แนวนโยบายและแนวปฏิบัติ

การใช้งานและการรักษาความปลอดภัยในระบบคอมพิวเตอร์และสารสนเทศ

เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของวิทยาลัยเทคนิคนครสวรรค์ เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกียวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับที่ ๒) วิทยาลัยเทคนิคนครสวรรค์ ได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของวิทยาลัยเทคนิคนครสวรรค์ ประกอบด้วยนโยบายและแนวทางปฏิบัติภายในกรอบนโยบายดังต่อไปนี้

๑. ด้านการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ เป็นนโยบายในการกำหนดการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสาหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๒. ด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน เป็นนโยบายในการธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability) รวมถึงกรณีที่เกิดเหตุการณ์สภาพของบริการหรือเครือข่ายทีแสดงให้เห็นความเป็นไปได้ทีจะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย

นิยามศัพท์

ผู้ใช้งาน หมายถึง ผู้บริหาร ข้าราชการ เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบของวิทยาลัยเทคนิคนครสวรรค์ รวมทั้ง ผู้รับบริการ ผู้ใช้งานทั่วไป ที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของวิทยาลัย

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าทีรับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ รวมทั้งผู้ดูแลระบบของหน่วยงานศูนย์ข้อมูลในวิทยาลัยเทคนิคนครสวรรค์

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของวิทยาลัยเทคนิคนครสวรรค์

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภารวมทั้งการอนุญาตเช่นว่านั้นสาหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของวิทยาลัยเทคนิคนครสวรรค์

ผู้ถือครองเครื่องคอมพิวเตอร์ หมายถึง ผู้ได้รับเครื่องคอมพิวเตอร์ไว้ใช้ประจำในการปฏิบัติงานและถือครอง รับผิดชอบ ดูแลเครื่อง/อุปกรณ์คอมพิวเตอร์

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจจะประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

เจ้าของข้อมูล หมายถึง เจ้าหน้าที่ของหน่วยงานในวิทยาลัยเทคนิคนครสวรรค์ ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบดูแลปรับปรุงข้อมูลของระบบงานนั้น ๆ ซึ่งเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดการสูญหาย

จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึงระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP , POP๓ และ IMAP

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึงระบบงานของ วิทยาลัยเทคนิคนครสวรรค์ ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ และอื่น ๆ

นโยบายด้านการใช้งานสารสนเทศ

การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๑ ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่ผู้ใช้งานได้รับอนุญาตหรือได้รับมอบอำนาจ

๑.๒ ผู้ดูแลระบบมีการกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้ อ่านข้อมูล , สร้างข้อมูล , นำเข้าข้อมูล แก้ไขข้อมูล , อนุมัติ และ ไม่มีสิทธิ

๑.๓ ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับชั้นความลับ

๑.๔ ผู้ดูแลระบบมีการถอดสิทธิการเข้าถึงการใช้งานสารสนเทศตามที่กำหนด

๑.๕ ผู้ดูแลระบบเป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด

๑.๖ ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ ข้อมูลภายในเป็นไปตามลำดับขั้นความลับของข้อมูล

๒. การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

๒.๑ เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ ตามหน้าที่งานหรือตามความจำเป็นเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิ์เกินความจำเป็นในการใช้งาน

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเมื่อลาออกไปหรือเมื่อเปลี่ยนตำแหน่งงานภายใน ๑๕ วันทำการ นับจากวันที่ ผู้มีอำนาจลงนามในคำสั่ง

การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

การบริหารรหัสผ่าน

๑. ศูนย์ข้อมูลและสารสนเทศต้องกำหนด ชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์เฉพาะบุคคลไม่ซ้ำกัน และกำหนดชื่อผู้ใช้ในส่วนของ ชื่อของผู้ใช้งาน ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่น ๆ ให้มีความแตกต่างกัน

การใช้งานรหัสผ่าน

๒. ผู้ใช้งานต้องเก็บรักษารหัสผ่าน (Password) ของตนเองและของกลุ่มไว้เป็นความลับ

๓. ห้ามทำการบันทึกรหัสผ่าน (Password) ไว้ในไปรษณีย์อิเล็กทรอนิกส์ หรือแบบฟอร์มอิเล็กทรอนิกส์ต่าง ๆ

