตีสามารถรับ – ส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

๘.๑๗ นโยบายควบคุมความปลอดภัยของกระบวนการจัดหา พัฒนา และบำรุงดูแลระบบสารสนเทศ (System acquisition, development and maintenance)

๘.๑๗.๑ เมื่อมีการจัดซื้อจัดหาระบบสารสนเทศใหม่ จะต้องกำหนดข้อกำหนดของโครงการให้มีข้อกำหนดด้านความปลอดภัยสารสนเทศของระบบด้วยทุกครั้ง

๘.๑๗.๒ การพัฒนาหรือติดตั้งระบบสารสนเทศ จะต้องเป็นไปตามกระบวนการพัฒนาระบบสารสนเทศอย่างปลอดภัยตลอดทั้งวงจรของการพัฒนา (Secure System Development Life Cycle)

๘.๑๗.๓ ชุดข้อมูลสารสนเทศซึ่งใช้ระหว่างกระบวนการพัฒนาหรือติดตั้งระบบสารสนเทศ หากเป็นข้อมูลที่ใช้งานจริง จะต้องควบคุมความปลอดภัยของข้อมูลที่ใช้ทดสอบนี้ (Test data) ให้มีความปลอดภัยเทียบเท่ากับข้อมูลจริง

๘.๑๘ นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy)

๘.๑๘.๑ บุคคลภายนอกที่ต้องการสิทธิในการขอเข้าถึงใช้งานระบบเครือข่าย หรือระบบแอปพลิเคชันขององค์กร ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเครือข่าย หรือระบบแอปพลิเคชันเพื่อขออนุมัติจากผู้บริหารระดับฝ่ายขึ้นไป

๘.๑๘.๒ หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายใน องค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๘.๑๘.๓ สำหรับโครงการขนาดใหญ่ ผู้ดูแลต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กรให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๘.๑๘.๔ ผู้ให้บริการ...

๘.๑๘.๔ ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

๘.๑๙ นโยบายการบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศและไซเบอร์ (Information and Cyber Security Incident Management)

๘.๑๙.๑ มีการจัดทำขั้นตอนการบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศและไซเบอร์ รวมถึงจัดหาเครื่องมือที่เหมาะสมไว้เพื่อบริหารจัดการเหตุการณ์ดังต่อไปนี้

(๑) เหตุการณ์ด้านความปลอดภัยสารสนเทศ

(๒) เหตุการณ์ด้านความอ่อนแอหรือช่องโหว่ของระบบสารสนเทศ

(๓) เหตุการณ์ด้านภัยคุกคามทางไซเบอร์

๘.๑๙.๒ ขั้นตอนและเครื่องมือที่ใช้สำหรับการบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศจะต้องได้รับการทบทวนอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๘.๒๐ นโยบายการบริหารความเนื่องและพร้อมใช้ของระบบสารสนเทศอย่างปลอดภัย (Information security aspects of business continuity management)

๘.๒๐.๑ มีการจัดการต่อความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศควบคู่กับการบริหารจัดการความต่อเนื่องทางธุรกิจขององค์กร

๘.๒๐.๒ มีการวางแผนความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศโดยระบุเป็นข้อกำหนดเพื่อนำไปใช้ภายใต้สถานการณ์ที่ไม่พึงประสงค์ เช่น ในช่วงวิกฤติภัยพิบัติหรือภัยคุกคามไซเบอร์

๘.๒๐.๓ มีการจัดการทวนสอบ ทบทวน และประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศและไซเบอร์ โดยการจัดทำขึ้นและนำไปปฏิบัติตามรอบระยะเวลาที่กำหนดเพื่อคงใช้มาตรการอย่างสมเหตุสมผล และมีประสิทธิผลในระหว่างสถานการณ์ที่ไม่พึงประสงค์

๘.๒๐.๔ มีการตรวจสอบความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล โดยกำหนดให้มีระบบสำรองไว้อย่างเพียงพอ เพื่อเป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน

๘.๒๐.๕ มีการตรวจสอบความพร้อมใช้ของระบบสำรองเพื่อให้มั่นใจว่าอุปกรณ์ประมวลผลข้อมูลมีความพร้อมใช้งานได้อย่างมีประสิทธิภาพ

๘.๒๑ นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Policy)

๘.๒๑.๑ มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๒๑.๒ มีแผนการรับมือภัยคุกคามทางไซเบอร์ โดยปฏิบัติตามคู่มือแนวปฏิบัติในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์

๘.๒๑.๓ มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และรายงานผลการตรวจสอบให้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ทุกปี

๘.๒๒ นโยบายด้านการปฏิบัติตามข้อบังคับ (Compliance Policy)

๘.๒๒.๑ มีการระบุข้อกำหนดด้านกฎหมายและสัญญาที่เกี่ยวข้องทั้งหมด โดยมีการระบุไว้อย่างชัดเจนเป็นเอกสาร และปรับปรุงให้ทันสมัยอยู่เสมอ สำหรับแต่ละระบบสารสนเทศและสำหรับองค์กร

๘.๒๒.๒ มีการ...

