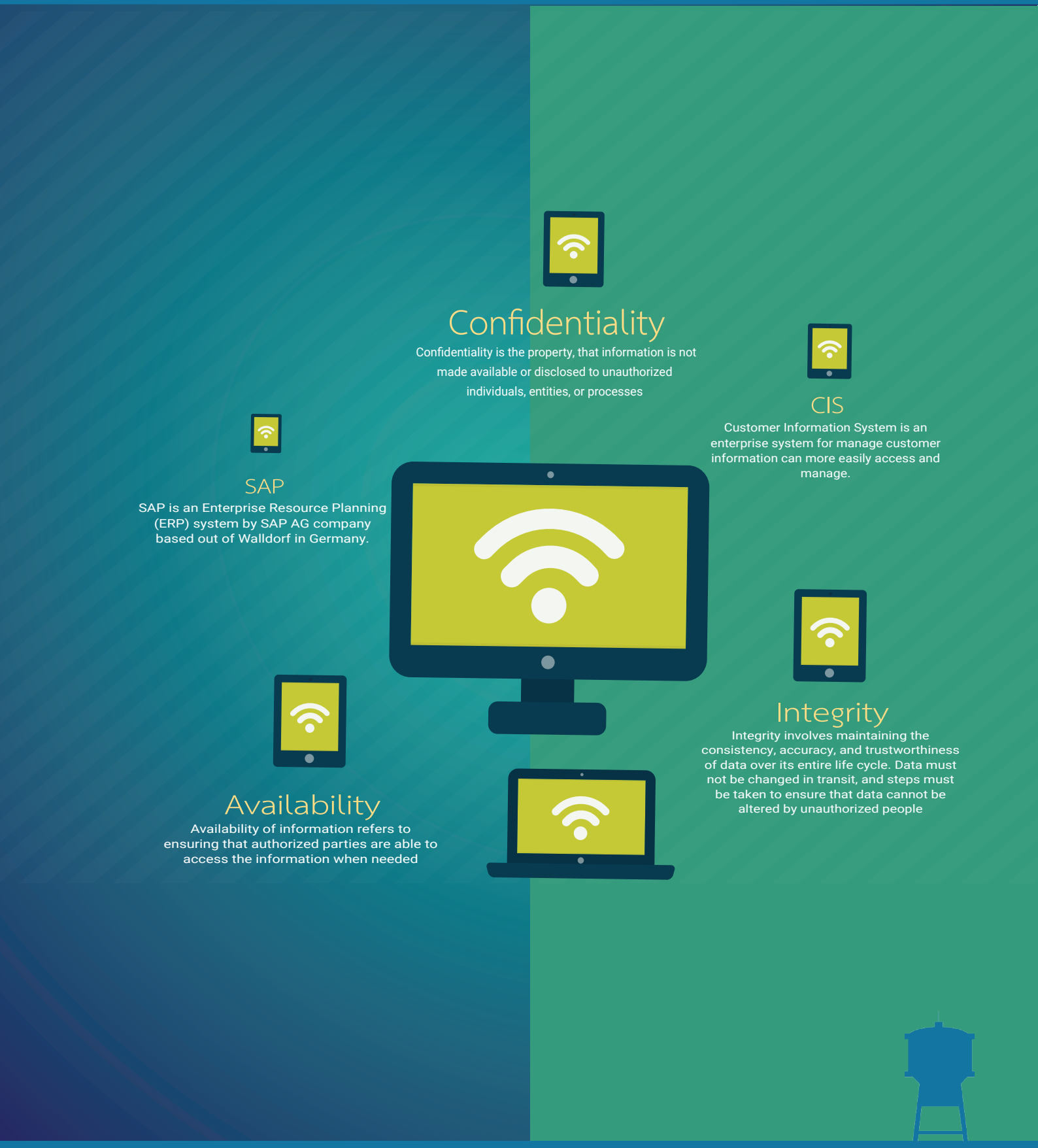
นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ.
(พ.ศ. ๒๕๖๘)



Confidentiality

Confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes

CIS

Customer Information System is an enterprise system for manage customer information can more easily access and manage.

SAP

SAP is an Enterprise Resource Planning (ERP) system by SAP AG company based out of Walldorf in Germany.

