นโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. 2568

ฝ่ายเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท ซีพีแอล กรุ๊ป จำกัด (มหาชน) หรือต่อไปนี้เรียกว่า “บริษัท” มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกัน ปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ บริษัทจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดให้มีแนวปฏิบัติที่ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 เพื่อกำหนดแนวทางปฏิบัติและวิธีปฏิบัติ ให้แก่ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งานของบริษัท และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

1.2 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและ การสื่อสารหรือเครือข่ายคอมพิวเตอร์ของบริษัทได้อย่างมีประสิทธิภาพและประสิทธิผล

1.3 เพื่อเผยแพร่ให้แก่พนักงานทุกคนในบริษัทได้รับทราบ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายที่ 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติดังนี้

หมวด 1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม

หมวด 2 การเข้าถึงและควบคุมการใช้งานสารสนเทศ

หมวด 3 การใช้งานเครื่องคอมพิวเตอร์

หมวด 4 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

หมวด 5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

หมวด 6 การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์

หมวด 7 การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์

หมวด 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

หมวด 9 การใช้ข้อมูลร่วมกัน (Information Sharing)

หมวด 10 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

หมวด 11 การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

หมวด 12 การเชื่อมต่อระยะไกล (Remote Connection)

นโยบายที่ 2 นโยบายการรักษาสภาพความพร้อมใช้งานของการให้บริการ มีแนวปฏิบัติดังนี้

หมวด 13 การรักษาสภาพความพร้อมใช้งานของการให้บริการ

หมวด 14 การตรวจสอบและรับมือภัยคุกคามทางไซเบอร์ (Detect & Response)

หมวด 15 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์(Cybersecurity Resilience and Recovery)

นโยบายที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ มีแนวปฏิบัติดังนี้

หมวด 16 การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

หมวด 17 การกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

นโยบายที่ 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติดังนี้

หมวด 1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and Environment Security)

1.วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าพื้นที่และการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของ อุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและจำเป็นต้องรักษาความลับ เพื่อป้องกันทรัพย์สินของบริษัทจากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือข้อมูลสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต โดยมาตรการนี้จะมีผลบังคับใช้กับพนักงาน และหน่วยงานภายนอก ซึ่งมี ส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1 ต้องมีการจำแนกและกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2.2 ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงาน ของผู้ดูแล ระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่ควบคุมพิเศษ และพื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

2.3 ต้องกำหนดสิทธิให้กับพนักงานให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ประกอบด้วย

2.3.1 จัดทำ“ทะเบียนผู้มีสิทธิเข้า - ออกพื้นที่”เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งาน

2.3.3 จัดให้มีพนักงานทำหน้าที่ตรวจสอบประวัติการเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ

2.3.4 ต้องมีการทบทวนปรับปรุง รายการผู้มีสิทธิเข้า - ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับสิทธิการเข้า-ออกพื้นที่ เช่น การ โอน ย้าย ลาออก หรือสิ้นสุดการจ้าง

3. การควบคุมการเข้า-ออก พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

3.1 หน่วยงานฝ่ายเทคโนโลยีสารสนเทศที่รับผิดชอบด้านความปลอดภัยของพื้นที่ฯ ต้องจัดให้มีพนักงานหรือวิธีการรักษาความปลอดภัย เพื่อควบคุมการเข้า - ออก สถานที่ทำงานได้เฉพาะบุคคลที่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

3.2 ต้องจัดทำทะเบียนระบุสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยกำหนดดังนี้

3.2.1 ต้องกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้า-ออกในแต่ละพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างชัดเจน

3.2.2 การเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของเจ้าหน้าที่เทคโนโลยีสารสนเทศจะเป็นผู้คีย์แจ้งเข้าระบบ Helpdesk เพื่อขออนุมัติเข้า-ออกและระบุรายละเอียดการเข้าดำเนินการพร้อมทั้งปิดงานเมื่อดำเนินการแล้วเสร็จ

3.2.3 การเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของบุคคลภายนอกหรือผู้มาติดต่อ

เจ้าหน้าที่เทคโนโลยีสารสนเทศผู้ควบคุมจะเป็นผู้คีย์แจ้งเข้าระบบ Helpdesk เพื่อขออนุมัติเข้า- ออก และระบุรายละเอียดในการเข้าดำเนินการ พร้อมทั้งปิดงานเมื่อดำเนินการแล้วเสร็จ

3.2.4 กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์แบบพกพาหรืออุปกรณ์เครือข่ายเข้าบริเวณพื้นที่ฯเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศจะต้องบันทึกรายการอุปกรณ์ที่นำเข้ามาไว้ในรายละเอียด ข้อ 3.2.3 ด้วย

3.3 ผู้ใช้งานจะได้รับสิทธิให้เข้า-ออกพื้นที่ฯทำงานได้ เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้สำหรับ ปฏิบัติงานเท่านั้น

3.4 หากมีบุคคลอื่นใดที่ไม่ใช้ผู้ใช้งานขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตทั้งนี้ จะต้องติดต่อเจ้าหน้าที่เทคโนโลยีสารสนเทศผู้ควบคุมจะเป็นผู้คีย์แจ้งเข้าระบบ Helpdesk เพื่อขออนุมัติเข้า-ออก และระบุรายละเอียดในการเข้าดำเนินการ พร้อมทั้งปิดงานเมื่อดำเนินการแล้วเสร็จ

4. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

จัดให้มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งาน ดังนี้

4.1 ติดตั้งระบบระงับเพลิง

4.2 ติดตั้งระบบปรับอากาศและควบคุมความชื้น

4.3 ติดตั้งระบบแจ้งเตือน กรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องแม่ข่ายทำงาน ผิดปกติ หรือหยุดการทำงาน

4.4 วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานอย่างสม่ำเสมอ ให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

5. การเดินสายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

5.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มี บุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงต้องติดตั้งระบบป้องกันที่ปลอดภัย

5.2 ให้มีการร้อยท่อสายสัญญาณต่าง ๆ หรือมีการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อป้องกันการตัด สายสัญญาณทำให้เกิดความเสียหาย หรือการดักรับข้อมูลโดยผู้ที่มิได้รับอนุญาต

5.3 สายสื่อสารต้องแยกกับสายไฟในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญาณ

5.4 ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

5.5 จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

5.6 ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ต้องปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

5.7 พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม

6. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

6.1 วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา และต้องมีการซ่อมบำรุงอย่างทันท่วงที ตาม ความสำคัญของระบบ

6.2 บันทึกประวัติการบำรุงรักษาและซ่อมบำรุงอุปกรณ์เข้าระบบทุกครั้ง เพื่อใช้ในการตรวจสอบหรือ

ในภายหลัง โดยมีรายละเอียดดังนี้ วันที่บำรุงรักษาและซ่อมบำรุง รายการอุปกรณ์ สถานะของอุปกรณ์ ปัญหาที่พบ และการแก้ไข ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุง

6.3 ถ้ามีการจัดจ้างหน่วยงานหรือผู้ให้บริการภายนอก เพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์ หน่วยงานที่

จัดจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการจ้าง กำหนดระยะเวลา ขอบเขตและการให้บริการอย่างชัดเจน

6.4 ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงานในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบหรือผู้รับผิดชอบการซ่อมบำรุงอุปกรณ์จะต้องอยู่ใน พื้นที่ทุกครั้ง

6.5 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างหรือผู้ให้บริการภายนอกที่เข้ามา บำรุงรักษาอุปกรณ์เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

7. การนำทรัพย์สินของหน่วยงานออกนอกพื้นที่ (Removal of Property)

7.1 หน่วยงานต้องมอบหมายเจ้าหน้าที่เทคโนโลยีสารสนเทศเป็น “ผู้ดูแลทรัพย์สิน” มีหน้าที่ควบคุมดูแลพัสดุหรือทรัพย์สินของหน่วยงานที่อยู่ในความครอบครองให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา โดยมิให้เกิดการสูญหาย และจัดทำ “ทะเบียนทรัพย์สิน” ของหน่วยงาน บันทึกการใช้งานผู้ใช้งาน สถานภาพและการเคลื่อนย้ายของทรัพย์สิน ทั้งนี้ ต้องตรวจสอบสถานภาพของทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เคลื่อนย้าย เช่น ได้รับ มอบทรัพย์สินเพิ่มเติม การตัดจำหน่าย การเปลี่ยนผู้ครอบครอง การยืม การโอน หรือการส่งซ่อม

7.2 ต้องขออนุญาตจากผู้จัดการฝ่ายของหน่วยงานและแจ้งให้ผู้ดูแลทรัพย์สินทราบ ก่อนนำอุปกรณ์หรือ ทรัพย์สินออกไปใช้งานภายนอกหน่วยงาน หรือนำไปซ่อมบำรุง

7.3 ต้องได้รับความเห็นชอบจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือหัวหน้าผู้รับผิดชอบ ก่อนนำ ทรัพย์สินคอมพิวเตอร์ส่งซ่อมภายนอกหน่วยงาน

7.4 การให้ยืมอุปกรณ์หรือทรัพย์สิน ผู้ดูแลทรัพย์สินจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมา ตามช่วงเวลาที่กำหนดและอยู่ในสภาพปกติ หรือไม่ต่างจากตอนที่ถูกยืม และต้องบันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน และบันทึกส่งคืน เพื่อเป็นหลักฐานป้องกันการสูญหาย

8. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off Premises)

8.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงาน ออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

8.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

8.3 เจ้าหน้าที่ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

9. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

9.1 การจำหน่ายทรัพย์สินคอมพิวเตอร์ อุปกรณ์เครือข่าย หน่วยงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ก่อนการจำหน่าย เพื่อให้มั่นใจว่าข้อมูลและซอฟต์แวร์ลิขสิทธิ์จะไม่สามารถนำกลับมาใช้ได้อีก (non-retrievable)

9.2 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ ต้องเสนอเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

9.3 ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัด โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

หมวด 2 การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access control)

1. วัตถุประสงค์

1.1 เพื่อให้ข้อมูลที่มีความสำคัญต่อหน่วยงาน ได้รับการจำแนกชั้นความลับอย่างเหมาะสมตามระดับ ความสำคัญของข้อมูล และเพื่อให้พนักงานที่เกี่ยวข้องรับรู้และสามารถนำข้อมูลแต่ละชั้นความลับไปใช้งานได้อย่างถูกต้องและเหมาะสม

