ประมวลแนวปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

โดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

2569

สารบัญ

บทนำ

หลักการ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

ขอบเขตการใช้

ใช้ภายในหน่วยงานทั้งหมดภายใต้สังกัดสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

คำนิยาม

คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม.	หมายถึง	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
หน่วยงานของรัฐ	หมายถึง	หน่วยงานของรัฐตามที่กฎหมายกำหนด
บริการที่สำคัญ	หมายถึง	ภารกิจหรือบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49
สำนักงาน	หมายถึง	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
สป.กษ.	หมายถึง	สำนักงานปลัดกระทรวงเกษตรและสหกรณ์
ดัชนีชี้วัดความเสี่ยงที่สำคัญ	หมายถึง	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย
ผู้ให้บริการภายนอก	หมายถึง	บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

		หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ทั้งนี้ ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์และบริการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
คอมไพเลอร์	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
แพตช์	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สป.กษ. ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

1.1 กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

1.2 บริการที่สำคัญตามผลการวิเคราะห์ในข้อ 1.1

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สป.กษ. กำหนดให้ต้องมีการประเมินอย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น รวมถึงให้มีแนวทางในการดำเนินงาน การกำกับดูแลในช่วงสถานการณ์ที่เกิดขึ้น และให้สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที โดยต้องประกอบไปด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

2.1 การประเมินความเสี่ยง (Risk Assessment)

1) การระบุความเสี่ยง (Risk Identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่างๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

2) การวิเคราะห์ความเสี่ยง (Risk Analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

3) การประเมินค่าความเสี่ยง (Risk Evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

2.2 การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสม สอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยง และผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

2.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

การติดตามและทบทวนความเสี่ยง ควรมีการดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการ

ภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นรวมถึงการแก้ไขปัญหาที่ถูกต้องและมีประสิทธิภาพ

2.4 การรายงานความเสี่ยง (Risk Reporting)

ให้มีการรายงานเหตุการณ์ความเสี่ยง ระดับความเสี่ยง และผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ทุกครั้ง

ทั้งนี้ต้องทบทวนระเบียบวิธีปฏิบัติ และกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากลอย่างมีนัยสำคัญ เป็นต้น

3. แผนการรับมือภัยคุกคามทางไซเบอร์

3.1 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กษ. ต้องจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan : CIRP) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

3.2 ให้มีการตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของ สป.กษ.

3.3 ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง

3.4 ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของ สป.กษ.

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify)

สป.กษ. จะต้องประเมินความเสี่ยง ว่าแต่ละทรัพย์สิน หรือข้อมูล มีโอกาสถูกโจมตีมากน้อยเพียงใด ผลกระทบหากถูกโจมตีรุนแรงเพียงใด การระบุ และประเมินความเสี่ยงอย่างชัดเจน เพื่อช่วยให้กระบวนการอื่น ได้แก่ การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการฟื้นฟู (Recover) มีประสิทธิภาพ มุ่งเน้นไปยังจุดที่อ่อนแอ เพื่อสร้างเกราะป้องกันได้ตรงจุด

1.1 การจัดการสินทรัพย์ (Asset Management)

สป.กษ. จัดทำรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศทั้งหมดที่อยู่ในสภาพแวดล้อมของหน่วยงาน ซึ่งเป็นข้อมูลพื้นฐานที่จำเป็นสำหรับการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ และเป็นจุดเริ่มต้นสำคัญในการดำเนินการระบุทรัพย์สินที่มีความสำคัญ ที่ต้องได้รับการปกป้องอย่างเข้มงวด ไม่ว่าจะเป็นฮาร์ดแวร์ ซอฟต์แวร์ โครงสร้างพื้นฐานเสมือน (Virtual Infrastructure) และข้อมูล เนื่องจากจะช่วยให้มีโอกาสดำเนินการป้องกันหรือแก้ไขก่อนที่จะเกิดเหตุภัยคุกคามทางไซเบอร์ โดยมีการดำเนินการการจัดการทรัพย์สิน ดังนี้

1) จัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

2) ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

3) มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือหากมีการเปลี่ยนแปลงใดๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าว

4) มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญตามรายการที่ระบุไว้ในทะเบียนทรัพย์ อย่างน้อยปีละ 1 ครั้ง

1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

1) ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) และจัดทำทะเบียนประเมินความเสี่ยง

2) กำหนดปัจจัยต่างๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยงที่เกิดขึ้นจากปัจจัยภายนอก เช่น สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

3) ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4) กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ ระบุโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง การระบุผลกระทบของเหตุการณ์ความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

5) วิเคราะห์และประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงทรัพย์สินของระบบสารสนเทศที่สำคัญ โดยมีการบริหารจัดการความเสี่ยง ดังนี้

5.1) จัดทำแผนการลดความเสี่ยง โดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

5.2) นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

5.3) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผน และรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะๆ จนกระทั่งเสร็จสิ้น

1.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

1) ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่างๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ หรือจากแหล่งอื่นที่น่าเชื่อถือ

2) ประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญ

3) ดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็น

4) การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

4.1) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

4.2) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

4.3) ตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

5) การประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

6) การทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบสารสนเทศ (Information Technology : IT) ที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing) เพื่อให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบ

7) ตรวจสอบขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ

8) ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบการรักษาความปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

9) ผู้ให้บริการทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ ต้องมีการรับรอง และได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ หรือเป็นไปตามที่กฎหมายกำหนด

10) การทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การควบคุมดูแลของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

11) ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบ และจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤติ และระดับสูง

12) ดำเนินการส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ หากมีการร้องขอจาก กกม. หรือ สกมช. ทราบภายใน 30 วันนับจากที่ได้รับการร้องขอ

1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

1) แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินการใดๆ ก็ตามในส่วนของบริการที่สำคัญของ สป.กษ.

2) กำหนดให้ผู้ให้บริการภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของหน่วยงาน เพื่อให้หน่วยงานได้รับทราบอย่างทันการณ์และสามารถประเมินผลกระทบที่มีต่อหน่วยงาน ทั้งนี้หากหน่วยงานประเมินแล้วพบว่าผลกระทบที่เกิดขึ้นมีผลต่อการดำเนินการของหน่วยงานอย่างมีนัยสำคัญ หน่วยงานต้องมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติดังกล่าว

3) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

3.1) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทางธุรกิจของ สป.กษ. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

3.3) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

3.4) สิทธิของ สป.กษ. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (Right to Audit)

4) สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา เช่น การตรวจสอบโดยบุคคลที่สามและการตรวจสอบผลิตภัณฑ์

5) ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

6) ทบทวนการประเมินศักยภาพ การประเมินผลการปฏิบัติงาน และการประเมินความเสี่ยงของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกทั้งในด้านประสิทธิภาพ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎหมาย เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่กำหนด ทั้งนี้ ควรดำเนินการทบทวนดังกล่าวอย่างน้อยปีละ 1 ครั้ง รวมถึงให้รายงานผลการประเมินดังกล่าวต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กษ.

7) รักษาความมั่นคงปลอดภัยไซเบอร์ในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารกับผู้ให้บริการภายนอกให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

8) กำหนดให้ผู้ให้บริการภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่อาจมีผลกระทบกับการให้บริการ โดยให้แจ้งล่วงหน้าในระยะเวลาที่ตกลงร่วมกัน เพื่อให้หน่วยงานพิจารณาแนวทางการลดผลกระทบต่อการให้บริการกับผู้ใช้งานของ สป.กษ.

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

2.1 การควบคุมการเข้าถึง (Access Control)

1) การเข้าถึงบริการที่สำคัญของ สป.กษ. ถูกจำกัดไว้ที่

1.1) บุคลากร/เจ้าหน้าที่ ที่ปฏิบัติงานให้ สป.กษ.

1.2) อุปกรณ์ และอินเทอร์เฟซ (Interface) ของบุคลากร/เจ้าหน้าที่ ที่ปฏิบัติงานให้ สป.กษ.

2) ให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของ สป.กษ. ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหลดการเข้าถึงบริการที่สำคัญ

3) เก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

4) ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้น และทำภายใต้การดูแลของ สป.กษ.

2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

1) เสริมสร้างความแข็งแกร่งของระบบ เพื่อช่วยลดพื้นผิวที่ถูกโจมตีเป็นประจำ

2) สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ

3) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

3.1) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

3.2) การแบ่งแยกหน้าที่ (Separation of Duties)

3.3) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

3.4) การลบบัญชีที่ไม่ได้ใช้

3.5) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Complier) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

3.6) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

3.7) การป้องกันมัลแวร์ (Malware)

3.8) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันต่อเหตุการณ์และเหมาะสม

4) มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนจะมีทรัพย์สินใดๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

5) ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อการรับมือกับภัยคุกคามทางไซเบอร์

6) จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

รายละเอียดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)	N/A	สิทธิพิเศษในการเข้าถึงน้อยที่สุดต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติ และทบทวนการแบ่งแยกหน้าที่ (Separation of Duties) อย่างน้อยปีละ 1 ครั้ง	สิทธิพิเศษในการเข้าถึงน้อยที่สุดต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติโดยมีการกำหนดสิทธิจากส่วนกลาง และทบทวนการแบ่งแยกหน้าที่ (Separation of Duties) อย่างน้อยปีละ 1 ครั้ง
(ข) การแบ่งแยกหน้าที่ (Separation of Duties)	N/A	การแบ่งแยกหน้าที่ต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติ และทบทวนการแบ่งแยกหน้าที่อย่างน้อยปีละ 1 ครั้ง	การแบ่งแยกหน้าที่ต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติโดยมีการกำหนดสิทธิจากส่วนกลาง และทบทวนการแบ่งแยกหน้าที่ อย่างน้อยปีละ 1 ครั้ง
(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน	รหัสผ่านต้องยาวกว่า 8 ตัวอักษร	รหัสผ่านต้องยาวกว่า 10 ตัวอักษรและควรมีการใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication)	รหัสผ่านต้องยาวกว่า 12 ตัวอักษรและต้องมีการใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication)
(ง) การลบบัญชีที่ไม่ได้ใช้	ลบบัญชีที่ไม่ได้ใช้หรือปิดการใช้งานไว้ (Disable) ภายใน 72 ชั่วโมงเมื่อสิ้นสุดกิจกรรม	ลบบัญชีที่ไม่ได้ใช้หรือปิดการใช้งานไว้ (Disable) ภายใน 48 ชั่วโมงเมื่อสิ้นสุดกิจกรรม	ลบบัญชีที่ไม่ได้ใช้หรือหรือปิดการใช้งานไว้ (Disable) ทันทีเมื่อสิ้นสุดกิจกรรม
(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)	ตรวจสอบการลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application) ก่อนนำมาใช้งาน และตรวจสอบ	ตรวจสอบการลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application) ก่อนนำมาใช้งาน และตรวจสอบอย่างน้อย	ตรวจสอบการลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application) ก่อนนำมาใช้งาน และตรวจสอบ

