ประกาศมหาวิทยาลัยทักษิณ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๙

เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยทักษิณมีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และสามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจส่งผลกระทบต่อความมั่นคง การดำเนินงาน ทรัพย์สิน ชื่อเสียง และข้อมูลสารสนเทศของมหาวิทยาลัย รวมถึงข้อมูลส่วนบุคคลของบุคลากรและผู้เกี่ยวข้อง อันเป็นไปตามหลักการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ

อาศัยอำนาจตามความในมาตรา ๓๑ แห่งพระราชบัญญัติมหาวิทยาลัยทักษิณ พ.ศ. ๒๕๕๑ ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศมหาวิทยาลัยทักษิณ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นมาตรฐานด้านการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เพื่อใช้เป็นแนวทางและเป็นไปตามกฎหมาย โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๔ กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ไว้ดังต่อไปนี้

<u>นโยบายที่ ๑</u> นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

หมวด ๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
หมวด ๒ การเข้าถึงและควบคุมการใช้งานสารสนเทศ
หมวด ๓ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
หมวด ๔ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
หมวด ๕ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
หมวด ๖ การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
หมวด ๗ การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์
หมวด ๘ การควบคุมการเข้าถึงระบบเครือข่าย
หมวด ๙ การแบ่งปันข้อมูล
หมวด ๑๐ การทำให้ระบบมีความแข็งแกร่ง
หมวด ๑๑ การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์
หมวด ๑๒ การเชื่อมต่อระยะไกล

<u>นโยบายที่ ๒</u> นโยบายการรักษาสภาพความพร้อมใช้

หมวด ๑๓ การรักษาสภาพความพร้อมใช้งานของการให้บริการ

หมวด ๑๔ การตรวจสอบและรับมือภัย คุกคามทางไซเบอร์

หมวด ๑๕ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

<u>นโยบายที่ ๓</u> นโยบายการตรวจสอบและประเมินความเสี่ยง

หมวด ๑๖ การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

หมวด ๑๗ การกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซบอร์

<u>นโยบายที่ ๔</u> นโยบายการติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณภายในอาคารและนอกอาคาร

หมวด ๑๘ การติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณภายในอาคารและนอกอาคาร

ข้อ ๕ กำหนดความรับผิดชอบในการรักษาความมั่นคงปลอดภัยไซเบอร์ ไว้ดังต่อไปนี้

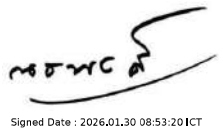
(๑) อธิการบดีมหาวิทยาลัยทักษิณ ในฐานะผู้บริหารสูงสุดของมหาวิทยาลัย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่มหาวิทยาลัยหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) หัวหน้าส่วนงาน เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะและคำปรึกษาตลอดจนติดตาม กำกับดูแล ตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของส่วนงานให้สอดคล้องกับนโยบายและแนวปฏิบัติตามประกาศนี้

(๓) ให้สถาบันทรัพยากรการเรียนรู้และเทคโนโลยีดิจิทัลและผู้ที่ได้รับมอบหมายเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยอย่างน้อยปีละ ๑ ครั้ง โดยประกาศให้ทราบเป็นการทั่วไป

ข้อ ๖ ให้อธิการบดีรักษาการให้เป็นไปตามประกาศนี้ และให้มีอำนาจในการวินิจฉัยหรือตีความกรณีมีปัญหาในการปฏิบัติตามประกาศนี้ คำวินิจฉัยของอธิการบดีให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๓๐ มกราคม พ.ศ. ๒๕๖๙



Signed Date : 2026.01.30 08:53:20 ICT

(รองศาสตราจารย์ ดร.ณฐพงศ์ จิตรนิรัตน์)

อธิการบดีมหาวิทยาลัยทักษิณ

เอกสารแนบท้ายประกาศมหาวิทยาลัยทักษิณ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๙

<u>นโยบายที่ ๑</u> นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

<u>หมวด ๑</u>
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. กำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๑.๑ ผู้บริหารส่วนงานต้องกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกเป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่ควบคุมพิเศษ (Data Center) และพื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

๑.๒ ส่วนงานต้องมีการจำแนกและกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม จากผู้ที่ไม่ได้รับอนุญาต

๑.๓ สำนักงานที่เก็บข้อมูลสารสนเทศที่สำคัญ จะต้องกำหนดผู้มีหน้าที่ตรวจสอบผู้เข้า – ออก และจัดทำบันทึก การเข้าออกพื้นที่ โดยจะต้องทำทะเบียนผู้มีสิทธิเข้าออกพื้นที่

๑.๔ ต้องมีการทบทวนปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับสิทธิการเข้าออกพื้นที่ เช่น การโอน ย้าย ลาออก หรือสิ้นสุดการจ้าง

๒. การควบคุมการเข้า - ออก อาคารและสถานที่

๒.๑ หน่วยงานภายในที่รับผิดชอบด้านความปลอดภัยของอาคารสถานที่ต้องจัดให้มีบุคลากรหรือวิธีการ รักษาความปลอดภัย เพื่อควบคุมให้เข้าสถานที่ทำงานได้เฉพาะบุคคลที่ได้รับอนุญาตจากเจ้าของพื้นที่เท่านั้น

๒.๒ ส่วนงานต้องจัดทำเอกสารระบุสิทธิ์ของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยกำหนดไว้ดังนี้

๒.๒.๑ ส่วนงานต้องกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้า - ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้า – ออก ในแต่ละพื้นที่ใช้งานอย่างชัดเจน

๒.๒.๒ การเข้าถึงอาคารของส่วนงานของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้แสดงบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในแบบฟอร์ม การเข้า - ออกพื้นที่

๒.๒.๓ บุคคลภายนอกที่เข้ามาติดต่อจะต้องลงชื่อขออนุญาตการเข้า - ออกในแบบฟอร์มการเข้า – ออก พื้นที่ให้ถูกต้องและชัดเจน

๒.๓ ผู้ใช้งานจะได้รับสิทธิให้เข้า - ออกสถานที่ทำงานได้ เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้สำหรับปฏิบัติงานเท่านั้น

๒.๔ หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิไว้เป็นการล่วงหน้า ส่วนงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้ จะต้องแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้โดยส่วนงานเจ้าของพื้นที่ต้องจดบันทึกการขอเข้า - ออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๓. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

จัดให้มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอและมีความพร้อมในการใช้งาน ดังนี้

๓.๑ ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

๓.๒ ติดตั้งระบบระดับเพลิง

๓.๓ ติดตั้งระบบปรับอากาศและควบคุมความชื้น

๓.๔ ติดตั้งระบบแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องแม่ข่ายทำงานผิดปกติหรือหยุดทำงาน

๓.๕ วางแผนการตรวจสอบ บำรุงงรักษา ระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของส่วนงานอย่างสม่ำเสมอ ให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

๔. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ล

๔.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของส่วนงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงต้องติดตั้งระบบป้องกันที่ปลอดภัย

๔.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ หรือมีการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อป้องกันการตัดสายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญาณ

๔.๓ ติดป้ายระบุสายสัญญาณและอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๔.๔ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๔.๕ ตู้เก็บอุปกรณ์เครือข่ายที่มีสายสัญญาณสื่อสารต่าง ๆ ต้องปิดสลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๔.๖ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดีทุก ๖ เดือน

๕. การบำรุงรักษาอุปกรณ์

๕.๑ วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา และต้องมีการซ่อมบำรุงอย่างทันท่วงทีตามความสำคัญของระบบ

๕.๒ บันทึกประวัติการบำรุงรักษาและซ่อมบำรุงอุปกรณ์ทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง โดยมีรายละเอียด เช่น วันที่บำรุงงรักษาและซ่อมบำรุง รายการอุปกรณ์ สถานะของอุปกรณ์ปัญหาที่พบ และการแก้ไข ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุงพร้อมลงลายมือชื่อ

๕.๓ ถ้ามีการจัดจ้างหน่วยงานหรือผู้ให้บริการภายนอก เพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์ส่วนงานที่จัดจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการจ้าง โดยต้องกำหนดระยะเวลา ขอบเขต และระดับการให้บริการอย่างชัดเจน

๕.๔ ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาททำการบำรุงรักษาอุปกรณ์ภายในส่วนงานในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบหรือผู้รับผิดชอบการซ่อมบำรุงอุปกรณ์ต้องอยู่ในพื้นที่ทุกครั้ง

๕.๕ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างหรือผู้ให้บริการภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. การนำทรัพย์สินของส่วนงานออกนอกพื้นที่

๖.๑ ตามระเบียบภาครัฐ ส่วนงานต้องมอบหมายบุคลากรเป็นผู้ดูแลครุภัณฑ์มีหน้าที่ควบคุมดูแลพัสดุ หรือทรัพย์สินของส่วนงานที่อยู่ในความครอบครองให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา และจัดทำทะเบียนครุภัณฑ์ของส่วนงาน บันทึกการใช้งาน สถานภาพและการเคลื่อนย้าย ของครุภัณฑ์ทั้งนี้ต้องตรวจสอบสถานภาพ ของครุภัณฑ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เคลื่อนย้าย เช่น ได้รับมอบครุภัณฑ์เพิ่มเติม การตัด จำหน่าย การเปลี่ยนผู้ครอบครอง การยืม การโอน หรือการส่งซ่อม