1.2 เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาต เข้าถึงระบบเทคโนโลยีสารสนเทศและการ สื่อสารของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้ไม่ประสงค์ดีผ่านโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการ สื่อสารของหน่วยงานได้อย่างถูกต้อง

2. การกำหนดลำดับความสำคัญของข้อมูลและการใช้งานข้อมูล

2.1 หน่วยงานใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ โดยมีการแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือ ลำดับชั้นความลับของ ข้อมูลดังนี้

2.1.1 จัดแบ่งประเภทของข้อมูลออกเป็น

1) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลแผนงบประมาณ เป็นต้น

2) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลการขอใช้บริการ Helpdesk ข้อมูลการขอใช้รถยนต์ส่วนกลาง ข้อมูลการขอใช้ห้องประชุม เอกสารเผยแพร่บนเว็บไซต์ของหน่วยงาน เป็นต้น

2.1.2 การรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการของ เอกสารที่สำคัญ การเข้าถึงข้อมูลแต่ละประเภทตามรความลับของหน่วยงาน ดังต่อไปนี้

1) ลับมาก (Secret) มีความสำคัญต่อหน่วยงานในระดับสูงมาก หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อหน่วยงานอย่างมาก

2) ลับที่สุด (Confidential) มีความสำคัญต่อหน่วยงานในระดับสูง หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อหน่วยงานอย่างมีนัยยะสำคัญ

3) ใช้ภายในหน่วยงาน (Internal Use) เป็นข้อมูลที่อนุญาตให้ใช้ภายในหน่วยงาน หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อหน่วยงาน

4) สาธารณะ (Public) เป็นข้อมูลที่ใช้เผยแพร่สู่สาธารณะ การเปิดเผยข้อมูลประเภทนี้ไม่ส่งผลกระทบใดกับหน่วยงาน

2.1.3 การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ 1 ระดับชั้นสำหรับผู้บริหาร

ระดับที่ 2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

ระดับที่ 3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

2.1.4 กำหนดเวลาที่สามารถเข้าถึงข้อมูลได้

การกำหนดช่องทางในการเข้าถึงข้อมูล ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการ เข้าถึงที่กำหนดไว้นั้น จะต้องได้รับสิทธิจากหน่วยงาน โดยมีการกำหนดบัญชีชื่อผู้ใช้งานตามระดับชั้นการเข้าถึงให้เข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงได้ เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น

2.2 การใช้งานข้อมูล

2.2.1 มีมาตรการให้ผู้ใช้งานต้องใช้งานข้อมูลของหน่วยงานตามกฎระเบียบและคำแนะนำที่ หน่วยงานกำหนดไว้

2.2.2 ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้งานข้อมูลประเภทลับมาก และลับที่สุด(ต่อไปในเอกสารนี้เรียกว่า “ข้อมูลลับ”) เพื่อป้องกันไม่ให้ข้อมูลถูกเข้าถึงหรือถูกเปิดเผย โดยไม่ได้รับอนุญาต

2.2.3 ข้อมูลลับของหน่วยงานต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น (ตามหลักการ “Need to Know”)

2.2.4 ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลลับที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไปข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัสหรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือแอปพลิเคชันอย่างเหมาะสม

2.2.5 ข้อมูลใดที่ผู้ใช้งานพิจารณาว่าเป็นข้อมูลลับหรือมีจุดอ่อนด้านความมั่นคงปลอดภัยต้องได้รับการเข้ารหัส

2.2.6 ผู้ใช้งานควรเก็บรักษาสื่อบันทึกข้อมูลที่มีข้อมูลลับ ในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องวางสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน

2.2.7 ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่าย เอกสาร ฯลฯ ทันที

2.2.8 ผู้ใช้งานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

2.2.9 ผู้ใช้งานต้องไม่พูดคุยหรือใช้งานข้อมูลลับของหน่วยงานในพื้นที่สาธารณะ เช่น ลิฟต์ ร้านอาหาร ฯลฯ

3. กระบวนการในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ต้องมีการควบคุมการ เข้า - ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็น ผ่านเข้าใช้งานได้เท่านั้น

3.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของ ผู้ใช้งานระบบและหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ และ การสื่อสารรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ งานจะต้องได้รับอนุญาตจาก ผู้บริหารและผู้ดูแลระบบตามความจำเป็นในการใช้งาน

3.2.1 กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

1) อ่านอย่างเดียว

2) สร้างข้อมูล หรือนำเข้าข้อมูล

3) แก้ไขข้อมูล

4) ลบข้อมูล

5) อนุมัติ

6) ไม่มีสิทธิ

3.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และ ระบบข้อมูลได้

3.4 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

3.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกประวัติการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการ ตรวจสอบ หากมีปัญหาเกิดขึ้น

4. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

4.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบแก่ผู้ใช้งาน ในการขออนุญาตเข้าใช้ระบบงานนั้น จะต้องมีบันทึกขอสิทธิในการเข้าสู่ระบบและมีการลงนามอนุมัติผ่านระบบ โดยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

4.2 ผู้ดูแลระบบต้องกำหนดระยะเวลาการเชื่อมต่อเข้าสู่ระบบสารสนเทศ/แอปพลิเคชันที่มีความสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.3 เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่รับผิดชอบเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนด

สิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

4.4 ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่รับผิดชอบข้อมูลและระบบงาน ตามหน้าที่และส่วนงานที่เกี่ยวข้องและความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

4.5 ผู้ปฏิบัติงานที่เกี่ยวข้องกับงานพัฒนาระบบ จะต้องมีทักษะเฉพาะและสังกัดในหน่วยงานฝ่ายเทคโนโลยีสารสนเทศเท่านั้น เพื่อป้องกันความเสี่ยงในการเข้าถึง โดยขาดทักษะความเชี่ยวชาญ ขาดการควบคุมดูแลและกระทบต่อเสถียรภาพของระบบงานโดยรวม

5. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงผู้ที่ไม่ได้รับอนุญาต

5.1 สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้ใช้งาน

5.1.1 ฝ่ายเทคโนโลยีสารสนเทศ จัดให้มีการให้ความรู้เพื่อความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ และรู้เท่าทันต่อภัยคุกคามและผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง ผ่านทางช่องทางต่างๆ ที่สามารถเข้าถึงได้จากทุกที่ อย่างน้อยเดือนละ 1 ครั้ง

5.1.2 กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย-ไซเบอร์ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของหน่วยงาน

5.2 การลงทะเบียนพนักงานใหม่ของฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่าง เป็นทางการ สำหรับ การลงทะเบียนพนักงานใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกหรือเปลี่ยนแปลงสิทธิการใช้งาน

5.3 การลงทะเบียนผู้ใช้งาน (User Registration)

5.3.1 ผู้ดูแลระบบจัดทำระบบการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

5.3.2 ผู้ดูแลระบบต้องตรวจสอบบัญชีรายชื่อผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

5.3.3 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิในแต่ละภารกิจ

5.3.4 ผู้ดูแลระบบต้องชี้แจงและแจ้งผู้ใช้งานเป็นลายลักษณ์อักษร เพื่อให้ผู้ใช้งานทราบถึงสิทธิ หน้าที่รับผิดชอบ และมาตรการด้านความมั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศ

5.3.5 กำหนดให้มีการยกเลิก การอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้เมื่อได้รับแจ้งจากต้นสังกัดหรือเมื่อมีการเปลี่ยนแปลงตำแหน่ง ลาออกหรือสิ้นสุดการจ้าง

5.4 การบริหารจัดการสิทธิผู้ใช้งาน (User Management)

5.4.1 กำหนดระดับสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบและความจำเป็นใน การใช้งาน และทบทวนสิทธิอย่างสม่ำเสมอหรืออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งโอนย้าย ลาออก หรือสิ้นสุดการจ้าง เป็นต้น

5.4.2 ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศตามหน้าที่รับผิดชอบและจัดเก็บข้อมูลการกำหนดสิทธิให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

5.4.3 ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนดจะต้องได้รับการอนุมัติ เห็นชอบจากต้นสังกัดและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศจัดทำคำร้องเป็นลายลักษณ์อักษรโดยการให้สิทธิพิเศษดังกล่าว จะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษแล้วจะต้องระงับการใช้งานทันที

5.5 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (Password Management)

5.5.1 ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน ส่งมอบให้ผู้ใช้งานเป็น ความลับหรือทางจดหมายอิเล็กทรอนิกส์ (e-mail) เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันที

5.5.2 การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักขระ (digits) ประกอบด้วยตัวอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ

5.5.3 กำหนดให้การกรอกรหัสผิดพลาดได้ไม่เกิน 3 ครั้ง ระบบจะต้องล็อคสิทธิการเข้าถึงของ ผู้ใช้งาน โดยผู้ใช้งานจะต้องแจ้งความจำนงให้ผู้ดูแลระบบปลดล็อคหรือรีเซ็ตรหัสผ่านใหม่ หรือรอ 15 นาทีระบบจะปลดล็อคอัตโนมัติ

5.5.4 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ 90 วัน

5.5.5 ผู้ใช้งานต้องเก็บรักษารหัสผ่านไว้เป็นความลับห้ามเปิดเผย

5.5.6 Password เก็บประวัติห้ามซ้ำกันย้อนหลัง 4 ครั้ง รวมที่ใช้ในปัจจุบันเป็น 5 ครั้ง

5.6 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต ที่สามารถเข้าถึงระบบงานสำคัญ เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และ ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและผู้ดูแลระบบเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวน สิทธิ ดังกล่าวอย่างสม่ำเสมอ

5.7 ผู้บังคับบัญชาของผู้ใช้งานต้องรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศผ่านการแจ้งขอสิทธิ์ผ่านระบบและสอบทานสิทธิ์ประจำปี

5.8 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) ของพนักงาน

5.8.1 ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของพนักงานในการเข้าถึงระบบ เทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

5.8.2 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ซึ่งผู้ใช้งานที่มีสิทธิสูงสุด จะต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

1) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

2) ต้องควบคุมการใช้งานอย่างเข้มงวด กำหนดการใช้งานเฉพาะกรณีจำเป็นเกี่ยวข้องดังกล่าวเท่านั้น

3) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อได้รับแจ้งให้ดำเนินการจากผู้เกี่ยวข้องดังกล่าว

4) ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้เป็นระยะเวลานานควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

5.8.3 การตั้งชื่อ Users Login กำหนดให้เป็นชื่อภาษาอังกฤษตัวพิมพ์เล็กคั่นด้วย จุลภาค(.) ตามด้วย 2 ตัวอักษรแรกของนามสกุล ตัวอย่างเช่น cpl.it, pangolin.it

5.8.4 หากมีรายชื่อผู้ใช้ซ้ำกันในระบบให้กำหนดชื่อภาษาอังกฤษตัวพิมพ์เล็กคั่นด้วย จุลภาค(.) ตามด้วยตัวอักษรแรกของนามสกุลมากกว่า 2 อักษรได้ ตัวอย่างเช่น cpl.ita, pangolin.ita เป็นต้น

<u>ยกเว้นกรณี</u> ซอฟต์แวร์ที่มีข้อจำกัดด้านใบอนุญาตในการใช้งาน สามารถ กำหนดชื่อผู้ใช้งานตามความเหมาะสม โดยให้ขออนุมัติชื่อผู้ใช้งานเป็นกรณีไป

5.9 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

5.9.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

5.9.2 ผู้ดูแลข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของ ผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

5.9.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูล ในแต่ละชั้นความลับข้อมูล

5.9.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่ เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

5.9.5 ต้องกำหนดให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสม เช่น ทุก ๆ 3 เดือนหรือ ขึ้นอยู่กับความสำคัญขอข้อมูลที่ผู้ใช้ดูแลรับผิดชอบ

5.9.6 ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อ บันทึกข้อมูลก่อน เป็นต้น

5.10 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ ประมวลผลสารสนเทศ

5.10.1 การใช้งานรหัสผ่าน (Password Use)

1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้ง ห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

2) การกำหนดรหัสผ่าน (Password) ที่คาดเดาได้ยาก ซึ่งประกอบด้วย

- กำหนดให้มีความยาวไม่น้อยกว่า 8 ตัวอักษรประกอบด้วย อักษรภาษาอังกฤษตัวพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระ พิเศษ เช่น ; < > $ # เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสเดิมครั้งสุดท้าย และต้องไม่ซ้ำกับ 4 ครั้งที่ผ่านมา
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งานเช่น ชื่อ นามสกุล วันเกิดหรือ หมายเลขโทรศัพท์ เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม

3) ไม่ใช้โปรแกรมคอมพิวเตอร์ในการจำรหัสผ่านอัตโนมัติสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

4) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยผู้อื่น

5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก 90 วัน หรือทุกครั้งที่มีการแจ้งเตือน ให้เปลี่ยนรหัสผ่าน

5.10.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน มีการกำหนดมาตรการป้องกันทรัพย์สินของหน่วยงาน และควบคุมไม่ให้มีการวางทรัพย์สินสารสนเทศที่สำคัญในสถานที่ที่ไม่ปลอดภัยโดยมีแนว ปฏิบัติดังนี้

1) ผู้ดูแลระบบหรือผู้รับผิดชอบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศและการเข้าใช้งานคอมพิวเตอร์ทันทีเมื่อเสร็จสิ้นการใช้งานหรือพักการใช้งานชั่วคราว(Logout) เพื่อ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2) ผู้ใช้งานจะต้องป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงาน ตลอดเวลาเพื่อไม่ให้เกิดความเสียหาย สูญหาย หรือมีผู้ไม่ประสงค์ดีเข้าถึงระบบและอุปกรณ์ โดยไม่ได้รับอนุญาต

3) กำหนดค่าให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา15 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

4) กำหนดรหัสผ่านสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ และต้องล็อคอุปกรณ์และ เครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

5) การใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์ เมื่อเสร็จสิ้นแล้วจะต้องทำการ log off ทุกครั้ง

6) มีการควบคุมการเข้า-ออกพื้นที่โดยผู้ไม่มีส่วนเกี่ยวข้องต้องได้รับอนุญาตก่อนเข้าถึงพื้นที่ปฏิบัติงาน

5.10.3 หน่วยงานต้องกำหนดแนวปฏิบัติ เพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ (Clear Desk and Clear Screen Policy) โดยมีแนวปฏิบัติดังนี้

1) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันที (Logout) ที่เสร็จสิ้นการใช้งานหรือเมื่อ มีเหตุให้ว่างเว้นจากการใช้งาน

2) ผู้ใช้งานต้องกำหนดให้เครื่องคอมพิวเตอร์ล็อคหน้าจอขณะที่ไม่ได้ใช้งานภายในระยะเวลา 15 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

3) ผู้ใช้งานต้องกำหนดรหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

4) กรณีข้อมูลสำคัญที่บันทึกไว้ในสื่อบันทึกข้อมูลเคลื่อนย้ายได้ เช่น ฮาร์ดดิสก์ เมื่อไม่ใช้งานต้องจัดเก็บไว้ในที่ปลอดภัย ไม่วางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

5) ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

6) การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ เจ้าของข้อมูลต้องปฏิบัติตาม แนวทางการทำลายดังนี้

ประเภทสื่อบันทึกข้อมูล

ประเภทที่ 1

- แฟลชไดรฟ์ (Flash Drive)
- ฮาร์ดดิสก์ (Hard disk)
- ฮาร์ดดิสก์พกพา (External Hard disk)

แนวทางการทำลาย

ทำลายข้อมูลตามแนวทางของ DOD 5220. 22- M ของกระทรวงกลาโหม สหรัฐอเมริกาซึ่งเป็นมาตรฐานการทำลาย ข้อมูลโดยการเขียนทับข้อมูลเดิม หลายๆ รอบ

ประเภทที่ 2

- แผ่นซีดี / ดีวีดี (CD/DVD)

แนวทางการทำลาย

- ใช้วิธีการตัด ทุบ ทำให้สิ้นสภาพการใช้งาน

7) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 โดยการรับ-ส่งข้อมูลสำคัญ หรือข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

8) มีการจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก และต้องมีผู้รับผิดชอบคอยควบคุมดูแลตลอดระยะเวลาการส่งมอบ ไม่ปล่อยให้บุคคลภายนอก อยู่ตามลำพังในพื้นที่ปฏิบัติงาน

5.10.4 การใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัยและไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน กำหนดแนวทางปฏิบัติ สำหรับผู้ใช้งาน ดังนี้

1) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อค หรือ เกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

2) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของ หน่วยงานหรือเป็นของบุคคลภายนอก

3) การกระทำใด ๆ ที่เกิดจากการใช้บัญชีชื่อผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตามให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

4) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจาก ผู้บริหารระดับสูงสุดของหน่วยงาน

5) ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษาใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้นยกเว้นในกรณีที่หน่วยงานต้องการ ตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับหน่วยงาน ซึ่งหน่วยงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้อง แจ้งให้ผู้ใช้งานทราบ

6) ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความรูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือ กระทบต่อ ภารกิจของหน่วยงาน

7) ห้ามใช้ระบบสารสนเทศของหน่วยงาน เพื่อก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของ หน่วยงาน

8) ห้ามใช้ระบบสารสนเทศของหน่วยงานเพื่อประโยชน์ทางการค้า

9) ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายของหน่วยงานโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

5.11 เป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของหน่วยงาน และการปรับปรุงเพื่อให้ สอดคล้องกับกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติ ดังนี้

5.11.1 การควบคุมการเข้าถึงสารสนเทศ

1) ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

2) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

5.11.2 ข้อกำหนดการใช้งานตามภารกิจ เพื่อให้การเข้าถึงและใช้งานสารสนเทศสอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย จึงจำแนกกลุ่มผู้ใช้งานและ กำหนดให้มีการแบ่งกลุ่มตามสิทธิและภารกิจ ดังนี้

- กลุ่มผู้บริหาร กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายในการกำกับดูแล เช่น สิทธิการอนุมัติ สิทธิการเข้าถึงรายงานสรุปผล

- กลุ่มของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดสิทธิการเข้าถึง ข้อมูลได้ตาม ภารกิจที่ได้รับมอบหมายจากผู้บริหาร เช่น สิทธิในการกำหนดสิทธิการ เข้าใช้งาน ของผู้ใช้งานในแต่ละระบบตามที่ผู้บริหารมอบหมาย

- กลุ่มผู้ใช้งาน กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายจาก ผู้บริหารของหน่วยงานภายใน เช่น สิทธิการเพิ่ม/แก้ไข/ลบข้อมูล ที่อยู่ในความรับผิดชอบ

- กลุ่มพนักงานของหน่วยงาน กำหนดสิทธิให้สามารถเข้าถึงข้อมูลทั่วไป เช่น สิทธิการ อ่านอย่างเดียว

- กลุ่มที่ปรึกษาจากภายนอกหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับหน่วยงาน กำหนดสิทธิ เฉพาะกิจตามความจำเป็นที่ต้องเข้าถึงข้อมูล

- ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว (Guest) ไม่มีสิทธิในการเข้าถึง

6. การควบคุมการเข้าถึงเครือข่าย (network access control)

6.1 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และ การสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซน ภายนอก (External Zone) เป็นต้น เพื่อควบคุมและป้องกันการบุกรุกได้ อย่างเป็นระบบ

6.2 การเข้าสู่ระบบเครือข่ายภายในของหน่วยงาน โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็น ลายลักษณ์อักษรจากหัวหน้าหน่วยงานก่อนที่จะสามารถใช้งานได้ในทุกกรณี

6.3 การเข้าถึงระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศภายในของหน่วยงาน ต้องดำเนินการโดยใช้ อุปกรณ์ที่หน่วยงานเป็นผู้จัดหา หรืออุปกรณ์ที่ได้รับอนุญาตซึ่งผ่านการลงทะเบียน

6.4 อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายภายในของหน่วยงาน ต้องได้รับการพิสูจน์ตัวตน ด้วยวิธีการที่ เหมาะสม ได้แก่ การตรวจสอบความถูกต้องของ Two Factor Authentication การตรวจสอบความถูกต้องของ Media Access Control Address (MAC) การตรวจสอบความ ถูกต้องของรหัสประจำเครื่อง หรือการตรวจสอบ Digital Certificate ของอุปกรณ์ เป็นต้น