Integrity

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people

Availability

Availability of information refers to ensuring that authorized parties are able to access the information when needed

การประปาส่วนภูมิภาค
Provincial Waterworks Authority

คณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัย
ของการประปาส่วนภูมิภาค
มิถุนายน ๒๕๖๘

คำนำ

การประปาส่วนภูมิภาค (กปภ.) เป็นหน่วยงานรัฐวิสาหกิจภายใต้กระทรวงมหาดไทย ที่ให้บริการสาธารณูปโภคพื้นฐานด้านน้ำประปาแก่ประชาชนในส่วนภูมิภาค ครอบคลุมพื้นที่ ๗๔ จังหวัด ทั่วประเทศ (ยกเว้น กรุงเทพฯ นนทบุรี สมุทรปราการ)

ปัจจุบัน กปภ. ได้นำเทคโนโลยีดิจิทัลเข้ามาเป็นเครื่องมือสนับสนุนการทำงานในส่วนต่างๆ เพื่อช่วยอำนวยความสะดวกให้กับพนักงาน และการให้บริการแก่ประชาชน ตามนโยบายการขับเคลื่อนดิจิทัลเพื่อเศรษฐกิจและสังคม (Digital Economy) ของรัฐบาล ถึงแม้ว่าเทคโนโลยีดิจิทัลจะมีประโยชน์และช่วยอำนวยความในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจใช้ช่องโหว่ของการนำเทคโนโลยีดิจิทัลมาใช้งาน เข้ามาสร้างความเสียหายหรือส่งผลกระทบต่อดำเนินธุรกิจของ กปภ.

กปภ. จึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ. และขั้นตอนแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. โดยอ้างอิงมาตรฐาน ISO/IEC ๒๗๐๐๑ ซึ่งเป็นมาตรฐานสากลว่าด้วยเรื่องการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) เพื่อใช้เป็นแนวทางปฏิบัติสำหรับผู้บริหาร พนักงาน และลูกจ้าง กปภ. สามารถใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศได้อย่างปลอดภัย

สารบัญ

เรื่อง **หน้า**

เรื่อง **หน้า**

เรื่อง **หน้า**

ประกาศการประปาส่วนภูมิภาค
เรื่อง นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ. (พ.ศ. ๒๕๖๘)

---

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยต้องจัดทำเป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

๒. วัตถุประสงค์

๒.๑ เพื่อให้ กปภ. มีนโยบายและแนวทางปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยครอบคลุมประเด็นด้านการรักษาความมั่นคงปลอดภัยตามที่กฎหมายกำหนด เพื่อป้องกันภัยคุกคามต่างๆ ที่อาจส่งผลกระทบต่อการดำเนินธุรกิจของ กปภ.

๒.๒ เพื่อใช้เป็นกรอบและแนวทางปฏิบัติในการดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย ทั้งในด้านของการรักษาความลับ (Confidentiality) การรักษาความถูกต้อง (Integrity) และความพร้อมใช้ (Availability)

๒.๓ เพื่อให้ผู้มีส่วนได้ส่วนเสีย (Stakeholders) ทั้งภายในและภายนอกเกิดความเชื่อมั่นในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ.

๓. เนื้อหา

๓.๑ ขอบข่าย

๓.๑.๑ ข้อมูลทั้งหมดในการดำเนินกิจการของ กปภ. ทั้งในส่วนที่เป็นอิเล็กทรอนิกส์หรือกระดาษ ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน รวมถึงการทำลาย

๓.๑.๒ ทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ที่เป็นฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์พกพาที่ใช้ปฏิบัติงาน อุปกรณ์ต่อพ่วงคอมพิวเตอร์ อุปกรณ์เครือข่ายคอมพิวเตอร์ ข้อมูลสารสนเทศ และโปรแกรมคอมพิวเตอร์ เป็นต้น

๓.๑.๓ บุคคลที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูล ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของ กปภ. ได้แก่ ผู้บริหาร พนักงาน ลูกจ้างของ กปภ. รวมถึงบุคคลภายนอกที่มาใช้บริการ

๓.๒ นโยบาย

๓.๒.๑ กำหนดให้มีนโยบายและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. โดยครอบคลุมประเด็นต่างๆ อย่างน้อยดังนี้

๓.๒.๑.๑ นโยบาย...