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
	อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	ไตรมาสละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	อย่างน้อยเดือนละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน	ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน และมีการป้องกันการเข้าถึงพอร์ตทางกายภาพ	ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน มีการป้องกันการเข้าถึงพอร์ตทางกายภาพ และมีการป้องกันการเข้าถึงทางกายภาพ เช่น มีกรงกั้น มีรั้ว และการควบคุมการเข้าถึงทางกายภาพ	ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งานโดยควบคุมจากส่วนกลาง เช่น ระบบบริหารจัดการจากศูนย์กลาง (Active Directory: AD) เป็นต้น และมีการป้องกันการเข้าถึงพอร์ตทางกายภาพ มีการป้องกันการเข้าถึงทางกายภาพ เช่น มีกรงกั้น มีรั้ว และการควบคุมการเข้าถึงทางกายภาพ
(ช) การป้องกันมัลแวร์ (Malware)	อัพเดทฐานข้อมูลสำหรับการตรวจสอบรูปแบบมัลแวร์ (Signature) และเวอร์ชันของซอฟต์แวร์สำหรับการป้องกันมัลแวร์อยู่อย่างสม่ำเสมอ	อัพเดทฐานข้อมูลสำหรับการตรวจสอบรูปแบบมัลแวร์ (Signature) และเวอร์ชันของซอฟต์แวร์สำหรับการป้องกันมัลแวร์อยู่อย่างสม่ำเสมอ	อัพเดทฐานข้อมูลสำหรับการตรวจสอบรูปแบบมัลแวร์ (Signature) และเวอร์ชันของซอฟต์แวร์สำหรับการป้องกันมัลแวร์อยู่อย่างสม่ำเสมอและมีการส่งล็อก (Log) ไปยังระบบส่วนกลางเพื่อตรวจจับและวิเคราะห์ความผิดปกติ รวมถึงมีเทคโนโลยีขั้นสูงอื่น ๆ เช่น IDS, IPS, EDR เป็นต้น
(ซ) การปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม	ปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน 7 วัน เมื่อมีแพตช์ระดับวิกฤต	ปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน 72 ชั่วโมง เมื่อมีแพตช์ระดับวิกฤต	ปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน 48 ชั่วโมง เมื่อมีแพตช์ระดับวิกฤต

2.3 การเชื่อมต่อระยะไกล (Remote Connection)

1) ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ ได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

2) สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้

2.1) เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็น

2.2) ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

2.3) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

2.4) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

2.5) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

2.6) โอนย้ายทรัพยากรที่มีความเสี่ยงสูงไปยังเครื่องแม่ข่ายที่มีความสามารถในการปกป้องทรัพยากรดังกล่าว (Migrate High-Risk Resources to Servers that Assume Responsibility for Protecting them) เช่น กำหนดให้ผู้ปฏิบัติงานจากระยะไกลต้องเชื่อมต่อกับเครื่องแม่ข่ายเทอร์มินัลที่เก็บข้อมูลสำคัญที่ผู้ปฏิบัติงานจากระยะไกลจำเป็นต้องใช้

2.7) จัดเก็บและอนุญาตเข้าถึงข้อมูลที่จำเป็นเท่านั้น (Store and Access Only the Minimum Data Necessary) ในกรณีที่หน่วยงานให้บุคลากรยืมอุปกรณ์ หน่วยงานควรล้าง (Wipe) ข้อมูลทั้งหมดก่อนและหลังการทำงานจากระยะไกลที่มีความเสี่ยงสูง (เช่น บุคลากรทำงานขณะการเดินทางไปต่างประเทศ) หน่วยงานควรใส่เฉพาะข้อมูลและแอปพลิเคชันที่ได้รับอนุญาตและจำเป็นสำหรับการทำงานจากระยะไกลเท่านั้นในอุปกรณ์สำหรับการให้ยืมดังกล่าว หน่วยงานอาจกำหนดให้บุคลากรใช้อุปกรณ์ดังกล่าวสำหรับการทำงานจากระยะไกลเท่านั้น และไม่อนุญาตเชื่อมต่อกับเครือข่ายภายในหน่วยงาน

2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

1) กำหนดมาตรฐานควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา โดยต้องดำเนินการ

1.1) ลงทะเบียนสื่อเก็บข้อมูลแบบถอดได้ (Removable Media Register)

1.2) ติดฉลากสื่อเก็บข้อมูลแบบถอดได้ (Labelling Media)

1.3) กำหนดชั้นความลับสื่อเก็บข้อมูลแบบถอดได้ (Classifying Media)

1.4) จัดประเภทหรือกำหนดชั้นความลับให้กับสื่อเก็บข้อมูลแบบถอดได้ใหม่ (Reclassifying Media)

1.5) จัดการสื่อเก็บข้อมูลแบบถอดได้ (Handling Media)

1.6) ใช้สื่อเก็บข้อมูลแบบถอดได้อย่างปลอดภัย (Using Removable Media Safely)

- ติดตั้งซอฟต์แวร์ป้องกันไวรัสบนคอมพิวเตอร์
- ปิดใช้งานคุณสมบัติการเล่นอัตโนมัติและการเปิดใช้งานอัตโนมัติของคอมพิวเตอร์ (Disable Computer's Autoplay and Auto-Run Features)

- ใส่รหัสผ่านป้องกันอุปกรณ์สื่อเก็บข้อมูลแบบถอดได้ (Password Protect Removable Media Devices)
- กำจัดข้อมูลที่อ่อนไหวบนอุปกรณ์สื่อเก็บข้อมูลแบบถอดได้ เมื่อใช้เสร็จแล้ว (Clear Removable Media Devices of Sensitive Data)
- เข้ารหัสข้อมูล (Encrypt the Data)
- ห้ามใช้สื่อเก็บข้อมูลแบบถอดได้ หากไม่มีหรือไม่สามารถระบุเจ้าของสื่อดังกล่าว (Prohibit the Use of Removable Storage Medias when Such Medias Have No Identifiable Owner)

1.7) ลบข้อมูลทั้งหมดจากสื่อเก็บข้อมูลแบบถอดได้ก่อนใช้ครั้งแรก (Sanitizing Media Before First Use)

1.8) ใช้สื่อเก็บข้อมูลแบบถอดได้ในการถ่ายโอนข้อมูล (Using Media for Data Transfers)

1.9) ควบคุมการใช้สื่อแบบถอดได้ร่วมกับส่วนประกอบของระบบ (Control the Use of Removable Media on System Components)

1.10) ตรวจสอบการควบคุมการเชื่อมต่อ

2) เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) บทบาทหน้าที่ความรับผิดชอบ กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การประชาสัมพันธ์และสื่อสารผ่านช่องทางต่างๆ ที่ สป.กษ. กำหนดให้กับบุคลากรในหน่วยงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ อย่างน้อยปีละ 1 ครั้ง รวมถึงทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้เนื้อหามีความเป็นปัจจุบัน และมีรายละเอียด ที่เหมาะสม

2.6 การแบ่งปันข้อมูล (Information Sharing)

1) กำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว

1.1) กำหนดช่องทาง และผู้ที่เกี่ยวข้องในการแบ่งปันข้อมูลให้ชัดเจน และจะต้องสื่อสารให้กับบุคลากร และผู้มีส่วนได้เสียทุกคนได้ทราบ

1.2) กำหนดเกณฑ์ของการเป็นเหตุการณ์ หรือภัยคุกคามทางไซเบอร์ที่จะต้องรายงานแก่ผู้ที่เกี่ยวข้อง รวมถึงการต้องแจ้งตามที่กำหนดไว้ในกฎหมาย เช่น การแจ้งหน่วยงานกำกับหรือผู้ที่ได้รับผลกระทบ

1.3) แยกประเภทหมวดหมู่ชั้นความลับ และความอ่อนไหวของข้อมูล และมีขั้นตอนในการแบ่งปันข้อมูลแต่ละประเภทที่แตกต่างกัน

1.4) มีช่องทางในการแบ่งปันข้อมูลแบบปลอดภัย และมีการเข้ารหัสข้อมูลหากข้อมูลนั้นเป็นความลับ หรือมีความอ่อนไหว

1.5) ก่อนทำการแบ่งปันข้อมูล ควรพิจารณาเรื่องการคุ้มครองข้อมูลส่วนบุคคลด้วย และหากมีข้อมูลส่วนบุคคลที่ไม่จำเป็นต้องแบ่งปัน จะต้องทำให้ข้อมูลนั้นเป็นข้อมูลนิรนามเสียก่อน (Anonymization)

1.6) มีข้อตกลงในการแบ่งปันข้อมูลกับหน่วยงานภายนอก โดยคำนึงถึงความมั่นคงปลอดภัย ธรรมาภิบาลข้อมูล และไม่ขัดต่อกฎหมายที่เกี่ยวข้อง และระดับความมั่นคงปลอดภัยและธรรมาภิบาลข้อมูลของหน่วยงานภายนอกควรจะอยู่ระดับเดียวกันหรือสูงกว่าหน่วยงานเจ้าของข้อมูล

1.7) สร้างวัฒนธรรมการแบ่งปันข้อมูลข้ามฝ่ายงานภายในหน่วยงาน และระหว่างหน่วยงาน

2) ควรมีการทบทวนกฎระเบียบของการแบ่งปันข้อมูลเป็นประจำ

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

มีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และวิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงระบุภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น โดยเฉพาะที่เกี่ยวข้องกับบริการที่สำคัญของ สป.กษ. โดยต้องมีการทบทวนกลไกและกระบวนการ อย่างน้อยปีละ 1 ครั้ง

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

4.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม การทบทวน และปรับปรุงตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้การรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง

4.3 การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

มีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ โดยกำหนดวัตถุประสงค์ของการฝึกซ้อมให้ชัดเจน รวบรวมผู้มีส่วนได้เสียให้ครบถ้วน ออกแบบสถานการณ์จำลองเสมือนจริง และทำการฝึกซ้อมโดยยึดแนวทางตามแผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งมีการตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

และมีการปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญเพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ โดยประสานงาน

กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อถูกร้องขอข้อมูล และประสานกับหน่วยงานกำกับ หรือคณะกรรมการอื่น ๆ ที่กำกับดูแลด้วย

5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

5.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

1) จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อให้พิจารณาความสอดคล้องกับแผนของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

2) การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) และกำหนดบริการสำคัญที่ส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ (Business Impact Analysis : BIA)

3) บริหารแผนความต่อเนื่องทางธุรกิจ

4) ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

1. ผู้ใช้งานทั่วไป

ส่วนที่ 1 การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

เพื่อให้การเข้าถึงและการควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย กำหนดให้ผู้ดูแลระบบมีแนวปฏิบัติดังนี้

1.1 การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล

1.1.1 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

1.1.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

1.1.2.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น
   - อ่านอย่างเดียว (Read)
   - สร้างข้อมูล/ป้อนข้อมูล
   - แก้ไข (Edit)
   - ลบ (Delete)
   - อนุมัติ (Authorize)
   - ไม่มีสิทธิ์
2) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้
3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศขององค์กรจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
4) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศขององค์กรจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

1.2 การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

สป.กษ. ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

1.2.1 จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการปฏิบัติงานและการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลด้านการเกษตร ข้อมูลเตือนภัยด้านการเกษตร ข้อมูลเพื่อการติดต่อประสานงาน เป็นต้น

1.2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ ดังนี้

- ระดับที่ 1 ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ระดับที่ 2 ข้อมูลที่มีระดับความสำคัญปานกลาง
- ระดับที่ 3 ข้อมูลที่มีระดับความสำคัญน้อย

1.2.3 จัดแบ่งลำดับชั้นความลับของข้อมูลดังนี้

- ข้อมูลลับที่สุด หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

1.2.4 การจัดแบ่งระดับชั้นการเข้าถึง

- ระดับที่ 1 ระดับชั้นสำหรับผู้บริหาร
- ระดับที่ 2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับที่ 3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

1.2.5 การกำหนดเวลาในการเข้าถึงข้อมูล

การเข้าถึงข้อมูลของ สป.กษ. กำหนดให้สามารถเข้าได้ตลอดเวลา 24 ชั่วโมง 7 วัน

1.3 การกำหนดช่องทางการเข้าถึง

ผู้ที่เกี่ยวข้องที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดได้นั้น จะต้องรับสิทธิ์จากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีการกำหนดบัญชีผู้เกี่ยวข้องตามระดับการเข้าถึงให้สามารถเข้าใช้งาน มีการแยกประเภทความรับผิดชอบ และมีการพิสูจน์ตัวตน สิทธิ์ในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

1.3.1 ระบบเครือข่ายภายใน (Intranet)

1.3.2 ระบบเครือข่ายอินเทอร์เน็ต (Internet)

1.3.3 ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

1.4 การกำหนดตั้งชื่อบัญชีผู้ใช้งาน (Username) และ รหัสผ่าน (Password) สำหรับการเข้าใช้งานดังนี้

1.4.1 การตั้งชื่อบัญชีผู้ใช้งานและผู้ดูแลระบบต้องแยกกันโดยขึ้นอยู่กับนโยบายของระบบสารสนเทศ หรือใช้เลขที่บัตรประจำตัวประชาชนตามความเหมาะสม

1.4.2 การตั้งรหัสผ่านชั่วคราวต้องยากต่อการคาดเดา และต้องมีความแตกต่างกัน

1.4.3 กำหนดรหัสผ่านให้มีตัวอักษรจำนวนอย่างน้อยหรือมากกว่า 7 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวอักษรเล็ก ตัวอักษรใหญ่ และสัญลักษณ์พิเศษ เข้าด้วยกัน

1.4.4 การตั้งชื่อบัญชีผู้ใช้งานและรหัสผ่านต้องแยกบัญชีและต้องตั้งรหัสผ่านไม่เหมือนกัน

ส่วนที่ 2 การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ
(Business Requirement for access control)

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของ สป.กษ. และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติดังนี้

2.1 การควบคุมการเข้าถึงสารสนเทศ

2.1.1 ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศขององค์กรและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

2.1.2 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไข เปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

2.2 จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ์ และภารกิจดังนี้

2.2.1 Executive คือ กลุ่มผู้บริหาร ปลัด,รองปลัด และผู้อำนวยการสำนัก

2.2.2 Administrator คือ กลุ่มของผู้ดูแลระบบศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2.2.3 Officer คือ กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของ สป.กษ.

2.2.4 Consultant คือ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับ สป.กษ.

2.2.5 Guest คือ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

ส่วนที่ 3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อบริหารจัดการการเข้าถึงระบบสารสนเทศของ สป.กษ. และมั่นใจได้ว่าเฉพาะผู้ที่ได้รับสิทธิ์การเข้าถึงระบบสารสนเทศตามที่กำหนดเท่านั้นสามารถเข้าใช้งานระบบสารสนเทศได้ โดยมีแนวปฏิบัติในการบริหารการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ดังนี้

3.1 สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน

3.1.1 สป.กษ. จัดให้มีการเผยแพร่ประชาสัมพันธ์ความรู้ความเข้าใจให้กับผู้ใช้งานเหตุการณ์ด้านความมั่นคงปลอดภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

3.1.2 สป.กษ. จัดให้มีการอบรมเพื่อสร้างความรู้ และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคาม และผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

3.1.3 กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิ์เพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเมื่อได้รับสิทธิ์การเข้าใช้งานระบบสารสนเทศขององค์กร

3.2 การลงทะเบียนผู้ใช้งาน (User Registration)

3.2.1 มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบที่ได้รับมอบหมาย

3.2.2 ผู้ดูแลระบบ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน/ขอใช้ระบบงานสารสนเทศสำหรับระบบเทคโนโลยีสารสนเทศ

3.2.3 ผู้ใช้งานจะต้องกรอกแบบฟอร์มเพื่อขออนุมัติใช้งานระบบงานตามแบบฟอร์มคำขอใช้บริการด้านสารสนเทศตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้จัดทำขึ้น

3.2.4 ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

3.2.5 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิ์ในแต่ละภารกิจ

3.2.6 ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการอนุมัติเข้าใช้งาน

3.2.7 ผู้ดูแลระบบต้องชี้แจง และแจ้งผู้ใช้งาน เพื่อให้ผู้ใช้งานทราบถึงสิทธิ์ หน้าที่รับผิดชอบและมาตรการด้านความมั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศ

3.2.8 กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากต้นสังกัด หรือเมื่อมีการลาออก เปลี่ยนแปลงตำแหน่ง โยกย้าย หรือสิ้นสุดการจ้างเป็นต้น

3.3 การบริหารจัดการสิทธิ์ผู้ใช้งาน (User Management)

3.3.1 กำหนดระดับสิทธิ์การเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบ ความจำเป็นในการใช้งาน และทบทวนสิทธิ์สม่ำเสมอ

3.3.2 ผู้ดูแลระบบต้องปรับปรุงสิทธิ์การเข้าถึงข้อมูล และระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการมอบสิทธิ์ให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

3.3.3 ในกรณีที่ต้องให้สิทธิ์พิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบจากต้นสังกัด และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จัดทำคำร้องเป็นลายลักษณ์อักษร โดยการให้สิทธิ์พิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิ์พิเศษจะต้องระงับการใช้งานทันที

3.3.4 มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

3.3.5 ทบทวนสิทธิ์การใช้งานสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

3.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

3.4.1 ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันทีภายใน 7 วัน

3.4.2 การส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นในการจัดส่ง

3.4.3 การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้องประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษ 7 หลัก (digits)

3.4.4 กำหนดให้การเข้ารหัสผิดได้ ไม่เกิน 3 ครั้ง กรณีบัญชีผู้ใช้งานไม่สามารถเข้าใช้งานได้เนื่องจากเข้ารหัสผิดเกินจำนวนครั้งที่กำหนด ให้ติดต่อผู้ดูแลระบบ และแจ้งความจำนงขอตั้งรหัสผ่านใหม่

3.4.5 กรณีผู้ใช้งานภายในหน่วยงานลาออก/โอน/ย้าย หรือสิ้นสุดการจ้างให้หน่วยงานประสานแจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้ผู้ดูแลระบบทำการยกเลิกสิทธิ์กรณีดังกล่าวออกจากระบบทันที หรือปรับปรุงข้อมูลผู้ใช้งานให้เป็นปัจจุบัน

3.4.6 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบเพื่อพิจารณาความเหมาะสม โดยมีการกำหนด

ระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

3.4.7 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ 180 วัน

3.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access right)

ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตจากผู้ที่ไม่สิทธิ์การเข้าถึง โดยมีแนวปฏิบัติ ดังนี้

3.5.1 พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิ์ที่ได้รับของแต่ละบุคคล

3.5.2 จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

3.5.3 ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับผู้ดูแลระบบ

3.5.4 ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน 3 วัน หรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 7 วัน

3.5.5 ทบทวนสิทธิ์ผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ผู้ดูแลระบบ ด้วยความถี่กว่าสิทธิ์ระดับผู้ใช้งาน เป็นต้น

ส่วนที่ 4 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีแนวปฏิบัติอย่างน้อย ดังนี้

4.1 การใช้งานรหัสผ่าน (Password Use)

4.1.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

4.1.2 การกำหนดรหัสผ่าน (Password) ที่เดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้ความยาวไม่น้อยกว่า 7 ตัวอักษร
- ใช้อักขระพิเศษประกอบ เช่น :;<> เป็นต้น
- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaa” เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องผู้ใช้งาน เช่น ชื่อ, นามสกุล หรือวันเกิด เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม
- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

4.1.3 เปลี่ยนรหัสผ่านชั่วคราวทันทีที่เข้าระบบครั้งแรก เพื่อป้องกันบุคคลอื่นลักลอบใช้งาน

4.1.4 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

4.1.5 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

4.1.6 ผู้ใช้งานมีหน้าที่ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ แม้ว่าจะไม่มีการบังคับให้เปลี่ยนจากระบบก็ตาม

4.1.7 หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนมีสิทธิ์ใช้งาน

4.1.8 หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

4.1.9 ผู้ใช้งานทุกคนของหน่วยงาน มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตน

4.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

การป้องกันอุปกรณ์เมื่อไม่มีผู้ใช้งาน มีแนวปฏิบัติเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแลได้ ดังนี้