6.5 ผู้ดูแลระบบต้องควบคุมพอร์ตของอุปกรณ์ต่าง ๆ ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยมีรายละเอียดดังนี้

6.5.1 พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Diagnostic และ Configuration Port) ต้องถูกจำกัดให้สามารถใช้งานได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น

6.5.2 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ต้องดำเนินการผ่านโพรโทคอลที่มีความมั่นคงปลอดภัย เช่น Secure Shell (SSH) หรือผ่านระบบเครือข่ายแบบ Out-of-band เท่านั้น

6.5.3 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบจากระยะไกลผ่านเครือข่าย ภายนอกต้องได้รับการพิสูจน์ตัวตนของผู้ใช้งานด้วยวิธีการตรวจสอบตั้งแต่ 2 ประเภท ขึ้นไป (two factors authentication) และใช้ช่องทางการเชื่อมต่อที่มั่นคงปลอดภัย

6.5.4 พอร์ตที่ไม่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินภารกิจต้องถูกระงับการใช้งาน

6.6 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

6.7 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

6.8 ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

6.9 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของ ระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละ 1 ครั้ง นอกจากนี้การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต้องแจ้ง บุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

6.10 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

6.11 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งาน ระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบ เครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่ เกี่ยวข้อง

6.12 การเข้าสู่ระบบสารสนเทศเครือข่ายภายในของหน่วยงาน จากผู้ใช้ทั้งที่อยู่ภายนอกและภายใน หน่วยงาน โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

6.13 IP Address ภายในของระบบสารสนเทศเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถล่วงรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของระบบเทคโนโลยีสารสนเทศและ การสื่อสารของ หน่วยงานได้โดยง่าย

6.14 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของ เครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

6.15 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บริหาร และผู้ดูแลระบบก่อนและต้องจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6.16 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

7. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความ รับผิดชอบในการใช้ระบบปฏิบัติการ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและ ข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ ดังนี้

7.1 ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานด้วยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัยดังนี้

1) ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ ระบบจะเสร็จสมบูรณ์

2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

3) จำกัดการป้อนรหัสผ่าน โดยป้อนรหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง

4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้าง ความเสียหายให้กับระบบได้

7.2 การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยกำหนดให้ผู้ใช้งานเลือกใช้ขั้นตอนในการยืนยันตัวตนที่เหมาะสม มีแนวปฏิบัติ ดังนี้

1) ผู้ใช้งานต้องระบุบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (Password) สำหรับยืนยัน ตัวตนเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศของหน่วยงาน

2) การใช้งานบัญชีรายชื่อผู้ใช้งานแบบกลุ่ม ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงาน หรือด้านเทคนิค

7.3 การบริหารจัดการรหัสผ่าน (Password Management System) ต้องมีระบบบริหารจัดการ รหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนด รหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านของผู้ใช้งานที่ถูก กำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

7.4 ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) สำหรับ โปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของ หน่วยงานที่ ได้กำหนดไว้ ให้ดำเนินการดังนี้

1) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุม ในการอนุญาตให้ใช้งานโปรแกรมเป็นรายครั้งไป

2) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาต และยังไม่ผ่านการตรวจสอบ

3) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์หรือละเมิด กฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

4) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

5) ต้องเก็บบันทึกการใช้ของงานโปรแกรมอรรถประโยชน์

6) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

7.5 กำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (Session Time-Out) กำหนดระยะเวลายุติการใช้งานระบบ เมื่อว่างเว้นจากการใช้งาน ให้พิจารณาเป็นรายระบบตามความเหมาะสมและจำเป็น เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต และต้องพิสูจน์ตัวตนเพื่อเข้าใช้งาน ระบบอีกครั้ง หลังจากระบบได้ตัดการใช้งานนั้นไปแล้ว

7.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือ แอปพลิเคชันที่มี ความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา 2 ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หากต้องการเชื่อมต่อใหม่ ต้องพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบอีกครั้งยกเว้นในระบบที่มีความ จำเป็นให้มีระยะเวลาที่นานขึ้น ให้พิจารณาเป็นรายระบบตามความเหมาะสมจำเป็น

8. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

8.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์ หรือแอปพลิเคชัน ดังนี้

8.1.1 ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามหน้าที่รับผิดชอบ โดยมีผู้บังคับบัญชาเป็นผู้อนุมัติการให้สิทธินั้น และต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ หรือ อย่างน้อยปี ละ 1 ครั้ง

8.1.2 ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) ระยะเวลาตามความเหมาะสมกับระบบงาน

8.1.3 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

1) กำหนดสิทธิให้กับผู้ใช้งานระบบโดยการกำหนดบัญชีชื่อผู้ใช้และรหัสผ่าน เพื่อใช้ใน การพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น

2) การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น และ ต้องมี การควบคุมการใช้งานสารสนเทศในระบบสารสนเทศตามหน้าที่รับผิดชอบของผู้ใช้งาน

3) การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็น ความลับของหน่วยงาน ต้องมีการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล

4) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใด ๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบ หลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้น ๆ ซึ่งหากหน่วยงาน ภายนอกดำเนินการใด ๆ ที่มีผลกระทบต่อระบบ ผู้ดูแลระบบจะต้องเป็นผู้รับผิดชอบ

8.1.4 ต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ พฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ

8.2 การควบคุมระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

8.2.1 ต้องแยกระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงออกจากระบบอื่น ๆ ให้ทำงานอยู่บนเครื่องแม่ข่าย (server) โดยไม่ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้ง ห้องควบคุมเครื่องแม่ข่ายที่มีสภาพแวดล้อมเหมาะสม

8.2.2 จัดพื้นที่ควบคุมพิเศษ (ห้องควบคุมเครื่องแม่ข่าย) เพื่อควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้าออกพื้นที่ควบคุมพิเศษ หรือ ทรัพยากรอื่นใดเพื่อป้องกันการหยุดชะงักการทำงานของระบบ

8.2.3 กำหนดค่าที่ไฟร์วอลล์ เพื่อควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก

8.2.4 มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

8.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ การปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

9. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

9.1 ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

9.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานต่อหัวหน้าหน่วยงานโดย ทันที

9.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet, ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

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

9.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

9.6 การเข้าถึง System Utilities ที่ปฏิบัติการด้วยสิทธิพิเศษในระดับสูง ซึ่งทำให้สามารถเลี่ยงผ่านกลไก การควบคุมระบบ/แอปพลิเคชันต่าง ๆ ได้นั้น ต้องถูกจำกัดให้เฉพาะผู้ใช้งาน หรือผู้ดูแลระบบที่มีความจำเป็นต้อง ใช้งานเป็นประจำเท่านั้น สำหรับการใช้งานและการเข้าถึง System Utilities เหล่านั้น โดยบุคคลอื่น ให้พิจารณา อนุมัติในลักษณะชั่วคราวในทุกกรณี

9.7 System Utilities ดังกล่าวข้างต้นต้องถูกแยกออกจากแอปพลิเคชัน และซอฟต์แวร์อื่น ๆ เพื่อ ประโยชน์ในการจำกัดการเข้าถึง ให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

9.8 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

9.9 ควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบ ดังนี้

9.9.1 ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

9.9.2 ผู้ดูแลระบบที่ได้รับการอบรมแล้วหรือมีความชำนาญเท่านั้นที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

9.9.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ ต้องมีการขออนุมัติจากหัวหน้า หน่วยงาน ก่อนดำเนินการ

9.9.4 ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์ แม่ข่ายที่ให้บริการ

9.9.5 กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ใน สถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

9.9.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่ กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

9.9.7 วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อน ดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

9.9.8 จัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้ อย่างปลอดภัยเพื่ออ้างอิง

9.10 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง ระบบปฏิบัติการ

9.10.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

9.10.2 วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

10. การบริหารจัดการการบันทึกและตรวจสอบ

10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ได้แก่ การบันทึกการทำงานขอระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึก รายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ ระบบ บันทึกการ ใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึก ดังกล่าวไว้อย่างน้อย 3 เดือน โดยมี รายละเอียดการบันทึกพฤติกรรมการใช้งาน (logs) การเข้าถึงระบบสารสนเทศ ดังนี้

1) ข้อมูลบัญชีชื่อผู้ใช้งาน
2) ข้อมูลวัน/เวลาที่เข้าถึงระบบ
3) ข้อมูลวัน/เวลาที่ออกจากระบบ
4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

5) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

7) ข้อมูลการเปลี่ยนการกำหนดค่า (Configuration) ของระบบ

8) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)

9) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

10) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง

11) ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้

12) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

13) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

10.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

10.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้ เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

11. การควบคุมการเข้าใช้งานระบบจากภายนอก

หน่วยงานต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

11.1 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของหน่วยงาน การควบคุม บุคคลที่เข้าสู่ระบบของหน่วยงานจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจาก มาตรฐานการเข้าสู่ระบบภายใน

11.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้า สู่ระบบและข้อมูลอย่างเคร่งครัด

11.3 ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

11.4 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมี การร้องขอที่จำเป็นเท่านั้น

12. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

12.1 ผู้ใช้งานระบบสารสนเทศ ต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

12.1.1 การแสดงตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงบัญชีชื่อผู้ใช้งาน(Username)

12.1.2 การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่า เป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB Token ที่มี เทคโนโลยี Public Key Infrastructure: PKI ด้วยการลงลายมือชื่อดิจิทัล (Digital Signature) และการ เข้ารหัสลับ (Encryption) รูปแบบของใบรับรองอิเล็กทรอนิกส์ เป็นต้น

12.2 การเข้าสู่ระบบสารสนเทศของหน่วยงานนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี

12.3 การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

12.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อ พิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

13. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

13.1 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ที่ จะมีการปฏิบัติงานจากภายนอกหน่วยงาน และระบบงานต่างๆ ภายในหน่วยงาน

13.2 การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล ด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับ อนุญาตจากหัวหน้าหน่วยงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

13.3 การเข้าสู่ระบบระบบสารสนเทศในหน่วยงานจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยบัญชีชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