๔. ไม่จดหรือบันทึกรหัสผ่าน (Password) ส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๕. ผู้ใช้งานทุกคนต้องเปลี่ยนรหัสผ่าน (Password) เริ่มต้นทันที หลังจากได้รับมอบรหัสผ่านเริ่มต้นจากผู้ดูแลระบบของศูนย์ข้อมูลและสารสนเทศ

๖. กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยควรมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

๗. ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๘. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

๙. ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบทำการเปลี่ยนแปลงรหัสผ่านทันที หรือแจ้งให้ศูนย์ข้อมูลและสารสนเทศทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

๑๐. หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้อง

๑๑. กรณีผู้ใช้งานของหน่วยงานภายในหน่วยงานลาออก ให้ศูนย์ข้อมูลและสารสนเทศทำการยกเลิกสิทธิของผู้ที่ลาออก ออกจากระบบทันที

๑๒. กรณีผู้ใช้งานของหน่วยงานภายใน มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้หน่วยงานต้นสังกัด แจ้งศูนย์ข้อมูลสารสนเทศ เพื่อทำการเปลี่ยนแปลงสิทธิ์ในการใช้งาน

๑๕. ผู้ใช้งานทุกคนของหน่วยงาน มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตน

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

แนวทางปฏิบัติ

๑. การบริหารจัดการทางกายภาพ (Physical security management)

๑.๑ กำหนดระดับความสำคัญของพื้นที่ในศูนย์ข้อมูลและสารสนเทศ

๑.๒ ผู้ดูแลระบบ ต้องปิดประตูและหน้าต่างห้องแม่ข่ายให้ล็อคอยู่เสมอ

๒. การควบคุมการเข้า-ออก (Physical entry controls)

๒.๑ ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒.๒ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๓. การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

๓.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในห้อง Data Center ให้น้อยที่สุด

๓.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่ความมั่นคงปลอดภัย

๓.๓ ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center)

๓.๔ ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณ

๔. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

๔.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงาน ที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบสำรองกระแสไฟฟ้า (UPS) และระบบปรับอากาศและควบคุมความชื้น

๔.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนตาม ๔.๑ อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)

๕.๑ ท าป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๕.๒ จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๕.๓ ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๖. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๖.๑ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๖.๒ ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาท าการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๖.๓ ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖.๔ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

นโยบายด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ

(Communications and operations management)

การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

แนวทางปฏิบัติ

๑. ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการ ใช้ไฟล์อื่นที่หน่วยงานไม่อนุญาตให้ใช้งาน

๒. ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศ ของหน่วยงาน

๓. ให้ผู้ดูแลระบบดำเนินการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องเซิร์ฟเวอร์ให้บริการ และอุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ณ จุดทางเข้า - ออกเครือข่ายอย่างสม่ำเสมอ เพื่อดักจับ โปรแกรม ไม่ประสงค์ดีที่เข้าสู่ระบบ

๔. มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๕.ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๖. เครื่องคอมพิวเตอร์ทั้งหมด ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่อง คอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา (Note book) ต้องได้รับการติดตั้ง โปรแกรมตรวจสอบและกำจัดไวรัสรุ่นล่าสุดของหน่วยงานจากเจ้าหน้าที่ศูนย์ข้อมูลและสารสนเทศ และจะต้องเปิดใช้งานโปรแกรมตรวจสอบและกำจัดไวรัสตลอดเวลา

๗. เครื่องคอมพิวเตอร์ Server ที่ให้บริการการตรวจสอบและกำจัดไวรัส ต้องมีการปรับปรุง ข้อมูลล่าสุดของไวรัสอยู่เสมอ และต้องเป็นผู้ให้บริการปรับปรุงข้อมูลไวรัสล่าสุดให้แก่เครื่อง คอมพิวเตอร์ Server เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพาทุกเครื่องโดยอัตโนมัติ