4.2.1 ออกจากระบบงาน (log out) โดยทันทีเมื่อเสร็จสิ้นงาน

4.2.2 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อไม่มีการใช้งานเกิน 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องแม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง

4.2.3 การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานหรือถือครองให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า 30 นาที

4.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

สป.กษ. ได้กำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ รวมถึงกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยมีแนวปฏิบัติ ดังนี้

4.3.1 ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

4.3.2 ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าขณะที่ไม่ได้ใช้งานภายใน 30 นาที ให้เครื่องล็อคหน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

4.3.3 ผู้ใช้งานต้องล็อคใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

4.3.4 กรณีข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูลแฟลชไดร์ฟ หรือ ฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

4.3.5 ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

4.3.6 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อไม่มีการใช้งานเกิน 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง

4.3.7 ให้ขออนุมัติจากผู้บังคับบัญชา ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึก อุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกหน่วยงานก่อนทุกครั้ง

4.3.8 หากทรัพย์สินเกิดความสูญหายโดยประมาทเลินเล่อผู้ใช้งานต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

4.3.9 มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยให้ครอบคลุมเรื่องต่าง ๆ คือ การจัดการบริเวณล้อมรอบ, การควบคุมการเข้าออก, การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก, การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย

4.3.10 การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
1	แฟลชไดรฟ์ (Flash Drive) ฮาร์ดดิสก์ (Harddisk) เอ็กเทอนอลฮาร์ดดิสก์ (External Harddisk)	1. ทำลายข้อมูลตามแนวทางของ DOD 5220. 22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายๆ รอบ 2. ทุบทำลาย หรือบดให้อุปกรณ์เสียหายไม่สามารถนำไปใช้งานได้
2	แผ่นซีดี / ดีวีดี (CD/DVD)	ใช้วิธีการตัด เผา ทำให้สิ้นสภาพการใช้งาน
3	เทป	ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน
4	กระดาษ	ตัดด้วยเครื่องทำลายเอกสาร

4.4 การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 ดังนี้

ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

4.5 การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศขององค์กร กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งานดังนี้

4.5.1 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

4.5.2 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อคก็ดีหรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

4.5.3 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นขององค์กร หรือเป็นบุคคลภายนอก

4.5.4 ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

4.5.5 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่องค์กรต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับองค์กร ซึ่งองค์กรอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

4.5.6 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

4.5.7 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น

4.5.8 ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจขององค์กร

4.5.9 ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจขององค์กร

4.5.10 ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อประโยชน์ทางการค้า

4.5.11 ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตามห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

ส่วนที่ 5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต จึงได้กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

5.1 การใช้งานบริการเครือข่าย

5.1.1 กำหนดให้ระบบสารสนเทศต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

5.1.2 กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

5.1.3 กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ 1 ครั้ง

5.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User authentication for external connections)

5.2.1 การเข้าสู่เครือข่ายของหน่วยงานผ่านเครือข่ายภายนอก จะต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้ง

5.2.2 มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

5.2.3 การอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิค รวมทั้งต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

5.2.4 หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

5.3 การระบุอุปกรณ์บนเครือข่าย (Equipment identification in network)

5.3.1 จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่ายขององค์กร โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์, IP Address, MAC Address, สถานที่ติดตั้ง, ผู้ใช้งาน เป็นต้น

5.3.2 กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย IP Address และ MAC Address

5.3.3 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนจึงจะสามารถดำเนินการได้ และดำเนินการโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับอนุญาตเท่านั้น

5.3.4 ผู้ดูแลระบบมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิ์ในการเชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

5.3.5 ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

5.3.6 จะต้องมีการจำกัดสิทธิ์การเข้าใช้งานอุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ ชื่อผู้ใช้ รหัสผ่าน หมายเลข MAC Address เพื่อความปลอดภัยและความเหมาะสมในการเข้าถึง

5.3.7 จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

5.3.8 แผนผังเครือข่าย เป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง

5.4 การป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

5.4.1 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่าน และให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

5.4.2 ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกุเรชันไว้ในห้องคอมพิวเตอร์แม่ข่ายกลางที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

5.4.3 ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมายก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

5.4.4 เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และ ยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

5.4.5 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น

5.4.6 ตรวจสอบและปิดพอร์ต ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง

5.4.7 มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

5.4.8 ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

5.4.9 กำหนดสิทธิ์บุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

5.4.10 ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่ายกลาง หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

5.4.11 บันทึกการเข้า-ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ เจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

5.4.12 ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลาง ที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิดกันการโจรกรรม

5.5 การแบ่งแยกเครือข่าย (Segregation in network)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการระบบสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มงานที่เกี่ยวข้อง เพื่อความปลอดภัย ดังนี้

5.5.1 ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายโดยใช้ VLAN แบ่งแยกเครือข่ายแต่ละกอง/สำนักหรือที่ตั้งอาคาร ออกจากกันเพื่อป้องกันการละเมิดสิทธิ์และทรัพยากรเครือข่ายของแต่ละหน่วยงาน

5.5.2 ผู้ดูแลระบบจะต้องแบ่งแยกเครือข่ายออกเป็นโซนเพื่อความมั่นคงปลอดภัยของระบบจากการบุกรุกทางเครือข่าย 2 เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

5.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้ให้มีความมั่นคงปลอดภัย ดังนี้

5.6.1 จำกัดสิทธิ์ของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย ตามสิทธิ์ที่ได้รับตามอำนาจหน้าที่ของตน

5.6.2 มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

5.6.3 การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น และต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

5.6.4 ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

5.6.5 ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

5.6.6 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

5.6.7 ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

5.6.7.1 จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่าย ที่ได้รับอนุญาตเท่านั้น

5.6.7.2 จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

5.6.7.3 จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

5.6.7.4 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

5.6.7.5 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

5.6.7.6 กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

5.6.7.7 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

5.6.7.8 IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

5.6.7.9 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.7 การควบคุมการเข้าใช้งานระบบจากภายนอก

5.7.1 การเข้าสู่ระบบเครือข่ายจากระยะไกล (remote access) สู่ระบบสารสนเทศต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายในและต้องดูแลและจัดการอย่างรัดกุม ได้แก่ ช่องทางการเชื่อมต่อเครือข่ายแบบปลอดภัย SSL VPN การควบคุมพอร์ต (Port) เป็นต้น

5.7.2 การเข้าสู่เครือข่ายของหน่วยงานผ่านเครือข่ายภายนอก จะต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้ง

5.7.3 ก่อนการกำหนดสิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบที่ได้รับมอบหมายอย่างเป็นทางการ

5.7.4 ผู้ใช้งานที่ได้รับสิทธิ์ต้องมีการปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด โดยจะต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว ซึ่งหากระบบมีความเสียหายและสืบทราบมาได้ว่าเกิดจากการผู้ใช้งานจะต้องรับผิดชอบ

5.8 การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือ สารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ ซึ่งมีแนวปฏิบัติ ในการจัดเส้นทางบนเครือข่าย ดังนี้

5.8.1 ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

5.8.2 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

5.8.3 กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

5.8.4 ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการขององค์กรโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

6.1 ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

6.1.1 กำหนดให้ระบบไม่ให้แสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

6.1.2 ผู้ใช้งานจะต้องทำการตั้งค่าให้ระบบปฏิบัติการทำการป้องกันด้วยรหัสผ่านทุกครั้งที่เปิดใช้งาน

6.1.3 มีการกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบ ตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของหน่วยงาน

6.1.4 กำหนดให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

6.1.5 ผู้ใช้งานจะต้องทำการตั้งค่าการใช้งานโปรแกรมพักหน้าจอเมื่อไม่มีการใช้งานให้ทำการล็อคหน้าจอด้วยรหัสผ่าน

6.1.6 จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

6.2 การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

6.2.1 ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศขององค์กร

6.2.2 ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่หน่วยงานกำหนดให้

6.2.3 หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านเทคนิค หรือสอดคล้องกับการปฏิบัติงาน โดยจะต้องขออนุญาตใช้จากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และกำหนดกรอบเวลาการใช้งานที่ชัดเจนและยุติการใช้งานทันทีเมื่อพบความผิดปกติหรือหมดช่วงเวลาที่ขออนุญาตไว้

6.3 การบริหารจัดการรหัสผ่าน (Password Management System)

กำหนดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

6.3.1 มีระบบการตรวจสอบการกำหนดรหัสผ่าน ซึ่งประกอบด้วยตัวอักขระ ตัวเลข และตัวอักขระพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) และมีคุณภาพ

6.3.2 เมื่อดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของรายชื่อผู้ใช้งานทั้งหมดที่ถูกกำหนดไว้เริ่มต้นซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที

6.3.3 การกำหนดรหัสผ่านให้กับผู้ใช้งานตามหลักเกณฑ์การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของหน่วยงาน

6.3.4 อนุญาตให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง โดยต้องกำหนดให้เป็นไปตามเงื่อนไขการกำหนดรหัสผ่าน

6.4 การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

กำหนดให้มีการจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด โดยมีแนวปฏิบัติดังนี้

6.4.1 การใช้งานโปรแกรมอรรถประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

6.4.2 โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

6.4.3 ให้ผู้ดูแลระบบทำบัญชีโปรแกรมที่อนุญาตให้ใช้งานได้

6.4.4 จัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน และเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

6.4.5 จำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เท่านั้น

6.4.6 กำหนดให้ผู้ดูแลระบบมีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

6.5 การกำหนดระยะเวลายุติการใช้งานระบบสารสนเทศ (Session Time - Out)

6.5.1 กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 30 นาที

6.5.2 ระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นระยะเวลา 15 นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

6.5.3 ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

6.5.4 เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

6.6 การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศ และโปรแกรมที่มีความเสี่ยงสูง หรือมีความสำคัญสูง กำหนดแนวปฏิบัติในการจำกัดระยะเวลาในการเชื่อมต่อเพื่อความมั่นคงปลอดภัยดังนี้

6.6.1 กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ให้ใช้งานได้ภายใน 2 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง

6.6.2 กำหนดให้ระบบสารสนเทศ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อไม่เกิน 3 ชั่วโมงต่อครั้ง

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบต้องดำเนินการดังนี้

7.1 จำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน โดยการเข้าใช้งาน การเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ได้กำหนดหลักเกณฑ์การจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศดังนี้