13.4 ผู้ได้รับอนุญาตเท่านั้นจึงจะสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงาน โดยไม่ให้ สมาชิก ภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

13.5 ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวัง สม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

13.6 ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงาน แก่ ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อหัวหน้า หน่วยงาน

13.7 ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ 1 ครั้ง

หมวด 3 การใช้งานเครื่องคอมพิวเตอร์ (Use of Personal Computer)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์นี้ ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานได้รับ ทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และผู้ใช้งานควรทำความเข้าใจ และปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของหน่วยงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้พนักงานใช้งาน เป็นทรัพย์สินของหน่วยงาน เพื่อใช้ในการปฏิบัติงาน ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ เพื่อประโยชน์ของ หน่วยงาน

2.2 เครื่องคอมพิวเตอร์ของหน่วยงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขทรัพย์สิน โดยอยู่ใน ความรับผิดชอบของหน่วยงาน ผู้ใช้งานต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลทรัพย์สินของหน่วยงาน จะต้องระบุว่าผู้ใดเป็นผู้ ครอบครองเครื่องคอมพิวเตอร์นั้น

2.3 เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์ รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) เท่านั้น

2.4 โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานซื้อลิขสิทธิ์มาอย่าง ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือ แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.5 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรือ อุปกรณ์คอมพิวเตอร์อื่นใด เพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

2.6 การเคลื่อนย้ายเครื่องคอมพิวเตอร์ออกนอกพื้นที่ปฏิบัติงานของหน่วยงาน จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษร โดยแจ้งเข้าระบบ Helpdesk หัวหน้าหน่วยงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศอนุมัติ และแจ้งให้ผู้ดูแลทรัพย์สินทราบก่อนนำออกนอกสถานที่

2.7 การนำเครื่องคอมพิวเตอร์ของหน่วยงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจากเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือหัวหน้างานมอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อม ภายนอกต้องได้รับการอนุมัติ จากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือมอบหมายให้หัวหน้าส่วนงานซ่อม โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับ ทางฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

2.8 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบหาไวรัส โดยโปรแกรมป้องกันไวรัส

2.9 ไม่ควรเก็บข้อมูลส่วนบุคคลและข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ท่านใช้งานอยู่ ยกตัวอย่าง ข้อมูลส่วนบุคคล เช่น รูปภาพบัตรประชาชน หรือ ภาพถ่ายส่วนตัว

2.10 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของหน่วยงาน

2.11 ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยหลีกเลี่ยงการวางอาหารหรือเครื่องดื่มบริเวณเครื่องคอมพิวเตอร์ และไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

3. การควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้งานต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

3.2 ผู้ใช้งานควรกำหนดรหัสผ่านที่มีคุณภาพตามคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

3.3 ฝ่ายเทคโนโลยีสารสนเทศต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 15 นาที และต้องใส่รหัสผ่าน ให้ถูกต้องเมื่อต้องการใช้งาน

3.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.5 ผู้ใช้ต้องทำการลงบันทึกออก (Logout) จากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็น เวลานาน

4. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

4.1 ผู้ใช้งานต้องให้ความร่วมมือในการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และป้องกันการโจมตีจากภัยคุกคาม

4.2 ผู้ดูแลระบบสารสนเทศมีหน้าที่รับผิดชอบในการติดตั้ง ตรวจสอบการติดตั้ง โปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ภายในหน่วยงานที่เชื่อมต่อกับเครือข่ายอินเตอร์เน็ต

4.3 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ ส่วนบุคคล และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อน นำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

4.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

4.5 ผู้ใช้งานต้องตรวจสอบว่าข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

5. การสำรองข้อมูลและการกู้คืน

5.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลในการทำงานจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกที่ บริษัทจัดไว้ให้และสื่อบันทึกอื่น ๆ ตามความเหมาะสม เพื่อป้องกันการสูญหายของข้อมูล

5.2 เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ใน สถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

หมวด 4 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงาน ภายนอกหน่วยงาน และเป็นการป้องกันทรัพยากรและข้อมูลที่มีค่าของหน่วยงานให้เกิดความปลอดภัย ผู้ใช้งาน จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงในการใช้งาน เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้บุคลากรใช้งาน เป็นทรัพย์สินของหน่วยงานเพื่อใช้ ในการปฏิบัติงาน ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพ เพื่อประโยชน์ของหน่วยงาน

2.2 เครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขทรัพย์สิน โดยอยู่ใน ความรับผิดชอบของหน่วยงาน ผู้ใช้งานต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลทรัพย์สินของหน่วยงาน จะต้องระบุว่าผู้ใดเป็นผู้ครอบครองหรือนำไปใช้งาน

2.3 เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและ ระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์ รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพา เท่านั้น

2.4 โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานซื้อลิขสิทธิ์มาอย่าง ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่อง คอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.5 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบพกพา ของหน่วยงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใด เพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

2.6 การนำเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจาก เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือหัวหน้างานที่มอบหมายให้ปฏิบัติหน้าที่ตรวจสอบงานซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากหัวหน้าหน่วยงาน โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางหน่วยงานเท่านั้น

2.7 การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ใส่ในกระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาให้เรียบร้อย เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน และการหลงลืมอุปกรณ์

2.8 กรณีที่ต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้นโดยเด็ดขาด

2.9 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Subcomponent) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่ และควรรักษาสภาพคอมพิวเตอร์ให้มีสภาพพร้อมใช้งานตลอดเวลา

2.10 ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมี ประสิทธิภาพ

2.11 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

2.12 ผู้ใช้งานต้องระมัดระวังในการเคลื่อนย้าย ให้รักษาเสมือนเป็นทรัพย์สินของตนเอง

2.13 ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์และฝาพับโน๊ตบุ๊ค และก่อนเปิดให้นำมือจับฐานก่อนแล้วจับกึ่งกลางฝาพับเพื่อเปิดขึ้น

2.14 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

3. ความปลอดภัยทางด้านกายภาพ

3.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ดังนั้นควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่ วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

3.3 ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

3.4 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

3.5 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน

3.6 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

3.7 ไม่ควรเสียบสายชาร์จตลอดระยะเวลาการใช้งานเนื่องจากจะทำให้แบตเตอรี่เสื่อมเร็ว เมื่อชาร์ท แบตเตอรี่เต็มแล้ว ควรถอดสายชาร์จออก

4. การควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ฝ่ายเทคโนโลยีสารสนเทศต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 15 นาที และต้องใส่รหัสผ่าน ให้ถูกต้องเมื่อต้องการใช้งาน

4.2 หากวางเครื่องคอมพิวเตอร์แบบพกพาไว้นอกสถานที่ปฏิบัติงาน ควรล็อคหน้าจอด้วยตัวเองทุกครั้ง (Logoff) เมื่อไม่ได้อยู่ที่หน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

4.3 ผู้ใช้งานต้องไม่อนุญาตให้บุคคลภายนอกที่ไม่มีความเกี่ยวข้อง ใช้งานเครื่องคอมพิวเตอร์แบบพกพา และไม่บอกรหัสผ่านการล็อคหน้าจอให้แก่ผู้อื่น

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัย คุกคาม ต่าง ๆ

5.2 ผู้ดูแลระบบสารสนเทศของหน่วยงาน มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ของหน่วยงานเป็นโปรแกรมพื้นฐาน

5.3 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อน นำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

5.5 หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware)ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่ พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และต้องรีบแจ้งผู้ดูแลระบบสารสนเทศของหน่วยงานโดยเร็ว

6. การสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกที่บริษัทจัดไว้ให้และบันทึกอื่น ๆ ตามความเหมาะสม เพื่อป้องกันการสูญหายของข้อมูล หรือควรจัดเก็บข้อมูลไว้บนคลาวด์

6.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อ การ รั่วไหลของข้อมูลแล

ทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

6.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

หมวด 5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third party access control)

1. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูก แก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เพื่อให้การควบคุมหน่วยงาน ภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานเป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก

2. แนวทางปฏิบัติ

2.1 ต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

2.2.1 บุคคลภายนอกที่ต้องการสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้าหน่วยงาน

2.2.2 จัดทำเอกสารหรือแจ้งเข้าระบบ Helpdesk เพื่อขอใช้งาน เพื่อระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

1) เหตุผลในการขอใช้
2) ระยะเวลาในการใช้
3) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
4) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
5) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

2.2.3 หน่วยงานภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหรือภายนอกหน่วยงาน จำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้ สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2.2.4 หน่วยงาน ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของ หน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

2.2.5 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

2.2.6 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะ ให้บริการ (Availability)

2.2.7 หน่วยงานมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจว่าหน่วยงานสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.2.8 ควรดำเนินการให้ผู้ให้บริการภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และ เอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของ ผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

2.3 การพัฒนาซอฟต์แวร์

2.3.1 ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

2.3.2 กำหนดให้มีสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับ โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

2.3.3 กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ก่อนการติดตั้ง

2.3.4 การทดสอบซอฟต์แวร์ ห้ามทดสอบบนระบบและฐานข้อมูลที่ใช้งาน ต้องสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

2.4 มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

2.4.1 ผู้ให้บริการภายนอกที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของหน่วยงาน จะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์ อักษร เพื่อขออนุมัติจากหัวหน้าหน่วยงาน

2.4.2 ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก ที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

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

2.4.4 การอนุญาตให้ผู้ให้บริการภายนอกเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลทิ้งไว้โดยไม่จำเป็นช่องทางดังกล่าว ต้องมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติ จากหัวหน้าหน่วยงานก่อนทุกครั้ง

2.5 มาตรการควบคุมช่องโหว่ทางเทคนิค

2.5.1 การบริหารจัดการช่องโหว่ของระบบ ควรมีการบันทึกดังต่อไปนี้

1) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

2) สถานที่ที่ติดตั้ง

3) เครื่องแม่ข่ายที่ติดตั้ง

4) ผู้ผลิตซอฟต์แวร์

5) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

2.5.2 กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

2.5.3 กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

1) มีการเฝ้าระวังและติดตามประเมินความเสี่ยง สำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงาน เพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

2) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน

3) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยง เมื่อได้รับแจ้งหรือทราบเกี่ยวกับ ช่องโหว่นั้น

