ประกาศมหาวิทยาลัยเชียงใหม่

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. 2567

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกสภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2556 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร และมาตรา 44 มาตรา 45 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ดังนั้น จึงสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบสารสนเทศและผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของส่วนงาน

อาศัยอำนาจตามความในมาตรา 25(3) มาตรา 35 และมาตรา 38 แห่งพระราชบัญญัติมหาวิทยาลัยเชียงใหม่ พ.ศ. 2551 ประกอบกับมติที่ประชุมสภามหาวิทยาลัย ในคราวประชุมครั้งที่ 10/2551 เมื่อวันที่ 27 กันยายน 2551 และ มติที่ประชุมคณะกรรมการบริหารมหาวิทยาลัย ในคราวประชุมครั้งที่ 8/2567 เมื่อวันที่ 21 พฤษภาคม 2567 จึงออกประกาศไว้ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่ถัดจากวันประกาศเป็นต้นไป

ข้อ 3 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

นโยบายที่ 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติดังนี้

1) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

2) การเข้าถึงและควบคุมการใช้งานสารสนเทศ

3) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

4) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

5) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

6) การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์

7) การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์

8) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

9) การแบ่งปันข้อมูล (Information Sharing)

10) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

11) การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

12) การเชื่อมต่อระยะไกล (Remote Connection)

นโยบายที่ 2 นโยบายการรักษาสภาพความพร้อมใช้งานของการให้บริการ มีแนวปฏิบัติดังนี้

1) การรักษาสภาพความพร้อมใช้งานของการให้บริการ

2) การตรวจสอบและรับมือภัยคุกคามทางไซเบอร์ (Detect & Response)

3) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

นโยบายที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ มีแนวปฏิบัติดังนี้

1) การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2) การกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ 4 การกำหนดความรับผิดชอบ

4.1 อธิการบดีมหาวิทยาลัยเชียงใหม่ ในฐานะผู้บริหารสูงสุดของมหาวิทยาลัย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่มหาวิทยาลัยหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

4.2 หัวหน้าส่วนงาน เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะและคำปรึกษา ตลอดจนติดตาม กำกับดูแล ตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของส่วนงานให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

4.3 เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้สำนักบริการเทคโนโลยีสารสนเทศ และผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ 1 ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย ให้ประกาศให้ส่วนงานรับทราบทุกครั้ง

ข้อ 5 นโยบายและแนวปฏิบัติในการักษาความมั่นคงปลอดภัยไซเบอร์ จัดเป็นมาตฐานด้านการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง จึงให้ใช้นโยบายและแนวปฏิบัติในการักษาความมั่นคงปลอดภัยไซเบอร์ตามเอกสารแนบท้ายประกาศนี้ ซึ่งบุคลากรของมหาวิทยาลัยทุกส่วนงานและผู้ที่เกี่ยวข้องที่ได้รับมอบหมายของส่วนงานจะต้องปฏิบัติตามอย่างเคร่งครัด

ข้อ 6 ให้อธิการบดีเป็นผู้รักษาการในประกาศนี้ ในกรณีมีปัญหาทางปฏิบัติตามประกาศนี้ ให้อธิการบดีเป็นผู้วินิจฉัยชี้ขาด โดยความเห็นชอบของคณะกรรมการบริหารมหาวิทยาลัย และให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๓ กรกฎาคม พ.ศ. 2567

(ศาสตราจารย์ ดร.นายแพทย์พงษ์รักษ์ ศรีบัณฑิตมงคล)
อธิการบดีมหาวิทยาลัยเชียงใหม่

เอกสารแนบท้ายประกาศ
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
มหาวิทยาลัยเชียงใหม่
พ.ศ. 2567

คำนำ

ระบบเทคโนโลยีสารสนเทศเป็นเครื่องมือสำคัญสำหรับมหาวิทยาลัย ในการอำนวยความสะดวกการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ ของมหาวิทยาลัย แต่ในขณะเดียวกันก็ทำให้มหาวิทยาลัยมีความเสี่ยงจากภัยคุกคามของระบบเทคโนโลยีสารสนเทศเพิ่มขึ้น ซึ่งอาจสร้างความเสียหายต่อการปฏิบัติราชการได้ เนื่องจากระบบเทคโนโลยีสารสนเทศมีการเชื่อมโยงข้อมูลไปยังส่วนงานต่าง ๆ ส่งผลให้ช่องทางในการถูกบุกรุกเปิดกว้างขึ้นและอาจก่อให้เกิดเหตุอาชญากรรมทางคอมพิวเตอร์กับมหาวิทยาลัยได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ส่งผลให้มหาวิทยาลัยเสียชื่อเสียงหรือภาพลักษณ์ได้ ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการดูแล บำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยไซเบอร์เป็นอย่างยิ่ง

ดังนั้น มหาวิทยาลัยเชียงใหม่ จึงจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคง ปลอดภัยและเชื่อถือได้ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของส่วนงานเป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ทั้งนี้ การดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยเชียงใหม่ ต้องได้รับความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว จึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของทุกส่วนงานในมหาวิทยาลัย ในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยเชียงใหม่ต่อไป

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
มหาวิทยาลัยเชียงใหม่

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเชียงใหม่ หรือต่อไปนี้เรียกว่า “มหาวิทยาลัย” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ มหาวิทยาลัยจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดให้มีแนวปฏิบัติที่ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 เพื่อกำหนดแนวทางปฏิบัติและวิธีปฏิบัติ ให้แก่ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งานของมหาวิทยาลัย และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

1.2 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยได้อย่างมีประสิทธิภาพและประสิทธิผล

1.3 เพื่อเผยแพร่ให้แก่บุคลากรทุกคนในมหาวิทยาลัยได้รับทราบ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายที่ 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติดังนี้

หมวด 1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
หมวด 2 การเข้าถึงและควบคุมการใช้งานสารสนเทศ
หมวด 3 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
หมวด 4 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
หมวด 5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
หมวด 6 การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
หมวด 7 การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์
หมวด 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
หมวด 9 การแบ่งปันข้อมูล (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

หมวด 1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ อีกทั้งเพื่อป้องกันทรัพย์สินของมหาวิทยาลัยจากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือข้อมูลสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต โดยมาตรการนี้จะมีผลบังคับใช้กับนักศึกษา บุคลากร และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1. ส่วนงาน ต้องมีการจำแนกและกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

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

2.3 ผู้บริหารส่วนงาน ต้องกำหนดสิทธิให้กับบุคลากรให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

2.3.1 จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

2.3.3 จัดให้มีบุคลากรทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ

2.3.4 ต้องมีการทบทวนปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ **1** ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับสิทธิการเข้าออกพื้นที่ เช่น การโอน ย้าย ลาออก หรือสิ้นสุดการจ้าง

3. การควบคุมการเข้าออก อาคาร สถานที่

3.1 หน่วยงานภายในที่รับผิดชอบด้านความปลอดภัยของอาคารสถานที่ หรือผู้บริหารที่รับผิดชอบพื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีบุคลากรหรือวิธีการรักษาความปลอดภัย เพื่อควบคุมให้เข้าสถานที่ทำงานได้เฉพาะบุคคลที่ได้รับอนุญาตจากเจ้าของพื้นที่เท่านั้น

3.2 ส่วนงานต้องจัดทำเอกสารระบุสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยกำหนด ดังนี้

3.2.1 ส่วนงานต้องกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้า-ออกในแต่ละพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างชัดเจน

3.2.2 การเข้าถึงอาคารของส่วนงานของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรใน “แบบฟอร์ม การเข้า-ออกพื้นที่”

3.2.3 กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์แบบพกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้า-ออกพื้นที่ในรายการอุปกรณ์ที่นำเข้ามา ให้ถูกต้องและชัดเจน

3.2.4 บุคคลภายนอกที่เข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้า-ออกในแบบฟอร์ม การเข้า-ออกพื้นที่ให้ถูกต้องและชัดเจน

3.3 ผู้ใช้งานจะได้รับสิทธิให้เข้า-ออกสถานที่ทำงานได้ เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้สำหรับปฏิบัติงานเท่านั้น

3.4 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ส่วนงานเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้ จะต้องแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้ โดยส่วนงานเจ้าของพื้นที่ต้องจดบันทึกการขอเข้า-ออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

4. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

จัดให้มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของส่วนงานที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งาน ดังนี้

4.1 ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

4.2 ติดตั้งระบบระงับเพลิง

4.3 ติดตั้งระบบปรับอากาศและควบคุมความชื้น

4.4 ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องแม่ข่ายทำงานผิดปกติ หรือหยุดการทำงาน

4.5 วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของส่วนงานอย่างสม่ำเสมอ ให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

5. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

5.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของส่วนงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงต้องติดตั้งระบบป้องกันที่ปลอดภัย

5.2 ให้มีการร้อยท่อสายสัญญาณต่าง ๆ หรือมีการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อป้องกันการตัดสายสัญญาณทำให้เกิดความเสียหาย หรือการดักรับข้อมูลโดยผู้ที่มิได้รับอนุญาต