๓.๒.๑.๑ นโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยด้านทรัพยากรบุคคล

๓.๒.๑.๒ นโยบายและแนวทางปฏิบัติด้านการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

๓.๒.๑.๓ นโยบายและแนวทางปฏิบัติด้านการควบคุมการเข้าถึง

๓.๒.๑.๔ นโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

๓.๒.๑.๕ นโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

๓.๒.๑.๖ นโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน

๓.๒.๑.๗ นโยบายและแนวทางปฏิบัติด้านการบริหารจัดการการรักษาความมั่นคงปลอดภัยในการติดต่อสื่อสาร

๓.๒.๑.๘ นโยบายและแนวทางปฏิบัติด้านการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ

๓.๒.๑.๙ นโยบายและแนวทางปฏิบัติด้านการบริหารจัดการผู้ให้บริการภายนอก

๓.๒.๑.๑๐ นโยบายและแนวทางปฏิบัติด้านการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ

๓.๒.๑.๑๑ นโยบายและแนวทางปฏิบัติด้านการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๓.๒.๑.๑๒ นโยบายและแนวทางปฏิบัติด้านการปฏิบัติตามข้อกำหนด

๓.๒.๑.๑๓ นโยบายและแนวทางปฏิบัติด้านการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓.๒.๑.๑๔ นโยบายและแนวทางปฏิบัติด้านการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒.๑.๑๕ นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๒ ผู้ใช้งานต้องปฏิบัติตามกฎหมาย นโยบาย ระเบียบ คำสั่ง ขั้นตอนและแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ. หากผู้ใช้งานฝ่าฝืนและก่อหรืออาจก่อให้เกิดความเสียหายแก่ กปภ. หรือบุคคลหนึ่งบุคคลใด กปภ. จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ใช้งานที่ฝ่าฝืนตามความเหมาะสม

๓.๒.๓ ให้มีการติดตามและประเมินผลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ.

๓.๒.๔ ให้มีการทบทวน/ปรับปรุง นโยบายและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. อย่างน้อย ปีละ ๑ ครั้ง

๓.๒.๕ ให้ผู้ว่าการ...

๓.๒.๕ ให้ผู้ว่าการ กปภ. เป็นผู้รับผิดชอบระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ กรณีเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

๔. กฎหมาย ระเบียบข้อบังคับ และประกาศที่เกี่ยวข้อง

๔.๑ พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๔.๒ พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๓ พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔.๔ พระราชบัญญัติ คุณสมบัติมาตรฐานสำหรับกรรมการและพนักงานรัฐวิสาหกิจ พ.ศ. ๒๕๑๘

๔.๕ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๔.๖ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๔.๗ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๔.๘ ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔

๔.๙ ระเบียบ กปภ. ว่าด้วยหลักเกณฑ์และวิธีการรับสมัคร การคัดเลือก การสอบคัดเลือก และการบรรจุพนักงานและลูกจ้าง พ.ศ.๒๕๒๕

๔.๑๐ ระเบียบ กปภ. ว่าด้วยหลักฐานเกี่ยวกับประวัติของผู้ปฏิบัติงาน พ.ศ. ๒๕๕๘

๔.๑๑ ระเบียบ กปภ. ว่าด้วยการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัย พ.ศ. ๒๕๕๘

๔.๑๒ ประกาศการประปาส่วนภูมิภาค เรื่อง นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๔

ประกาศ ณ วันที่ ๒๖ มิถุนายน พ.ศ. ๒๕๖๘

(นายจักรพงศ์ คำจันทร์)
ผู้ว่าการการประปาส่วนภูมิภาค

แนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ อย่างปลอดภัยของ กปภ. (พ.ศ. ๒๕๖๘)

คำนิยาม

“ผู้ใช้งาน” หมายความถึง ผู้ที่ได้รับอนุญาต (Authorized) ให้สามารถเข้ามาใช้งานหรือดูแลรักษาระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ. โดยมีสิทธิและหน้าที่ตามหน้าที่ความรับผิดชอบ

“ผู้บริหารระดับสูง” หมายความถึง ผู้ว่าการ รองผู้ว่าการ ผู้ช่วยผู้ว่าการ ที่ปรึกษาฯ ผู้เชี่ยวชาญ ผู้อำนวยการฝ่าย ผู้อำนวยการสำนัก ผู้อำนวยการการประปาส่วนภูมิภาคเขต ผู้ช่วยผู้อำนวยการการประปาส่วนภูมิภาคเขต ผู้จัดการการประปาส่วนภูมิภาค (ชั้นพิเศษ)