๖.๒ ต้องขออนุญาตจากผู้บริหารของส่วนงานและแจ้งให้ผู้ดูแลครุภัณฑ์ทราบ ก่อนนำอุปกรณ์หรือทรัพย์สินออกไปใช้งานภายนอกส่วนงานหรือนำไปซ่อมบำรุง

๖.๓ ต้องได้รับความเห็นชอบจากหัวหน้าส่วนงาน ก่อนนำครุภัณฑ์คอมพิวเตอร์ส่งซ่อมภายนอกส่วนงาน

๖.๔ การให้ยืมอุปกรณ์หรือทรัพย์สินผู้ดูแลครุภัณฑ์จะต้องตรวจสอบติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนดและอยู่ในสภาพปกติหรือไม่ต่างจากตอนที่ถูกยืม และต้องบันทึกข้อมูลการนำอุปกรณ์ของส่วนงานออกไปใช้งานนอกส่วนงานและบันทึกส่งคืนเพื่อเป็นหลักฐาน ป้องกันการสูญหาย

๗. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกส่วนงาน

๗.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของส่วนงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๗.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของส่วนงานไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

๗.๓ บุคลากรผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๘. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

๘.๑ การจำหน่ายครุภัณฑ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ส่วนงานที่เป็นเจ้าของทรัพย์สินต้องจัดให้มีการทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ก่อนการจำหน่าย เพื่อให้มั่นใจว่าข้อมูลและซอฟต์แวร์ลิขสิทธิ์จะไม่สามารถนำกลับมาใช้ได้อีก

๘.๒ หัวหน้าส่วนงานเป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ ต้องเสนอเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

๘.๓ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัด โดยต้องมั่นใจว่าข้อมูลดังกล่าว จะไม่สามารถนำกลับมาใช้

<u>หมวด ๒</u>
การเข้าถึงและควบคุมการใช้งานสารสนเทศ

๙. กำหนดลำดับความสำคัญของข้อมูลและการใช้งานข้อมูล

๙.๑ ส่วนงานใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ในการจัดการเอกสารอิเล็กทรอนิกส์ โดยมีการแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ดังนี้

๙.๑.๑ จัดแบ่งประเภทของข้อมูลออกเป็น

๙.๑.๑.๑ ข้อมูลสารสนเทศด้านการบริหารและจัดการ ได้แก่ ข้อมูลบุคลากร ข้อมูลแผนงบประมาณ การเงินและบัญชี เป็นต้น

๙.๑.๑.๒ ข้อมูลสารสนเทศด้านการเรียนการสอน ได้แก่ ข้อมูลนิสิต ข้อมูลหลักสูตร ผลการเรียน เป็นต้น

๙.๑.๒ การรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการของการเข้าถึงข้อมูลแต่ละประเภทตามระดับชั้นความลับของส่วนงาน ดังต่อไปนี้

๙.๑.๒.๑ ลับที่สุด (Top Secret) มีความสำคัญต่อส่วนงานในระดับสูงมาก หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อส่วนงานอย่างมาก

๙.๑.๒.๒ ลับมาก (Secret) มีความสำคัญต่อส่วนงานในระดับสูงหากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อส่วนงานอย่างมีนัยยะสำคัญ

๙.๑.๒.๓ ลับ (Confidential) มีความสำคัญต่อส่วนงานหากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อส่วนงาน

๙.๑.๒.๔ ใช้ภายในส่วนงาน (Internal Use) เป็นข้อมูลที่อนุญาตให้ใช้ภายในส่วนงาน หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อส่วนงาน

๙.๑.๒.๕ สาธารณะ (Public) เป็นข้อมูลที่ใช้เผยแพร่สู่สาธารณะ การเปิดเผยข้อมูลประเภทนี้ ไม่ส่งผลกระทบใดกับส่วนงาน

๙.๑.๓ การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ ๑ ระดับชั้นสำหรับผู้บริหาร

ระดับที่ ๒ ระดับชั้นสำหรับผู้ปฏิบัติงาน

ระดับที่ ๓ ระดับชั้นสำหรับใช้งานทั่วไป

ระดับที่ ๔ ระดับชั้นสำหรับผู้ดูแลระบบ

๙.๑.๔ กำหนดเวลาที่สามารถเข้าถึงข้อมูลได้

๙.๑.๕ การกำหนดช่องทางในการเข้าถึงข้อมูล ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้ ต้องได้รับสิทธิจากส่วนงาน โดยมีการกำหนดบัญชีชื่อผู้ใช้งานตามระดับชั้นการเข้าถึงให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูล และสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาต

๙.๒ การใช้งานข้อมูล

๙.๒.๑ มีมาตรการให้ผู้ใช้งานต้องใช้งานข้อมูลของส่วนงานตามกฎระเบียบและคำแนะนำที่ส่วนงานกำหนดไว้

๙.๒.๒ ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้งานข้อมูลประเภทลับมากและลับที่สุด เพื่อป้องกันไม่ให้ข้อมูลถูกเข้าถึงหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต

๙.๒.๓ ข้อมูลลับของส่วนงานต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

๙.๒.๔ ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลลับที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการหรือแอปพลิเคชันอย่างเหมาะสม

๙.๒.๕ ข้อมูลใดที่ผู้ใช้งานพิจารณาว่าเป็นข้อมูลลับหรือมีจุดอ่อนด้านความมั่นคงปลอดภัย ต้องได้รับการเข้ารหัส

๙.๒.๖ ผู้ใช้งานควรเก็บรักษาสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องวางสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน

๙.๒.๗ ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร ทันที

๙.๒.๘ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

๙.๒.๙ ผู้ใช้งานต้องไม่พูดคุยหรือใช้งานข้อมูลลับของส่วนงานในพื้นที่สาธารณะ เช่น ลิฟต์ ร้านอาหาร ฯลฯ

๑๐. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑๐.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ต้องมีการควบคุมการเข้า - ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๑๐.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของบุคลากรในการปฏิบัติงาน ก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะต้อง ได้รับอนุญาตจาก ผู้บริหารและผู้ดูแลระบบตามความจำเป็น

๑๐.๒.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

๑๐.๒.๑.๑ อ่านอย่างเดียว

๑๐.๒.๑.๒ สร้างข้อมูลหรือนำเข้าข้อมูล

๑๐.๒.๑.๓ แก้ไขข้อมูล

๑๐.๒.๑.๔ ลบข้อมูล

๑๐.๒.๑.๕ อนุมัติ

๑๐.๒.๑.๖ ไม่มีสิทธิ

๑๐.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๑๐.๔ ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารของส่วนงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๑๐.๕ ผู้ดูแลระบบต้องจัดให้มีการบันทึกประวัติการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า - ออก สถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๑๑. การตรวจสอบการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑๑.๑ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบแก่ผู้ใช้งานในการขออนุญาตเข้าใช้ระบบงานนั้นจะต้องมีบันทึกเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและมีการลงนามอนุมัติโดยผู้บริหาร

๑๑.๒ ผู้ดูแลระบบต้องกำหนดระยะเวลาการเชื่อมต่อเข้าสู่ระบบสารสนเทศ/แอปพลิเคชันที่มีความสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๑.๓ เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นตามหน้าที่รับผิดชอบเท่านั้น

๑๑.๔ ผู้ใช้งานจะต้องได้รับอนุญาตจากบุคลากรที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๑๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๑๒.๑ สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้ใช้งาน

๑๒.๑.๑ ส่วนงานจัดให้มีการอบรมเพื่อสร้างความรู้และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์และรู้เท่าทันต่อภัยคุกคามและผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศ โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๑๒.๑.๒ กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศจะต้องได้รับ การชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของส่วนงาน

๑๒.๒ การลงทะเบียนบุคลากรใหม่ของส่วนงาน ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนบุคลากรใหม่ เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกหรือเปลี่ยนแปลงสิทธิการใช้งาน

๑๒.๓ การลงทะเบียนผู้ใช้งาน

๑๒.๓.๑ ผู้ดูแลระบบจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศ

๑๒.๓.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีรายชื่อผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๑๒.๓.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิในแต่ละภารกิจ

๑๒.๓.๔ ผู้ดูแลระบบต้องชี้แจงและแจ้งผู้ใช้งานเป็นลายลักษณ์อักษร เพื่อให้ผู้ใช้งานทราบถึงสิทธิ หน้าที่รับผิดชอบ และมาตรการด้านความมั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศ

๑๒.๓.๕ กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากต้นสังกัดหรือเมื่อมีการเปลี่ยนแปลงตำแหน่ง โอนย้าย ลาออก หรือสิ้นสุดการจ้าง เป็นต้น

๑๒.๔ การบริหารจัดการสิทธิผู้ใช้งาน

๑๒.๔.๑ กำหนดระดับสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบและความจำเป็นในการใช้งานและทบทวนสิทธิอย่างสม่ำเสมอหรืออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่ง โอนย้าย ลาออก หรือสิ้นสุดการจ้าง เป็นต้น

๑๒.๔.๒ ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการกำหนดหนดสิทธิให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

๑๒.๔.๓ ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบจากต้นสังกัดและผู้บริหาร จัดทำคำร้องเป็นลายลักษณ์อักษร โดยการให้สิทธิพิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษแล้ว จะต้องระงับการใช้งานทันที