5.3 สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญาณ

5.4 ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

5.5 จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

5.6 ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ต้องปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

5.7 พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม

5.8 ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี 3 เดือน หรือ 6 เดือน สำหรับสายไฟเบอร์ออฟติก

6. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

6.1 วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา และต้องมีการซ่อมบำรุงอย่างทันท่วงที ตามความสำคัญของระบบ

6.2 บันทึกประวัติการบำรุงรักษาและซ่อมบำรุงอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง โดยมีรายละเอียดดังนี้ วันที่บำรุงรักษาและซ่อมบำรุง รายการอุปกรณ์ สถานะของอุปกรณ์ ปัญหาที่พบและการแก้ไข ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุงพร้อมลงลายมือชื่อ

6.3 ถ้ามีการจัดจ้างหน่วยงานหรือผู้ให้บริการภายนอก เพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์ ส่วนงานที่จัดจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการจ้าง โดยต้องกำหนดระยะเวลา ขอบเขต และระดับการให้บริการอย่างชัดเจน

6.4 ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในส่วนงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบหรือผู้รับผิดชอบการซ่อมบำรุงอุปกรณ์จะต้องอยู่ในพื้นที่ทุกครั้ง

6.5 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างหรือผู้ให้บริการภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

7. การนำทรัพย์สินของส่วนงานออกนอกพื้นที่ (Removal of Property)

7.1 ส่วนงานต้องมอบหมายบุคลากรเป็น “ผู้ดูแลครุภัณฑ์” มีหน้าที่ควบคุมดูแลพัสดุหรือทรัพย์สินของส่วนงานที่อยู่ในความครอบครองให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา โดยมิให้เกิดการสูญหาย และจัดทำ “ทะเบียนครุภัณฑ์” ของส่วนงาน บันทึกการใช้งาน ผู้ใช้งาน สถานภาพและการเคลื่อนย้ายของครุภัณฑ์ ทั้งนี้ต้องตรวจสอบสถานภาพของครุภัณฑ์อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เคลื่อนย้าย เช่น ได้รับมอบครุภัณฑ์เพิ่มเติม การตัดจำหน่าย การเปลี่ยนผู้ครอบครอง การยืม การโอน หรือการส่งซ่อม

7.2 ต้องขออนุญาตจากผู้บริหารของส่วนงานและแจ้งให้ผู้ดูแลครุภัณฑ์ทราบ ก่อนนำอุปกรณ์หรือทรัพย์สินออกไปใช้งานภายนอกส่วนงาน หรือนำไปซ่อมบำรุง

7.3 ต้องได้รับความเห็นชอบจากหัวหน้าส่วนงาน ก่อนนำครุภัณฑ์คอมพิวเตอร์ส่งซ่อมภายนอกส่วนงาน

7.4 การให้ยืมอุปกรณ์หรือทรัพย์สิน ผู้ดูแลครุภัณฑ์จะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนด และอยู่ในสภาพปกติ หรือไม่ต่างจากตอนที่ถูกยืม และต้องบันทึกข้อมูลการนำอุปกรณ์ของส่วนงานออกไปใช้งานนอกส่วนงาน และบันทึกส่งคืน เพื่อเป็นหลักฐานป้องกันการสูญหาย

8. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกส่วนงาน (Security of Equipment off Premises)

8.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของส่วนงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

8.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของส่วนงานไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

8.3 บุคลากรผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

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

9.1 การจำหน่ายครุภัณฑ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ส่วนงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ก่อนการจำหน่าย เพื่อให้มั่นใจว่าข้อมูลและซอฟต์แวร์ลิขสิทธิ์จะไม่สามารถนำกลับมาใช้ได้อีก (Non - Retrievable)

9.2 หัวหน้าส่วนงาน เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ ต้องเสนอเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

9.3 ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัด โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

หมวด 2 การเข้าถึงและควบคุมการใช้งานสารสนเทศ
(Access control)

1. วัตถุประสงค์

1.1 เพื่อให้ข้อมูลที่มีความสำคัญต่อส่วนงาน ได้รับการจำแนกชั้นความลับอย่างเหมาะสมตามระดับความสำคัญของข้อมูล และเพื่อให้บุคลากรที่เกี่ยวข้องรับรู้และสามารถนำข้อมูลแต่ละชั้นความลับไปใช้งานได้อย่างถูกต้องและเหมาะสม

1.2 เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาต เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้ไม่ประสงค์ดีผ่านโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงานได้อย่างถูกต้อง

2. การกำหนดลำดับความสำคัญของข้อมูลและการใช้งานข้อมูล

2.1 ส่วนงานใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ โดยมีการแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือ ลำดับชั้นความลับของข้อมูล ดังนี้

2.1.1 จัดแบ่งประเภทของข้อมูลออกเป็น

1) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลคำรับรอง ข้อมูลบุคลากร ข้อมูลแผนงบประมาณ การเงินและบัญชี เป็นต้น

2) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลการขอใช้รถยนต์ส่วนกลาง ข้อมูลการขอใช้ห้องประชุม เอกสารเผยแพร่บนเว็บไซต์ของส่วนงาน เป็นต้น

2.1.2 การรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการของเอกสารที่สำคัญ การเข้าถึงข้อมูลแต่ละประเภทตามระดับชั้นความลับของส่วนงาน ดังต่อไปนี้

1) ลับมาก (Secret) มีความสำคัญต่อส่วนงานในระดับสูงมาก หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อส่วนงานอย่างมาก

2) ลับที่สุด (Confidential) มีความสำคัญต่อส่วนงานในระดับสูง หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อส่วนงานอย่างมีนัยยะสำคัญ

3) ใช้ภายในส่วนงาน (Internal Use) เป็นข้อมูลที่อนุญาตให้ใช้ภายในส่วนงาน หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อส่วนงาน

4) สาธารณะ (Public) เป็นข้อมูลที่ใช้เผยแพร่สู่สาธารณะ การเปิดเผยข้อมูลประเภทนี้ไม่ส่งผลกระทบใดกับส่วนงาน

2.1.3 การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ 1 ระดับชั้นสำหรับผู้บริหาร

ระดับที่ 2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

ระดับที่ 3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

2.1.4 กำหนดเวลาที่สามารถเข้าถึงข้อมูลได้

2.1.5 การกำหนดช่องทางในการเข้าถึงข้อมูล ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้นั้น จะต้องได้รับสิทธิจากส่วนงาน โดยมีการกำหนดบัญชีชื่อผู้ใช้งานตามระดับชั้นการเข้าถึง ให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูล และสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น

2.2 การใช้งานข้อมูล

2.2.1 มีมาตรการให้ผู้ใช้งานต้องใช้งานข้อมูลของส่วนงานตามกฎระเบียบและคำแนะนำที่ส่วนงานกำหนดไว้

2.2.2 ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้งานข้อมูลประเภทลับมาก และลับที่สุด (ต่อไปในเอกสารนี้เรียกว่า “ข้อมูลลับ”) เพื่อป้องกันไม่ให้ข้อมูลถูกเข้าถึงหรือถูกเปิดเผย โดยไม่ได้รับอนุญาต

2.2.3 ข้อมูลลับของส่วนงานต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น (ตามหลักการ “Need to Know”)

2.2.4 ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลลับที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือแอปพลิเคชันอย่างเหมาะสม

2.2.5 ข้อมูลใดที่ผู้ใช้งานพิจารณาว่าเป็นข้อมูลลับหรือมีจุดอ่อนด้านความมั่นคงปลอดภัย ต้องได้รับการเข้ารหัส

2.2.6 ผู้ใช้งานควรเก็บรักษาสื่อบันทึกข้อมูลที่มีข้อมูลลับ ในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องวางสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน

2.2.7 ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร ฯลฯ ทันที

2.2.8 ผู้ใช้งานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

2.2.9 ผู้ใช้งานต้องไม่พูดคุยหรือใช้งานข้อมูลลับของส่วนงานในพื้นที่สาธารณะ เช่น ลิฟต์ ร้านอาหาร ฯลฯ

3. กระบวนการในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ต้องมีการควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็น ผ่านเข้าใช้งานได้เท่านั้น

3.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของบุคลากรในการปฏิบัติงาน ก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหารและผู้ดูแลระบบตามความจำเป็นในการใช้งาน

3.2.1 กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

1) อ่านอย่างเดียว

2) สร้างข้อมูล หรือนำเข้าข้อมูล

3) แก้ไขข้อมูล

4) ลบข้อมูล

5) อนุมัติ

6) ไม่มีสิทธิ

3.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และระบบข้อมูลได้

3.4 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

3.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกประวัติการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

4. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

4.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบแก่ผู้ใช้งาน ในการขออนุญาตเข้าใช้ระบบงานนั้น จะต้องมีบันทึกเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและมีการลงนามอนุมัติโดยผู้บริหาร เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

4.2 ผู้ดูแลระบบต้องกำหนดระยะเวลาการเชื่อมต่อเข้าสู่ระบบสารสนเทศ/แอปพลิเคชันที่มีความสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.3 เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่รับผิดชอบเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