“ผู้บริหาร” หมายความถึง ผู้อำนวยการกอง ผู้จัดการประปา และหัวหน้างาน

“พนักงานและลูกจ้าง” หมายความถึง พนักงานและลูกจ้างของ กปภ. รวมถึงบุคคลอื่นที่ กปภ. มอบหมายให้ปฏิบัติงานตามสัญญา หรือ ข้อตกลง

“ผู้ปฏิบัติงานชั่วคราว (Temporary Worker)” หมายความถึง บุคคลที่ได้รับอนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ กปภ. ได้ชั่วคราว เพื่อประโยชน์ในการดำเนินธุรกิจของ กปภ. เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับองค์กร ได้แก่ ที่ปรึกษา (Consultant) ผู้ปฏิบัติงานตามสัญญาจ้าง (Contractor) นิสิตนักศึกษาฝึกงาน เป็นต้น

“สิทธิของผู้ใช้งาน” หมายความถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ กปภ.

“ทรัพย์สินด้านเทคโนโลยีสารสนเทศ” หมายความถึง รายการฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ของ กปภ. เช่น เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์เครือข่ายคอมพิวเตอร์ อุปกรณ์ที่ใช้ปฏิบัติงานแบบพกพา อุปกรณ์ต่อพ่วงคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความถึง การอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้แก่ผู้ใช้งาน ในการเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศของ กปภ. ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนการกำหนดข้อปฏิบัติต่างๆ สำหรับการเข้าใช้งานระบบ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความถึง การรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความถึง สถานการณ์ใดๆ ที่เกิดขึ้นโดยไม่ได้คาดการณ์ไว้ล่วงหน้า อันส่งผลกระทบต่อความมั่นคงปลอดภัย และก่อให้เกิดความเสียหายต่อระบบสารสนเทศ รวมทั้งเกิดการรั่วไหลของข้อมูลของ กปภ.

“เครือข่ายคอมพิวเตอร์” หมายความถึง เครือข่ายคอมพิวเตอร์ของ กปภ. ประกอบด้วย ระบบเครือข่ายระยะใกล้ (LAN) ระบบเครือข่ายอินเทอร์เน็ต (Internet) ระบบเครือข่ายเสมือน (VPN) และระบบเครือข่ายไร้สาย (Wireless LAN)

“ระบบสารสนเทศ” หมายความถึง ระบบงานที่ถูกออกแบบขึ้นมาเพื่อเก็บรวบรวมข้อมูล จัดการข้อมูลเพื่อนำไปใช้ประโยชน์ในการปฏิบัติงาน การตัดสินใจของ กปภ. โดยการใช้เทคโนโลยีสารสนเทศอันได้แก่ ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ รวมทั้งระบบอื่นๆ ที่เกี่ยวข้องของ กปภ. เข้ามาช่วย ในการดำเนินงาน

“ระบบสารสนเทศที่สำคัญ” หมายความถึง ระบบสารสนเทศที่มีความสำคัญสูงต่อการดำเนินธุรกิจของ กปภ. ได้แก่ ระบบสารสนเทศด้านผู้ใช้น้ำ (CIS) ระบบควบคุมและสั่งการจากระยะไกล (SCADA) ระบบงานทางธุรกิจ (SAP) ฯลฯ เป็นต้น

“ระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความถึง ระบบสารสนเทศของ กปภ. ที่ให้บริการพื้นฐานสารสนเทศที่สำคัญของประเทศ ต้องมีการควบคุมให้มีความมั่นคงปลอดภัยและสามารถให้บริการได้อย่างต่อเนื่อง เช่น บริการที่เกี่ยวข้องกับงานควบคุมคุณภาพน้ำประปา (ระบบ LIMS) บริการที่เกี่ยวข้องกับการผลิตน้ำ บริการจำหน่ายน้ำ/รับชำระค่าน้ำประปา (ระบบ CIS) รวมถึงระบบเครือข่าย และระบบ Datacenter ที่สนับสนุนการให้บริการดังกล่าว เป็นต้น