๑๒.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๑๒.๕.๑ ผู้ดูแลระบบกำหนดรหัสผ่านครั้งแรกให้แก่ผู้ใช้งานผ่านการลงทะเบียนด้วยการยืนยันตัวตน

๑๒.๕.๒ การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้องมีความยาวอย่างน้อย ๘ ตัวอักขระ ประกอบด้วยตัวอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ

๑๒.๕.๓ กำหนดให้การกรอกรหัสผิดพลาดได้ไม่เกิน ๕ ครั้ง ระบบจะต้องล็อคสิทธิการเข้าถึงของผู้ใช้งาน โดยผู้ใช้งานจะต้องแจ้งความจำนงให้ผู้ดูแลระบบปลดล็อคหรือรีเซ็ตรหัสผ่านใหม่

๑๒.๕.๔ กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ ๑๘๐ วัน

๑๒.๖ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑๒.๗ ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๑๒.๘ การบริหารจัดการบัญชีรายชื่อผู้ใช้งานของบุคลากร

๑๒.๘.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของบุคลากรในการเข้าถึงระบบ เทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

๑๒.๘.๒ มีการกำหนดการเปลี่ยนแปลงรหัสผ่านของบัญชีผู้ใช้งานของบุคลากรตามระยะเวลาที่เหมาะสมของแต่ละส่วนงาน ๖ เดือน

๑๒.๘.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ซึ่งผู้ใช้งานที่มีสิทธิสูงสุดจะต้องพิจารณา การควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๑๒.๘.๓.๑ ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

๑๒.๘.๓.๒ ต้องควบคุมการใช้งานอย่างเข้มงวด กำหนดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๑๒.๘.๓.๓ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๑๒.๘.๓.๔ ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน

๑๒.๙ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๒.๙.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑๒.๙.๒ เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๔ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๒.๙.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดบัญชีรายชื่อผู้ใช้งานและรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูล ในแต่ละชั้นความลับข้อมูล

๑๒.๙.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล เช่น SSL VPN เป็นต้น

๑๒.๙.๕ ต้องกำหนดให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสมขึ้นอยู่กับความสำคัญของข้อมูลที่ผู้ใช้ดูแลรับผิดชอบ

๑๒.๙.๖ ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของส่วนงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน เป็นต้น

๑๒.๑๐ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๑๒.๑๐.๑ การใช้งานรหัสผ่าน

๑๒.๑๐.๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านโดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๑๒.๑๐.๑.๒ การกำหนดรหัสผ่าน ที่คาดเดาได้ยาก ซึ่งประกอบด้วย

(๑) กำหนดให้มีความยาวไม่น้อยกว่า ๘ ตัวอักษร

(๒) ประกอบด้วย อักษรภาษาอังกฤษตัวพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษประกอบ เช่น ; < > เป็นต้น

(๓) การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสเดิมครั้งสุดท้าย

(๔) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วันเกิด หรือหมายเลขโทรศัพท์ เป็นต้น

(๕) ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม

๑๒.๑๐.๑.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจจำรหัสผ่านส่วนบุคคลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๑๒.๑๐.๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยผู้อื่น

๑๒.๑๐.๑.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๑๘๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๑๒.๑๐.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน มีการกำหนดมาตรการป้องกันทรัพย์สินของส่วนงาน และควบคุมไม่ให้มีการวางทรัพย์สินสารสนเทศที่สำคัญในสถานที่ที่ไม่ปลอดภัย โดยมีแนวปฏิบัติดังนี้

๑๒.๑๐.๒.๑ ผู้ดูแลระบบหรือผู้รับผิดชอบต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศและการเข้าใช้งานคอมพิวเตอร์ทันทีเมื่อเสร็จสิ้นการใช้งานหรือพักการใช้งานชั่วคราวเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๒.๑๐.๒.๒ ผู้ใช้งานจะต้องป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่าย

ของส่วนงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหาย สูญหายหรือมีผู้ไม่ประสงค์ดี เข้าถึงระบบและอุปกรณ์โดยไม่ได้รับอนุญาต

๑๒.๑๐.๒.๓ กำหนดค่าให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา๑๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๑๒.๑๐.๒.๔ กำหนดรหัสผ่านสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์และต้องล็อคอุปกรณ์ เครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง ไว้โดยไม่ได้ดูแลชั่วคราว

๑๒.๑๐.๒.๕ การใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์ เมื่อเสร็จสิ้นแล้วจะต้องทำการ log off ทุกครั้ง

๑๒.๑๐.๒.๖ มีการควบคุมการเข้า - ออกพื้นที่ โดยผู้ไม่มีส่วนเกี่ยวข้องต้องได้รับอนุญาตก่อนการเข้าถึงพื้นที่ปฏิบัติงาน

๑๒.๑๐.๓ ส่วนงานต้องกำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ โดยมีแนวปฏิบัติดังนี้

๑๒.๑๐.๓.๑ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันที ที่เสร็จสิ้นการใช้งานหรือเมื่อมีเหตุให้ว่างเว้นจากการใช้งาน

๑๒.๑๐.๓.๒ ผู้ใช้งานต้องกำหนดให้เครื่องคอมพิวเตอร์ล็อคหน้าจอขณะที่ไม่ได้ใช้งานภายในระยะเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๑๒.๑๐.๓.๓ ผู้ใช้งานต้องกำหนดรหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูลและเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๑๒.๑๐.๓.๔ กรณีข้อมูลสำคัญที่บันทึกไว้ในสื่อบันทึกข้อมูลเคลื่อนย้ายได้ เช่น ฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัยไม่วางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๑๒.๑๐.๓.๕ ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

๑๒.๑๐.๓.๖ ต้องทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ

๑๒.๑๐.๓.๗ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยการรับและส่งข้อมูลสำคัญหรือข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๑๒.๑๐.๓.๘ มีการจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกและต้องมีผู้รับผิดชอบคอยควบคุมดูแลตลอดระยะเวลา การส่งมอบ ไม่ปล่อยให้บุคคลภายนอกอยู่ตามลำพังในพื้นที่ปฏิบัติงาน

๑๒.๑๐.๔ การใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัยและไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศของส่วนงาน กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

๑๒.๑๐.๔.๑ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของส่วนงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิด จากรหัสผ่านล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๑๒.๑๐.๔.๒ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของส่วนงานหรือเป็นของบุคคลภายนอก

๑๒.๑๐.๔.๓ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีชื่อผู้ใช้งานอันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

๑๒.๑๐.๔.๔ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของส่วนงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงสุดของส่วนงาน

๑๒.๑๐.๔.๕ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษาใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ส่วนงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับส่วนงาน ซึ่งส่วนงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๑๒.๑๐.๔.๖ ห้ามใช้สินทรัพย์ของส่วนงานที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของส่วนงาน

๑๒.๑๐.๔.๗ ห้ามใช้ระบบสารสนเทศของส่วนงาน เพื่อก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของส่วนงาน

๑๒.๑๐.๔.๘ ห้ามใช้ระบบสารสนเทศของส่วนงานเพื่อประโยชน์ทางการค้า

๑๒.๑๐.๔.๙ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายของส่วนงานโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

๑๒.๑๑ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของส่วนงานและการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ มีแนวปฏิบัติดังนี้

๑๒.๑๑.๑ การควบคุมการเข้าถึงสารสนเทศ

๑๒.๑๑.๑.๑ ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของส่วนงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑๒.๑๑.๑.๒ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๑๒.๑๑.๒ ข้อกำหนดการใช้งานตามภารกิจ เพื่อให้การเข้าถึงและใช้งานสารสนเทศสอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย จึงจำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิและภารกิจ ดังนี้

(๑) กลุ่มผู้บริหาร กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายในการกำกับดูแล เช่น สิทธิการอนุมัติ สิทธิการเข้าถึงรายงานสรุปผล

(๒) กลุ่มของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายจากผู้บริหาร เช่น สิทธิในการกำหนดสิทธิการเข้าใช้งานของผู้ใช้งานในแต่ละระบบตามที่ผู้บริหารมอบหมาย

(๓) กลุ่มผู้ใช้งาน กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายจากผู้บริหารของส่วนงานภายใน เช่น สิทธิการเพิ่ม แก้ไข ลบข้อมูล ที่อยู่ในความรับผิดชอบ

(๔) กลุ่มบุคลากรของส่วนงาน กำหนดสิทธิให้สามารถเข้าถึงข้อมูลทั่วไป เช่น สิทธิการอ่านอย่างเดียว

(๕) กลุ่มที่ปรึกษาจากภายนอกหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับส่วนงาน กำหนดสิทธิเฉพาะกิจตามความจำเป็นที่ต้องเข้าถึงข้อมูล

(๖) ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว (Guest) ไม่มีสิทธิในการเข้าถึง

๑๓. การควบคุมการเข้าถึงเครือข่าย

๑๓.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่มีการใช้งานกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๑๓.๒ การเข้าถึงระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศภายในของส่วนงาน ต้องดำเนินการโดยใช้อุปกรณ์ที่ส่วนงานเป็นผู้จัดหาหรืออุปกรณ์ที่ได้รับอนุญาตซึ่งผ่านการลงทะเบียน

๑๓.๓ อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายภายในของส่วนงาน ต้องได้รับการพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสม ได้แก่ การตรวจสอบความถูกต้องของ Media Access Control Address (MAC) การตรวจสอบความถูกต้องของรหัสประจำเครื่องหรือการตรวจสอบ Digital Certificate ของอุปกรณ์