2.5.4 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

หมวด 6 การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
(Use of the Internet and Social Network)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์ อย่างปลอดภัย และเป็นการป้องกันไม่ให้เกิดการละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันก่อให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของหน่วยงานถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น ห้าม ผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขอ อนุญาตจากหัวหน้าหน่วยงาน เป็นลายลักษณ์อักษรผ่านระบบ Helpdesk แล้ว

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

2.3 การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการตรวจสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

2.4 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของหน่วยงานนอกเหนือจากเพื่อประโยชน์ของทางราชการ หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เว้นแต่เป็นการดำเนินงานตามภารกิจของหน่วยงาน

2.5 ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของ เครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน

2.6 ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน

2.7 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน ที่ยังไม่ได้ประกาศอย่างเป็น ทางการผ่านอินเทอร์เน็ต

2.8 ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอัน ลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.9 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด อันจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.10 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.11 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือFixes ต่าง ๆ จากผู้ขายต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.12 การใช้งานเว็บบอร์ด (Web Board) ของหน่วยงาน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

2.13 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสีย ต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

2.14 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

3. แนวทางปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

3.1 หน่วยงานต้องกำหนดแนวปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์ในเวลาราชการ เพื่อให้เกิดการ ใช้งานในเชิงสร้างสรรค์และเป็นประโยชน์ต่อการดำเนินงาน เช่น ใช้เพื่อการติดต่อสื่อสาร เพื่อการประชาสัมพันธ์ เป็นต้น

3.2 อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

3.3 หากต้องการใช้งานเครือข่ายสังคมออนไลน์ในลักษณะอื่นใดนอกเหนือจากที่หน่วยงานกำหนด ให้ขอ อนุญาตจากหัวหน้าหน่วยงานก่อนใช้งาน

3.4 ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของหน่วยงาน

3.5 ผู้ใช้งานพึงตระหนักว่าข้อความหรือความเห็นที่เผยแพร่บนเครือข่ายสังคมออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ ข้อความที่ยั่วยุ ให้ร้าย ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

3.6 ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่ มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนาม บัญชีชื่อผู้ใช้ ส่วนตัว แต่อาจส่งผลกระทบกับหน่วยงานได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์

3.7 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อหน่วยงาน ผู้ใช้งานต้องแจ้ง ต่อหัวหน้าหน่วยงานโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

3.8 ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความ ของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

หมวด 7 การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์
(Use of Electronic Mail and Cloud Service)

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์ผ่านระบบเครือข่ายของหน่วยงาน ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์และ บริการคลาวด์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบสารสนเทศวางไว้ ไม่ ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำ ของผู้ดูแลระบบสารสนเทศอย่างเคร่งครัด อันจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์ผ่าน ระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้งาน

2.1 เจ้าหน้าที่เทคโนโลยีสารสนเทศจะทำการเปลี่ยนรหัสผ่านใหม่ทุกครั้งที่มีพนักงานลาออก

โดยรหัสผ่านที่เปลี่ยนต้องเป็นรหัสผ่านที่ไม่เคยใช้มา ก่อน และเป็นรหัสผ่านที่คาดเดาได้ยากตาม หลักเกณฑ์การกำหนดรหัสผ่านที่ดี

2.2 ผู้ใช้งานต้องไม่เปิดหน้าจอระบบจดหมายอิเล็กทรอนิกส์ทิ้งเอาไว้ ขณะที่ไม่ได้อยู่หน้าจอ

2.3 ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงานหรือ ละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และ ไม่แสวงหา ประโยชน์หรือ อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

2.4 ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของแล้วเท่านั้น และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบ ต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.5 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของหน่วยงาน เพื่อการติดต่อสื่อสารในนามของของหน่วยงานเท่านั้น

2.7 ผู้ใช้ต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด ด้วยโปรแกรมป้องกันไวรัส เป็นการป้องกันการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

2.8 ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก หรือไม่น่าไว้ใจ

2.9 ผู้ใช้งานต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์ และใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง และระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป รวมทั้งจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

2.10 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.11 ผู้ใช้งานควรตรวจสอบกล่องเก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรลบ จดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

2.12 ผู้ใช้งานควรทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่สำคัญตามความจำเป็นอย่างสม่ำเสมอ

2.13 ข้อควรระวัง ผู้ใช้งานไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่อง คอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

2.14 ผู้ใช้ไม่ควรใช้งานจดหมายอิเล็กทรอนิกส์บนเครื่องคอมพิวเตอร์สาธารณะ เพื่อความปลอดภัยของข้อมูลและบัญชีผู้ใช้งาน

3. แนวทางแนวทางปฏิบัติในการใช้งานบริการคลาวด์

3.1 ผู้ใช้งานควรทำความเข้าใจบริการคลาวด์ของบริษัท (Office 365) ที่ช่วยสนับสนุนการปฏิบัติงานให้มีประสิทธิภาพ

3.2 ผู้ใช้งานไม่ควรให้บุคคลอื่นที่ไม่ใช่พนักงานของบริษัทร่วมใช้งานบริการคลาวด์เพื่อประโยชน์ส่วนตัว

3.3 ไม่อนุญาตให้ผู้ใช้งานเก็บไฟล์ส่วนตัวที่ไม่เกี่ยวข้องกับงาน และลบไฟล์ที่ไม่ได้ใช้งานแล้ว

3.4 ผู้ใช้งานไม่ควรเก็บข้อมูลที่ละเมิดลิขสิทธิ์ ขัดต่อกฎหมายและศีลธรรมไว้บนบริการคลาวด์

3.5 ผู้ใช้ไม่ควรเปิดใช้งานบริการคลาวด์ทิ้งไว้ โดยไม่ได้อยู่ที่หน้าจอ เพื่อป้องกันข้อมูลรั่วไหล

3.6 ผู้ใช้ไม่ควรใช้งานบริการคลาวด์บนเครื่องคอมพิวเตอร์สาธารณะ เพื่อความปลอดภัยของข้อมูลและบัญชีผู้ใช้งาน

หมวด 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุม ป้องกัน และการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของหน่วยงาน เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของหน่วยงาน

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแล ระบบ ของหน่วยงาน และต้องได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงาน

2.2 ผู้ดูแลระบบของหน่วยงาน กำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่และความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับ อนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สายของหน่วยงาน

2.4 ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access Point: AP) ให้ เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตี สามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

2.5 ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไป ภายนอกหรือไม่ ทั้งนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลด การรั่วไหลของสัญญาณได้ดีขึ้น

2.6 ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

2.7 ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้ โดยง่าย

2.8 ผู้ดูแลระบบต้องกำหนดค่าใช้มาตรฐานความปลอดภัยแบบ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ เพื่อให้ยากต่อการดักจับ ช่วยให้ปลอดภัยมากขึ้น

2.9 ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address ร่วมกับบัญชีชื่อผู้ใช้งาน (username) และ รหัสผ่าน (password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่ มี MAC Address บัญชีชื่อผู้ใช้งาน และรหัสผ่านตามที่กำหนดไว้เท่านั้น ในการเชื่อมต่อกับเครือข่ายไร้สายตาม SSID ที่กำหนดไว้ สำหรับบุคคลภายนอก กำหนดให้ใช้งานเครือข่ายไร้สายโดยไม่ควบคุม MAC Address แต่ให้ใช้ งานได้ตาม SSID ที่ผู้ดูแลระบบกำหนดแยกเฉพาะสำหรับบุคคลภายนอกเท่านั้น

2.10 ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

2.11 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สาย ติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

2.12 ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

หมวด 9 การใช้ข้อมูลร่วมกัน

(Information Sharing)

1. วัตถุประสงค์

เพื่อกำหนดขั้นตอนในการใช้ข้อมูลร่วมกันเกี่ยวกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์และมาตรการบรรเทาผลกระทบที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัย คุกคามดังกล่าวกับบุคคลที่อาจได้รับผลกระทบ เพื่อให้สามารถกำหนดเป็นมาตรการป้องกันที่จำเป็นได้

2. แนวทางปฏิบัติในการใช้ข้อมูลร่วมกัน

2.1 กำหนดขอบเขตและระดับความลับของข้อมูล โดยให้ความสำคัญกับการระบุขอบเขตของข้อมูลที่จะใช้ร่วมกัน เพื่อให้เหมาะสมกับใช้ร่วมกันและการเข้าถึงข้อมูล

2.2 มีข้อกำหนดในการใช้ข้อมูลร่วมกัน รวมถึงการบริหารจัดการการอนุญาตเพื่อให้มั่นใจได้ว่ามีผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลที่ใช้ร่วมกันนี้ได้

2.3 มีข้อกำหนดในการใช้ข้อมูลที่ได้รับการร่วมกัน เช่น การกำหนดขอบเขตการใช้ข้อมูล หรือการห้ามนำข้อมูลไปใช้ในวัตถุประสงค์ที่ไม่เกี่ยวข้อง

2.4 การตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้ข้อมูลร่วมกัน รวมถึงการจัดการและ ควบคุมเพื่อลดความเสี่ยงที่เป็นไปได้

2.5 การฝึกอบรมพนักงานที่เกี่ยวข้อง ผ่านช่องทางต่างๆ ที่สามารถเข้าถึงได้จากทุกที่ เพื่อเพิ่มความ เข้าใจในการข้อมูลร่วมกันและการใช้ข้อมูลอย่างมี ประสิทธิภาพ รวมถึงการบันทึกข้อมูลเกี่ยวกับการใช้ ข้อมูลร่วมกันเพื่อการติดตามและการประเมินประสิทธิภาพ

2.6 การตรวจสอบและประเมินการใช้ข้อมูลร่วมกันเพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามหลักเกณฑ์และ แนวทางที่กำหนดไว้

3. รูปแบบการใช้ข้อมูลร่วมกัน

3.1 การใช้ข้อมูลร่วมกันทั่วไป (General Sharing) เป็นการใช้ข้อมูลร่วมกันที่มีความสำคัญและเกี่ยวข้องกับผู้ใช้ หลายกลุ่ม โดยไม่จำกัดเฉพาะกับกลุ่มหรือบุคคลใด