7.1.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิ์ของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูล และจะต้องมีการทบทวนสิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

7.1.2 ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา 30 นาที ต้องทำการยุติการใช้งานทันที

7.1.3 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

- กำหนดสิทธิ์ให้กับผู้เข้าใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการ พิสูจน์ตัวตนของผู้เข้าถึงข้อมูลแต่ละระดับชั้น
- กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัสอย่างน้อย SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
- การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

7.1.4 ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน

7.1.5 การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใด ๆ จะต้องได้รับสิทธิ์และได้รับอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิ์ที่ให้กับหน่วยงานนั้น ๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใด ๆ ที่มีผลต่อกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

7.1.6 ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

7.1.7 ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

7.2 ระบบซึ่งไวต่อการรบกวน

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking) โดยกำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยไว้ดังนี้

7.2.1 แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

7.2.2 ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

1) ระบบซึ่งไวต่อการรบกวน จะต้องควบคุมการเข้าถึงอุปกรณ์ และระบบโดยติดตั้งไว้ในในพื้นที่ปลอดภัย

2) ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณ์ผิดปกติ

7.2.3 ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับ ระบบดังกล่าวโดย

1) อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกหน่วยงาน ต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ

2) การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเปิดสิทธิ์ให้ปฏิบัติงานจากภายนอกได้

3) ผู้ปฏิบัติงานจากภายนอก ต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบสารสนเทศขององค์กร

7.2.4 ควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนด

7.2.5 วางแผนการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายการสำรองระบบสารสนเทศ

7.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังนี้

7.3.1 การป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ครอบคลุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ได้แก่ Smart Phone, Notebook, Laptop, Tablet หรืออุปกรณ์อื่นใดในลักษณะเดียวกันนี้ โดยกำหนดให้มีการป้องกัน การเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เข้ากับเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต

7.3.2 กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ซึ่งจะต้องแสดงตัวตนเมื่อเข้าใช้งาน

7.3.3 ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของตนเอง

7.4 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอกหน่วยงาน กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยดังนี้

7.4.1 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่างๆ ภายในหน่วยงาน

7.4.2 ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

7.4.3 การเข้าถึงระบบสารสนเทศขององค์กรจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

7.4.4 การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียดดังนี้

1) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน
2) รายละเอียดและลักษณะของระบบงาน
3) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก
4) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน
5) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน

7.4.5 ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

7.4.6 การเข้าสู่ระบบระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

7.4.7 ผู้ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงาน โดย ไม่ให้สมาชิกภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

7.4.8 ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในหน่วยงาน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึง

7.4.9 ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

7.4.10 การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

7.4.11 ผู้ดูแลระบบจะทำการยกเลิกสิทธิ์การเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

7.4.12 ผู้ดูแลระบบต้องทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

เพื่อให้การเข้าถึงระบบเครือข่ายไร้สายในหน่วยงาน มีความมั่นคงปลอดภัยกำหนดแนวทางปฏิบัติเพื่อควบคุมการเข้าถึงระบบเครือข่ายไร้สายไว้ดังนี้

8.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องลงทะเบียนกับผู้ดูแลระบบโดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

8.2 ผู้ดูแลระบบต้องดำเนินการลงทะเบียนผู้ใช้งานดังนี้

8.2.1 ลงทะเบียน และกำหนดสิทธิ์ผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายเหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

8.2.2 ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

8.2.3 ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

8.2.4 ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier) เพื่อความปลอดภัย

8.2.5 เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

8.2.6 กำหนดค่าใช้ WEP(Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจาย (Access Point) เพื่อให้ยากต่อการดักจับ เพื่อความปลอดภัย

8.2.7 เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Addressชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้สามารถเข้าใช้ระบบเครือข่ายไร้สายได้

8.2.8 มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

8.2.9 กำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

8.2.10 ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทันที

ส่วนที่ 9 การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัยดังนี้

9.1 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น

9.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

9.3 การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

9.4 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

9.5 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

9.6 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

9.7 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

9.8 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

9.9 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

9.10 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ (Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

9.11 ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ 10 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ส่วนบุคคล (Personal Computer)

เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลให้มีความปลอดภัย กำหนดแนวปฏิบัติดังนี้

10.1 เครื่องคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตให้ผู้ใช้ระบบสารสนเทศใช้งานเป็นทรัพย์สินของหน่วยงาน ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

10.2 โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคล หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย (กรณีการติดตั้งโปรแกรมเป็นหน้าที่ของผู้ดูแลระบบ ให้ระบุว่าห้ามผู้ใช้งานติดตั้ง แก้ไขโปรแกรมด้วยตนเอง ผู้ดูแลระบบมีหน้าที่จัดหาและลงโปรแกรมในเครื่องของหน่วยงานเท่านั้น)

10.3 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น เมื่อตรวจซ่อมเสร็จแล้วต้องให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบของหน่วยงานในหน่วยงานที่มีศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศเท่านั้น

10.4 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล

10.5 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงาน เท่านั้น

10.6 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานเท่านั้น

10.7 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมอรรถประโยชน์ในเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ของหน่วยงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานเท่านั้น

10.8 ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในหน่วยงาน และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้มีสภาพเดิม

10.9 เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของหน่วยงานจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

10.10 การนำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ทุกเครื่องออกไปใช้งานนอกหน่วยงาน เมื่อนำกลับมาที่หน่วยงานต้องทำการเชื่อมต่อระบบเครือข่ายภายในหน่วยงานเพื่อทำการอัปเดท (Update) ข้อมูลไวรัสล่าสุด

10.11 ห้ามเจ้าหน้าที่ผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ของหน่วยงานทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครองถูกแก้ไขการตั้งเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธ

ความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบทันที

10.12 การเชื่อมต่อเพื่อใช้ระบบงานจากภายนอกให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

10.13 ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลดรหัสผ่านสำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ทุกครั้ง

10.14 ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดย

10.14.1 กำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเปิดใช้เครื่องและเก็บรักษารหัสผ่านอย่างปลอดภัย

10.14.2 เมื่อไม่ได้ใช้งานเกิน 30 นาที เครื่องควรตั้งโปรแกรม Screen Saver และต้องใช้รหัสผ่านเพื่อเข้าใช้งานอีกครั้ง

10.14.3 ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของหน่วยงาน

10.14.4 ต้องไม่ถอดถอนการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในเครื่องคอมพิวเตอร์ส่วนบุคคล

10.14.5 ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่มิได้ขึ้นทะเบียนอุปกรณ์กับผู้ดูแลระบบมาใช้งานและเชื่อมต่อกับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับอนุญาตเป็นลายลักษณ์อักษรและนำมาขึ้นทะเบียนกับผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

10.14.6 ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

10.14.7 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

10.15 ผู้ใช้งาน ต้องคำนึงถึงความปลอดภัยด้านกายภาพของเครื่องคอมพิวเตอร์ ดังนี้

10.15.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

10.15.2 ผู้ใช้งานไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์การสื่อสารเคลื่อนที่ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองและต้องระวังป้องกันการตกกระทบ

10.15.3 ไม่ใส่เครื่องคอมพิวเตอร์และอุปกรณ์การสื่อสารเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

10.15.4 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์การสื่อสารเคลื่อนที่ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์หรืออุปกรณ์เฉพาะ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

10.15.5 หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์และอุปกรณ์การสื่อสารเคลื่อนที่แตกเสียหายได้

10.15.6 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าที่มีรอยขีดข่วนได้

10.15.7 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

10.15.8 ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

10.15.9 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ใกล้สิ่งที่เป็นของเหลว

10.15.10 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

10.15.11 ไม่วางเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ และในที่มีการสั่นสะเทือน

ส่วนที่ 11 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

11.1 เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพร้อมใช้งาน

11.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

11.3 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเปิดเข้าใช้งานเครื่องทุกครั้ง และควรกำหนดรหัสผ่านให้ยากต่อการคาดเดา และเก็บรักษาไว้เป็นความลับ

11.4 เมื่อไม่ได้ใช้งานเกิน 30 นาที เครื่องควรตั้งโปรแกรม Screen Saver และต้องใช้รหัสผ่านเพื่อเข้าใช้งานอีกครั้ง

11.5 ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

11.6 ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ลงบนสื่อจัดเก็บที่ปลอดภัยเพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย หรือกำหนดรหัสการเข้าสื่อบันทึกข้อมูล รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

11.7 การเคลื่อนย้ายคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือพลัดหลุดมือ เป็นต้น หลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทาง เพราะอาจถูกกดทับ เกิดความเสียหายได้

11.8 หลีกเลี่ยงการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดอยู่ กรณีต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

11.9 ผู้ใช้งาน ต้องคำนึงถึงความปลอดภัยด้านกายภาพของเครื่องคอมพิวเตอร์แบบพกพา ดังนี้

11.9.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

11.9.2 ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

11.9.3 หลีกเลี่ยงการวางเครื่องคอมพิวเตอร์พกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ และวางไว้หรือใช้งานในที่ที่มีแรงสั่นสะเทือนมาก

11.9.4 ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

11.9.5 หลีกเลี่ยงการใช้วัสดุ หรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนไม่วางของทับบนหน้าจอและแป้นพิมพ์ หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

11.9.6 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดด้วยความระมัดระวัง ควรเช็ดไปในแนวทางเดียวกัน ไม่ควรเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

11.9.7 ดูแลบำรุงรักษาเครื่องคอมพิวเตอร์แบบพกพาให้อยู่ในสภาพร้อมใช้งาน พักเครื่องเมื่อต้องใช้เป็นระยะเวลานานเกินไป หรือในสภาพที่มีอากาศร้อนจัด

ส่วนที่ 12 การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

12.1 การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

12.1.1 กำหนดให้มี รหัสผู้ใช้/รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

12.1.2 กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ หากเกินกว่าที่กำหนดระบบต้องทำการ LOCK ไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง

12.1.3 ผู้ดูแลระบบต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของหน่วยงาน

12.1.4 ผู้ดูแลระบบตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานต้องใส่รหัสผ่าน

12.1.5 ผู้ดูแลระบบต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

12.2 ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบดังนี้

12.2.1 ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศขององค์กรเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

12.2.2 ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศขององค์กร

12.2.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องดำเนินการโดยเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น

12.2.4 ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

12.2.5 กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

12.2.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ

12.2.7 วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

12.2.8 ทำการปรับปรุง Library สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกับทั้งหมดที่ทำการติดตั้ง