๑๓.๔ ผู้ดูแลระบบต้องควบคุมพอร์ตของอุปกรณ์ต่าง ๆ ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบโดยมีรายละเอียดดังนี้

๑๓.๔.๑ พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Diagnostic และ Configuration Port) ต้องถูกจำกัดให้สามารถใช้งานได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น

๑๓.๔.๒ การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบต้องดำเนินการผ่านโพรโทคอล ที่มีความมั่นคงปลอดภัย เช่น Secure Shell (SSH) หรือผ่านระบบเครือข่ายแบบ Out-of-band เท่านั้น

๑๓.๔.๓ การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบจากระยะไกลผ่านเครือข่ายภายนอก ต้องได้รับการพิสูจน์ตัวตนของผู้ใช้งานด้วยวิธีการตรวจสอบตั้งแต่ ๒ ประเภท ขึ้นไป (two factors authentication) และใช้ช่องทางการเชื่อมต่อที่มั่นคงปลอดภัย

๑๓.๔.๔ พอร์ตที่ไม่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินภารกิจต้องถูกระงับการใช้งาน

๑๓.๕ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๑๓.๖ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๑๓.๗ ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

๑๓.๘ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๑๓.๙ ระบบเครือข่ายทั้งหมดของส่วนงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกส่วนงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๑๓.๑๐ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ งาน ระบบเครือข่ายของส่วนงานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบ เครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๑๓.๑๑ การเข้าสู่ระบบสารสนเทศเครือข่ายภายในของส่วนงาน จากผู้ใช้ทั้งที่อยู่ภายนอกและภายใน ส่วนงาน โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๑๓.๑๒ IP Address ภายในของระบบสารสนเทศเครือข่ายภายในของส่วนงาน จำเป็นต้องมีการป้องกัน มิให้ส่วนงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอก

สามารถล่วงรู้ข้อมูล เกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

๑๓.๑๓ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๓.๑๔ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บริหาร และผู้ดูแลระบบก่อน และต้องจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๑๓.๑๕ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

๑๔. การควบคุมการเข้าถึงระบบปฏิบัติการ

๑๔.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานด้วยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

(๑) ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๑๔.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยกำหนดให้ผู้ใช้งานเลือกใช้ขั้นตอนในการยืนยันตัวตนที่เหมาะสม มีแนวปฏิบัติดังนี้

(๑) ผู้ใช้งานต้องระบุบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับยืนยันตัวตนเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศ

(๒) การใช้งานบัญชีรายชื่อผู้ใช้งานแบบกลุ่ม ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงานหรือด้านเทคนิค

(๓) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key หรือเครื่องอ่านลายนิ้วมือ (Finger Print) เป็นต้น

๑๔.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ต้องมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านของผู้ใช้งานที่ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

๑๔.๔ ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของส่วนงานที่ได้กำหนดไว้ ให้ดำเนินการดังนี้

(๑) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุม ในการอนุญาตให้ใช้งานโปรแกรมเป็นรายครั้งไป

(๒) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาตและยังไม่ผ่านการตรวจสอบ

(๓) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์หรือละเมิดกฎหมาย อันจะก่อให้เกิดความเสียหายต่อตนเองและต่อส่วนงาน

(๔) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๕) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๖) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๑๔.๕ กำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (Session Time Out) เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาตและต้องพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบอีกครั้ง หลังจากระบบได้ตัดการใช้งานนั้นไปแล้ว

๑๕. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

๑๕.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ดังนี้

๑๕.๑.๑ ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามหน้าที่รับผิดชอบ โดยมีผู้บังคับบัญชาเป็นผู้อนุมัติการให้สิทธินั้น และต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

๑๕.๑.๒ ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา ๓๐ นาที ต้องทำการยุติการใช้งานทันที

๑๕.๑.๓ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๑) กำหนดสิทธิให้กับผู้ใช้งานระบบโดยการกำหนดบัญชีชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น

(๒) การรับ - ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น และต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศตามหน้าที่รับผิดชอบของผู้ใช้งาน

(๓) การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกส่วนงาน กรณีข้อมูลที่เป็นความลับของส่วนงาน ต้องมีการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล

(๔) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใด ๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้น ๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใด ๆ ที่มีผลกระทบต่อระบบ ผู้ดูแลระบบจะต้องเป็นผู้รับผิดชอบ

๑๕.๑.๔ ต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ พฤติกรรมการใช้งานการเข้าถึงระบบสารสนเทศที่สำคัญ

๑๕.๒ การควบคุมระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อส่วนงาน

๑๕.๒.๑ ต้องแยกระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงออกจากระบบอื่น ๆ ให้ทำงานอยู่บนเครื่องแม่ข่าย (Server) โดยไม่ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องควบคุมเครื่องแม่ข่ายที่มีสภาพแวดล้อมเหมาะสม

๑๕.๒.๒ จัดพื้นที่ควบคุมพิเศษ (ห้องควบคุมเครื่องแม่ข่าย) เพื่อควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้าออกพื้นที่ควบคุมพิเศษหรือทรัพยากรอื่นใด เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

๑๕.๒.๓ กำหนดค่าที่ไฟร์วอลล์ เพื่อควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก

๑๕.๒.๔ มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

๑๖. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๑๖.๑ ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๑๖.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวม ทั้งมีการรายงานต่อหัวหน้าส่วนงานโดยทันที

๑๖.๓ ต้องเปิดใช้บริการ เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๑๖.๔ ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๑๖.๕ ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๑๖.๖ การเข้าถึง System Utilities ที่ปฏิบัติการด้วยสิทธิพิเศษในระดับสูง ซึ่งทำให้สามารถเลี่ยงผ่านกลไกการควบคุมระบบ/แอปพลิเคชันต่าง ๆ ได้นั้น ต้องถูกจำกัดให้เฉพาะผู้ใช้งาน หรือผู้ดูแลระบบที่มีความจำเป็นต้องใช้งานเป็นประจำเท่านั้น สำหรับการใช้งานและการเข้าถึง System Utilities เหล่านั้นโดยบุคคลอื่นให้พิจารณาอนุมัติในลักษณะชั่วคราวในทุกกรณี

๑๖.๗ System Utilities ดังกล่าวข้างต้นต้องถูกแยกออกจากแอปพลิเคชันและซอฟต์แวร์อื่น ๆ เพื่อประโยชน์ในการจำกัดการเข้าถึงให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

๑๖.๘ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

๑๖.๙ ควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบดังนี้

๑๖.๙.๑ ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของสำนักงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

๑๖.๙.๒ ผู้ดูแลระบบที่ได้รับการอบรมแล้วหรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของส่วนงาน

๑๖.๙.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ ต้องมีการขออนุมัติจากหัวหน้าส่วนงานก่อนดำเนินการ

๑๖.๙.๔ ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๑๖.๙.๕ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัยและจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

๑๖.๙.๖ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

๑๖.๙.๗ วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๑๖.๙.๘ จัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

๑๖.๑๐ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

๑๖.๑๐.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๑๖.๑๐.๒ วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๑๗. การบริหารจัดการการบันทึกและตรวจสอบ

๑๗.๑ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ได้แก่ การบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึก ดังกล่าวไว้อย่างน้อย ๓ เดือน โดยมีรายละเอียดการบันทึกพฤติกรรมการใช้งาน (Logs) การเข้าถึงระบบ สารสนเทศ ดังนี้

(๑) ข้อมูลบัญชีชื่อผู้ใช้งาน
(๒) ข้อมูลวัน/เวลา ที่เข้าถึงระบบ
(๓) ข้อมูลวัน/เวลา ที่ออกจากระบบ
(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
(๕) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ
(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
(๗) ข้อมูลการเปลี่ยนการกำหนดค่า (Configuration) ของระบบ
(๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)
(๙) ข้อมูลแสดงการเข้าถึง ไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
(๑๐) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง
(๑๑) ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้
(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๗.๒ ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๗.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๘. การควบคุมการเข้าใช้งานระบบจากภายนอก

๑๘.๑ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของส่วนงานก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของส่วนงาน การควบคุมบุคคลที่เข้าสู่ระบบของส่วนงานจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๑๘.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้าส่วนงานก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๑๘.๓ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับส่วนงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๑๘.๔ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑๙. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๑๙.๑ ผู้ใช้งานระบบสารสนเทศ ต้องผ่านการพิสูจน์ตัวตนจากระบบของส่วนงาน สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

๑๙.๑.๑ การแสดงตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงบัญชีชื่อผู้ใช้งาน (Username)

๑๙.๑.๒ การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB Token ที่มีเทคโนโลยี Public Key Infrastructure : PKI ด้วยการลงลายมือชื่อดิจิทัล (Digital Signature) และการเข้ารหัสลับ (Encryption) รูปแบบของใบรับรองอิเล็กทรอนิกส์ เป็นต้น

๑๙.๒ การเข้าสู่ระบบสารสนเทศของส่วนงานนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี

๑๙.๓ การเข้าสู่ระบบสารสนเทศของส่วนงานจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

๑๙.๔ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๒๐. การปฏิบัติงานจากภายนอกสำนักงาน

๒๐.๑ การปฏิบัติงานจากภายนอกส่วนงาน ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกส่วนงานและระบบงานต่าง ๆ ภายในส่วนงาน