4.4 ผู้ใช้งานจะต้องได้รับอนุญาตจากบุคลากรที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

5. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

5.1 สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้ใช้งาน

5.1.1 ส่วนงาน จัดให้มีการอบรมเพื่อสร้างความรู้และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ และรู้เท่าทันต่อภัยคุกคามและผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

5.1.2 กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของส่วนงาน

5.2 การลงทะเบียนบุคลากรใหม่ของส่วนงาน ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนบุคลากรใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกหรือเปลี่ยนแปลงสิทธิการใช้งาน

5.3 การลงทะเบียนผู้ใช้งาน (User Registration)

5.3.1 ผู้ดูแลระบบจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

5.3.2 ผู้ดูแลระบบต้องตรวจสอบบัญชีรายชื่อผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

5.3.3 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิในแต่ละภารกิจ

5.3.4 ผู้ดูแลระบบต้องชี้แจงและแจ้งผู้ใช้งานเป็นลายลักษณ์อักษร เพื่อให้ผู้ใช้งานทราบถึงสิทธิหน้าที่รับผิดชอบ และมาตรการด้านความมั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศ

5.3.5 กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากต้นสังกัดหรือเมื่อมีการเปลี่ยนแปลงตำแหน่ง โอนย้าย ลาออก หรือสิ้นสุดการจ้าง เป็นต้น

5.4 การบริหารจัดการสิทธิผู้ใช้งาน (User Management)

5.4.1 กำหนดระดับสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบและความจำเป็นในการใช้งาน และทบทวนสิทธิอย่างสม่ำเสมอหรืออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่ง โอนย้าย ลาออก หรือสิ้นสุดการจ้าง เป็นต้น

5.4.2 ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศตามหน้าที่รับผิดชอบและจัดเก็บข้อมูลการกำหนดสิทธิให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

5.4.3 ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบ จากต้นสังกัด และผู้บริหาร จัดทำคำร้องเป็นลายลักษณ์อักษร โดยการให้สิทธิพิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษแล้ว จะต้องระงับการใช้งานทันที

5.5 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

5.5.1 ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน ส่งมอบให้ผู้ใช้งานเป็นเอกสารปิดผนึกที่เป็นความลับหรือทางจดหมายอิเล็กทรอนิกส์ (e-mail) เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันที ภายใน 7 วัน หรือใช้งานระบบร่วมกับระบบตรวจสอบสิทธิส่วนกลาง (CMU OAuth) เพื่อความสะดวกในการจัดการ

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

5.5.3 กำหนดให้การกรอกรหัสผิดพลาดได้ไม่เกิน 3 ครั้ง ระบบจะต้องล็อคสิทธิการเข้าถึงของผู้ใช้งาน โดยผู้ใช้งานจะต้องแจ้งความจำนงให้ผู้ดูแลระบบปลดล็อคหรือรีเซ็ตรหัสผ่านใหม่ หรือใช้งานระบบร่วมกับระบบตรวจสอบสิทธิส่วนกลาง (CMU OAuth) เพื่อความสะดวกในการจัดการ

5.5.4 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ 180 วัน

5.6 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างสม่ำเสมอ

5.7 ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

5.8 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) ของบุคลากร

5.8.1 ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของบุคลากรในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

5.8.2 มีการกำหนดการเปลี่ยนแปลงรหัสผ่านของบัญชีผู้ใช้งานของบุคลากร ตามระยะเวลาที่เหมาะสมของแต่ละส่วนงาน ทุก 3 หรือ 6 เดือน เป็นต้น

5.8.3 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ซึ่งผู้ใช้งานที่มีสิทธิสูงสุด จะต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

1) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

2) ต้องควบคุมการใช้งานอย่างเข้มงวด กำหนดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

3) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4) ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

5.9 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

5.9.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

5.9.2 เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

5.9.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูล ในแต่ละชั้นความลับข้อมูล

5.9.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

5.9.5 ต้องกำหนดให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสม เช่น ทุก ๆ 3 หรือ 6 เดือน ขึ้นอยู่กับความสำคัญของข้อมูลที่ผู้ใช้ดูแลรับผิดชอบ

5.9.6 ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของส่วนงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน เป็นต้น

5.10 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

5.10.1 การใช้งานรหัสผ่าน (Password Use)

1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

2) การกำหนดรหัสผ่าน (Password) ที่คาดเดาได้ยาก ซึ่งประกอบด้วย

- กำหนดให้มีความยาวไม่น้อยกว่า 8 ตัวอักษร
- ประกอบด้วย อักษรภาษาอังกฤษตัวพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษประกอบ เช่น ; < > เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสเดิมครั้งสุดท้าย

- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วันเกิด หรือหมายเลขโทรศัพท์ เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม

3) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Password Management) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

4) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยผู้อื่น

5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก 180 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

5.10.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน มีการกำหนดมาตรการป้องกันทรัพย์สินของส่วนงาน และควบคุมไม่ให้มีการวางทรัพย์สินสารสนเทศที่สำคัญในสถานที่ที่ไม่ปลอดภัย โดยมีแนวปฏิบัติดังนี้

1) ผู้ดูแลระบบหรือผู้รับผิดชอบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศและการเข้าใช้งานคอมพิวเตอร์ทันทีเมื่อเสร็จสิ้นการใช้งานหรือพักการใช้งานชั่วคราว (Logout) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2) ผู้ใช้งานจะต้องป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของส่วนงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหาย สูญหาย หรือมีผู้ไม่ประสงค์ดีเข้าถึงระบบและอุปกรณ์โดยไม่ได้รับอนุญาต

3) กำหนดค่าให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

4) กำหนดรหัสผ่านสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ และต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

5) การใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์ เมื่อเสร็จสิ้นแล้วจะต้องทำการ log off ทุกครั้ง

6) มีการควบคุมการเข้า-ออกพื้นที่ โดยผู้ไม่มีส่วนเกี่ยวข้องต้องได้รับอนุญาตก่อนการเข้าถึงพื้นที่ปฏิบัติงาน

5.10.3 ส่วนงานต้องกำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ (Clear Desk and Clear Screen Policy) โดยมีแนวปฏิบัติดังนี้

1) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันที (Logout) ที่เสร็จสิ้นการใช้งาน หรือเมื่อมีเหตุให้ว่างเว้นจากการใช้งาน

2) ผู้ใช้งานต้องกำหนดให้เครื่องคอมพิวเตอร์ล็อคหน้าจอขณะที่ไม่ได้ใช้งานภายในระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

3) ผู้ใช้งานต้องกำหนดรหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

4) กรณีข้อมูลสำคัญที่บันทึกไว้ในสื่อบันทึกข้อมูลเคลื่อนย้ายได้ เช่น ฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่วางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

5) ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

6) การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
1	- แฟลชไดรฟ์ (Flash Drive) - ฮาร์ดดิสก์ (Hard disk) - ฮาร์ดดิสก์พกพา (External Hard disk)	- ทำลายข้อมูลตามแนวทางของ DOD 5220. 22- M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายๆ รอบ - ทุบทำลาย หรือบดให้อุปกรณ์เสียหายไม่สามารถนำไปใช้งานได้
2	แผ่นซีดี / ดีวีดี (CD/DVD)	ใช้วิธีการตัด ทุบ ทำให้สิ้นสภาพการใช้งาน
3	เทป	ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน

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

8) มีการจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก และต้องมีผู้รับผิดชอบคอยควบคุมดูแลตลอดระยะเวลาการส่งมอบ ไม่ปล่อยให้บุคคลภายนอกอยู่ตามลำพังในพื้นที่ปฏิบัติงาน

5.10.4 การใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัยและไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศของส่วนงาน กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

1) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของส่วนงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

2) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของส่วนงานหรือเป็นของบุคคลภายนอก

3) การกระทำใด ๆ ที่เกิดจากการใช้บัญชีชื่อผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

4) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของส่วนงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงสุดของส่วนงาน

5) ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ส่วนงานต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับส่วนงาน ซึ่งส่วนงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

6) ห้ามใช้สินทรัพย์ของส่วนงานที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของส่วนงาน

7) ห้ามใช้ระบบสารสนเทศของส่วนงาน เพื่อก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของส่วนงาน

8) ห้ามใช้ระบบสารสนเทศของส่วนงานเพื่อประโยชน์ทางการค้า

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

5.11 การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for access control) เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของส่วนงาน และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติ ดังนี้

5.11.1 การควบคุมการเข้าถึงสารสนเทศ

1) ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของส่วนงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

2) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

5.11.2 ข้อกำหนดการใช้งานตามภารกิจ เพื่อให้การเข้าถึงและใช้งานสารสนเทศสอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย จึงจำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิและภารกิจ ดังนี้