12.2.9 จัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

12.2.10 กำหนดให้ผู้ที่เกี่ยวข้องจัดทำแผนถอยหลังกลับ (Rollback Strategy) ก่อนที่จะดำเนินการติดตั้งระบบงานบนเครื่องให้บริการ

12.3 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

12.3.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

12.3.2 วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

12.4 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

12.4.1 กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

12.4.2 หน่วยงานเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

12.4.3 กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

12.4.4 กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ก่อนมีการติดตั้ง

12.4.5 การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบ และฐานข้อมูลที่ใช้งาน เลือกสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

12.4.6 การดำเนินการพัฒนาซอฟต์แวร์และดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ดำเนินการโดยหน่วยงานภายนอกนั้น ซึ่งหน่วยงานภายนอกจะต้องมีการลงนามในสัญญา

รักษาความลับรักษาข้อมูลของหน่วยงานก่อนการดำเนินการใด ๆ รวมทั้งจะต้องปฏิบัติตามนโยบายและแนวปฏิบัติของหน่วยงานอย่างเคร่งครัดด้วย

12.5 มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

12.5.1 ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศขององค์กรจะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

12.5.2 ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

12.5.3 กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

12.5.4 การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนทุกครั้ง

12.6 มาตรการควบคุมช่องโหว่ทางเทคนิค

12.6.1 กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงานบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องแม่ข่ายที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

12.6.2 กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่าง เหมาะสมโดยทันที

12.6.3 กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบ ดำเนินการ ดังนี้

- มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศขององค์กร
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้ง หรือทราบเกี่ยวกับช่องโหว่นั้น

12.6.4 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

12.6.5 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

- ข้อมูลชื่อบัญชีผู้ใช้งาน
- ข้อมูลวันเวลาที่เข้าถึงระบบ
- ข้อมูลวันเวลาที่ออกจากระบบ
- ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
- ข้อมูลการล็อคอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ
- ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- ข้อมูลการเปลี่ยนค่าคอนฟิกกูเรชั่น (Configuration) ของระบบ
- ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)
- ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
- ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง
- ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้
- ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
- ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

12.7 ความเป็นเจ้าของและความรับผิดชอบ

12.7.1 หน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย ต้องกำหนดผู้มีหน้าที่รับผิดชอบเพื่อดูแลเครื่องคอมพิวเตอร์แม่ข่าย โดยทำการ Update service pack หรือ patch ต่างๆ ให้ทันสมัยอยู่เสมอ เพื่อปิดรูรั่วของตัวระบบปฏิบัติการ และตัวโปรแกรม และต้องมีเอกสารในการปรับเปลี่ยนค่าปรับแต่งบนเครื่องคอมพิวเตอร์แม่ข่าย และต้องมีการระบุรายละเอียดของเครื่องคอมพิวเตอร์แม่ข่ายในระบบการจัดการเครือข่าย (Enterprise Management System)

12.7.2 กำหนด ชื่อ/รหัส ระดับสิทธิ์การใช้ ให้ผู้ใช้งานแต่ละคน

12.8 การติดตั้ง

12.8.1 ห้ามเปิด Services และ Application ใด ๆ ที่ไม่เกี่ยวข้องกับของเครื่องคอมพิวเตอร์แม่ข่าย นั้น ๆ โดยเด็ดขาด

12.8.2 เมื่อมีการปรับแต่งหรือแก้ไขค่า ต้องมีการแจ้งผู้ดูแลรับผิดชอบเครื่องคอมพิวเตอร์แม่ข่าย นั้น ๆ

12.9 การเฝ้าดูและตรวจสอบ

12.9.1 ต้องดำเนินการเก็บ log และ Audit Trails ของเหตุการณ์ละเมิดความมั่นคงปลอดภัยดังต่อไปนี้

- Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา 90 วัน
- ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า 90 วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้ เมื่อพนักงานเจ้าหน้าที่ต้องการ ต้องสามารถนำออกมามอบให้กับพนักงานเจ้าหน้าที่ได้

12.9.2 ผู้ดูแลระบบต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับผู้บังคับบัญชาทราบ ดังนี้

- การโจมตีในรูปแบบ Post-Scan
- การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิ์ในการใช้งานระบบนั้น
- เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์แม่ข่าย ที่เกิดขึ้น

12.9.3 ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ

12.9.4 ต้องมีการประเมินความเสี่ยงทุก 1 ปีหรือตามความเหมาะสม

12.10 กรณีการจัดซื้อเครื่องคอมพิวเตอร์แม่ข่าย และหรือแอปพลิเคชัน (Application) ใหม่ ที่ให้บริการบนเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องมีข้อกำหนดจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในการจัดซื้อ และต้องมีการกำหนดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นทิศทางเดียวกับหน่วยงาน โดยจะต้องประสานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน

ส่วนที่ 13 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

13.1 ห้องศูนย์เครื่องคอมพิวเตอร์แม่ข่าย (Server Room)

13.1.1 กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงาน พื้นที่ควบคุมเฉพาะให้ชัดเจน และควบคุม เพื่อกำหนดสิทธิ์การเข้าถึงพื้นที่ โดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

13.1.2 กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารดังนี้

1) ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิ์การเข้าใช้งานพื้นที่เท่านั้น
2) ควบคุมการเข้าใช้งานในพื้นที่โดย แบบพิมพ์นิ้วมือ (Finger Scan)
3) ติดตั้งกล้องวงจรปิดเพื่อติดตาม/เฝ้าระวัง การเข้าพื้นที่ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

13.1.3 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

13.1.4 จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศขององค์กรที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งานดังนี้

1) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง
2) ติดตั้ง ระบบระงับเพลิง
3) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น
4) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน
5) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

13.2 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

13.2.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงติดตั้งระบบป้องกันที่ปลอดภัย

13.2.2 ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณหรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

13.2.3 ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

13.2.4 ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่างๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

13.2.5 ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

13.2.6 พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

13.2.7 ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

13.3 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

13.3.1 วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

13.3.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

13.3.3 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

13.3.4 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

13.3.5 ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบจะต้องอยู่ในพื้นที่ทุกครั้ง

13.3.6 จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้าง ผู้ให้บริการจากภายนอก ที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

13.4 การนำทรัพย์สินของห้องศูนย์เครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ออกนอกหน่วยงาน (Removal of Property)

13.4.1 ต้องขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบ ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือ นำไปซ่อมบำรุงภายนอก

13.4.2 ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนด และตรวจสอบอยู่ในสภาพดี

13.4.3 บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

13.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off Premises)

13.5.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

13.5.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะเสี่ยงต่อการสูญหาย

13.5.3 เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

13.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

13.6.1 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือ นำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

13.6.2 ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

13.7 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

13.8 เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

13.8.1 คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับและไม่แน่ใจว่าลับหรือไม่ ให้อยู่ในกลุ่มเอกสารลับ

13.8.2 ทำลายเอกสารลับเหล่านั้นโดยใช้วิธีการดังนี้

ประเภทสื่อข้อมูล	**วิธีการทำลาย**
Flash Drive	วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น CD/DVD
เทป	วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

ส่วนที่ 14 การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

14.1 จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

14.2 ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

14.3 ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

ส่วนที่ 15 การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail)

15.1 กำหนดให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน หรือระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ เท่านั้น ในการติดต่อราชการ หรือรับ-ส่งข้อมูลของทางราชการผ่านทางจดหมายอิเล็กทรอนิกส์

15.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมออย่างน้อยปีละครั้ง

15.3 การรับ-ส่งข้อมูลของทางราชการที่เป็นความลับ ห้ามรับ-ส่งผ่านทางระบบจดหมายอิเล็กทรอนิกส์

15.4 ผู้ดูแลระบบรับเรื่องการขอใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ขององค์กร โดยกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งาน e-mail รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน

15.5 กำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) และต้องเปลี่ยนรหัสผ่านใหม่ทุก 180 วัน

15.6 ผู้ดูแลระบบไม่สามารถเข้ารหัสผ่านจดหมายอิเล็กทรอนิกส์เมื่อใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

15.7 กำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง

15.8 ระบบจดหมายอิเล็กทรอนิกส์จะออกจากระบบ (Log out) เพื่อตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาภายในระยะเวลา 30 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

15.9 ผู้ใช้งานควรหลีกเลี่ยงค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

15.10 ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ (e-mail) เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงาน ได้แก่ การละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรมและไม่แสวงหาประโยชน์รวมทั้งไม่ อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้ e-mail ผ่านระบบเครือข่ายของ หน่วยงาน

15.11 ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์

15.12 หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้งเพื่อ ป้องกันบุคคลอื่นเข้าใช้งาน e-mail โดยไม่ได้รับอนุญาต

15.13 ผู้ใช้งานควรตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ (e-mail) ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัส โดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

15.14 ผู้ใช้งานไม่ควรเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ (e-mail) หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

15.15 ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ-ส่ง จดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียง หรือข้อมูลทำให้เกิดความแตกแยกผ่านทาง e-mail

15.16 ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (e-mail Inbox) ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

15.17 ผู้ใช้งานต้องไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้

15.17.1 ข้อมูลคอมพิวเตอร์อันเป็นเท็จ

15.17.2 ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

15.17.3 ข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

15.17.4 ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกอนาจาร

15.18 ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ส่วนที่ 16 การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

16.1 ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือ ข้อมูลความลับของหน่วยงาน

16.2 ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

16.3 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อหน่วยงาน ผู้ใช้งานต้องแจ้งต่อ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

2. ผู้ดูแลระบบ / เจ้าของระบบ

ส่วนที่ 1 การสำรองข้อมูล (Back Up)

คัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

1.1 จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และวางแผนการกำหนดการสำรองข้อมูล โดยพิจารณาจากความสำคัญของข้อมูล, ความถี่ในการเปลี่ยนแปลงข้อมูล โดยมีรายละเอียดการสำรองข้อมูลดังนี้

1.2.1 กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ดังนี้

1) ข้อมูลคอนฟิกกูเรชัน (Configuration) สำหรับระบบ
2) ฐานข้อมูล (Database) ในระบบสารสนเทศ
3) ซอฟต์แวร์ (Software) ต่างๆ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่นๆ ที่สำคัญ