๒๐.๒ การเข้าถึงระบบสารสนเทศของส่วนงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับอนุญาตจากหัวหน้าส่วนงาน

๒๐.๓ การเข้าสู่ระบบระบบสารสนเทศในส่วนงานจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยบัญชีชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๒๐.๔ ผู้ได้รับอนุญาตเท่านั้นจึงจะสามารถเข้าถึงระบบสารสนเทศและข้อมูลของส่วนงาน โดยไม่ให้สมาชิกภายในครอบครัวหรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

๒๐.๕ ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๒๐.๖ ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกส่วนงานแก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อหัวหน้าส่วนงาน

๒๐.๗ ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกส่วนงานอย่างน้อยปีละ ๑ ครั้ง

หมวด ๓
การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๒๑. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๒๑.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลที่ส่วนงานอนุญาตให้บุคลากรใช้งาน เป็นทรัพย์สินของส่วนงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่อประโยชน์ของส่วนงาน

๒๑.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลของส่วนงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของส่วนงาน ผู้ใช้งานต้องได้รับอนุญาตจาก หัวหน้าส่วนงานก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลครุภัณฑ์ของส่วนงานจะต้องระบุว่าผู้ใดเป็นผู้ครอบครองเครื่องคอมพิวเตอร์นั้น

๒๑.๓ ผู้ดูแลระบบของส่วนงาน เป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคล ทั้งนี้ต้องเป็นผู้ที่หัวหน้าส่วนงาน มอบหมายให้ทำหน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

๒๑.๔ โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของส่วนงาน ต้องเป็นโปรแกรมที่ส่วนงานซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์

ส่วนตัว แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒๑.๕ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคล ของส่วนงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใด เพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๒๑.๖ การเคลื่อนย้ายเครื่องคอมพิวเตอร์ส่วนบุคคลออกนอกพื้นที่ปฏิบัติงานของส่วนงานจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงาน และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

๒๑.๗ การนำเครื่องคอมพิวเตอร์ส่วนบุคคลของส่วนงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจากบุคลากรที่หัวหน้าส่วนงานมอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากหัวหน้าส่วนงาน โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยบุคลากรหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางส่วนงานเท่านั้น

๒๑.๘ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบหาไวรัส โดยโปรแกรมป้องกันไวรัส

๒๑.๙ ไม่ควรเก็บข้อมูลสำคัญของส่วนงานไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๒๑.๑๐ ไม่ควรสร้าง Short-Cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของส่วนงาน

๒๑.๑๑ ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยหลีกเลี่ยงการวางอาหารหรือเครื่องดื่มบริเวณเครื่องคอมพิวเตอร์ และไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

๒๒. การควบคุมการเข้าถึงระบบปฏิบัติการ

๒๒.๑ ผู้ใช้งานต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

๒๒.๒ ผู้ใช้งานควรกำหนดรหัสผ่านที่มีคุณภาพตามคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

๒๒.๓ ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๑๐ นาทีและต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

๒๒.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๒๒.๕ ผู้ใช้ต้องทำการลงบันทึกออก (Logout) จากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒๓. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๒๓.๑ ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการเว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๒๓.๒ ผู้ดูแลระบบสารสนเทศของส่วนมีหน้าที่รับผิดชอบในการติดตั้งตรวจสอบการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ภายในส่วนงานที่เชื่อมต่อกับเครือข่ายอินเตอร์เน็ต

๒๓.๓ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๒๓.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๒๓.๕ ผู้ใช้งานต้องตรวจสอบว่าข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๒๔. การสำรองข้อมูลและการกู้คืน

๒๔.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เพื่อป้องกันการสูญหายของข้อมูล

๒๔.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๒๔.๓ ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

<u>หมวด ๔</u>
การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๒๕. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๒๕.๑ เครื่องคอมพิวเตอร์แบบพกพาที่ส่วนงานอนุญาตให้บุคลากรใช้งาน เป็นทรัพย์สินของส่วนงาน เพื่อใช้ในงานราชการ ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพ เพื่อประโยชน์ของส่วนงาน

๒๕.๒ เครื่องคอมพิวเตอร์แบบพกพาของส่วนงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของส่วนงาน ผู้ใช้งานต้องได้รับอนุญาตจากหัวหน้าส่วนงานของส่วนงานก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลครุภัณฑ์ของส่วนงาน จะต้องระบุว่าผู้ใดเป็นผู้ครอบครองหรือนำไปใช้งาน

๒๕.๓ บุคลากรผู้ดูแลระบบสารสนเทศของส่วนงานเป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์ รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer Name) แบบพกพา ทั้งนี้ ต้องเป็นผู้ที่หัวหน้า ส่วนงานมอบหมายให้หน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

๒๕.๔ โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของส่วนงาน ต้องเป็นโปรแกรมที่ส่วนงานซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒๕.๕ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบพกพาของส่วนงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใด เพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๒๕.๖ การนำเครื่องคอมพิวเตอร์แบบพกพาของส่วนงานไปใช้งานภายนอกพื้นที่ปฏิบัติงานของส่วนงาน จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงาน และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

๒๕.๗ การนำเครื่องคอมพิวเตอร์แบบพกพาของส่วนงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจากบุคลากรผู้ดูแลระบบสารสนเทศที่หัวหน้าส่วนงานมอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อนหากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากหัวหน้าส่วนงาน โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยบุคลากรผู้ดูแลระบบสารสนเทศ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางส่วนงานเท่านั้น

๒๕.๘ การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ใส่ในกระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาให้เรียบร้อย เพื่อป้องกันอันตรายที่เกิดจาก

การกระทบกระเทือน การหลงลืมอุปกรณ์

๒๕.๙ กรณีที่ต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้นโดยเด็ดขาด

๒๕.๑๐ ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่ และควรรักษาสภาพคอมพิวเตอร์ให้มีสภาพพร้อมใช้งานตลอดเวลา

๒๕.๑๑ ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๒๕.๑๒ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกากดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๒๕.๑๓ ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

๒๕.๑๔ การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๒๖. ความปลอดภัยทางด้านกายภาพ

๒๖.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ดังนั้นควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๒๖.๒ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒๖.๓ ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๒๖.๔ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๒๖.๕ ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน

๒๖.๖ ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๒๗. การควบคุมการเข้าถึงระบบปฏิบัติการ

๒๗.๑ ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

๒๗.๒ หากวางเครื่องคอมพิวเตอร์แบบพกพาไว้นอกสถานที่ปฏิบัติงาน ควรล็อคหน้าจอด้วยตัวเองทุกครั้ง (Log off) เมื่อไม่ได้อยู่ที่หน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

๒๗.๓ ผู้ใช้งานต้องไม่อนุญาตให้บุคคลภายนอกที่ไม่มีความเกี่ยวข้อง ใช้งานเครื่องคอมพิวเตอร์แบบพกพา และไม่บอกรหัสผ่านการล็อคหน้าจอให้แก่ผู้อื่น

๒๘. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๒๘.๑ ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๒๘.๒ บุคลากรผู้ดูแลระบบสารสนเทศของส่วนงาน มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ของส่วนงานเป็นโปรแกรมพื้นฐาน

๒๘.๓ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๒๘.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๒๘.๕ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และต้องรีบแจ้งผู้ดูแลระบบสารสนเทศของส่วนงานโดยเร็ว

๒๙. การสำรองข้อมูลและการกู้คืน

๒๙.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่น ๆ เพื่อป้องกันการสูญหายของข้อมูล หรือควรจัดเก็บข้อมูลไว้บนคลาวด์

๒๙.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๒๙.๓ ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

๒๙.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

<u>หมวด ๕</u>
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓๐. การควบคุมหน่วยงานภายนอก

๓๐.๑ ต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงานหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงานได้

๓๐.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๓๐.๒.๑ บุคคลภายนอกที่ต้องการสิทธิในการเข้า ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้าส่วนงาน

๓๐.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก เพื่อระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงาน ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

(๑) เหตุผลในการขอใช้

(๒) ระยะเวลาในการใช้

(๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๔) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓๐.๒.๓ หน่วยงานภายนอกที่ปฏิบัติงานให้กับส่วนงาน ไม่ว่าจะทำงานอยู่ภายในหรือภายนอกส่วนงานจำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลของส่วนงาน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศของส่วนงาน

๓๐.๒.๔ ส่วนงานควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

๓๐.๒.๕ เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๓๐.๒.๖ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของส่วนงาน ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษา

ความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๓๐.๒.๗ ส่วนงานมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจว่าส่วนงานสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๓๐.๒.๘ ควรดำเนินการให้ผู้ให้บริการภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๓๑. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๓๑.๑ กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

๓๑.๒ ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

๓๑.๓ กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับ โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๓๑.๔ กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ก่อนการติดตั้ง

๓๑.๕ การทดสอบซอฟต์แวร์ ห้ามทดสอบบนระบบและฐานข้อมูลที่ใช้งาน ต้องสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

๓๒. มาตรการควบคุมผู้ให้บริการภายนอก

๓๒.๑ ผู้ให้บริการภายนอกที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของส่วนงาน จะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากหัวหน้าส่วนงาน