- กลุ่มผู้บริหาร กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายในการกำกับดูแล เช่น สิทธิการอนุมัติ สิทธิการเข้าถึงรายงานสรุปผล
- กลุ่มของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายจากผู้บริหาร เช่น สิทธิในการกำหนดสิทธิการเข้าใช้งานของผู้ใช้งานในแต่ละระบบตามที่ผู้บริหารมอบหมาย
- กลุ่มผู้ใช้งาน กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายจากผู้บริหารของส่วนงานภายใน เช่น สิทธิการเพิ่ม/แก้ไข/ลบข้อมูล ที่อยู่ในความรับผิดชอบ
- กลุ่มบุคลากรของส่วนงาน กำหนดสิทธิให้สามารถเข้าถึงข้อมูลทั่วไป เช่น สิทธิการอ่านอย่างเดียว
- กลุ่มที่ปรึกษาจากภายนอกหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับส่วนงาน กำหนดสิทธิเฉพาะกิจตามความจำเป็นที่ต้องเข้าถึงข้อมูล
- ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว (Guest) ไม่มีสิทธิในการเข้าถึง

6. การควบคุมการเข้าถึงเครือข่าย (network access control)

6.1 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อควบคุมและป้องกันการบุกรุกได้ อย่างเป็นระบบ

6.2 การเข้าสู่ระบบเครือข่ายภายในของส่วนงาน โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงานก่อนที่จะสามารถใช้งานได้ในทุกกรณี

6.3 การเข้าถึงระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศภายในของส่วนงาน ต้องดำเนินการโดยใช้อุปกรณ์ที่ส่วนงานเป็นผู้จัดหา หรืออุปกรณ์ที่ได้รับอนุญาตซึ่งผ่านการลงทะเบียน

6.4 อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายภายในของส่วนงาน ต้องได้รับการพิสูจน์ตัวตน ด้วยวิธีการที่เหมาะสม ได้แก่ การตรวจสอบความถูกต้องของ Media Access Control Address (MAC) การตรวจสอบความถูกต้องของรหัสประจำเครื่อง 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 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบจากระยะไกลผ่านเครือข่ายภายนอก ต้องได้รับการพิสูจน์ตัวตนของผู้ใช้งานด้วยวิธีการตรวจสอบตั้งแต่ 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) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

6.9 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละ 1 ครั้ง นอกจากนี้การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

6.10 ระบบเครือข่ายทั้งหมดของส่วนงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกส่วนงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

6.11 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของส่วนงานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

6.12 การเข้าสู่ระบบสารสนเทศเครือข่ายภายในของส่วนงาน จากผู้ใช้ทั้งที่อยู่ภายนอกและภายในส่วนงาน โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

6.13 IP Address ภายในของระบบสารสนเทศเครือข่ายภายในของส่วนงาน จำเป็นต้องมีการป้องกันมิให้ส่วนงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถล่วงรู้ข้อมูล

เกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงานได้โดยง่าย

6.14 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

6.15 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บริหารและผู้ดูแลระบบก่อน และต้องจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6.16 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

7. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของส่วนงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ ดังนี้

7.1 ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานด้วยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

1) ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

3) จำกัดการป้อนรหัสผ่าน โดยป้อนรหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง

4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

7.2 การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยกำหนดให้ผู้ใช้งานเลือกใช้ขั้นตอนในการยืนยันตัวตนที่เหมาะสม มีแนวปฏิบัติ ดังนี้

1) ผู้ใช้งานต้องระบุบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (Password) สำหรับยืนยันตัวตนเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศของส่วนงาน

2) การใช้งานบัญชีรายชื่อผู้ใช้งานแบบกลุ่ม ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงานหรือด้านเทคนิค

3) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key หรือเครื่องอ่านลายนิ้วมือ (finger print) เป็นต้น

7.3 การบริหารจัดการรหัสผ่าน (Password Management System) ต้องมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนด

รหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านของผู้ใช้งานที่ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

7.4 ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของส่วนงานที่ได้กำหนดไว้ ให้ดำเนินการดังนี้

1) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุม ในการอนุญาตให้ใช้งานโปรแกรมเป็นรายครั้งไป

2) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาต และยังไม่ผ่านการตรวจสอบ

3) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์หรือละเมิดกฎหมาย อันจะก่อให้เกิดความเสียหายต่อตนเองและต่อส่วนงาน

4) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

5) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

6) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

7.5 กำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (Session Time-Out) เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลา 15 นาที ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้พิจารณาเป็นรายระบบตามความเหมาะสมและจำเป็น เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต และต้องพิสูจน์ตัวตนเพื่อเข้าใช้งาน ระบบอีกครั้ง หลังจากระบบได้ตัดการใช้งานนั้นไปแล้ว

7.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือ แอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา 1 ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หากต้องการเชื่อมต่อใหม่ ต้องพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบอีกครั้ง ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้พิจารณาเป็นรายระบบตามความเหมาะสมจำเป็น

8. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

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

8.1.1 ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามหน้าที่รับผิดชอบ โดยมีผู้บังคับบัญชาเป็นผู้อนุมัติการให้สิทธินั้น และต้องมีการทบทวนสิทธิการใช้งาน อย่างสม่ำเสมอ หรืออย่างน้อยปี ละ 1 ครั้ง

8.1.2 ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา 30 นาที ต้องทำการยุติการใช้งานทันที

8.1.3 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

1) กำหนดสิทธิให้กับผู้ใช้งานระบบโดยการกำหนดบัญชีชื่อผู้ใช้และรหัสผ่าน เพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น

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

3) การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกส่วนงาน กรณีข้อมูลที่เป็นความลับของส่วนงาน ต้องมีการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล

4) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมาย เพื่อดำเนินการใด ๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้น ๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใด ๆ ที่มีผลกระทบต่อระบบ ผู้ดูแลระบบจะต้องเป็นผู้รับผิดชอบ

8.1.4 ต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ พฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ

8.2 การควบคุมระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อส่วนงาน

8.2.1 ต้องแยกระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงออกจากระบบอื่น ๆ ให้ทำงานอยู่บนเครื่องแม่ข่าย (server) โดยไม่ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องควบคุมเครื่องแม่ข่ายที่มีสภาพแวดล้อมเหมาะสม

8.2.2 จัดพื้นที่ควบคุมพิเศษ (ห้องควบคุมเครื่องแม่ข่าย) เพื่อควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้าออกพื้นที่ควบคุมพิเศษ หรือทรัพยากรอื่นใด เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

8.2.3 กำหนดค่าที่ไฟร์วอลล์ เพื่อควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก

8.2.4 มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

8.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ การปฏิบัติงานจากภายนอกส่วนงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

9. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

9.1 ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

9.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานต่อหัวหน้าส่วนงานโดยทันที

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 ซึ่งทำให้สามารถเลี่ยงผ่านกลไกการควบคุมระบบ/แอปพลิเคชันต่าง ๆ ได้นั้น ต้องถูกจำกัดให้เฉพาะผู้ใช้งาน หรือผู้ดูแลระบบที่มีความจำเป็นต้องใช้งานเป็นประจำเท่านั้น สำหรับการใช้งานและการเข้าถึง System Utilities เหล่านั้นโดยบุคคลอื่น ให้พิจารณาอนุมัติในลักษณะชั่วคราวในทุกกรณี

9.7 System Utilities ดังกล่าวข้างต้นต้องถูกแยกออกจากแอปพลิเคชัน และซอฟต์แวร์อื่น ๆ เพื่อประโยชน์ในการจำกัดการเข้าถึง ให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

9.8 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

9.9 ควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบ ดังนี้

9.9.1 ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของสำนักงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

9.9.2 ผู้ดูแลระบบที่ได้รับการอบรมแล้วหรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของส่วนงาน

9.9.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ ต้องมีการขออนุมัติจากหัวหน้าส่วนงาน ก่อนดำเนินการ

9.9.4 ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

9.9.5 กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

9.9.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

9.9.7 วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

9.9.8 จัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

9.10 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

9.10.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวน ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

9.10.2 วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

10. การบริหารจัดการการบันทึกและตรวจสอบ

10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ได้แก่ การบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 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 และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

11. การควบคุมการเข้าใช้งานระบบจากภายนอก

ส่วนงานต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายใน เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

11.1 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของส่วนงาน ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของส่วนงาน การควบคุมบุคคลที่เข้าสู่ระบบของส่วนงานจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

11.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้าส่วนงานก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

11.3 ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับส่วนงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

11.4 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

12. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

12.1 ผู้ใช้งานระบบสารสนเทศ ต้องผ่านการพิสูจน์ตัวตนจากระบบของส่วนงาน สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

12.1.1 การแสดงตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงบัญชีชื่อผู้ใช้งาน (Username)

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

12.2 การเข้าสู่ระบบสารสนเทศของส่วนงานนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี

12.3 การเข้าสู่ระบบสารสนเทศของส่วนงานจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

12.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

13. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

13.1 การปฏิบัติงานจากภายนอกส่วนงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกส่วนงานและระบบงานต่างๆ ภายในส่วนงาน

13.2 การเข้าถึงระบบสารสนเทศของส่วนงานจากระยะไกล ด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับอนุญาตจากหัวหน้าส่วนงาน