3.2 การใช้ข้อมูลร่วมกันตามความจำเป็น (Need-to-Know Sharing) เป็นการใช้ข้อมูลเฉพาะกับบุคคลหรือ กลุ่มผู้ใช้ที่จำเป็นต้องมีข้อมูลนั้นเพื่อการปฏิบัติงาน

3.3 การใช้ข้อมูลร่วมกันตามระดับความลับ (Security Clearance-based Sharing) เป็นการใช้ข้อมูลร่วมกันโดย พิจารณาจากระดับความลับของข้อมูล และแบ่งปันเฉพาะกับบุคคลหรือกลุ่มผู้ใช้ตามความ เหมาะสมการเลือกรูปแบบการใช้ข้อมูลร่วมกันจะขึ้นอยู่กับลักษณะของข้อมูล ชั้นความลับ และ วัตถุประสงค์ของการ ใช้ข้อมูลร่วมกัน ทั้งนี้ให้ยึดถือประโยชน์ของบริษัทเป็นสำคัญ

หมวด 10 การทำให้ระบบมีความแข็งแกร่ง
(System Hardening)

1. วัตถุประสงค์

เพื่อปรับปรุงและตั้งค่าระบบปฏิบัติการของทรัพย์สินสารสนเทศของหน่วยงาน ให้มีความแข็งแกร่ง ทนทานต่อการถูกโจมตีทางไซเบอร์ เป็นการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และเพิ่มความเชื่อถือได้ของ ระบบให้แก่ผู้ใช้งาน

2. แนวทางปฏิบัติในการทำให้ระบบมีความแข็งแกร่ง

2.1 ปรับแต่งค่าเริ่มต้นของระบบและแอปพลิเคชัน โดยเปลี่ยนรหัสผ่านตั้งต้น (Default Password) ปิดการใช้งานบริการที่ไม่จำเป็น และปรับเป็นการตั้งค่าที่ปลอดภัย

2.2 เปิดใช้งานเฉพาะ Port ที่มีความจำเป็นเท่านั้น ส่วน Port ใดที่ไม่ได้ใช้งานให้ทำการปิด เพื่อลด ความเสี่ยงจากการถูกโจมตีโดยผู้ไม่ประสงค์ดี

2.3 อัปเดทซอฟต์แวร์และระบบปฏิบัติการเป็นประจำ (Patch Management) เพื่อแก้ไขช่องโหว่และลดความเสี่ยงจากการถูกโจมตีโดยผู้ไม่ประสงค์ดี

2.4 ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านของเครื่องแม่ข่ายเป็นประจำทุก ๆ 3 เดือน โดยรหัสผ่านที่เปลี่ยนต้องไม่เคยถูกใช้งานมาก่อน เพื่อป้องกันปัญหาจากการเกิดข้อมูลรั่วไหล

2.5 กำหนดสิทธิของผู้ใช้ในส่วนต่าง ๆ ให้น้อยที่สุด (Least Privilege) ตามความจำเป็นเฉพาะหน้าที่ที่เกี่ยวข้องเท่านั้น

2.6 หลีกเลี่ยงการเข้าถึงเครื่องแม่ข่ายโดยตรงผ่าน Public IP ต้องเป็นการเข้าถึงผ่าน Private IP และผ่าน VPN เท่านั้น หากเป็นการเข้าถึงจากภายนอกเครือข่ายของบริษัท

2.7 ต้องติดตั้งซอฟต์แวร์ Antivirus ที่บริษัทจัดสรรให้ ในเครื่องแม่ข่ายหรือทรัพย์สินสารสนเทศ ของหน่วยงาน

2.8 จำกัดสิทธิการเข้าถึงเครื่องแม่ข่ายหรือทรัพย์สินสารสนเทศที่สำคัญเฉพาะผู้ดูแลระบบของหน่วยงานเท่านั้น หากมีการปรับเปลี่ยนสิทธิต้องดำเนินการเป็นลายลักษณ์อักษรและอนุมัติโดยหัวหน้าหน่วยงาน

หมวด 11 การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Awareness)

1.วัตถุประสงค์

เพื่อเสริมสร้างความรู้ ความเข้าใจ ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานของหน่วยงาน เพื่อการ ตระหนัก และรู้เท่าทันภัยคุกคามทางไซเบอร์ในปัจจุบัน เป็นการลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ ทางอ้อม รวมถึงลดความเสี่ยงจากการกระทำผิดกฎหมายที่เกี่ยวข้องโดยรู้เท่าไม่ถึงการณ์

2. แนวปฏิบัติในการสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์

2.1 จัดให้มีการให้ความรู้เสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ให้แก่พนักงานของหน่วยงาน ผ่านทุกช่องทางที่เข้าได้ทุกที่ เพื่อให้เข้าถึงความรู้ได้ง่ายและรวดเร็วตามภัยคุกคามที่เปลี่ยนแปลงวิธีอย่างรวดเร็ว

2.2 กำหนดแนวปฏิบัติให้ติดตั้งซอฟต์แวร์ Antivirus ในเครื่องคอมพิวเตอร์ที่หน่วยงานจัดสรรให้ และเครื่องคอมพิวเตอร์แบบพกพาที่นำมาปฏิบัติงานภายในหน่วยงาน

2.3 ผู้ใช้ต้องอัปเดท Virus Definition ของซอฟต์แวร์ Antivirus เป็นประจำอย่างน้อยสัปดาห์ละ 1 ครั้ง

2.4 ผู้ใช้ควรสแกนไวรัสบนสื่อแบบถอดได้ทุกครั้งก่อนนำมาใช้งาน

2.5 ผู้ใช้ไม่ควรใช้งานสื่อแบบถอดได้ที่ได้รับมาจากแหล่งที่ไม่น่าเชื่อถือ เช่น พบว่าตกอยู่บนพื้น หรือ วาง อยู่บนโต๊ะแบบไม่มีเจ้าของ เพื่อป้องกันซอฟต์แวร์ไม่พึงประสงค์

2.6 ผู้ใช้ต้องไม่ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์จากสื่อต่าง ๆ หรือจากการดาวน์โหลดผ่านเครือข่ายอินเตอร์เน็ต

2.7 ผู้ใช้ต้องมีความระมัดระวังในการใช้งานเว็บไซต์ โดยสังเกตจากชื่อ URL เพื่อป้องกันการถูกขโมยข้อมูลจากผู้ไม่ประสงค์ดี

2.8 ผู้ใช้ต้องมีความระมัดระวังในการใช้งานอีเมล โดยไม่ดาวน์โหลดหรือเปิดไฟล์แนบจากอีเมลที่ไม่น่าเชื่อถือ

2.9 ผู้ใช้ต้องมีความระมัดระวังในการใช้งานโซเชียลมีเดีย เพื่อป้องกันการถูกหลอกลวง โดยผู้ไม่ประสงค์ดี

หมวด 12 การเชื่อมต่อระยะไกล

(Remote Connection)

1. วัตถุประสงค์

เพื่อเป็นการป้องกันความเสี่ยงที่เกี่ยวข้องกับการเชื่อมต่อระยะไกล (Remote Connection) จากการ เข้าถึงที่ไม่ได้รับอนุญาตโดยผู้ไม่ประสงค์ดี การเข้าถึงและการใช้งานที่ไม่ปลอดภัยโดยผู้ใช้ หรือการเข้าถึงจาก เครือข่ายที่ไม่ปลอดภัย

2. แนวปฏิบัติการเชื่อมต่อระยะไกล

2.1 หลีกเลี่ยงการเชื่อมต่อระยะไกล หากไม่มีความจำเป็นหรือเร่งด่วนใด ๆ

2.2 เครือข่ายของหน่วยงานที่อนุญาตให้ผู้ใช้เข้าถึงได้ หากมีความจำเป็นต้องให้มีการเข้าถึงผ่านการ เชื่อมต่อระยะไกล ต้องให้เชื่อมต่อผ่าน VPN ที่บริษัทกำหนดไว้เท่านั้น

2.3 เครื่องคอมพิวเตอร์หรือคอมพิวเตอร์แบบพกพา ที่ทำการเชื่อมต่อระยะไกลผ่าน VPN ต้องติดตั้ง ซอฟต์แวร์ Antivirus ที่บริษัทจัดสรรให้

2.4 เครื่องคอมพิวเตอร์หรือคอมพิวเตอร์แบบพกพา ที่ทำการเชื่อมต่อระยะไกลผ่าน VPN ต้องอัปเดทซอฟต์แวร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ

2.5 ผู้ใช้ต้องไม่มอบบัญชีผู้ใช้งานของตนให้กับผู้อื่น เพื่อใช้งาน VPN ในการเชื่อมต่อระยะไกลกับเครือข่ายของบริษัท

2.6 ผู้ใช้ต้องไม่ใช้เครื่องคอมพิวเตอร์สาธารณะในการเชื่อมต่อระยะไกลกับเครือข่ายของบริษัท

2.7 หน่วยงานต้องมีการประเมินความเสี่ยงในการเชื่อมต่อระยะไกล เพื่อหามาตรการป้องกันแก้ไขปัญหาที่ อาจจะเกิดขึ้น

นโยบายที่ 2 นโยบายการรักษาสภาพความพร้อมใช้งานของการให้บริการ มีแนวปฏิบัติดังนี้

หมวด 13 การรักษาสภาพความพร้อมใช้งานของการให้บริการ

(Service Continuity)

1. วัตถุประสงค์

เพื่อมั่นใจได้ว่าระบบสารสนเทศที่ให้บริการและข้อมูลสำคัญของหน่วยงาน มีความพร้อมใช้งานอยู่ตลอด และสามารถดำเนินการต่อไปได้ในขณะที่หน่วยงานเผชิญกับภาวะวิกฤตหรือภัยพิบัติ เพื่อลดผลกระทบที่อาจเกิด ขึ้นกับหน่วยงาน โดยมีการลำดับความสำคัญจากผลกระทบจากความเสียหายของทรัพย์สิน และผลการวิเคราะห์ ความเสี่ยง เพื่อใช้ในการพิจารณาวิธีการสร้างความต่อเนื่อง

2. แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

2.1 เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีความสำคัญ ต้องมีการสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน

2.2 ผู้ดูแลระบบต้องสำรองข้อมูลและซอฟต์แวร์เก็บไว้ โดยคัดเลือกและจัดเรียงลำดับตามผลกระทบจากความสูญเสียของระบบที่มีผลต่อภารกิจหลักของหน่วยงาน