๓๒.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

๓๒.๓ กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น ทั้งนี้ หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๓๒.๔ การอนุญาตให้ผู้ให้บริการภายนอกเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลทิ้งไว้โดยไม่จำเป็นต้องมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากหัวหน้าส่วนงานก่อนทุกครั้ง

๓๒.๕ มาตรการควบคุมช่องโหว่ทางเทคนิค

๓๒.๕.๑ การบริหารจัดการช่องโหว่ของระบบ ควรมีการบันทึกดังต่อไปนี้

(๑) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

(๒) สถานที่ที่ติดตั้ง

(๓) เครื่องแม่ข่ายที่ติดตั้ง

(๔) ผู้ผลิตซอฟต์แวร์

(๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๓๒.๕.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๓๒.๕.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

(๑) มีการเฝ้าระวังและติดตามประเมินความเสี่ยง สำหรับช่องโหว่ของระบบ

สารสนเทศ รวมทั้งการประสานงาน เพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(๒) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของส่วนงาน

(๓) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยง เมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๓๒.๕.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

หมวด ๖
การใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์

๓๓. การใช้งานอินเทอร์เน็ต

๓๓.๑ ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ส่วนงานจัดสรรไว้เท่านั้น เช่น Proxy Firewall IP-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหัวหน้าส่วนงานเป็นลายลักษณ์อักษรแล้ว

๓๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

๓๓.๓ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

๓๓.๔ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของส่วนงานนอกเหนือจากเพื่อประโยชน์ของทางราชการหรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เว้นแต่เป็นการดำเนินงานตามภารกิจของส่วนงาน

๓๓.๕ ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของส่วนงาน

๓๓.๖ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับส่วนงาน

๓๓.๗ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของส่วนงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๓๓.๘ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๓๓.๙ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด อันจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๓๓.๑๐ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๓๓.๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขายต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๓๓.๑๒ การใช้งานเว็บบอร์ด (WebBoard) ของส่วนงาน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของส่วนงาน

๓๓.๑๓ ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของส่วนงาน การทำลายความสัมพันธ์กับบุคลากรของส่วนงานอื่น ๆ

๓๓.๑๔ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๓๔. แนวปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

๓๔.๑ ส่วนงานต้องกำหนดแนวปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์ในเวลาราชการเพื่อให้เกิดการใช้งานในเชิงสร้างสรรค์และเป็นประโยชน์ต่อการดำเนินงาน เช่น ใช้เพื่อการติดต่อสื่อสารเพื่อการประชาสัมพันธ์ เป็นต้น

๓๔.๒ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะ ตามที่ส่วนงานได้กำหนดไว้เท่านั้น

๓๔.๓ หากต้องการใช้งานเครือข่ายสังคมออนไลน์ในลักษณะอื่นใดนอกเหนือจากที่ส่วนงานกำหนดให้ขออนุญาตจากหัวหน้าส่วนงานก่อนใช้งาน

๓๔.๔ ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของส่วนงาน

๓๔.๕ ผู้ใช้งานพึงตระหนักว่าข้อความหรือความเห็นที่เผยแพร่บนเครือข่ายสังคมออนไลน์เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุ ให้ร้าย ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

๓๔.๕ ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามบัญชีชื่อผู้ใช้ส่วนตัว แต่อาจส่งผลกระทบกับส่วนงานได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์

๓๔.๖ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อส่วนงาน ผู้ใช้งานต้องแจ้งต่อหัวหน้าส่วนงานโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๓๔.๗ ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

หมวด ๗
การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์

๓๕. แนวปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

๓๕.๑ ผู้ใช้งานควรเปลี่ยนรหัสผ่านใหม่ทุก ๖ เดือน โดยรหัสผ่านที่เปลี่ยนต้องเป็นรหัสผ่านที่ไม่เคยใช้มาก่อนและเป็นรหัสผ่านที่คาดเดาได้ยากตามหลักเกณฑ์การกำหนดรหัสผ่านที่ดี

๓๕.๒ ผู้ใช้งานไม่ควรใช้โปรแกรมช่วยจำรหัสผ่านหรือกำหนดให้มีการจำรหัสผ่านของจดหมายอิเล็กทรอนิกส์

๓๕.๓ ผู้ใช้งานต้องไม่เปิดหน้าจอระบบจดหมายอิเล็กทรอนิกส์ทิ้งเอาไว้ขณะที่ไม่ได้อยู่หน้าจอ

๓๕.๔ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อส่วนงาน หรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

๓๕.๕ ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-Mail Address) ของผู้อื่น เพื่ออ่าน รับ ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของแล้วเท่านั้น และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๓๕.๖ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของส่วนงาน เพื่อการติดต่อสื่อสารในนามของของส่วนงานเท่านั้น

๓๕.๗ หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Log out ออกจากระบบและปิดเว็บเบราว์เซอร์ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

๓๕.๘ ผู้ใช้ต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดด้วยโปรแกรมป้องกันไวรัสเป็นการป้องกันการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

๓๕.๙ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จักหรือไม่น่าไว้ใจ

๓๕.๑๐ ผู้ใช้งานต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์และใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง และระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป รวมทั้งจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

๓๕.๑๑ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๓๕.๑๒ ผู้ใช้งานควรตรวจสอบกล่องเก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรลบ จดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๓๕.๑๓ ผู้ใช้งานควรทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่สำคัญตามความจำเป็นอย่างสม่ำเสมอ

๓๕.๑๔ ข้อควรระวัง ผู้ใช้งานไม่ควรโอนย้ายจดหมาย อิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

๓๕.๑๕ ผู้ใช้ไม่ควรใช้งานจดหมายอิเล็กทรอนิกส์บนเครื่องคอมพิวเตอร์สาธารณะ เพื่อความปลอดภัยของข้อมูลและบัญชีผู้ใช้งาน

๓๖. แนวปฏิบัติในการใช้งานบริการคลาวด์

๓๖.๑ ผู้ใช้งานไม่ควรให้บุคคลอื่นใช้งานบริการคลาวด์ของมหาวิทยาลัยเพื่อประโยชน์ส่วนตัว

๓๖.๒ ผู้ใช้งานไม่ควรเก็บข้อมูลที่ละเมิดลิขสิทธิ์ ขัดต่อกฎหมายและศีลธรรมไว้บนบริการคลาวด์

๓๖.๓ ผู้ใช้ไม่ควรเปิดใช้งานบริการคลาวด์ทิ้งไว้ โดยไม่ได้อยู่ที่หน้าจอ เพื่อป้องกันข้อมูลรั่วไหล

๓๖.๔ ผู้ใช้ไม่ควรใช้งานบริการคลาวด์บนเครื่องคอมพิวเตอร์สาธารณะ เพื่อความปลอดภัยของข้อมูลและบัญชีผู้ใช้งาน

<u>หมวด ๘</u>
การควบคุมการเข้าถึงระบบเครือข่าย

๓๗. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

๓๗.๑ ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่และความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓๗.๒ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สายของส่วนงาน

๓๗.๓ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access Point : AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

๓๗.๔ ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ ทั้งนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๓๗.๕ ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจาก ผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๓๗.๖ ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๓๗.๗ ผู้ดูแลระบบต้องกำหนดค่าใช้มาตรฐานความปลอดภัยแบบ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ เพื่อให้ยากต่อการดักจับ ช่วยให้ปลอดภัยมากขึ้น

๓๗.๘ ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในส่วนงาน

๓๗.๙ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

หมวด ๙
การแบ่งปันข้อมูล

๓๘. แนวปฏิบัติในการแบ่งปันข้อมูล

๓๘.๑ กำหนดขอบเขตและระดับความลับของข้อมูล โดยให้ความสำคัญกับการระบุขอบเขตของข้อมูลที่จะแบ่งปัน เพื่อให้เหมาะสมกับการแบ่งปันและการเข้าถึงข้อมูล

๓๘.๒ มีข้อกำหนดในการแบ่งปันข้อมูล รวมถึงการบริหารจัดการการอนุญาตเพื่อให้มั่นใจได้ว่ามีผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลการแบ่งปันนี้ได้

๓๘.๓ มีข้อกำหนดในการใช้ข้อมูลที่ได้รับการแบ่งปัน เช่น การกำหนดขอบเขตการใช้ข้อมูลหรือการห้ามนำข้อมูลไปใช้ในวัตถุประสงค์ที่ไม่เกี่ยวข้อง

๓๘.๔ การตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการแบ่งปันข้อมูล รวมถึงการจัดการและควบคุมเพื่อลดความเสี่ยงที่เป็นไปได้

๓๘.๕ การฝึกอบรมบุคลากรที่เกี่ยงข้อง เพื่อเพิ่มความเข้าใจในการแบ่งปันข้อมูลและการใช้ข้อมูลอย่างมีประสิทธิภาพ รวมถึงการบันทึกข้อมูลเกี่ยวกับการแบ่งปันข้อมูลเพื่อการติดตามและการประเมินประสิทธิภาพ

๓๘.๖ การตรวจสอบและประเมินการแบ่งปันข้อมูลเพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามหลักเกณฑ์และแนวทางที่กำหนดไว้

๓๙. รูปแบบการแบ่งปันข้อมูล

๓๙.๑ การแบ่งปันทั่วไป (General Sharing) เป็นการแบ่งปันข้อมูลที่มีความสำคัญและเกี่ยวข้องกับผู้ใช้หลายกลุ่ม โดยไม่จำกัดเฉพาะกับกลุ่มหรือบุคคลใด