13.3 การเข้าสู่ระบบระบบสารสนเทศในส่วนงานจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยบัญชีชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

13.4 ผู้ได้รับอนุญาตเท่านั้นจึงจะสามารถเข้าถึงระบบสารสนเทศและข้อมูลของส่วนงาน โดยไม่ให้สมาชิกภายในครอบครัวหรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

13.5 ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

13.6 ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกส่วนงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อหัวหน้าส่วนงาน

13.7 ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกส่วนงานอย่างน้อยปีละ 1 ครั้ง

หมวด 3 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Use of Personal Computer)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้งานควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของส่วนงาน ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์ส่วนบุคคลที่ส่วนงานอนุญาตให้บุคลากรใช้งาน เป็นทรัพย์สินของส่วนงาน เพื่อใช้ในงานราชการ ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ เพื่อประโยชน์ของส่วนงาน

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลของส่วนงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของส่วนงาน ผู้ใช้งานต้องได้รับอนุญาตจากหัวหน้าส่วนงานก่อนใช้งานเครื่องคอมพิวเตอร์นั้นและผู้ดูแลครุภัณฑ์ของส่วนงาน จะต้องระบุว่าผู้ใดเป็นผู้ครอบครองเครื่องคอมพิวเตอร์นั้น

2.3 ผู้ดูแลระบบของส่วนงาน เป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์ รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล ทั้งนี้ต้องเป็นผู้ที่หัวหน้าส่วนงาน มอบหมายให้ทำหน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

2.4 โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของส่วนงาน ต้องเป็นโปรแกรมที่ส่วนงานซื้อลิขสิทธิ์มา อย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.5 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของส่วนงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรือ อุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

2.6 การเคลื่อนย้ายเครื่องคอมพิวเตอร์ส่วนบุคคลออกนอกพื้นที่ปฏิบัติงานของส่วนงาน จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงาน และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

2.7 การนำเครื่องคอมพิวเตอร์ส่วนบุคคลของส่วนงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจากบุคลากรที่หัวหน้าส่วนงานมอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากหัวหน้าส่วนงาน โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยบุคลากรหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางส่วนงานเท่านั้น

2.8 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบหาไวรัส โดยโปรแกรมป้องกันไวรัส

2.9 ไม่ควรเก็บข้อมูลสำคัญของส่วนงานไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

2.10 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของส่วนงาน

2.11 ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยหลีกเลี่ยงการวางอาหารหรือเครื่องดื่มบริเวณเครื่องคอมพิวเตอร์ และไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

3. การควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้งานต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

3.2 ผู้ใช้งานควรกำหนดรหัสผ่านที่มีคุณภาพตามคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

3.3 ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

3.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.5 ผู้ใช้ต้องทำการลงบันทึกออก (Logout) จากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

4. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

4.1 ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

4.2 ผู้ดูแลระบบสารสนเทศของส่วนมีหน้าที่รับผิดชอบในการติดตั้ง ตรวจสอบการติดตั้ง โปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ภายในส่วนงานที่เชื่อมต่อกับเครือข่ายอินเตอร์เน็ต

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

4.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

4.5 ผู้ใช้งานต้องตรวจสอบว่าข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

5. การสำรองข้อมูลและการกู้คืน

5.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เพื่อป้องกันการสูญหายของข้อมูล

5.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

5.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

หมวด 4 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงานภายนอกส่วนงาน และเป็นการป้องกันทรัพยากรและข้อมูลที่มีค่าของส่วนงานให้เกิดความปลอดภัย ผู้ใช้งานจึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงในการใช้งานเครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์แบบพกพาที่ส่วนงานอนุญาตให้บุคลากรใช้งาน เป็นทรัพย์สินของส่วนงานเพื่อใช้ในงานราชการ ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพ เพื่อประโยชน์ของส่วนงาน

2.2 เครื่องคอมพิวเตอร์แบบพกพาของส่วนงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของส่วนงาน ผู้ใช้งานต้องได้รับอนุญาตจากหัวหน้าส่วนงานของส่วนงานก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลครุภัณฑ์ของส่วนงาน จะต้องระบุว่าผู้ใดเป็นผู้ครอบครองหรือนำไปใช้งาน

2.3 บุคลากรผู้ดูแลระบบสารสนเทศของส่วนงานเป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์ รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพา ทั้งนี้ ต้องเป็นผู้ที่หัวหน้าส่วนงานมอบหมายให้ทำหน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

2.4 โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของส่วนงาน ต้องเป็นโปรแกรมที่ส่วนงานซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.5 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบพกพาของส่วนงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

2.6 การนำเครื่องคอมพิวเตอร์แบบพกพาของส่วนงานไปใช้งานภายนอกพื้นที่ปฏิบัติงานของส่วนงาน จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงาน และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

2.7 การนำเครื่องคอมพิวเตอร์แบบพกพาของส่วนงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจากบุคลากรผู้ดูแลระบบสารสนเทศที่หัวหน้าส่วนงานมอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากหัวหน้าส่วนงาน โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยบุคลากรผู้ดูแลระบบสารสนเทศ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางส่วนงานเท่านั้น

2.8 การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ใส่ในกระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาให้เรียบร้อย เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การหลงลืมอุปกรณ์

2.9 กรณีที่ต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้นโดยเด็ดขาด

2.10 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่ และควรรักษาสภาพคอมพิวเตอร์ให้มีสภาพพร้อมใช้งานตลอดเวลา

2.11 ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.12 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

2.13 ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

2.14 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

3. ความปลอดภัยทางด้านกายภาพ

3.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ดังนั้นควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

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

4. การควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

4.2 หากวางเครื่องคอมพิวเตอร์แบบพกพาไว้นอกสถานที่ปฏิบัติงาน ควรล็อคหน้าจอด้วยตัวเองทุกครั้ง (Logoff) เมื่อไม่ได้อยู่ที่หน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

4.3 ผู้ใช้งานต้องไม่อนุญาตให้บุคคลภายนอกที่ไม่มีความเกี่ยวข้อง ใช้งานเครื่องคอมพิวเตอร์แบบพกพาและไม่บอกรหัสผ่านการล็อคหน้าจอให้แก่ผู้อื่น

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

5.2 บุคลากรผู้ดูแลระบบสารสนเทศของส่วนงาน มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ของส่วนงานเป็นโปรแกรมพื้นฐาน

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

5.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

5.5 หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และต้องรีบแจ้งผู้ดูแลระบบสารสนเทศของส่วนงานโดยเร็ว

6. การสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่น ๆ เพื่อป้องกันการสูญหายของข้อมูล หรือควรจัดเก็บข้อมูลไว้บนคลาวด์

6.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

6.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

หมวด 5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third party access control)

1. วัตุประสงค์

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงานเป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก

2. แนวทางปฏิบัติ

2.1 ต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงานหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงานได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

2.2.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้าส่วนงาน

2.2.2 จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก เพื่อระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนงาน ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

1) เหตุผลในการขอใช้

2) ระยะเวลาในการใช้

3) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

4) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

5) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

2.2.3 หน่วยงานภายนอกที่ปฏิบัติงานให้กับส่วนงาน ไม่ว่าจะทำงานอยู่ภายในหรือภายนอกส่วนงาน จำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลของส่วนงาน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศของส่วนงาน

2.2.4 ส่วนงาน ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

2.2.5 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

2.2.6 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของส่วนงาน ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2.2.7 ส่วนงานมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจว่าส่วนงานสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.2.8 ควรดำเนินการให้ผู้ให้บริการภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

2.3 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

2.3.1 กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

2.3.2 ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

2.3.3 กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับ โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

2.3.4 กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ก่อนการติดตั้ง

2.3.5 การทดสอบซอฟต์แวร์ ห้ามทดสอบบนระบบและฐานข้อมูลที่ใช้งาน ต้องสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

2.4 มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

2.4.1 ผู้ให้บริการภายนอกที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของส่วนงาน จะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้าส่วนงาน

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) และอุปกรณ์เชื่อมต่อระยะไกลทิ้งไว้โดยไม่จำเป็น

ช่องทางดังกล่าว ต้องมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากหัวหน้าส่วนงานก่อนทุกครั้ง

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 สำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงาน เพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

2) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของส่วนงาน

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

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์อย่างปลอดภัย และเป็นการป้องกันไม่ให้เกิดการละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันก่อให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของส่วนงานถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ส่วนงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหัวหน้าส่วนงาน เป็นลายลักษณ์อักษรแล้ว

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

2.3 การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการตรวจสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

2.4 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของส่วนงานนอกเหนือจากเพื่อประโยชน์ของทางราชการ หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เว้นแต่เป็นการดำเนินงานตามภารกิจของส่วนงาน

2.5 ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของส่วนงาน

2.6 ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับส่วนงาน

2.7 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของส่วนงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

2.8 ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.9 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด อันจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.10 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.11 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.12 การใช้งานเว็บบอร์ด (Web Board) ของส่วนงาน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของส่วนงาน