๘. ต้องทำการตรวจสอบไวรัสกับแฟ้มข้อมูล (file) ต่าง ๆ ที่ download มา แฟ้มข้อมูลที่ แนบมากับไปรษณีย์อิเล็กทรอนิกส์, แฟ้มข้อมูลที่ได้มาจากสื่อบันทึกข้อมูลภายนอก (CD, Thumb Drive, Diskette or share file)

๙. ศูนย์ข้อมูลและสารสนเทศ ต้องกำหนดให้เครื่องลูกข่ายทุกเครื่องในหน่วยงาน ทำการตรวจสอบไวรัส (Scan Virus) เป็นประจำ

การบริหารจัดการการเข้าถึงระบบเครือข่ายสื่อสารข้อมูล

แนวปฏิบัติ

๑. มาตรการทางเครือข่ายสื่อสารข้อมูล (Network controls)

๑.๑ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญ เมื่อต้อง ส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ

๑.๒ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๑.๓ มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) ของอุปกรณ์เครือข่ายเพื่อใช้ ในการตรวจสอบอย่างสม่ำเสมอ

๒. การควบคุมการเข้าถึงระบบเครือข่าย

๒.๑ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒.๒ มีการจำกัดการเชื่อมต่อทางเครือข่ายโดยมีการติดตั้ง Firewall เป็นเกตเวย์สาหรับเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ เพื่อทำการกรองข้อมูลจราจรในเครือข่ายให้เป็นไปตามความเหมาะสม กับการใช้งานระบบเครือข่ายได้อย่างปลอดภัย

๒.๓ การเข้าสู่ระบบงานเครือข่ายภายในหน่วยงานผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๒.๔ IP address ภายในของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบได้โดยง่าย

๒.๕ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ ตามกลุ่มของเครือข่ายที่แยกตามกลุ่มเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๖ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์ข้อมูลและสารสนเทศเท่านั้น

๒.๗ การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๓ เดือน

๓. การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์

๓.๑ เครื่องคอมพิวเตอร์ทุกเครื่องต้องตั้งอยู่หลัง Firewall เพื่อป้องกันการละเมิดความมั่นคงปลอดภัยจากเครือข่ายภายนอก

๓.๒ ห้ามผู้ใช้งานที่ใช้งานอยู่ภายในเครือข่ายคอมพิวเตอร์ของสานักงาน ใช้ Modem หรืออุปกรณ์อื่นใดในการเชื่อมต่อระบบเครือข่ายภายนอกในขณะเดียวกัน

๓.๓ ห้ามผู้ใช้งานทำการต่อขยายหรือเชื่อมการบริการเครือข่าย (Switch Hub) โดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ และห้ามเจ้าหน้าที่เปลี่ยนแปลงหรือแก้ไข (configuration) อุปกรณ์ใด ๆ ในระบบเครือข่ายคอมพิวเตอร์

๓.๔ ห้ามติดตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ หรือ Software ที่ให้บริการเครือข่ายคอมพิวเตอร์โดยไม่ได้รับการอนุญาตจากศูนย์ข้อมูลและสารสนเทศ

๓.๕ ห้ามผู้ใช้งานทำการ Download ติดตั้ง หรือทำการใช้โปรแกรมตรวจสอบทางด้านความมั่นคงปลอดภัยในเครือข่ายคอมพิวเตอร์ของสานักงานโดยไม่ได้รับอนุญาต

๓.๖ เครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายทุกเครื่องจะต้องมีการกำหนดผู้รับผิดชอบประจำแต่ละเครื่อง หากเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายที่ใช้เป็นส่วนกลางต้องกำหนดเจ้าหน้าที่ฝ่ายบริหารงานทั่วไปหรือเจ้าหน้าที่ในหน่วยงานที่ได้รับมอบหมายเป็นเจ้าของเครื่อง

๓.๘ กรณีได้รับเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายมาใหม่ หรือจากหน่วยงานอื่น และต้องการเข้าใช้งานระบบเครือข่ายหน่วยงาน เจ้าของเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายนั้น ๆ จะต้องปฏิบัติดังนี้