“ข้อมูล” หมายความถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือ สิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ระบบข้อมูล” หมายความถึง กระบวนการประมวลผลข้อมูลที่เก็บรวบรวมด้วยเครื่องมืออิเล็กทรอนิกส์ เครื่องคอมพิวเตอร์

“การรักษาความปลอดภัยข้อมูล” หมายความถึง แนวทางปฏิบัติตลอดจนการดำเนินการใดๆ เพื่อปกป้องมิให้เกิดความเสียหายหรือสูญเสียของระบบข้อมูลรวมทั้งเกิดการรั่วไหลของข้อมูล

“ผู้ดูแลเครือข่ายคอมพิวเตอร์” หมายความถึง พนักงานที่ได้รับมอบหมายจากผู้ว่าการให้มีหน้าที่รับผิดชอบในการดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์ให้สามารถทำงานได้อย่างต่อเนื่อง ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของพนักงานเพื่อให้เป็นไปตามขั้นตอนและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

“ผู้ดูแลระบบสารสนเทศ” หมายความถึง พนักงานที่ได้รับมอบหมายจากผู้ว่าการให้มีหน้าที่รับผิดชอบในการดูแลรักษาและปรับปรุงระบบสารสนเทศให้สามารถทำงานได้อย่างต่อเนื่อง รวมทั้งจะต้องสอดส่องดูแลการใช้ระบบสารสนเทศของพนักงานเพื่อให้เป็นไปตามขั้นตอนและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

“เหตุละเมิดความมั่นคงปลอดภัย” หมายความถึง เหตุการณ์ใดๆ ที่ส่งผลกระทบหรือเป็นภัยคุกคามต่อความมั่นคงปลอดภัยของ กปภ. ซึ่งเหตุนั้นอาจเกิดขึ้นโดยตั้งใจ (Deliberate) โดยอุบัติเหตุ (Accidental) หรือโดยความประมาทเลินเล่อของพนักงาน (Human Error) และมีได้หลายรูปแบบ ทั้งเหตุละเมิดความมั่นคงปลอดภัยในเชิงกายภาพ (Physical Incident) เชิงเทคนิค (Technical Incident) และเชิงกระบวนการ (Procedural Incident)

“สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media)” หมายความถึง Flash Drive, CD, External Drive และอุปกรณ์เคลื่อนย้ายอื่นๆ ที่สามารถบันทึกและจัดเก็บข้อมูลได้

คำนิยามอื่นๆ ให้เป็นไปตามเอกสารในภาคผนวก อภิธานศัพท์

หมวดที่ ๑
นโยบายความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
(Human resource security policy)

เพื่อให้ กปภ. มีกระบวนการในการคัดเลือก การควบคุมการปฏิบัติงาน และการฝึกอบรมของบุคลากรตลอดระยะเวลาการจ้างงาน และสร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานให้กับพนักงาน โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติด้านการบริหารจัดการทรัพยากรบุคคล
  (Human resource management guideline)

ส่วนที่ ๑
แนวทางปฏิบัติด้านการบริหารจัดการทรัพยากรบุคคล
(Human resource management guideline)

วัตถุประสงค์

- เพื่อกำหนดกระบวนการในการบริหารจัดการทรัพยากรบุคคลให้มีความมั่นคงปลอดภัยตั้งแต่กระบวนการก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดการจ้างงาน
- เพื่อสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานให้กับบุคลากรของ กปภ.

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- ฝ่ายบริหารทรัพยากรบุคคล
- ฝ่ายพัฒนาทรัพยากรบุคคลและนวัตกรรม

แนวทางการปฏิบัติ

๑. กระบวนการก่อนการจ้างงาน (Prior of employment)

๑.๑. ในการพิจารณารับพนักงาน และลูกจ้างของ กปภ. เข้าทำงานต้องดำเนินการตรวจสอบประวัติและคุณสมบัติโดยต้องปฏิบัติตามกฎหมายและระเบียบข้อบังคับ ดังนี้

๑.๑.๑. พ.ร.บ. คุณสมบัติมาตรฐานสำหรับกรรมการและพนักงานรัฐวิสาหกิจ พ.ศ. ๒๕๑๘ และฉบับที่มีการแก้ไขเพิ่มเติม