2.13 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของส่วนงาน การทำลายความสัมพันธ์กับบุคลากรของส่วนงานอื่น ๆ

2.14 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

3. แนวทางปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

3.1 ส่วนงานต้องกำหนดแนวปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์ในเวลาราชการ เพื่อให้เกิดการใช้งานในเชิงสร้างสรรค์และเป็นประโยชน์ต่อการดำเนินงาน เช่น ใช้เพื่อการติดต่อสื่อสาร เพื่อการประชาสัมพันธ์ เป็นต้น

3.2 อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่ส่วนงานได้กำหนดไว้เท่านั้น

3.3 หากต้องการใช้งานเครือข่ายสังคมออนไลน์ในลักษณะอื่นใดนอกเหนือจากที่ส่วนงานกำหนด ให้ขออนุญาตจากหัวหน้าส่วนงานก่อนใช้งาน

3.4 ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของส่วนงาน

3.5 ผู้ใช้งานพึงตระหนักว่าข้อความหรือความเห็นที่เผยแพร่บนเครือข่ายสังคมออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุ ให้ร้าย ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

3.6 ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามบัญชีชื่อผู้ใช้ส่วนตัว แต่อาจส่งผลกระทบกับส่วนงานได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์

3.7 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อส่วนงาน ผู้ใช้งานต้องแจ้งต่อหัวหน้าส่วนงานโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

3.8 ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

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

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์ผ่านระบบเครือข่ายของส่วนงาน ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์และบริการคลาวด์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบสารสนเทศวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบสารสนเทศอย่างเคร่งครัด อันจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์และบริการคลาวด์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

2.1 ผู้ใช้งานควรเปลี่ยนรหัสผ่านใหม่ทุก 6 เดือน โดยรหัสผ่านที่เปลี่ยนต้องเป็นรหัสผ่านที่ไม่เคยใช้มาก่อน และเป็นรหัสผ่านที่คาดเดาได้ยาก ตามหลักเกณฑ์การกำหนดรหัสผ่านที่ดี

2.2 ผู้ใช้งาน ไม่ควรใช้โปรแกรมช่วยจำรหัสผ่านหรือกำหนดให้มีการจำรหัสผ่านของจดหมายอิเล็กทรอนิกส์

2.3 ผู้ใช้งานต้องไม่เปิดหน้าจอระบบจดหมายอิเล็กทรอนิกส์ทิ้งเอาไว้ ขณะที่ไม่ได้อยู่หน้าจอ

2.4 ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อส่วนงาน หรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และ ไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

2.5 ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของแล้วเท่านั้น และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.6 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของส่วนงาน เพื่อการติดต่อสื่อสารในนามของของส่วนงานเท่านั้น

2.7 หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Logout ออกจากระบบ และปิดเว็บเบราว์เซอร์ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

2.8 ผู้ใช้ต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด ด้วยโปรแกรมป้องกันไวรัส เป็นการป้องกันการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็น

2.9 ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก หรือไม่น่าไว้ใจ

2.10 ผู้ใช้งานต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์ และใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง และระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป รวมทั้งจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

2.11 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.12 ผู้ใช้งานควรตรวจสอบกล่องเก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

2.13 ผู้ใช้งานควรทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่สำคัญตามความจำเป็นอย่างสม่ำเสมอ

2.14 ข้อควรระวัง ผู้ใช้งานไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

2.15 ผู้ใช้ไม่ควรใช้งานจดหมายอิเล็กทรอนิกส์บนเครื่องคอมพิวเตอร์สาธารณะ เพื่อความปลอดภัยของข้อมูลและบัญชีผู้ใช้งาน

3. แนวทางแนวทางปฏิบัติในการใช้งานบริการคลาวด์

3.1 ผู้ใช้งานควรทำความเข้าใจบริการคลาวด์ของมหาวิทยาลัย (Office 365) ที่ช่วยสนับสนุนการปฏิบัติงานให้มีประสิทธิภาพ เช่น Microsoft Teams, OneDrive, SharePoint เป็นต้น

3.2 ผู้ใช้งานไม่ควรให้บุคคลอื่นที่ไม่ใช่บุคลากรของมหาวิทยาลัยร่วมใช้งานบริการคลาวด์เพื่อประโยชน์ส่วนตัว

3.3 ผู้ใช้งานไม่ควรเก็บข้อมูลที่ละเมิดลิขสิทธิ์ ขัดต่อกฎหมายและศีลธรรมไว้บนบริการคลาวด์

3.4 ผู้ใช้ไม่ควรเปิดใช้งานบริการคลาวด์ทิ้งไว้ โดยไม่ได้อยู่ที่หน้าจอ เพื่อป้องกันข้อมูลรั่วไหล

3.5 ผู้ใช้ไม่ควรใช้งานบริการคลาวด์บนเครื่องคอมพิวเตอร์สาธารณะ เพื่อความปลอดภัยของข้อมูลและบัญชีผู้ใช้งาน

หมวด 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุม ป้องกัน และการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของส่วนงาน เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของส่วนงาน

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของส่วนงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบของส่วนงาน และต้องได้รับการพิจารณาอนุญาตจากหัวหน้าส่วนงาน

2.2 ผู้ดูแลระบบของส่วนงาน กำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่และความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สายของส่วนงาน

2.4 ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access Point: AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

2.5 ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ ทั้งนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

2.6 ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

2.7 ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.8 ผู้ดูแลระบบต้องกำหนดค่าใช้มาตรฐานความปลอดภัยแบบ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ เพื่อให้ยากต่อการดักจับ ช่วยให้ปลอดภัยมากขึ้น

2.9 ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address ร่วมกับบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address บัญชีชื่อผู้ใช้งาน และรหัสผ่านตามที่กำหนดไว้เท่านั้น ในการเชื่อมต่อกับเครือข่ายไร้สายตาม SSID ที่กำหนดไว้ สำหรับบุคคลภายนอก กำหนดให้ใช้งานเครือข่ายไร้สายโดยไม่ควบคุม MAC Address แต่ให้ใช้งานได้ตาม SSID ที่ผู้ดูแลระบบกำหนดแยกเฉพาะสำหรับบุคคลภายนอกเท่านั้น

2.10 ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในส่วนงาน

2.11 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สาย ติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

2.12 ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

หมวด 9 การแบ่งปันข้อมูล
(Information Sharing)

1. วัตุประสงค์

เพื่อกำหนดขั้นตอนในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ และมาตรการบรรเทาผลกระทบที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่อาจได้รับผลกระทบ เพื่อให้สามารถกำหนดเป็นมาตรการป้องกันที่จำเป็นได้

2. แนวทางปฏิบัติในการแบ่งปันข้อมูล

2.1 กำหนดขอบเขตและระดับความลับของข้อมูล โดยให้ความสำคัญกับการระบุขอบเขตของข้อมูลที่จะแบ่งปัน เพื่อให้เหมาะสมกับการแบ่งปันและการเข้าถึงข้อมูล

2.2 มีข้อกำหนดในการแบ่งปันข้อมูล รวมถึงการบริหารจัดการการอนุญาตเพื่อให้มั่นใจได้ว่ามีผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลการแบ่งปันนี้ได้

2.3 มีข้อกำหนดในการใช้ข้อมูลที่ได้รับการแบ่งปัน เช่น การกำหนดขอบเขตการใช้ข้อมูล หรือการห้ามนำข้อมูลไปใช้ในวัตถุประสงค์ที่ไม่เกี่ยวข้อง

2.4 การตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการแบ่งปันข้อมูล รวมถึงการจัดการและควบคุมเพื่อลดความเสี่ยงที่เป็นไปได้

2.5 การฝึกอบรมบุคลากรที่เกี่ยงข้อง เพื่อเพิ่มความเข้าใจในการแบ่งปันข้อมูลและการใช้ข้อมูลอย่างมีประสิทธิภาพ รวมถึงการบันทึกข้อมูลเกี่ยวกับการแบ่งปันข้อมูลเพื่อการติดตามและการประเมินประสิทธิภาพ

2.6 การตรวจสอบและประเมินการแบ่งปันข้อมูลเพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามหลักเกณฑ์และแนวทางที่กำหนดไว้

3. รูปแบบการแบ่งปันข้อมูล

3.1 การแบ่งปันทั่วไป (General Sharing) เป็นการแบ่งปันข้อมูลที่มีความสำคัญและเกี่ยวข้องกับผู้ใช้หลายกลุ่ม โดยไม่จำกัดเฉพาะกับกลุ่มหรือบุคคลใด

3.2 การแบ่งปันตามความจำเป็น (Need-to-Know Sharing) เป็นการแบ่งปันข้อมูลเฉพาะกับบุคคลหรือกลุ่มผู้ใช้ที่จำเป็นต้องมีข้อมูลนั้นเพื่อการปฏิบัติงาน

3.3 การแบ่งปันตามระดับความลับ (Security Clearance-based Sharing) เป็นการแบ่งปันข้อมูลโดยพิจารณาจากระดับความลับของข้อมูล และแบ่งปันเฉพาะกับบุคคลหรือกลุ่มผู้ใช้ตามความเหมาะสม

