ประกาศศูนย์สนับสนุนบริการสุขภาพเขตที่ ๔
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๔ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่เกิดจากการใช้งานเครื่องมืออุปกรณ์เทคโนโลยีในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่ศูนย์สนับสนุนบริการสุขภาพที่ ๔ และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญบัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ รวมทั้งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ และกฎหมายอื่นๆลฯ ที่เกี่ยวข้องได้ ศูนย์สนับสนุนบริการสุขภาพที่ ๔ จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและป้องกันภัยคุกคามต่างๆ ดังต่อไปนี้

๑. ประกาศนี้ เรียกว่า “ประกาศศูนย์สนับสนุนบริการสุขภาพที่ ๔ เรื่องนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

๒. นโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๔ มีวัตถุประสงค์ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของศูนย์สนับสนุนบริการสุขภาพที่ ๔ ทำให้ดำเนินงานได้มีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ ศูนย์สนับสนุนบริการสุขภาพที่ ๔ ได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับศูนย์สนับสนุนบริการสุขภาพที่ ๔ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๓. นโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๔ กำหนดประเด็นสำคัญดังต่อไปนี้

๓.๑ การควบคุมเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ (Access Control)

๓.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

๓.๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๓.๕ การควบคุม...

๓.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๓.๖ การสำรองข้อมูลสำหรับระบบสารสนเทศ (Data Recovery) โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

๔. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๖๓

(นายประวิทย์ สัพพะเลข)

ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๔

แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวทางปฏิบัติในด้านความมั่นคงปลอดภัยด้านสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๔ จัดทำขึ้นเพื่อกำหนดวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ ดังนี้

๑. การเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ (Access Control) และการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

๑.๑ การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผล ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัยดังนี้

๑.๑.๑ ผู้ดูแลระบบ (Administrator) มีหน้าที่กำหนดสิทธิ์ให้แก่ผู้ใช้งาน (user) ตามเจ้าของระบบอนุมัติ

๑.๑.๒ ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๑.๓ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ และอุปกรณ์ที่เป็นการประมวลผล ทั้งทางกายภาพ และจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าว ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจ จากศูนย์สนับสนุนบริการสุขภาพ และต้องรักษาความลับทางราชการ ในกรณีเกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดขึ้น

๑.๑.๔ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องปฏิบัติการคอมพิวเตอร์ (Data center) ต้องได้รับอนุมัติจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศก่อนเริ่มดำเนินการทุกครั้ง

๑.๑.๕ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องปฏิบัติการคอมพิวเตอร์ (Data center) เว้นแต่ได้รับอนุญาตจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๔

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ การลงทะเบียนผู้ใช้งาน ดำเนินการดังนี้

๒.๑.๑ ศูนย์สนับสนุนบริการสุขภาพที่ ๔ กำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากร

๒.๑.๒ ให้บุคลากรใหม่กรอกข้อมูลแบบฟอร์มการเข้าถึงระบบฯ เพื่อรับการอนุมัติจากผู้อำนวยการ และงานเทคโนโลยีสารสนเทศดำเนินการสร้างบัญชีผู้ใช้

๒.๒ การยกเลิกสิทธิ์การใช้งานของบุคลากร ดำเนินการดังนี้

๒.๒.๑ ศูนย์สนับสนุนบริการสุขภาพที่ ๔ จะดำเนินการทบทวนสิทธิ์ ตรวจสอบบัญชีผู้ใช้งานปีละ ๑ ครั้ง

๒.๒.๒ งานเทคโนโลยีสารสนเทศดำเนินการถอดถอนหรือปรับปรุงสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ที่โอน ย้าย ลาออกและสิ้นสุดการจ้างงาน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

๓.๑ สำหรับผู้ดูแลระบบ

๓.๑.๑ จัดทำทะเบียนบัญชีทรัพย์สิน(อุปกรณ์คอมพิวเตอร์ เครือข่ายและซอฟแวร์) โดยมีรายละเอียดของผู้รับผิดชอบ รายการอุปกรณ์ต่างๆ สถานที่ตั้ง หมายเลขเครื่อง ปีที่ได้รับ การบำรุงรักษา เป็นต้น

๓.๑.๒ ปรับปรุงรายชื่อผู้ใช้ อุปกรณ์คอมพิวเตอร์ เครือข่ายและซอฟแวร์ ทุกครั้งเมื่อมีการเปลี่ยนแปลง

๓.๑.๓ ตรวจสอบ ปรับปรุง ทบทวนทะเบียนบัญชีทรัพย์สิน ปีละ ๑ ครั้ง

๓.๑.๔ จัดทำแบบฟอร์ม กำหนดเวลาการยืม-คืน เครื่องคอมพิวเตอร์แบบพกพา(notebook)และอุปกรณ์ที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศ

๓.๑.๕ จัดทำคู่มือการใช้อุปกรณ์คอมพิวเตอร์ เครือข่ายและซอฟแวร์ รวมทั้งกำหนดขั้นตอนการดูแลรักษารายอุปกรณ์

๓.๑.๖ กำหนดแผนการตรวจสอบ บำรุงอุปกรณ์คอมพิวเตอร์ เครือข่ายและซอฟแวร์ให้มีความพร้อมใช้งาน ไตรมาสและ ๑ ครั้ง

๓.๑.๗ ดำเนินการตั้งรหัสผ่านก่อนการเข้าใช้อุปกรณ์คอมพิวเตอร์โดย รหัสผ่านมีความยาวไม่เกิน ๘ ตัวอักษรประกอบด้วยตัวอักษรภาษาอังกฤษและตัวเลข (a-z,A-Z,0-9)

๓.๒ สำหรับผู้ปฏิบัติงาน

๓.๒.๑ ผู้ใช้ต้องคืนทรัพย์สินรวมทั้งข้อมูลของศบส.๔ ทั้งหมด ที่ ศบส.๔ ถือครอง เมื่อมีการสิ้นสุดการจ้างงาน ลาออก หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลงของ ศบส.๔

๓.๒.๒ กรณีที่ผู้ใช้งานนำสินทรัพย์ออกนอกสำนักงาน ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของสำนักงานที่ได้รับไว้ใช้งาน

๓.๒.๓ ผู้ใช้งานต้องชดใช้ค่าเสียหาย ไม่ว่าสินทรัพย์นั้นจะชำรุด หรือสูญหายตามมูลค่าของสินทรัพย์ หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ใช้งาน

๓.๒.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมสินทรัพย์ ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๔.๑ ผู้ใช้งานที่จะนำคอมพิวเตอร์ อุปกรณ์ใด ๆ มาเชื่อมต่อกับระบบคอมพิวเตอร์ ระบบเครือข่ายของสำนักงานต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๔.๒ ห้ามผู้ใด เคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก เป็นต้น โดยไม่ได้รับอนุญาตจากผู้อำนวยการหน่วยงานหรือผู้ปฏิบัติหน้าที่แทน

๔.๓ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อให้สามารถบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๔.๓.๑ ใช้วิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๔.๓.๒ มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๔.๓.๓ มีการกำหนดให้จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๔.๓.๔ ระบบเครือข่ายทั้งหมดของสำนักงาน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกสำนักงาน ได้ถูกเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก และมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware)

๔.๓.๕ การเข้าสู่ระบบเครือข่ายภายในสำนักงาน ผ่านทางระบบอินเทอร์เน็ตได้ กำหนดให้เข้าระบบ (Login) โดยระบุชื่อผู้ใช้งานและรหัสผ่านผู้ใช้งานผ่านระบบพิสูจน์ยืนยันตัวตน(Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

๔.๓.๖ เลขที่อยู่ไอพี (IP Address) ของระบบเครือข่ายภายในสำนักงาน ได้มีการ ป้องกันหน่วยงานภายนอกที่เชื่อมต่อ ไม่สามารถมองเห็นได้

๔.๔ ควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

๔.๔.๑ ผู้ใช้งานต้องออกจาก (Log out) ระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานๆ

๔.๔.๒ สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เมื่อผู้ใช้งานระบบสารสนเทศทิ้งไว้โดยไม่ใช้งานเป็นเวลานาน ระบบจะยุติการใช้งานระบบภายในระยะเวลา ๑๕ นาที หรือตามความเหมาะสมขึ้นอยู่กับระบบนั้นๆ

๔.๔.๓ ผู้ใช้ ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที เพื่อให้ ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่านซึ่งการบริหารจัดการรหัสผ่าน ปฏิบัติดังนี้

- รหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆด้วย ควรใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น
- ไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ และไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”“aaaaaa” หรือ “๑๒๓๔๕๖” เป็นต้น
- ทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล
- ผู้ใช้งานควรเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๔.๔.๔ หากมีการนำอุปกรณ์สื่อสารสนเทศอื่นๆเข้ามาต่อพวงอย่างเช่น แฟลชไดร์ฟ, สมาร์ทโฟน, กล้องดิจิตอล ผู้ใช้งานจะต้องแน่ใจว่าอุปกรณ์เหล่านั้นไม่ก่อให้เกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์ภายในสำนักงาน หากจำเป็นต้องมีการเชื่อมต่อควรแจ้งเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเพื่อทำการตรวจสอบก่อนการใช้งาน

๔.๔.๕ ผู้ใช้ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

๕. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๕.๑ ทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน ผู้ดูแลระบบ ต้องเปลี่ยนค่าSSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) จากผู้ผลิต และให้ซ่อนค่าดังกล่าวด้วย