1.2.2 กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

1.2.3 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับการกู้คืนระบบ

1.2.4 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง เป็นต้น

1.2.5 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

1.2.6 ในกรณีที่จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล ต้องชี้บ่งสื่อบันทึกข้อมูลไว้อย่างชัดเจน โดยมีรายละเอียดของ ชื่อ วัน/เวลาสำรองข้อมูล ผู้รับผิดชอบ โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย และข้อมูลที่สำรองต้องเข้ารหัสเพื่อความปลอดภัย

1.2.7 จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้น้ำท่วม แผ่นดินไหว การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทั้งนี้สอดคล้องตามแผนเตรียมความพร้อมกรณีเหตุฉุกเฉินที่กำหนดไว้

1.2.8 วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอบไว้เป็นหลักฐาน

1.2.9 ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

1.2.10 จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

1.2.11 ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

1.3 กำหนดผู้รับผิดชอบในการสำรองข้อมูล

1.4 กำหนดชนิดของระบบงานนั้น ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

1.5 การเก็บสื่อบันทึกข้อมูลสำรองต้องถูกเก็บไว้บริเวณพื้นที่ภายนอกอาคารของหน่วยงานเดือนละ 1 ครั้ง

1.6 ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูล ในการสำรองข้อมูลทุกครั้ง

1.7 ต้องทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

1.8 จัดทำแผนเตรียมความพร้อมกรณีเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด

1.9 การสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสาร และมีการตรวจสอบความถูกต้องเป็นระยะ ๆ

1.10 ต้องตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำทุกปี หรือตามความเหมาะสม

1.11 สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนสื่อตามอายุการใช้งานของสื่อตามประเภทของสื่อแต่ละชนิด

ส่วนที่ 2 การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

2.1 จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

2.1.1 กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2.1.2 ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นรวมทั้งมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทำให้ไม่สามารถเข้ามาใช้งานระบบสารสนเทศได้

2.1.3 กำหนดขั้นตอนปฏิบัติในการกู้คืน (Recover) ระบบสารสนเทศ และระยะเวลาในการกู้คืนระบบที่สอดคล้องตามเป้าหมายที่หน่วยงานกำหนดไว้

2.1.4 กำหนดขั้นตอนปฏิบัติในกู้คืนระบบ และการทดสอบแผนฉุกเฉิน

2.1.5 กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายในหน่วยงานและผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อผู้ให้บริการ

2.1.6 สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

2.3 กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

2.4 ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

2.5 ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

แนวปฏิบัติการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition Development and Maintenance Policy)

แนวปฏิบัติ

1. การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย

1.1 หน่วยงานเจ้าของระบบสารสนเทศ ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นเอกสาร ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน

1.2 หน่วยงานที่เกี่ยวข้องกับการพัฒนาระบบงาน ต้องปฏิบัติตามนโยบายและแนวปฏิบัติต่างๆ ของหน่วยงานในการพัฒนาระบบงาน และโปรแกรมประยุกต์

2. ข้อกำหนดด้านการประมวลผลในระบบสารสนเทศ

2.1 การตรวจสอบข้อมูลนำเข้า

2.1.1 โปรแกรมประยุกต์ของหน่วยงานที่มีการป้อนข้อมูลเข้าสู่ระบบ จะต้องมีการตรวจสอบความถูกต้องของข้อมูลที่ได้รับจากการป้อนข้อมูล ก่อนที่จะนำข้อมูลนั้นไปประมวลผลต่อ

2.1.2 ในระบบประมวลผลที่สำคัญของหน่วยงาน ต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลที่ป้อนเข้า รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการป้อนข้อมูล

2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล

2.2.1 ระบบประมวลผล ต้องออกแบบให้มีความสามารถแจ้งถึงความผิดพลาดต่างๆ จากการประมวลผล การสอบทานเพื่อตรวจจับกรณีการประมวลผลข้อมูลมีความผิดพลาดหรือเสียหาย

2.2.2 ระบบประมวลผลที่สำคัญ ต้องมีการตรวจสอบความถูกต้องของการประมวลผลอย่างสม่ำเสมอ

2.3 การตรวจสอบความถูกต้องของข้อมูล

สำหรับระบบที่มีความสำคัญและต้องการความครบถ้วนถูกต้องของข้อมูล ต้องมีการพิจารณาใช้เทคนิคที่เหมาะสมมาใช้กับระบบงาน โดยประโยชน์ของการใช้งานรับรองข้อมูล ได้แก่

2.3.1 รักษาความถูกต้องของข้อมูล

2.3.2 ตรวจสอบการลักลอบแก้ไขข้อมูล

2.4 การตรวจสอบข้อมูลผลลัพธ์

2.4.1 กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์เพื่อมั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์ ทั้งนี้ การตรวจสอบครอบคลุมถึง

- การสอบเทียบความครบถ้วนของข้อมูลผลลัพธ์ที่ได้จากการประมวลผล
- การตรวจสอบถึงความผิดพลาดต่าง ๆ ของรายงาน
- กำหนดให้มีระเบียบปฏิบัติในการทดสอบข้อมูลผลลัพธ์

2.4.2 ในระบบประมวลที่สำคัญของหน่วยงาน ต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลผลลัพธ์ รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการนำข้อมูลผลลัพธ์ไปใช้

3. มาตรการในการเข้ารหัสข้อมูล

3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล

3.1.1 กำหนดให้มีระเบียบปฏิบัติในเรื่องการใช้การเข้ารหัส รวมถึงซอฟต์แวร์และมาตรฐานวิธีการเข้ารหัสที่หน่วยงานอนุญาตให้ใช้งานสำหรับข้อมูลในลำดับชั้นต่างๆ

3.1.2 ต้องมีการปรับปรุงรายชื่อซอฟต์แวร์และมาตรฐานในด้านการเข้ารหัสให้ทันสมัยอยู่เสมอ

3.1.3 ต้องมีการพิจารณาถึงลำดับชั้นของข้อมูลและแนวทางในการจัดการข้อมูลในลำดับชั้นดังกล่าวประกอบการพิจารณาในการใช้งานการเข้ารหัส

3.1.4 ต้องมีการประเมินความเสี่ยง และพิจารณาผลการประเมินความเสี่ยงก่อนในการเลือกวิธีในการเข้ารหัสมาใช้งานในระบบงาน

3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล

ผู้ดูแลระบบแต่ละระบบเป็นผู้จัดการกุญแจรหัสในระบบของตน และต้องกำหนดการป้องกันด้วยวิธีการที่เหมาะสม การจัดการดังกล่าวรวมถึงขั้นตอนการปฏิบัติงานต่าง ๆ มีดังนี้

3.2.1 การสร้างและการแจกจ่ายกุญแจรหัส

3.2.2 ความลับของกุญแจส่วนบุคคล

3.2.3 ความถูกต้องของกุญแจสาธารณะ

3.2.4 การยกเลิกการใช้กุญแจรหัส

3.2.5 การกู้คืนกุญแจรหัส

3.2.6 การสำรองข้อมูลกุญแจรหัส

3.2.7 การยกเลิกและทำลายกุญแจรหัสที่ไม่ใช้งานแล้ว

3.2.8 การจัดการที่ไม่ขัดแย้งต่อกฎหมายใด ๆ

3.2.9 การจำกัดให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ในการเข้าใช้อุปกรณ์ที่ใช้ในการสร้างเก็บหรือสำรองกุญแจรหัส

4. การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการหรือระบบที่ใช้งานจริง

4.1.1 ก่อนมีการปรับปรุงโปรแกรมเวอร์ชันใหม่ในระบบใช้งานจริงจะต้องได้รับการอนุมัติการใช้โปรแกรมเวอร์ชันใหม่และหลักฐานประกอบอื่น ๆ เช่น รายการผลการทดสอบเพื่อการรับรองความถูกต้องจากผู้ใช้เป็นต้น และต้องปรับเปลี่ยน Source Code ให้สอดคล้องกัน

4.1.2 ไม่จัดเก็บ Source Code ของโปรแกรมไว้ในระบบใช้งานจริง

4.1.3 ต้องจัดเก็บรายการบันทึกเพื่อการตรวจสอบต่าง ๆ ของการแก้ไข Source Code และโปรแกรม

4.1.4 ต้องมีการสำรองและจัดเก็บโปรแกรมเวอร์ชันก่อนการแก้ไขเพื่อนำกลับมาใช้เมื่อมีความจำเป็น

4.1.5 ก่อนที่จะอนุญาตให้ผู้ให้บริการ/จำหน่ายระบบเข้าถึงระบบที่ใช้งานจริง เพื่อติดตั้งแก้ปัญหา และ/หรือดูแลรักษาระบบ จะต้องได้รับการอนุมัติจากผู้บริหาร หรือเจ้าหน้าที่ที่ได้รับมอบหมาย โดยมีเจ้าหน้าที่ที่ได้รับมอบหมายของหน่วยงานในการเฝ้าติดตามกิจกรรมต่าง ๆ ของผู้ให้บริการ/จำหน่ายมีเจ้าหน้าที่ที่ได้รับมอบหมาย

4.1.6 มีการลงโปรแกรมแก้ไข (Software Patches) เมื่อผู้ผลิตได้ออกโปรแกรมดังกล่าวเพื่อใช้ในการลดหรือกำจัดข้อบกพร่องด้านความมั่นคงปลอดภัย ที่เกี่ยวข้องกับลักษณะการใช้งานซอฟต์แวร์ในปัจจุบัน

4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบระบบ

ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงไปใช้เพื่อการทดสอบระบบงานที่พัฒนาใหม่ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง โดยการควบคุมต่างๆ ต้องประกอบด้วย

4.2.1 ได้รับอนุญาตก่อนการนำสำเนาข้อมูลจริงไปใช้ในระบบงานทดสอบในแต่ละครั้ง

4.2.2 มีการควบคุมในการเข้าถึงข้อมูลที่ใช้ในการทดสอบระบบ

4.2.3 มีการดัดแปลงข้อมูลจริงบางส่วนก่อนนำมาใช้ในการทดสอบ

4.2.4 ทำการลบข้อมูลทดสอบออกจากระบบทันทีเมื่อเสร็จสิ้นการทดสอบ

4.2.5 มีการจัดเก็บบันทึกการทำรายงานในระบบ (Audit Log) เพื่อตรวจสอบกิจกรรมการทดสอบ

4.3 การควบคุมการเข้าถึง Source Code ของโปรแกรม

4.3.1 การอัปเดท Source Code ของโปรแกรมใน Library และการนำ Source Code ของโปรแกรมให้กับผู้พัฒนาระบบ จะต้องดำเนินการโดยเจ้าหน้าที่ผู้ดูแล Library ที่ได้รับมอบหมายในแต่ละระบบ