การเลือกรูปแบบการแบ่งปันข้อมูลจะขึ้นอยู่กับลักษณะของข้อมูล ชั้นความลับ และวัตถุประสงค์ของการแบ่งปันข้อมูล ทั้งนี้ให้ยึดถือประโยชน์ของมหาวิทยาลัยเป็นสำคัญ

หมวด 10 การทำให้ระบบมีความแข็งแกร่ง
(System Hardening)

1. วัตถุประสงค์

เพื่อปรับปรุงและตั้งค่าระบบปฏิบัติการของทรัพย์สินสารสนเทศของส่วนงาน ให้มีความแข็งแกร่งทนทานต่อการถูกโจมตีทางไซเบอร์ เป็นการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และเพิ่มความเชื่อถือได้ของระบบให้แก่ผู้ใช้งาน

2. แนวทางปฏิบัติในการทำให้ระบบมีความแข็งแกร่ง

2.1 ปรับแต่งค่าเริ่มต้นของระบบและแอปพลิเคชัน โดยเปลี่ยนรหัสผ่านตั้งต้น (Default Password) ปิดการใช้งานบริการที่ไม่จำเป็น และปรับเป็นการตั้งค่าที่ปลอดภัย

2.2 เปิดใช้งานเฉพาะ Port ที่มีความจำเป็นเท่านั้น ส่วน Port ใดที่ไม่ได้ใช้งานให้ทำการปิด เพื่อลดความเสี่ยงจากการถูกโจมตีโดยผู้ไม่ประสงค์ดี

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 หากเป็นการเข้าถึงจากภายนอกเครือข่ายของมหาวิทยาลัย

2.7 ต้องติดตั้งซอฟต์แวร์ Antivirus ที่มหาวิทยาลัยจัดสรรให้ ในเครื่องแม่ข่ายหรือทรัพย์สินสารสนเทศของส่วนงาน

2.8 จำกัดสิทธิการเข้าถึงเครื่องแม่ข่ายหรือทรัพย์สินสารสนเทศที่สำคัญเฉพาะผู้ดูแลระบบของส่วนงานเท่านั้น หากมีการปรับเปลี่ยนสิทธิต้องดำเนินการเป็นลายลักษณ์อักษรและอนุมัติโดยหัวหน้าส่วนงาน

หมวด 11 การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Awareness)

1. วัตถุประสงค์

เพื่อเสริมสร้างความรู้ ความเข้าใจ ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรของส่วนงาน เพื่อการตระหนัก และรู้เท่าทันภัยคุกคามทางไซเบอร์ในปัจจุบัน เป็นการลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ทางอ้อม รวมถึงลดความเสี่ยงจากการกระทำผิดกฎหมายที่เกี่ยวข้องโดยรู้เท่าไม่ถึงการณ์

2. แนวปฏิบัติในการสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์

2.1 จัดให้มีการอบรมเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ให้แก่บุคลากรของส่วนงาน อย่างน้อยปีละ 1 ครั้ง

2.2 กำหนดแนวปฏิบัติให้บุคลากรของส่วนงานติดตั้งซอฟต์แวร์ Antivirus ในเครื่องคอมพิวเตอร์ส่วนบุคคลที่ส่วนงานจัดสรรให้ และเครื่องคอมพิวเตอร์แบบพกพาที่นำมาปฏิบัติงานภายในส่วนงาน

2.3 ผู้ใช้ต้องอัปเดท Virus Definition ของซอฟต์แวร์ Antivirus เป็นประจำ อย่างน้อยสัปดาห์ละ 1 ครั้ง

2.4 ผู้ใช้ควรสแกนไวรัสบนสื่อแบบถอดได้ทุกครั้งก่อนนำมาใช้งาน

2.5 ผู้ใช้ไม่ควรใช้งานสื่อแบบถอดได้ที่ได้รับมาจากแหล่งที่ไม่น่าเชื่อถือ เช่น พบว่าตกอยู่บนพื้น หรือวางอยู่บนโต๊ะแบบไม่มีเจ้าของ เพื่อป้องกันซอฟต์แวร์ไม่พึงประสงค์

2.6 ผู้ใช้ต้องไม่ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์จากสื่อต่าง ๆ หรือจากการดาวน์โหลดผ่านเครือข่ายอินเตอร์เน็ต

2.7 ผู้ใช้ต้องมีความระมัดระวังในการใช้งานเว็บไซต์ โดยสังเกตจากชื่อ URL เพื่อป้องกันการถูกขโมยข้อมูลจากผู้ไม่ประสงค์ดี

2.8 ผู้ใช้ต้องมีความระมัดระวังในการใช้งานอีเมล โดยไม่ดาวน์โหลดหรือเปิดไฟล์แนบจากอีเมลที่ไม่น่าเชื่อถือ

2.9 ผู้ใช้ต้องมีความระมัดระวังในการใช้งานโซเชียลมีเดีย เพื่อป้องกันการถูกหลอกลวงโดยผู้ไม่ประสงค์ดี

หมวด 12 การเชื่อมต่อระยะไกล
(Remote Connection)

1. วัตถุประสงค์

เพื่อเป็นการป้องกันความเสี่ยงที่เกี่ยวข้องกับการเชื่อมต่อระยะไกล (Remote Connection) จากการเข้าถึงที่ไม่ได้รับอนุญาตโดยผู้ไม่ประสงค์ดี การเข้าถึงและการใช้งานที่ไม่ปลอดภัยโดยผู้ใช้ หรือการเข้าถึงจากเครือข่ายที่ไม่ปลอดภัย

2. แนวปฏิบัติการเชื่อมต่อระยะไกล

2.1 หลีกเลี่ยงการเชื่อมต่อระยะไกลโดยผู้ใช้ประเภทบุคลากร หากไม่มีความจำเป็นหรือเร่งด่วนใด ๆ

2.2 เครือข่ายของส่วนงานที่อนุญาตให้ผู้ใช้เข้าถึงได้ หากมีความจำเป็นต้องให้มีการเข้าถึงผ่านการเชื่อมต่อระยะไกล ต้องให้เชื่อมต่อผ่าน VPN ที่มหาวิทยาลัยกำหนดไว้เท่านั้น โดยใช้ CMU Account ในการยืนยันตัวตน

2.3 เครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์แบบพกพา ที่ทำการเชื่อมต่อระยะไกลผ่าน CMU VPN ต้องติดตั้งซอฟต์แวร์ Antivirus ที่มหาวิทยาลัยจัดสรรให้

2.4 เครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์แบบพกพา ที่ทำการเชื่อมต่อระยะไกลผ่าน CMU VPN ต้องอัปเดทซอฟต์แวร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ

2.5 ผู้ใช้ต้องไม่มอบบัญชีผู้ใช้งานของตนให้กับผู้อื่น เพื่อใช้งาน CMU VPN ในการเชื่อมต่อระยะไกลกับเครือข่ายของมหาวิทยาลัย

2.6 ผู้ใช้ต้องไม่ใช้เครื่องคอมพิวเตอร์สาธารณะในการเชื่อมต่อระยะไกลกับเครือข่ายของมหาวิทยาลัย

2.7 ส่วนงานต้องมีการประเมินความเสี่ยงในการเชื่อมต่อระยะไกล เพื่อหามาตรการป้องกันแก้ไขปัญหาที่อาจจะเกิดขึ้น

หมวด 13 การรักษาสภาพความพร้อมใช้งานของการให้บริการ (Service Continuity)

1. วัตถุประสงค์

เพื่อมั่นใจได้ว่าระบบสารสนเทศที่ให้บริการและข้อมูลสำคัญของส่วนงาน มีความพร้อมใช้งานอยู่ตลอดและสามารถดำเนินการต่อไปได้ในขณะที่ส่วนงานเผชิญกับภาวะวิกฤตหรือภัยพิบัติ เพื่อลดผลกระทบที่อาจเกิดขึ้นกับส่วนงาน โดยมีการลำดับความสำคัญจากผลกระทบจากความเสียหายของทรัพย์สิน และผลการวิเคราะห์ความเสี่ยง เพื่อใช้ในการพิจารณาวิธีการสร้างความต่อเนื่อง

2. แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

2.1 เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีความสำคัญ ต้องมีการสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน

2.2 ผู้ดูแลระบบต้องสำรองข้อมูลและซอฟต์แวร์เก็บไว้ โดยคัดเลือกและจัดเรียงลำดับตามผลกระทบจากความสูญเสียของระบบที่มีผลต่อภารกิจหลักของส่วนงาน

2.3 ต้องมีขั้นตอนการปฏิบัติการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

2.4 ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองในสื่อบันทึกข้อมูลสำรอง โดยมีการแสดงชื่อระบบที่สำรอง วัน เดือน ปี และเวลาในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง และต้องมีการทดสอบสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

2.5 หัวหน้าส่วนงานต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมฉุกเฉิน

2.6 ส่วนงานต้องดำเนินการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินปีละ 1 ครั้ง

2.7 ผู้ดูแลระบบต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยระบบสารสนเทศได้ตามปกติ โดยต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวอย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