๓.๘.๑ ทำหนังสือขอเข้าใช้ระบบเครือข่ายต่อศูนย์ข้อมูลและสารสนเทศ

๓.๘.๒ ผู้ดูแลระบบของศูนย์ข้อมูลและสารสนเทศ เป็นผู้บริหารจัดการการใช้งานระบบเครือข่าย

๔. การใช้งานอินเตอร์เน็ตจากระบบเครือข่ายในหน่วยงานต้องทำการพิสูจน์ตัวตน (Authentication) ผู้ใช้งานภายใน ให้ใช้ ชื่อผู้ใช้ และ รหัสผ่าน ตามที่ศูนย์ข้อมูลและสารสนเทศกำหนด

การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

แนวทางปฏิบัติ

๑. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑.๑ กำหนดให้มีรหัสผู้ใช้/รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

๑.๒ ผู้ดูแลระบบควรตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๑.๓ ผู้ดูแลระบบต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒. การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ (Control of operational software)

๒.๑ ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วยงาน

๒.๒ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๒.๓ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๒.๔ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๓. ให้มีการทบทวนการท างานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)

๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๓.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่หน่วยงาน ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๔. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

๔.๑ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๔.๒ หน่วยงานเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนา ซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๔.๓ ให้ก าหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๔.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๕. ความเป็นเจ้าของและความรับผิดชอบ

๕.๑ หน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์ Server ต้องกำหนดผู้มีหน้าที่รับผิดชอบเพื่อดูแลเครื่องคอมพิวเตอร์ Server โดยทำการ update service pack หรือ patch ต่างๆ ให้ทันสมัยอยู่

เสมอ เพื่อปิดรูรั่วของตัวระบบปฏิบัติการ และตัวโปรแกรม และต้องมีเอกสารในการปรับเปลี่ยนค่าปรับแต่งบนเครื่องคอมพิวเตอร์ Server และต้องมีการระบุรายละเอียดของเครื่องคอมพิวเตอร์ Server ในระบบการจัดการเครือข่าย (Enterprise Management System)

๕.๒ กำหนด ชื่อ/รหัส ระดับสิทธิ์การใช้ ให้ผู้ใช้งานแต่ละคน

๖. การติดตั้ง

๖.๑ ห้ามเปิด Services และ Application ใด ๆ ที่ไม่เกี่ยวข้องกับงานของเครื่องคอมพิวเตอร์ Server นั้น ๆ โดยเด็ดขาด

๖.๒ เมื่อมีการปรับแต่งหรือแก้ไขค่า ต้องมีการแจ้งผู้ดูแลรับผิดชอบเครื่องคอมพิวเตอร์ Server นั้น ๆ

๗. การเฝ้าดูและตรวจสอบ

๗.๑ ต้องดำเนินการเก็บ Log และ Audit Trails ของหตุการณ์ละเมิดความมั่นคงปลอดภัยดังต่อไปนี้

๗.๑.๑ Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา ๙๐ วัน

๗.๑๒ ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า ๙๐ วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้ เมื่อพนักงานเจ้าหน้าที่ต้องการ ต้องสามารถนำออกมามอบให้กับ พนักงานเจ้าหน้าที่ได้

๘. กรณีการจัดซื้อ Server และหรือ Application ใหม่ ที่ให้บริการบนเครื่องแม่ข่ายของหน่วยงานที่มีศูนย์สารสนเทศ ต้องมีข้อกำหนดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในการจัดซื้อ และต้องมีการกำหนดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นทิศทางเดียวกับหน่วยงาน โดยต้องประสานกับ ศูนย์ข้อมูลและสารสนเทศก่อน

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

แนวทางปฏิบัติ

๑ การปฏิบัติทั่วไป

๑.๑ เครื่องคอมพิวเตอร์ที่หน่วยงาน อนุญาตให้ผู้ใช้งาน ใช้งานเป็นสินทรัพย์ของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วย ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย

๑.๓ ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆของหน่วยงาน และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๔ ไม่อนุญาตให้ ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ ของศูนย์ข้อมูลและสารสนเทศ หรือผู้ดูแลระบบของหน่วยงาน