๘.๒๒.๒ มีการปฏิบัติตามข้อกำหนดด้านกฎหมายและสัญญา เพื่อหลีกเลี่ยงการละเมิดกฎหมาย ระเบียบข้อบังคับ ข้อกำหนด หรือข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ และข้อกำหนดด้านความมั่นคงปลอดภัยใด ๆ ก็ตาม

๘.๒๒.๓ มีการกำหนดสิทธิในทรัพย์สินทางปัญญาตามขั้นตอนปฏิบัติที่เหมาะสมเพื่อนำไปปฏิบัติ โดยสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับสิทธิในทรัพย์สินทางปัญญา และการใช้ซอฟต์แวร์ที่มีกรรมสิทธิ์

๘.๒๒.๔ มีการป้องกันการบันทึกเพื่อป้องกันจากการสูญหาย การทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่ออกไปโดยไม่ได้รับอนุญาต ตามที่กฎหมาย ระเบียบข้อบังคับ ข้อผูกพันตามสัญญา และข้อกำหนดทางธุรกิจที่ได้กำหนดไว้

๘.๒๒.๕ มีการจัดการความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล เพื่อเป็นไปตามที่ระบุไว้ในกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องที่เหมาะสม

๘.๒๒.๖ มีการจัดตั้งข้อบังคับของมาตรการควบคุมการเข้าถึงข้อมูล โดยการเข้ารหัสเพื่อนำไปใช้ให้สอดคล้องกับข้อตกลงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด

๘.๒๒.๗ มีการทบทวนความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อนำไปปฏิบัติและดำเนินการตามนโยบายและขั้นตอนปฏิบัติงานขององค์กร

๘.๒๒.๘ มีการทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศและไซเบอร์อย่างเป็นอิสระ โดยสอดคล้องกับวัตถุประสงค์ของมาตรการควบคุม นโยบาย กระบวนการ และขั้นตอนปฏิบัติงานสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ และมีการทบทวนอย่างเป็นอิสระตามรอบระยะเวลาที่กำหนดหรือเมื่อมีความเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น

๘.๒๒.๙ มีการปฏิบัติตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย โดยมีการทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลข้อมูล และขั้นตอนปฏิบัติงานที่อยู่ภายใต้ความรับผิดชอบ กับนโยบายและมาตรฐานความมั่นคงปลอดภัยอย่างเหมาะสม

๘.๒๒.๑๐ มีการทบทวนความสอดคล้องทางเทคนิคต่อระบบสารสนเทศอย่างสม่ำเสมอเพื่อสอดคล้องกับนโยบายและมาตรฐานความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

ข้อ ๙ การกำหนดความรับผิดชอบ

๙.๑ ระดับนโยบาย

๙.๑.๑ ให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์หรือข้อมูลเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผู้บริหารระดับสูงมีหน้าที่กำกับดูแลรับผิดชอบให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

๙.๑.๒ ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่ผู้ปฏิบัติงานระดับปฏิบัติ

๙.๒ ระดับปฏิบัติการ

๙.๒.๑ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Risk Assessment Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองตรวจสอบสารสนเทศ

(๒) ผู้ตรวจสอบ...

(๒) ผู้ตรวจสอบภายใน (Internal Auditor)

(๓) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๒ นโยบายการบริหารโครงสร้างองค์กรและทรัพยากรมนุษย์ เพื่อการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Organization and Human Resource Security) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของฝ่ายบริหารทรัพยากรบุคคล

๙.๒.๓ นโยบายด้านการจัดการทรัพย์สินสารสนเทศ (Asset Management) ผู้รับผิดชอบได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๔ นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครื่องแม่ข่าย

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๕ นโยบายการใช้งานอุปกรณ์พกพา (User of Personal Computer and Mobile) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๖ นโยบายการควบคุมการเข้าถึงข้อมูลสารสนเทศ (Data Access Control Policy) ผู้รับผิดชอบ ได้แก่

(๑) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

(๒) บริกรข้อมูล (Data Stewards)

๙.๒.๗ นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Control Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๘ นโยบายการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๙ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครื่องแม่ข่าย

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๐ นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการฝ่ายพัฒนาระบบงานดิจิทัล

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๑ นโยบาย...

๙.๒.๑๑ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical Entry Control Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองอาคารและสถานที่

(๒) ผู้อำนวยการกองทรัพย์สินเทคโนโลยีดิจิทัล

(๓) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๒ นโยบายการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์ (Data Center Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองทรัพย์สินเทคโนโลยีดิจิทัล

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๓ นโยบายการเข้ารหัสข้อมูล (Cryptography Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๔ นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครื่องแม่ข่าย

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๕ นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์ (Internet and E-Mail Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครื่องแม่ข่าย

(๒) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๓) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๖ นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๗ นโยบายควบคุมความปลอดภัยของกระบวนการจัดหา พัฒนาและบำรุงดูแลระบบสารสนเทศ (System acquisition, development and maintenance) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการฝ่ายพัฒนาระบบงานดิจิทัล

(๒) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๓) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๘ นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๑๙ นโยบายการบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศ (Information Security Incident Management) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๒๐ นโยบาย...

๙.๒.๒๐ นโยบายการบริหารความต่อเนื่องและพร้อมใช้ของระบบสารสนเทศอย่างปลอดภัย (Information security aspects of business continuity management) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๒๑ นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้ช่วยผู้ว่าการ (เทคโนโลยีดิจิทัล) ปฏิบัติงานในฐานะ Head of Information Security

(๒) ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ปฏิบัติงานในฐานะ Chief Information Security Officer : CISO

(๓) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๔) พนักงานของหน่วยงานที่ได้รับมอบหมาย

๙.๒.๒๒ นโยบายด้านการปฏิบัติตามข้อบังคับ (Compliance Policy) ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

(๒) พนักงานของหน่วยงานที่ได้รับมอบหมาย

ข้อ ๑๐ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา ๑ ครั้งต่อปี

ข้อ ๑๑ นโยบายตามข้อ ๘ ถือเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร โดยให้ดำเนินอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวง” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งผู้บริหาร ผู้ปฏิบัติงานขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่๒๘สิงหาคม พ.ศ. ๒๕๖๖

(นายมานิต ปานเอม)
ผู้ว่าการการประปานครหลวง