๕.๒ ผู้ดูแลระบบ ต้องกำหนดรูปแบ Wireless Security ให้เป็น WPA/WPA๒ (Wi-Fi Protected Access)ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (AccessPoint) โดยไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

๕.๓ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address(Media Access Control Address) และบัญชีผู้ใช้งาน (User Account) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย ตามที่กำหนดไว้เท่านั้น

๕.๔ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สาย ติดต่อสื่อสารกับเครือข่าย ภายในสำนักงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สายผู้ดูแลระบบ ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้เข้าถึงระบบเครือข่ายไร้สาย

๕.๕ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และส่งรายงานผลการตรวจสอบทุก ๓ เดือนและในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ทราบทันที

๕.๖ ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศของสำนักงาน

๕.๗ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของสำนักงาน จะต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นลายลักษณ์อักษร

๕.๘ ผู้ดูแลระบบ ต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ ความรับผิดชอบในการปฏิบัติงาน รวมทั้ง ทบทวนสิทธิในการเข้าถึงอย่างสม่ำเสมอ

๖. การควบคุมการใช้งานอินเตอร์เน็ต(Internet)

๖.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาที่จะเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องติดตั้งโปรแกรมป้องกันไวรัส และอุดช่องโหว่ของระบบปฏิบัติการ

๖.๒ ต้องตรวจจับไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ต

๖.๓ ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๖.๔ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

๖.๕ ให้ระมัดระวังการดาวน์โหลดโปรแกรมใช้งาน จากระบบอินเตอร์เน็ต (Internet) และการปรับปรุงโปรแกรมต่าง ๆ ให้เป็นปัจจุบัน (Update) ต้องไม่ละเมิดลิขสิทธิ์

๖.๖ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ผ่านกระดานสนทนาอิเล็กทรอนิกส์(Web board) หรือ เครือข่ายสังคมออนไลน์ (Social Media)

๖.๗ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน หรือทำลายความสัมพันธ์กับบุคลากรของหน่วยงานภายนอก ผ่านกระดานสนทนาอิเล็กทรอนิกส์ (Web board)หรือ เครือข่ายสังคมออนไลน์ (Social Media)

๖.๘ ให้ออกจากระบบอินเตอร์เน็ต (Internet) และปิดเว็บเบราเซอร์ หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้วเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๖.๙ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๗. การปฏิบัติการบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี

๗.๑ ซอฟต์แวร์ที่สำนักงานอนุญาตให้ใช้งาน หรือที่สำนักงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่และความจำเป็น โดยห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๗.๒ ซอฟท์แวร์ที่สำนักงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานติดตั้ง ถอดถอนเปลี่ยนแปลงแก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๗.๓ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่สำนักงานประกาศให้ใช้

๗.๔ ต้องตรวจสอบข้อมูล แฟ้มข้อมูล ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น เพื่อตรวจจับไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๗.๕ ผู้ใช้งานต้องระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานจะต้องแจ้งให้ผู้ดูแลระบบรับทราบเพื่อดำเนินการแก้ไข

๗.๖ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๗.๗ ห้ามเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อสินทรัพย์ของสำนักงาน

๘. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๘.๑ การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

๘.๑.๑ ผู้ดูแลระบบ(Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้ (User) การกำหนดสิทธิ์ ตามตำแหน่งและหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย โอน ลาออก หรือสิ้นสุดการจ้าง ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๘.๑.๒ ผู้ดูแลระบบ(Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)

๘.๒ เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งาน ต้องระมัดระวังไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์ และต้องออกจากระบบ (Log out) ทันทีเมื่อไม่ใช้งาน

๙. การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

๙.๑ ผู้ดูแลระบบ(Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ

๙.๒ ผู้ดูแลระบบ(Administrator) กำหนดรูปแบบการสำรองข้อมูล โดยรวบรวมรายชื่อของระบบสารสนเทศและกำหนดรูปแบบการกู้คืนโดยมีความถี่ตามความเหมาะสมของการเปลี่ยนแปลงของข้อมูล

๙.๓ ผู้ดูแลระบบ(Administrator) ต้องดำเนินการทดสอบความพร้อใช้งานของระบบตามระดับความเสี่ยงที่ยอมรับได้ ปีละ ๑ ครั้ง

๙.๔ ผู้ใช้ (User) สำรองข้อมูลไฟล์งานทุกประเภทไปที่โฟลเดอร์ Share Data ที่ผู้ดูแลระบบเตรียมไว้ให้ หรือสำรองข้อมูลผ่าน External Hard disk โดยมีความถี่ เดือนละ ๑ ครั้ง หรือ ไตรมาสละ ๑ ครั้งขึ้นอยู่กับความเปลี่ยนแปลงของข้อมูล