๑.๕ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๑.๖ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

๑.๗ ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ ๑๕ นาทีเพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่ รหัสผ่านเพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๑.๘ ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ส่วนบุคคลต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่ของศูนย์ข้อมูลและสารสนเทศ หรือผู้ดูแลระบบของหน่วยงานเท่านั้น

๑.๙ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบของหน่วยงานในสานักงานที่มีศูนย์สารสนเทศเท่านั้น

๑.๑๐ การเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายในหน่วยงาน จะต้องแจ้งศูนย์ข้อมูลและสารสนเทศ หรือผู้ดูแลระบบของหน่วยงาน

๑.๑๑ กรณีส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้ผู้ดูแลระบบของหน่วยงานเป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของหน่วยงาน

๑.๑๒ ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงานทุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของศูนย์ข้อมูลและสารสนเทศ หรือ ผู้ดูแลระบบของหน่วยงาน

๑.๑๓ เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสโดยโปรแกรมป้องกันไวรัสของหน่วยงาน จากเจ้าหน้าที่ของศูนย์ข้อมูลและสารสนเทศ

๑.๑๔ ผู้ใช้งานไม่ควรสร้าง short-cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของสำนักงาน

๑.๑๕ ผู้ใช้งานมีหน้าที่และความรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้องปฏิบัติ ดังนี้

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ disk drive

๑.๑๖ ห้ามเจ้าหน้าที่ทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงานทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่า เวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ศูนย์ข้อมูลและสารสนเทศทราบทันที

๑.๑๗ ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่องรายใหม่พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

๒. การป้องกันจากโปรแกรมชุดคาสั่งไม่พึงประสงค์ (Malware)

๒.๑ ผู้ใช้งาน ควรตรวจสอบหาไวรัสจากสื่อต่างๆก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๒.๒ ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๒.๓ ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๓. การสำรองข้อมูลและการกู้คืน

๓.๑ ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่องมีหน้าที่ต้องทาการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลภายนอก

๓.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๔. การสำรองข้อมูลและการกู้คืน

๔.๑ ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่องมีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลภายนอก

๔.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

การใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ (mobile computing**)**

แนวทางปฏิบัติ

๑. **การใช้งานทั่วไป**

๑.๑ เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่หน่วยอนุญาตให้ผู้ใช้งานใช้งานเป็นสินทรัพย์ของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมายดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๓ ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๑.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์ข้อมูลและสารสนเทศ เท่านั้น

๑.๕ กรณีส่งเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้เจ้าหน้าที่ หรือผู้ดูแลระบบของ เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศขอหน่วยงาน

๑.๖ ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่ของศูนย์ข้อมูลและสารสนเทศ หรือผู้ดูแลระบบของหน่วยงานเท่านั้น

๑.๗ ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนทีของหน่วยงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของศูนย์ข้อมูล

๑.๘ ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของศูนย์ข้อมูลและสารสนเทศ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้มีสภาพเดิม

๑.๙ เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของสำนักงาน จากเจ้าหน้าที่ของศูนย์ข้อมูลและสารสนเทศ

๑.๑๐ การนำเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องออกไปใช้งานนอกหน่วยงาน เมื่อนำกลับมาที่หน่วยงาน ต้องทำการเชื่อมต่อระบบเครือข่ายภายในหน่วยงาน เพื่อทำการอัพเดท (Update) ข้อมูลไวรัสล่าสุด

๑.๑๑ ห้ามผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของหน่วยงานทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ศูนย์ข้อมูลและสารสนเทศทราบทันที

๒. ความปลอดภัยทางด้านกายภาพ

๒.๑ ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๒.๒ ผู้ใช้งาน ไม่ควรเก็บหรือใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

๒.๓ ไม่ควรใส่เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

๒.๔ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

๒.๕ หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้

๒.๗ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๒.๖ การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าที่มีรอยขีดข่วนได้

๒.๗ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๒.๘ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสค์กำลังทำงาน