หมวด 14 การตรวจสอบและรับมือภัยคุกคามทางไซเบอร์
(Detect & Response)

1. วัตถุประสงค์

เพื่อให้มีกระบวนการตรวจสอบ เฝ้าระวังภัยคุกคามทางไซเบอร์ และการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Detect & Response) ในระดับส่วนงาน เพื่อการแก้ไขและป้องกันในเบื้องต้นก่อนแจ้งให้มหาวิทยาลัยทราบในลำดับถัดไป

2. แนวทางปฏิบัติในการตรวจสอบและรับมือภัยคุกคามทางไซเบอร์

2.1 ส่วนงาน ต้องมอบหมายให้มีผู้ที่ทำหน้าที่ในการตรวจสอบและรับมือภัยคุกคามทางไซเบอร์ เพื่อแก้ไขและป้องกันปัญหาในเบื้องต้นก่อนแจ้งให้มหาวิทยาลัยทราบ

2.2 เมื่อส่วนงานพบเหตุที่ประเมินแล้วว่าอยู่ในระดับวิกฤต ต้องรีบแจ้งหัวหน้าส่วนงาน และดำเนินการป้องกันแก้ไขในเบื้องต้น ก่อนที่จะรายงานให้กับมหาวิทยาลัยทราบผ่านระบบ Ticket Management System (CMU TMS) ที่ URL: https://incident.csd.itsc.cmu.ac.th/

2.3 ส่วนงานต้องบันทึกเหตุและการเผชิญเหตุในระบบ CMU TMS ทุกครั้ง ถึงแม้ว่าจะสามารถแก้ไขปัญหาภัยคุกคามนั้น ๆ ได้แล้ว

2.4 ส่วนงานต้องมอบหมายให้ผู้ที่รับผิดชอบตามข้อ 2.1 เข้าร่วมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ที่มหาวิทยาลัยจัดขึ้นทุกครั้ง

2.5 ส่วนงานต้องกำหนดผู้รับผิดชอบด้านการรับมือภัยคุกคามทางไซเบอร์ ตามแนวทางที่มหาวิทยาลัยกำหนด และทบทวนเป็นประจำทุกปี

2.6 ส่วนงานต้องมอบหมายให้ผู้ที่รับผิดชอบตามข้อ 2.1 และผู้ที่เกี่ยวข้องร่วมฝึกซ้อมแผนรับมือภัยคุกคามทางไซเบอร์ร่วมกับมหาวิทยาลัยเป็นประจำทุกปี

หมวด 15 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

1. วัตถุประสงค์

เพื่อให้ส่วนงานมีความพร้อมในการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ด้วยการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของส่วนงานสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงการฝึกซ้อมแผน BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

2. แนวปฏิบัติการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

2.1 ส่วนงานต้องมีการมอบหมายให้มีผู้ทำหน้าที่จัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) จากความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์อย่างเป็นทางการหรือลายลักษณ์อักษร

2.2 ส่วนงานต้องมีการสำรองข้อมูลหรือระบบที่สำคัญนอกเหนือจากการดูแลของสำนักบริการเทคโนโลยีสารสนเทศ เป็นประจำตามระดับความสำคัญของข้อมูลและระบบ ตามที่ได้ทำการวิเคราะห์ความเสี่ยงแล้ว

2.3 ส่วนงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) จากความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ และต้องมีการจัดเตรียมทรัพย์สินสารสนเทศสำรองให้ครบถ้วนตามที่ระบุไว้ในแผน

2.4 ส่วนงานต้องมีการฝึกซ้อมแผน BCP ตามข้อ 2.3 อย่างน้อยปีละ 1 ครั้งเพื่อประเมินประสิทธิภาพของแผนต่อภัยคุกคามทางไซเบอร์ ในรูปแบบที่เหมาะสมและจัดทำเป็นเอกสารรายงาน

2.5 ส่วนงานต้องมีการทบทวนแผน BCP ตามข้อ 2.3 อย่างน้อยปีละ 1 ครั้งเพื่อปรับปรุงเปลี่ยนแปลงให้มีความเหมาะสมและทันต่อเหตุการณ์

หมวด 16 การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management)

1. วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์การตรวจสอบและประเมินความเสี่ยงของระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศของส่วนงาน ให้มั่นใจได้ว่าความเสี่ยงของระบบสารสนเทศของส่วนงานได้ถูกพิจารณาและได้มีการจัดเตรียมมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับส่วนงานได้

2. แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2.1 ระบุความเสี่ยงให้สอดคล้องกับความเสี่ยงที่อาจจะเกิดขึ้น ดังนี้

2.1.1 ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายของส่วนงานผ่านเครือข่ายอินเทอร์เน็ต

2.1.2 ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายของส่วนงานโดยไม่ได้รับอนุญาต

2.1.3 ความเสี่ยงที่เกิดจากเครื่องมือสารสนเทศหรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

2.1.4 ความเสี่ยงที่เกิดจากการลงบันทึกเข้าใช้งาน (Login) สารสนเทศที่สำคัญของส่วนงานผ่านระบบเครือข่ายที่ไม่ปอลดภัย เช่น เครือข่ายอินเตอร์เน็ตสาธารณะ เป็นต้น

2.1.5 ความเสี่ยงอื่นที่เกี่ยวข้องกับระบบสารสนเทศของส่วนงาน ที่อาจจะส่งผลกระทบกับการปฏิบัติงานของส่วนงาน

2.2 การตรวจสอบและประเมินความเสี่ยง ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น ให้คำนึงถึงองค์ประกอบดังต่อไปนี้

2.2.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ ทำการประเมินในแต่ละด้านของผลกระทบโดยให้พิจารณาถึงมาตรการควบคุมที่มีอยู่ในปัจจุบันด้วย

2.2.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่จะเกิดขึ้น ต้องพิจารณา 2 ปัจจัยหลัก คือ

1) แนวโน้มการเกิดขึ้นของเหตุการณ์ความเสี่ยง โดยพิจารณาจากความน่าจะเป็นหรือค่าทางสถิติที่มีการบันทึกไว้ เช่น เหตุการณ์ความเสี่ยง เหตุภัยธรรมชาติต่าง ๆ เป็นต้น

2) ความยากง่ายที่จะถูกกระทำ ให้พิจารณาจากจุดอ่อนหรือข้อบกพร่องที่มีอยู่และตัวควบคุมในปัจจุบัน หากมีจุดอ่อนหรือข้อบกพร่องมากและไม่มีตัวควบคุมเลย โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงจะสูงกว่าในกรณีที่มีตัวควบคุมอยู่

2.2.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ พิจารณาข้อบกพร่องของระบบหรือข้อบกพร่องของการควบคุมที่ปัจจุบันอาจจะไม่มีอยู่ และจะส่งผลให้ระบบไม่มีความมั่นคงปลอดภัยที่ดี

2.2.4 ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบสารสนเทศของส่วนงานอย่างน้อยปีละ 1 ครั้ง

2.2.5 การตรวจสอบจะต้องดำเนินการโดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของส่วนงาน (Internal Auditor) อย่างน้อยปีละ 1 ครั้ง

2.3 รายละเอียดเพิ่มเติมของการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สามารถศึกษาเพิ่มเติมได้ในเอกสารรหัส CMU-CS-002 “แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์”

หมวด 17 การกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Duty and responsibility)

1. วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ระดับส่วนงานของผู้บริหารส่วนงาน (รองคณบดี รองผู้อำนวยการ) หัวหน้าฝ่าย/งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และผู้ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร

2. แนวทางปฏิบัติ

2.1 ระดับนโยบาย

2.1.1 ผู้บริหารส่วนงานที่ได้รับมอบหมายจากหัวหน้าส่วนงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่ส่วนงานหรือบุคลากร อันเนื่องมาจากความบกพร่อง ละเลย หรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

2.1.2 ผู้บริหารส่วนงานที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศของส่วนงาน เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะและคำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

2.2 ระดับปฏิบัติการ

ระดับผู้ปฏิบัติงานประกอบด้วย ผู้ดูแลระบบสารสนเทศของส่วนงาน ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจดังนี้

2.2.1 ผู้ดูแลระบบสารสนเทศ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นผู้รับผิดชอบ ดังนี้

1) ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

2) เป็นผู้ประสานงานและร่วมปฏิบัติตามแผนรับมือภัยคุกคามทางไซเบอร์ของมหาวิทยาลัย

3) ควบคุม ดูแล รักษาความปลอดภัยและบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของส่วนงาน

4) ทำการสำรองข้อมูลหรือเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนดของส่วนงาน

5) ป้องกันและเฝ้าระวังภัยคุกคามทางไซเบอร์ในระดับส่วนงาน และแจ้งเหตุให้มหาวิทยาลัยทราบทันทีที่เกิดเหตุภัยคุกคามทางไซเบอร์ผ่านระบบ CMU TMS (หมวดที่ 14 ข้อ 2.2)

6) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยไซเบอร์ของส่วนงาน

2.2.2 ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของส่วนงานตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้อย่างเคร่งครัด