๓๙.๒ การแบ่งปันตามความจำเป็น (Need-to-Know Sharing) เป็นการแบ่งปันข้อมูลเฉพาะกับบุคคลหรือกลุ่มผู้ใช้ที่จำเป็นต้องมีข้อมูลนั้นเพื่อการปฏิบัติงาน

๓๙.๓ การแบ่งปันตามระดับความลับ (Security Clearance-based Sharing) เป็นการแบ่งปันข้อมูลโดยพิจารณาจากระดับความลับของข้อมูล และแบ่งปันเฉพาะกับบุคคลหรือกลุ่มผู้ใช้ตามความเหมาะสม

การเลือกรูปแบบการแบ่งปันข้อมูลจะขึ้นอยู่กับลักษณะของข้อมูล ชั้นความลับ และวัตถุประสงค์ของการแบ่งปันข้อมูล ทั้งนี้ให้ยึดถือประโยชน์ของมหาวิทยาลัยเป็นสำคัญ

หมวด ๑๐
การทำให้ระบบมีความแข็งแกร่ง

๔๐. แนวปฏิบัติในการทำให้ระบบมีความแข็งแกร่ง

๔๐.๑ ปรับแต่งค่าเริ่มต้นของระบบและแอปพลิเคชัน โดยเปลี่ยนรหัสผ่านตั้งต้น (Default Password) ปิดการใช้งานบริการที่ไม่จำเป็น และปรับเป็นการตั้งค่าที่ปลอดภัย

๔๐.๒ เปิดใช้งานเฉพาะ Port ที่มีความจำเป็นเท่านั้น ส่วน Port ใดที่ไม่ได้ใช้งานให้ทำการปิด เพื่อลดความเสี่ยงจากการถูกโจมตีโดยผู้ไม่ประสงค์ดี

๔๐.๓ อัพเดทซอฟต์แวร์และระบบปฏิบัติการเป็นประจำ (Patch Management) เพื่อแก้ไขช่องโหว่และลดความเสี่ยงจากการถูกโจมตีโดยผู้ไม่ประสงค์ดี

๔๐.๔ ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านของเครื่องแม่ข่ายเป็นประจำทุก ๆ ๓ เดือน โดยรหัสผ่านที่เปลี่ยนต้องไม่เคยถูกใช้งานมาก่อน เพื่อป้องกันปัญหาจากการเกิดข้อมูลรั่วไหล

๔๐.๕ กำหนดสิทธิของผู้ใช้ในส่วนต่าง ๆ ให้น้อยที่สุด (Least Privilege) ตามความจำเป็นเฉพาะหน้าที่ที่เกี่ยวข้องเท่านั้น

๔๐.๖ หลีกเลี่ยงการเข้าถึงเครื่องแม่ข่ายโดยตรงผ่าน Public IP ต้องเป็นการเข้าถึงผ่าน Private IP และผ่าน VPN เท่านั้น หากเป็นการเข้าถึงจากภายนอกเครือข่ายของมหาวิทยาลัย

๔๐.๗ ต้องติดตั้งซอฟต์แวร์ Antivirus ที่มหาวิทยาลัยจัดสรรให้ในเครื่องแม่ข่ายหรือทรัพย์สินสารสนเทศ ของส่วนงาน

๔๐.๘ จำกัดสิทธิการเข้าถึงเครื่องแม่ข่ายหรือทรัพย์สินสารสนเทศที่สำคัญเฉพาะผู้ดูแลระบบของส่วนงาน เท่านั้น หากมีการปรับเปลี่ยนสิทธิต้องดำเนินการเป็นลายลักษณ์อักษรและอนุมัติโดยหัวหน้าส่วนงาน

หมวด ๑๑
การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์

๔๑. แนวปฏิบัติในการสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์

๔๑.๑ จัดให้มีการอบรมเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ให้แก่นิสิตและบุคลากรของมหาวิทยาลัยอย่างน้อยปีละ ๑ ครั้ง

๔๑.๒ กำหนดแนวปฏิบัติให้บุคลากรของส่วนงานติดตั้งซอฟต์แวร์ Antivirus ในเครื่องคอมพิวเตอร์ส่วนบุคคลที่ส่วนงานจัดสรรให้ และเครื่องคอมพิวเตอร์แบบพกพาที่นำมาปฏิบัติงานภายในส่วนงาน

๔๑.๓ ผู้ใช้ต้องอัพเดทVirus Definition ของซอฟต์แวร์ Antivirus เป็นประจำอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๔๑.๔ ผู้ใช้ควรสแกนไวรัสบนสื่อแบบถอดได้ทุกครั้งก่อนนำมาใช้งาน

๔๑.๕ ผู้ใช้ไม่ควรใช้งานสื่อแบบถอดได้ที่ได้รับมาจากแหล่งที่ไม่น่าเชื่อถือ เช่น พบว่าตกอยู่บนพื้นหรือวางอยู่บนโต๊ะแบบไม่มีเจ้าของ เพื่อป้องกันซอฟต์แวร์ไม่พึงประสงค์

๔๑.๖ ผู้ใช้ต้องไม่ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์จากสื่อต่าง ๆ หรือจากการดาวน์โหลดผ่านเครือข่ายอินเตอร์เน็ต

๔๑.๗ ผู้ใช้ต้องมีความระมัดระวังในการใช้งานเว็บไซต์ โดยสังเกตจากชื่อ URL เพื่อป้องกันการถูกขโมยข้อมูลจากผู้ไม่ประสงค์ดี

๔๑.๘ ผู้ใช้ต้องมีความระมัดระวังในการใช้งานอีเมล โดยไม่ดาวน์โหลดหรือเปิดไฟล์แนบจากอีเมลที่ไม่น่าเชื่อถือ

๔๑.๙ ผู้ใช้ต้องมีความระมัดระวังในการใช้งานโซเชียลมีเดีย เพื่อป้องกันการถูกหลอกลวงโดยผู้ไม่ประสงค์ดี

<u>หมวด ๑๒</u>

การเชื่อมต่อระยะไกล

๔๒. แนวปฏิบัติการเชื่อมต่อระยะไกล

๔๒.๑ หลีกเลี่ยงการเชื่อมต่อระยะไกลโดยผู้ใช้ประเภทบุคลากร หากไม่มีความจำเป็นหรือเร่งด่วนใด ๆ

๔๒.๒ เครือข่ายของส่วนงาน ที่อนุญาตให้ผู้ใช้เข้าถึงได้ หากมีความจำเป็นต้องให้มีการเข้าถึงผ่านการเชื่อมต่อระยะไกล ต้องให้เชื่อมต่อผ่าน VPN ที่มหาวิทยาลัยกำหนดไว้เท่านั้น โดยใช้ IPASS ในการยืนยันตัวตน

๔๒.๓ เครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์แบบพกพา ที่ทำการเชื่อมต่อระยะไกลผ่าน VPN ต้องติดตั้งซอฟต์แวร์ Antivirus ที่มหาวิทยาลัยจัดสรรให้

๔๒.๔ เครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์แบบพกพา ที่ทำการเชื่อมต่อระยะไกลผ่าน VPN ต้องอัพเดทซอฟต์แวร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ

๔๒.๕ ผู้ใช้ต้องไม่มอบบัญชีผู้ใช้งานของตนให้กับผู้อื่นเพื่อใช้งาน VPN ในการเชื่อมต่อระยะไกลกับเครือข่ายของมหาวิทยาลัย

๔๒.๖ ผู้ใช้ต้องไม่ใช้เครื่องคอมพิวเตอร์สาธารณะในการเชื่อมต่อระยะไกลกับเครือข่ายของมหาวิทยาลัย

๔๒.๗ ส่วนงานต้องมีการประเมินความเสี่ยงในการเชื่อมต่อระยะไกล เพื่อหามาตรการป้องกันแก้ไขปัญหาที่อาจจะเกิดขึ้น

<u>นโยบายที่ ๒</u> นโยบายการรักษาสภาพความพร้อมใช้

<u>หมวด ๑๓</u>

การรักษาสภาพความพร้อมใช้งานของการให้บริการ

๔๓. แนวปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

๔๓.๑ เครื่องคอมพิวเตอร์แม่ข่ายที่มีความสำคัญ ต้องมีการสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน

๔๓.๒ ผู้ดูแลระบบต้องสำรองข้อมูลและซอฟต์แวร์เก็บไว้ โดยคัดเลือกและจัดเรียงลำดับตามผลกระทบจากความสูญเสียของระบบที่มีผลต่อภารกิจหลักของส่วนงาน

๔๓.๓ ต้องมีขั้นตอนการปฏิบัติการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๔๓.๔ ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองในสื่อบันทึกข้อมูลสำรอง โดยมีการแสดงชื่อระบบที่สำรอง วัน เดือน ปี และเวลาในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรอง ซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง และต้องมีการทดสอบสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

๔๓.๕ หัวหน้าส่วนงานต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมฉุกเฉิน

๔๓.๖ ส่วนงานต้องดำเนินการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินปีละ ๑ ครั้ง

๔๓.๗ ผู้ดูแลระบบต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยระบบสารสนเทศได้ตามปกติ โดยต้องทบทวนแผนเตรียมความพร้อมกรณี ฉุกเฉินดังกล่าวอย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