๑.๑.๒. ระเบียบ กปภ. ว่าด้วยหลักเกณฑ์และวิธีการรับสมัคร การคัดเลือก การสอบคัดเลือก และการบรรจุพนักงานและลูกจ้าง พ.ศ. ๒๕๕๕ และฉบับที่มีการแก้ไขเพิ่มเติม

๑.๑.๓. ระเบียบ กปภ. ว่าด้วยหลักฐานเกี่ยวกับประวัติของผู้ปฏิบัติงาน พ.ศ. ๒๕๕๘ และฉบับที่มีการแก้ไขเพิ่มเติม

๑.๒. ในการเก็บรวบรวม เปิดเผย และทำลายหลักฐานเกี่ยวกับประวัติของผู้ปฏิบัติงานต้องปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคล พ.ศ. ๒๕๖๒

๒. กระบวนการระหว่างการจ้างงาน (During of employment)

๒.๑. พนักงานหรือลูกจ้างของ กปภ. ที่ได้รับบรรจุเข้ามาใหม่ทุกคนต้องได้รับการอบรมเกี่ยวกับนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ กปภ. โดยจัดให้เป็นส่วนหนึ่งของการปฐมนิเทศพนักงานใหม่

๒.๒. ต้องมีการประกาศแจ้งเวียนนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้กับผู้บริหาร พนักงาน และลูกจ้างของ กปภ. ทราบและถือปฏิบัติ

๒.๓. จัดให้มีการอบรมหรือเผยแพร่ความรู้เพื่อสร้างความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับผู้บริหาร พนักงาน และลูกจ้างของ กปภ. อย่างน้อยปีละ ๑ ครั้ง

๒.๔. กองความมั่นคงปลอดภัยไซเบอร์และฝ่ายพัฒนาทรัพยากรบุคคลและนวัตกรรมต้องจัดให้มีมาตรการในการพัฒนาศักยภาพบุคลากรของ กปภ. ในด้านทักษะของบุคลากร โดยให้มีการส่งเสริมและสนับสนุนการเรียนรู้ และการพัฒนาบุคลากรอย่างต่อเนื่อง โดยให้กำหนดแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม โดยอาจอยู่ในรูปแบบ ดังนี้

๒.๔.๑. แบบรวมศูนย์

๒.๔.๒. แบบกระจายอำนาจบางส่วน

๒.๔.๓. แบบกระจายอำนาจอย่างเต็มที่

๒.๕. ให้ทบทวนแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม รวมถึงเอกสาร สื่อ หรือเนื้อหาที่ใช้ในการดำเนินการตามแผนงานหรือโครงการดังกล่าวให้สอดคล้องกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้นอยู่เสมอ ทั้งนี้ ให้ทบทวนอย่างน้อยปีละ ๑ ครั้ง

๓. กระบวนการโยกย้ายและสิ้นสุดการจ้างงาน (Rotation and terminate of employment)

๓.๑. ผู้บริหาร พนักงาน และลูกจ้างของ กปภ. ซึ่งเป็นผู้ที่จะพ้นสภาพการเป็นพนักงานหรือสิ้นสุดสัญญาจ้างงานจะต้องคืนทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ที่ตนเองถือครองทั้งหมดให้กับหน่วยงานต้นสังกัดภายในวันสิ้นสุดการจ้างงาน หรือสิ้นสุดสัญญาจ้างงาน

๓.๒. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องดำเนินการ ถอดถอน ยกเลิก หรือแก้ไขสิทธิ์การใช้งานของพนักงานหรือลูกจ้าง โดยแบ่งเป็น ๒ กรณี ดังนี้

๓.๒.๑. กรณีโยกย้ายหน่วยงาน (Rotation)

ให้ดำเนินการ ถอดถอน ยกเลิก หรือแก้ไขสิทธิ์การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของพนักงานหรือลูกจ้างผู้นั้นทันที หลังจากพนักงานหรือลูกจ้างผู้นั้นเข้ารับตำแหน่งใหม่หรือจนกว่าเสร็จสิ้นการยืมตัวปฏิบัติหน้าที่จากหน่วยงานต้นสังกัดเดิม

๓.๒.๒. กรณีสิ้นสุดการจ้างงาน (Terminate)