๒.๙ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ใกล้สิ่งที่เป็นของเหลว

๒.๑๐ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

๒.๑๑ ไม่ควรวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนทีไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้

๒.๑๒ ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน

๓. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๓.๑ ผู้ใช้งาน ควรตรวจสอบหาไวรัสจากสื่อต่างๆก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๓.๒ ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๓.๓ ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคาสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๔. การสำรองข้อมูลและการกู้คืน

๔.๑ ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่องมีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลภายนอก

๔.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

การใช้งานอินเทอร์เน็ต (Use of the Internet)

แนวทางปฏิบัติ

๑. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

๒. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของหน่วย เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

๓. ผู้ใช้งานต้องไม่กระทำการเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของหน่วยงาน ที่ไม่เข้า หลักเกณฑ์การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ต

๔. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๕. การใช้งานเว็บบอร์ด (Web Board) ของหน่วยงาน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๖. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๗. ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับที่ ๒) อย่างเคร่งครัด

การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

แนวทางปฏิบัติ

๑. ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของหน่วย หรือระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐเท่านั้น ในการติดต่อราชการ หรือรับ - ส่งข้อมูลของทางราชการผ่านทางจดหมายอิเล็กทรอนิกส์

๒. ศูนย์ข้อมูลและสารสนเทศ เป็นผู้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานและระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งานรวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เมื่อมีการลาออก เป็นต้น

๓. การรับ - ส่งข้อมูลของทางราชการที่เป็นความลับ ห้ามรับ - ส่งผ่านทางระบบจดหมายอิเล็กทรอนิกส์

๔. ผู้ใช้งานรายใหม่จะต้องทำการเปลี่ยนรหัสผ่าน (Password) โดยทันที เมื่อได้รับรหัสผ่าน (default password) ในการผ่านเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก โดยต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๕.รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องแสดงออกมาในรูปของสัญลักษณ์เท่านั้น ได้แก่ “X” หรือ ● ในการพิมพ์แต่ละครั้ง

๖. ห้ามผู้ใช้งานตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๗. ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

๘. ผู้ใช้งาน ต้องไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงาน หรือละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของหน่วยงาน

๙. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ให้ทำการออกจากระบบ (Log out)ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๑๐. ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ทีเป็น Executable file

๑๑. ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จักในเครื่องที่อยู่ในระบบเครือข่ายของ หน่วยงาน

๑๒. ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๓. ผู้ใช้งาน ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๑๖. ผู้ใช้งานต้องไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้

๑๖.๑ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ

๑๖.๒ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๑๖.๓ ข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกียวกับความมั๋นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๑๖.๔ ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกอนาจาร

๑๗. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับส่ง - ข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑๘. ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๑๙. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

การสำรองและกู้คืนข้อมูล (Backup and and Recovery)

แนวทางปฏิบัติ

๑. การสำรองข้อมูลและกู้คือข้อมูลในสถานการณ์ปกติ เมือมีระบบงานใหม่หรือข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่กำหนดให้ใช้แนวทางปฏิบัติในการจัดทานโยบายการสำรอง และกู้คืนข้อมูลดังต่อไปนี้

๑.๑ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสารองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการส ารองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ขนาด ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ระบบปฏิบัติการ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ ตามปกติ
- จัดทำขั้นตอนปฏิบัติสาหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑.๒ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๑.๓ กำหนดชนิดของระบบงานนั้น ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อย ต้องประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

๑.๓ กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล

๑.๔ กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

๑.๕ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูลในการสำรวจข้อมูลทุกครั้ง

๑.๖ ต้องทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองรองไว้สามารถกู้ข้อมูลกลับมา ได้อย่างสมบูรณ์

๑.๗ สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนสื่อตามอายุการใช้งานของสื่อตามประเภทของสื่อแต่ละชนิด

ความมั่นคงปลอดภัยของ Firewall

แนวทางปฏิบัติ

๑. ศูนย์ข้อมูลและสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Fire wall) ทั้งหมด

๒. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๓. ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

๔. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๕. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๖. ต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๗. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๘. ศูนย์ข้อมูลและสารสนเทศ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

๙. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ต