4.3.2 ต้องมีการจัดเก็บบันทึกการทำรายการในระบบ (Audit Log) เพื่อตรวจสอบการเข้าถึง Library ต่าง ๆ

4.3.3 บันทึกรายละเอียดโปรแกรมเวอร์ชันเก่าที่จะทำการจัดเก็บอย่างชัดเจน โดยมีรายละเอียดต่าง ๆ เช่น วัน-เดือน-ปี ที่โปรแกรมเวอร์ชันนี้ได้ใช้งานอยู่ในระบบใช้งานจริง ซอฟต์แวร์ต่างๆ ที่ทำงานร่วมกันกับโปรแกรมนี้ เป็นต้น

4.3.4 การปรับปรุงเปลี่ยนแปลงและการทำสำเนา Library จะต้องปฏิบัติตามข้อที่ควรพิจารณาในการควบคุมการเปลี่ยนแปลงของระบบ

5. การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและการสนับสนุน

5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ

5.1.1 การปรับปรุงแก้ไขระบบงานหรือโปรแกรมต่าง ๆ ต้องปฏิบัติตามระเบียบปฏิบัติของหน่วยงาน

5.1.2 การปรับปรุงแก้ไขระบบงานต่าง ๆ ต้องจัดทำเป็นเอกสารและสามารถติดตามสถานะได้ รวมถึงต้องมีเอกสารสนับสนุน เช่น แผนการทดสอบการปรับปรุงแก้ไขโปรแกรม และผลการทดสอบ เป็นต้น

5.1.3 การปรับปรุงแก้ไขระบบงานควรพิจารณาถึง

- การอนุมัติโดยหน่วยงานเจ้าของระบบงาน
- การระบุถึงเครื่องคอมพิวเตอร์ ซอฟต์แวร์ ฐานข้อมูล ที่จะต้องเปลี่ยนแปลง
- การป้องกันผลกระทบที่อาจเกิดขึ้นกับการทำงาน
- การสำรองข้อมูลก่อนการปรับปรุงแก้ไขหรือบำรุงรักษาระบบ
- การจัดทำเอกสารประกอบการเปลี่ยนแปลงให้ทันสมัย
- การควบคุมเวอร์ชันของซอฟต์แวร์ที่เปลี่ยนแปลง

- การจัดเก็บบันทึกเพื่อการตรวจสอบการแก้ไข

5.1.4 การปรับปรุงแก้ไขระบบต้องจัดทำเป็นหนังสือขออนุมัติแก้ไขระบบงานหรือโปรแกรม ซึ่งประกอบด้วยรายละเอียดตามมาตรฐานที่หน่วยงานกำหนด

5.2 การตรวจสอบการทำงานของโปรแกรมประยุกต์ภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

5.2.1 ทบทวนมาตรการควบคุม และขั้นตอนปฏิบัติของโปรแกรมประยุกต์ในด้านความถูกต้องสมบูรณ์ภายหลังการเปลี่ยนแปลงระบบปฏิบัติการ

5.2.2 ดำเนินการแจ้งการเปลี่ยนแปลงระบบปฏิบัติการให้กับผู้ที่เกี่ยวข้องทราบในเวลาที่เหมาะสมเพียงพอสำหรับการเตรียมการทดสอบและการทบทวนก่อนที่จะติดตั้งใช้งานจริง ทั้งนี้ ให้มีการพิจารณาแต่งตั้งกลุ่มบุคคลเฉพาะเพื่อรับผิดชอบในการตรวจเฝ้าระวังช่องโหว่ และการแก้ไขอุดช่องโหว่ของผู้ให้บริการ/จำหน่ายระบบ

5.3 การจำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่มาจากผู้ผลิต

ซอฟต์แวร์สำเร็จรูปควรใช้งานโดยปราศจากการแก้ไข ถ้ามีความจำเป็นในการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูปต้องมีการพิจารณาการควบคุมต่าง ๆ ดังนี้

5.3.1 ความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ซึ่งอาจมีการละเลยการควบคุมด้านความมั่นคงปลอดภัย

5.3.2 การได้รับความยินยอมในการแก้ไขจากผู้จำหน่ายซอฟต์แวร์

5.3.3 ข้อกำหนดความต้องการต่าง ๆ ด้านเทคนิคจากผู้จำหน่ายซอฟต์แวร์

5.3.4 ผลกระทบและการดูแลรักษาระบบภายหลังการเปลี่ยนแปลง

5.3.5 การจัดทำสำเนาของซอฟต์แวร์ก่อนการเปลี่ยนแปลง

5.3.6 การทดสอบการเปลี่ยนแปลง

5.3.7 การจัดทำเอกสารประกอบการเปลี่ยนแปลง

5.4 การป้องกันการรั่วไหลของสารสนเทศ

หน่วยงานต้องมีการควบคุมเพื่อป้องกันการรั่วไหลของสารสนเทศ ซึ่งมีโอกาสที่จะเกิดขึ้นได้จากผลของชุดคำสั่งที่แอบแฝงมากับซอฟต์แวร์สำเร็จรูป ส่งผลกระทบให้ระบบทำงานผิดพลาดหรือแอบเปิดเผยข้อมูลของหน่วยงาน ดังนั้น จึงต้องมีการควบคุมเพื่อป้องกันโปรแกรมหรือชุดคำสั่งที่อาจแอบแฝงมากับซอฟต์แวร์สำเร็จรูปก่อนการจัดซื้อซอฟต์แวร์สำเร็จรูปต้องพิจารณาการควบคุม ดังต่อไปนี้

5.4.1 จัดซื้อซอฟต์แวร์ที่เป็นเวอร์ชันซึ่งจัดจำหน่ายในเชิงพาณิชย์แล้ว (ไม่ใช่เวอร์ชันทดลอง) โดยจัดซื้อซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น

5.4.2 ถ้าเป็นไปได้ให้นำ Source Code มาตรวจสอบก่อนนำมาใช้งานจริง โดยทำการสแกนหาข้อมูลหรือชุดคำสั่งแอบแฝง ตลอดจนการทดสอบก่อนที่จะนำไปติดตั้งในระบบใช้งานจริง

5.4.3 มีการควบคุมการเข้าถึง Source Code เพื่อป้องกันการแก้ไขโดยไม่ได้รับอนุญาต

5.4.4 ตรวจและเฝ้าระวังการใช้ทรัพยากรในระบบคอมพิวเตอร์หลังจากที่นำซอฟต์แวร์มาใช้งาน

5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

การให้หน่วยงานภายนอกพัฒนาซอฟต์แวร์เพื่อใช้งานภายในหน่วยงานต้องพิจารณาหัวข้อดังต่อไปนี้

5.5.1 สิทธิบัตรหรือลิขสิทธิ์ความเป็นเจ้าของซอฟต์แวร์

5.5.2 สิทธิ์ความเป็นเจ้าของใน Source Code ของโปรแกรม

5.5.3 สัญญาหรือข้อตกลงด้านความมั่นคงปลอดภัยในการพัฒนาโปรแกรม เช่น การไม่เขียนโปรแกรมแอบแฝง เป็นต้น

5.5.4 ความรับผิดชอบหากเกิดปัญหาในซอฟต์แวร์

5.5.5 ความน่าเชื่อถือของหน่วยงานภายนอก

5.5.6 การทดสอบการติดตั้งเพื่อป้องกันชุดคำสั่งหรือโปรแกรมแอบแฝง

5.5.7 ข้อตกลงการเข้าใช้ Source Code ในกรณีบริษัทผู้ผลิตไม่สามารถให้บริการได้ (Escrow Arrangement)

5.5.8 การอบรมให้ความรู้แก่พนักงานและลูกจ้างของหน่วยงาน

5.5.9 เอกสารประกอบระบบงาน

6. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

หน่วยงานต้องทำการตรวจสอบความเสี่ยงของช่องโหว่ ปรับปรุงโปรแกรมตลอดจนติดตามข้อมูลข่าวสารที่เกี่ยวกับช่องโหว่ในระบบต่าง ๆ อย่างสม่ำเสมอเป็นระยะ ๆ โดยมีแนวทางปฏิบัติดังนี้

6.1 กำหนดบทบาทและหน้าที่ความรับผิดชอบ เพื่อมอบหมายให้มีผู้รับผิดชอบในการบริหารจัดการช่องโหว่ ซึ่งรวมถึงการเฝ้าระวังภัยจากช่องโหว่ การประเมินความเสี่ยงที่มีจากช่องโหว่ การอุดช่องโหว่ การติดตามทรัพย์สินสารสนเทศ และการประสานงานตามที่จำเป็นในการบริหารจัดการควบคุมช่องโหว่

6.2 มีแหล่งข้อมูลที่เชื่อถือได้ในการติดตามข่าวสารภัยจากช่องโหว่ และการจัดการด้านเทคนิคเพื่อให้ตระหนักถึงช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์และเทคโนโลยีอื่นๆ

6.3 จัดการแก้ไขช่องโหว่ตามความรุนแรงของเหตุการณ์

6.4 หากไม่มีชุดคำสั่งอุดช่องโหว่ (Patch) ให้ดำเนินการประเมินความเสี่ยงในการติดตั้งชุดคำสั่งดังกล่าวโดยเปรียบเทียบกับความเสี่ยงจากภัยที่มีจากช่องโหว่

6.5 ทำการทดสอบชุดคำสั่งอุดช่องโหว่ (Patch) และทำการประเมินก่อนที่จะติดตั้งแก้ไขระบบ

6.6 หากไม่มีคำสั่งอุดช่องโหว่ (Patch) ให้พิจารณามาตรการควบคุมอื่นๆ อย่างเช่น

- ปิดการให้บริการหรือการใช้ระบบในส่วนที่เกี่ยวข้องกับช่องโหว่
- ดัดแปลงหรือเพิ่มมาตรการควบคุม เช่น การกำหนดไฟร์วอลล์ เป็นต้น
- เฝ้าระวังมากขึ้นเพื่อตรวจจับหรือป้องกันการบุกรุกจริง
- แจ้งข่าวสารหรือเพิ่มความตระหนักถึงภัยช่องโหว่

6.7 จัดเก็บ Audit Log ตามระเบียบปฏิบัติ

6.8 ทำการติดตามและประเมินกระบวนการในการบริหารจัดการช่องโหว่อย่างสม่ำเสมอ ในกรณีระบบที่มีความเสี่ยงสูง ต้องมีการจัดการอย่างเข้มงวด