2.3ต้องมีขั้นตอนการปฏิบัติการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

2.4 ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองในสื่อบันทึกข้อมูลสำรอง โดยมีการแสดงชื่อระบบที่สำรอง วัน เดือน ปี และเวลาในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรอง ซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง และต้องมีการทดสอบสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

2.5 หัวหน้าหน่วยงานต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมฉุกเฉิน

2.6 หน่วยงานต้องดำเนินการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินปีละ 1 ครั้ง

2.7 ผู้ดูแลระบบต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยระบบสารสนเทศได้ตามปกติ โดยต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวอย่างน้อยปีละ 1 ครั้ง เพื่อให้ สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

หมวด 14 การตรวจสอบและรับมือภัยคุกคามทางไซเบอร์

(Detect & Response)

1.วัตถุประสงค์

เพื่อให้มีกระบวนการตรวจสอบ เฝ้าระวังภัยคุกคามทางไซเบอร์ และการเผชิญเหตุเมื่อมีการตรวจพบภัย คุกคามทางไซเบอร์ (Detect & Response) ในระดับหน่วยงาน เพื่อการแก้ไขและป้องกันในเบื้องต้นก่อนแจ้งให้บริษัททราบในลำดับถัดไป

2.แนวทางปฏิบัติในการตรวจสอบและรับมือภัยคุกคามทางไซเบอร์

2.1 หน่วยงาน ต้องมอบหมายให้มีผู้ที่ทำหน้าที่ในการตรวจสอบและรับมือภัยคุกคามทางไซเบอร์ เพื่อแก้ไข และป้องกันปัญหาในเบื้องต้นก่อนแจ้งให้บริษัททราบ

2.2 เมื่อหน่วยงานพบเหตุที่ประเมินแล้วว่าอยู่ในระดับวิกฤต ต้องรีบแจ้งหัวหน้าหน่วยงาน และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เพื่อดำเนินการ ป้องกันแก้ไขในเบื้องต้น ก่อนที่จะรายงานให้กับบริษัททราบ ผ่านระบบ Helpdesk เพื่อแจ้งปัญหาที่พบ

2.3 หน่วยงานต้องบันทึกเหตุและการเผชิญเหตุในระบบ Helpdesk ทุกครั้ง ถึงแม้ว่าจะสามารถแก้ไขปัญหาภัยคุกคามนั้น ๆ ได้แล้ว

2.4 หน่วยงานต้องมอบหมายให้ผู้ที่รับผิดชอบตามข้อ 2.1 เข้าร่วมฝึกอบรมด้านความมั่นคงปลอดภัย ไซเบอร์ที่บริษัทจัดขึ้นทุกครั้ง

2.5 หน่วยงานต้องกำหนดผู้รับผิดชอบด้านการรับมือภัยคุกคามทางไซเบอร์ตามแนวทางที่บริษัทกำหนด และทบทวนเป็นประจำทุกปี

หมวด 15 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(Cybersecurity Resilience and Recovery)

1.วัตถุประสงค์

เพื่อให้หน่วยงานมีความพร้อมในการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ด้วย การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของ หน่วยงานสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์ รวมถึงการฝึกซ้อมแผน BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนต่อภัย คุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

2.แนวปฏิบัติการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

2.1 หน่วยงานต้องมีการมอบหมายให้มีผู้ทำหน้าที่จัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) จากความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์อย่างเป็นทางการหรือลายลักษณ์อักษร

2.2 หน่วยงานต้องมีการสำรองข้อมูลหรือระบบที่สำคัญนอกเหนือจากการดูแลของสำนักบริการเทคโนโลยี สารสนเทศ เป็นประจำตามระดับความสำคัญของข้อมูลและระบบ ตามที่ได้ทำการวิเคราะห์ความเสี่ยงแล้ว

2.3 หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) จากความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ และต้องมีการจัดเตรียมทรัพย์สินสารสนเทศสำรองให้ครบถ้วนตามที่ระบุไว้ในแผน

2.4 หน่วยงานต้องมีการฝึกซ้อมแผน BCP ตามข้อ 2.3 อย่างน้อยปีละ 1 ครั้งเพื่อประเมินประสิทธิภาพของแผนต่อภัยคุกคามทางไซเบอร์ ในรูปแบบที่เหมาะสมและจัดทำเป็นเอกสารรายงาน

2.5 หน่วยงานต้องมีการทบทวนแผน BCP ตามข้อ 2.3 อย่างน้อยปีละ 1 ครั้งเพื่อปรับปรุงเปลี่ยนแปลงให้ มีความเหมาะสมและทันต่อเหตุการณ์

นโยบายที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ มีแนวปฏิบัติดังนี้

หมวด 16 การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Risk Management)

1. วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์การตรวจสอบและประเมินความเสี่ยงของระบบเครือข่ายและระบบเทคโนโลยี สารสนเทศของหน่วยงาน ให้มั่นใจได้ว่าความเสี่ยงของระบบสารสนเทศของหน่วยงานได้ถูกพิจารณาและได้มีการ จัดเตรียมมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัย ไซเบอร์ที่อาจจะเกิดขึ้นกับหน่วยงานได้

2. แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2.1 ระบุความเสี่ยงให้สอดคล้องกับความเสี่ยงที่อาจจะเกิดขึ้น ดังนี้

2.1.1 ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์ แม่ข่ายของหน่วยงานผ่านเครือข่ายอินเทอร์เน็ต

2.1.2 ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายของหน่วยงานโดยไม่ได้รับอนุญาต

2.1.3 ความเสี่ยงที่เกิดจากเครื่องมือสารสนเทศหรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

2.1.4 ความเสี่ยงที่เกิดจากการลงบันทึกเข้าใช้งาน (Login) สารสนเทศที่สำคัญของหน่วยงานผ่านระบบเครือข่ายที่ไม่ปอลดภัย เช่น เครือข่ายอินเตอร์เน็ตสาธารณะ เป็นต้น

2.1.5 ความเสี่ยงอื่นที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน ที่อาจจะส่งผลกระทบกับการ ปฏิบัติงานของหน่วยงาน

2.2 การตรวจสอบและประเมินความเสี่ยง ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น ให้คำนึงถึงองค์ประกอบดังต่อไปนี้

2.2.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ ทำการประเมินในแต่ละด้านของผลกระทบโดยให้พิจารณาถึงมาตรการควบคุมที่มีอยู่ในปัจจุบันด้วย

2.2.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่จะเกิดขึ้น ต้องพิจารณา 2 ปัจจัยหลัก คือ

1) แนวโน้มการเกิดขึ้นของเหตุการณ์ความเสี่ยง โดยพิจารณาจากความน่าจะเป็นหรือ ค่าทางสถิติที่มีการบันทึกไว้ เช่น เหตุการณ์ความเสี่ยง เหตุภัยธรรมชาติต่าง ๆ เป็นต้น

2) ความยากง่ายที่จะถูกกระทำ ให้พิจารณาจากจุดอ่อนหรือข้อบกพร่องที่มีอยู่และตัว ควบคุมในปัจจุบัน หากมีจุดอ่อนหรือข้อบกพร่องมากและไม่มีตัวควบคุมเลย โอกาสที่จะเกิด เหตุการณ์ความเสี่ยงจะสูงกว่าในกรณีที่มีตัวควบคุมอยู่

2.2.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ พิจารณาข้อบกพร่องของระบบหรือข้อบกพร่องของการควบคุมที่ปัจจุบันอาจจะไม่มีอยู่ และจะส่งผลให้ระบบไม่มีความมั่นคงปลอดภัยที่ดี

2.2.4 ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ 1 ครั้ง

2.2.5 การตรวจสอบจะต้องดำเนินการโดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ 1 ครั้ง

2.3 รายละเอียดเพิ่มเติมของการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์

หมวด 17 การกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Duty and responsibility)

1.วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ระดับหน่วยงานของผู้บริหารหน่วยงาน หัวหน้าฝ่าย/งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และผู้ที่ได้รับ มอบหมาย เป็นลายลักษณ์อักษร

2.แนวทางปฏิบัติ

2.1 ระดับนโยบาย

2.1.1 ผู้บริหารหน่วยงานที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรือ อันตรายใด ๆ แก่หน่วยงานหรือพนักงาน อันเนื่องมาจากความบกพร่อง ละเลยหรือไม่ปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

2.1.2 ผู้บริหารหน่วยงานที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศของหน่วยงาน เป็นผู้รับผิดชอบในการสั่งการกำกับนโยบาย ให้ข้อเสนอแนะและคำปรึกษา ตลอดจนติดตาม ดูแลและ ควบคุมตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแนว ปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัท

2.2 ระดับปฏิบัติการ

ระดับผู้ปฏิบัติงานประกอบด้วย ผู้ดูแลระบบสารสนเทศของหน่วยงาน ผู้ที่ได้รับมอบหมายให้ ปฏิบัติ หน้าที่ และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจดังนี้

2.2.1 ผู้ดูแลระบบสารสนเทศ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นผู้รับผิดชอบ ดังนี้

1) ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

2) เป็นผู้ประสานงานและร่วมปฏิบัติตามแผนรับมือภัยคุกคามทางไซเบอร์ของ บริษัท

3) ควบคุม ดูแล รักษาความปลอดภัยและบำรุงรักษาระบบคอมพิวเตอร์ ระบบ เครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน

4) ทำการสำรองข้อมูลหรือเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลา ที่กำหนดของหน่วยงาน

5) ป้องกันและเฝ้าระวังภัยคุกคามทางไซเบอร์ในระดับหน่วยงาน และแจ้งเหตุให้ บริษัททราบทันทีที่เกิดเหตุภัยคุกคามทางไซเบอร์ผ่านระบบ Helpdesk

6) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

2.2.2 ผู้ใช้งานเป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของหน่วยงานตามสิทธิที่ได้รับอนุญาตโดย ให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้อย่างเคร่งครัด

ประกาศ ณ วันที่ 2 มกราคม พ.ศ. 2568

ผู้อนุมัติ	ผู้จัดทำ
- -ลงนามแล้ว-	ลงนามแล้ว
นายภูวสิษฏ์ วงษ์เจริญสิน	(นายณัฐปกรณ์ ชีรนรวนิชย์)
ประธานเจ้าหน้าที่บริหาร	ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