หมวด ๑๔
การตรวจสอบและรับมือภัยคุกคามทางไซเบอร์

๔๔. แนวปฏิบัติในการตรวจสอบและรับมือภัยคุกคามทางไซเบอร์

๔๔.๑ มอบหมายให้มีผู้ที่ทำหน้าที่ในการตรวจสอบและรับมือภัยคุกคามทางไซเบอร์ เพื่อแก้ไขและป้องกันปัญหาในเบื้องต้นก่อนแจ้งให้มหาวิทยาลัยทราบ

๔๔.๒ เมื่อพบเหตุที่ประเมินแล้วว่าอยู่ในระดับวิกฤต ต้องรีบแจ้งหัวหน้าส่วนงาน และดำเนินการป้องกัน แก้ไขในเบื้องต้น ก่อนที่จะรายงานให้กับมหาวิทยาลัยทราบ

๔๔.๓ ต้องบันทึกเหตุและการเผชิญเหตุทุกครั้ง ถึงแม้ว่าจะสามารถแก้ไขปัญหาภัยคุกคามนั้น ๆ ได้แล้ว

๔๔.๔ ต้องมอบหมายให้ผู้ที่รับผิดชอบ เข้าร่วมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ

๔๔.๕ ต้องกำหนดผู้รับผิดชอบด้านการรับมือภัยคุกคามทางไซเบอร์ ตามแนวทางที่มหาวิทยาลัยกำหนดและทบทวนเป็นประจำทุกปี

๔๔.๖ ต้องมอบหมายให้ผู้ที่รับผิดชอบ และผู้ที่เกี่ยวข้องร่วมฝึกซ้อมแผนรับมือภัยคุกคามทางไซเบอร์เป็นประจำทุกปี

หมวด ๑๕
การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

๔๕. แนวปฏิบัติการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

๔๕.๑ ต้องมีการมอบหมายให้มีผู้ทำหน้าที่จัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) จากความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์อย่างเป็นทางการหรือลายลักษณ์อักษร

๔๕.๒ ต้องมีการสำรองข้อมูลหรือระบบที่สำคัญนอกเหนือจากการดูแลของสถาบันทรัพยากรการเรียนรู้และเทคโนโลยีดิจิทัลเป็นประจำตามระดับความสำคัญของข้อมูลและระบบตามที่ได้ทำการวิเคราะห์ความเสี่ยงแล้ว

๔๕.๓ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) จากความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์และต้องมีการจัดเตรียมทรัพย์สินสารสนเทศสำรองให้ครบถ้วนตามที่ระบุไว้ในแผน

๔๕.๔ ส่วนงานต้องมีการฝึกซ้อมแผน BCP อย่างน้อยปีละ ๑ ครั้งเพื่อประเมินประสิทธิภาพของแผนต่อภัยคุกคามทางไซเบอร์ ในรูปแบบที่เหมาะสมและจัดทำเป็นเอกสารรายงาน

๔๕.๕ ส่วนงานต้องมีการทบทวนแผน BCP อย่างน้อยปีละ ๑ ครั้งเพื่อปรับปรุงเปลี่ยนแปลงให้มีความเหมาะสมและทันต่อเหตุการณ์

นโยบายที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยง

หมวด ๑๖
การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๔๕. แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๔๕.๑ ระบุความเสี่ยงให้สอดคล้องกับความเสี่ยงที่อาจจะเกิดขึ้น ดังนี้

๔๕.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายของส่วนงานผ่านเครือข่ายอินเทอร์เน็ต

๔๕.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายของส่วนงานโดยไม่ได้รับอนุญาต

๔๕.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือสารสนเทศหรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๔๕.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้าใช้งาน (Login) สารสนเทศที่สำคัญของส่วนงานผ่านระบบเครือข่ายที่ไม่ปลอดภัย เช่น เครือข่ายอินเตอร์เน็ตสาธารณะ เป็นต้น

๔๕.๑.๕ ความเสี่ยงอื่นที่เกี่ยวข้องกับระบบสารสนเทศของส่วนงานที่อาจจะส่งผลกระทบกับการปฏิบัติงานของส่วนงาน

๔๖.๒ การตรวจสอบและประเมินความเสี่ยง ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น ให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๔๖.๒.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ ทำการประเมินในแต่ละด้านของผลกระทบโดยให้พิจารณาถึงมาตรการควบคุมที่มีอยู่ในปัจจุบันด้วย

๔๖.๒.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่จะเกิดขึ้น ต้องพิจารณา ๒ ปัจจัยหลัก คือ

(๑) แนวโน้มการเกิดขึ้นของเหตุการณ์ความเสี่ยง โดยพิจารณาจากความน่าจะเป็นหรือค่าทางสถิติที่มีการบันทึกไว้ เช่น เหตุการณ์ความเสี่ยง เหตุภัยธรรมชาติต่าง ๆ เป็นต้น

(๒) ความยากง่ายที่จะถูกกระทำ ให้พิจารณาจากจุดอ่อนหรือข้อบกพร่องที่มีอยู่และตัวควบคุมในปัจจุบัน หากมีจุดอ่อนหรือข้อบกพร่องมากและไม่มีตัวควบคุมเลย โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงจะสูงกว่าในกรณีที่มีตัวควบคุมอยู่

๔๖.๒.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้ เกิดเหตุการณ์ที่ระบุ พิจารณาข้อบกพร่องของระบบหรือข้อบกพร่องของการควบคุมที่ปัจจุบันอาจจะไม่มีอยู่ และจะส่งผลให้ระบบไม่มีความมั่นคงปลอดภัยที่ดี

๔๖.๒.๔ ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบสารสนเทศของส่วนงานอย่างน้อยปีละ ๑ ครั้ง

๔๖.๒.๕ การตรวจสอบจะต้องดำเนินการโดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของส่วนงาน (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง

๔๖.๓ กระบวนการบริหารความเสี่ยง ต้องมีการดำเนินการตรวจสอบและประเมินช่องโหว่ (Vulnerability Assessment) ก่อนนำระบบสารสนเทศมาใช้งาน หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญของระบบสารสนเทศและส่วนงานจะต้องมีการประเมินผลอย่างน้อยปีละ ๑ ครั้ง ระบบสารสนเทศที่สำคัญต้องมีการดำเนินการทดสอบการเจาะระบบ (Penetration Testing) อย่างมีมาตรฐาน เพื่อประเมินความสามารถในการรับมือกับภัยคุกคามภายนอก ทั้งนี้ ผลจากการประเมินช่องโหว่และการทดสอบการเจาะระบบต้องถูกรายงานต่อผู้บริหาร และต้องมีการจัดทำแผนการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดอย่างเหมาะสม

<u>หมวด ๑๗</u>

การกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

๔๗. แนวปฏิบัติการกำหนดหน้าที่และความรับผิดชอบ

๔๗.๑ ระดับนโยบาย

๔๗.๑.๑ ผู้บริหารส่วนงานที่ได้รับมอบหมายจากหัวหน้าส่วนงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายแก่ส่วนงานหรือบุคลากร อันเนื่องมาจากความบกพร่อง ละเลย หรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔๗.๑.๒ ผู้บริหารส่วนงานที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศของส่วนงาน เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะและคำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบ การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

๔๗.๒ ระดับปฏิบัติการ

ระดับผู้ปฏิบัติงานประกอบด้วย ผู้ดูแลระบบสารสนเทศของส่วนงาน ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจดังนี้

๔๗.๒.๑ ผู้ดูแลระบบสารสนเทศหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นผู้รับผิดชอบ ดังนี้

(๑) ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) เป็นผู้ประสานงานและร่วมปฏิบัติตามแผนรับมือภัยคุกคามทางไซเบอร์ของมหาวิทยาลัย

(๓) ควบคุม ดูแล รักษาความปลอดภัยและบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายของส่วนงาน

(๔) ทำการสำรองข้อมูลหรือเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนดของส่วนงาน

(๕) ป้องกันและเฝ้าระวังภัยคุกคามทางไซเบอร์ในระดับส่วนงาน และแจ้งเหตุให้มหาวิทยาลัยทราบทันทีที่เกิดเหตุภัยคุกคามทางไซเบอร์

(๖) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยไซเบอร์ของส่วนงาน

๔๗.๒.๒ ผู้ใช้งานเป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของส่วนงานตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้อย่างเคร่งครัด

นโยบายที่ ๔ นโยบายการติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณภายในอาคารและนอกอาคาร

หมวด ๑๘
การติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณภายในอาคารและนอกอาคาร

๔๘. แนวปฏิบัติการติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณภายในอาคารและนอกอาคาร

๔๘.๑ ห้ามส่วนงาน บุคลากรภายในและบุคคลภายนอกมหาวิทยาลัยดำเนินการติดตั้ง ปรับย้าย หรือดัดแปลง อุปกรณ์เครือข่าย เช่น Switch Router Access Point Firewall หรือสายสัญญาณ เช่น สาย LAN Fiber Optic CCTV ด้วยตนเองโดยไม่ได้รับความเห็นชอบจากสถาบันทรัพยากรการเรียนรู้และเทคโนโลยีดิจิทัล

๔๘.๒ หากพบการติดตั้งอุปกรณ์หรือการเดินสายโดยไม่ได้รับความเห็นชอบจากสถาบันทรัพยากรการเรียนรู้และเทคโนโลยีดิจิทัล ทางสถาบันฯ มีสิทธิ์ถอดถอนหรือระงับการใช้งานทันที