ให้ดำเนินการ ถอดถอน หรือยกเลิกสิทธิ์การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของพนักงานหรือลูกจ้างผู้นั้นทันทีหลังจากที่ได้รับบันทึกคำสั่ง ลาออก/เกษียณอายุ/ให้ออก/ไล่ออก จากหน่วยงานที่เกี่ยวข้อง

เอกสารอ้างอิง

๑. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

หมวดที่ ๒
นโยบายการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(IT asset management policy)

เพื่อให้ทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ได้รับการป้องกันและปกป้องอย่างเหมาะสม โดยจัดให้มีการจัดทำทะเบียน ทบทวน บำรุงรักษา และการเรียกคืนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างถูกต้องครบถ้วน โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

ส่วนที่ ๑
แนวทางปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(IT assets management guideline)

วัตถุประสงค์

- เพื่อให้มีการจัดทำรายการทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศและมีการปรับปรุงรายการทะเบียนทรัพย์สินให้เป็นปัจจุบัน
- เพื่อให้มีการบำรุงรักษา การรับประกัน และวางแผนจัดหาหรือทดแทนทรัพย์สินด้านเทคโนโลยีสารสนเทศให้สามารถใช้งานได้อย่างต่อเนื่อง
- เพื่อให้มีการเรียกคืนทรัพย์สินด้านเทคโนโลยีสารสนเทศกรณีที่พ้นสภาพหรือสิ้นสุดสัญญาจ้างงานของ กปภ.

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ หรือ หน่วยงานที่มีหน้าที่รับผิดชอบในการดูแลและบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ.

แนวทางการปฏิบัติ

๑. รายการทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT assets inventory list)
เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT assets owner) หรือหน่วยงานที่มีหน้าที่รับผิดชอบในการดูแลและบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ต้องมีการจัดทำรายการทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ ได้แก่ รายการฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) เพื่อประโยชน์ในการค้นหาและสามารถติดตามรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. โดยต้องระบุรายละเอียดครอบคลุมหัวข้ออย่างน้อย ดังนี้
๑.๑. ชื่อผู้ใช้งาน หรือ ชื่อหน่วยงานของทรัพย์สินด้านเทคโนโลยีสารสนเทศ

๑.๒. หมายเลขครุภัณฑ์ หรือ หมายเลขผลิตภัณฑ์ (Serial Number)
๑.๓. รายละเอียด (ยี่ห้อ/รุ่น/ระบบปฏิบัติการและเวอร์ชัน (ถ้ามี))
๑.๔. ประเภทของทรัพย์สินด้านเทคโนโลยีสารสนเทศ เช่น PC, Notebook, Server, Network ฯลฯ
๑.๕. สถานที่ตั้งของทรัพย์สินด้านเทคโนโลยีสารสนเทศ
๑.๖. ประเภทการจัดหา (จัดซื้อ/เช่า)
๑.๗. ชื่อบริษัทผู้รับจ้างและเลขที่สัญญา
๑.๘. วันที่ได้มาหรือวันที่เริ่มติดตั้ง
๑.๙. วันสิ้นสุดสัญญารับประกัน (Warranty)
๑.๑๐. วันสิ้นสุดการให้บริการจากผู้ผลิต (End of support) (ถ้ามี)
๑.๑๑. รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา

๒. การปรับปรุงรายการทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT assets inventory list review)
เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ หรือหน่วยงานที่มีหน้าที่รับผิดชอบในการดูแลและบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ต้องมีการปรับปรุงรายการทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน โดยจะต้องดำเนินการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับรายการทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๓. การรับประกันและการบำรุงรักษาเชิงป้องกันทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของ กปภ. (IT assets warranty support and preventive maintenance)
๓.๑. เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ หรือหน่วยงานที่มีหน้าที่รับผิดชอบในการดูแลและบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ต้องกำหนดให้มีการรับประกันการซ่อมแซมแก้ไข (Warranty Support) กรณีที่ทรัพย์สินด้านเทคโนโลยีสารสนเทศเสียหายหรือชำรุดอย่างต่อเนื่อง
๓.๒. เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ หรือหน่วยงานที่มีหน้าที่รับผิดชอบในการดูแลและบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ต้องกำหนดให้มีการบำรุงรักษาเชิงป้องกัน (Preventive maintenance) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคตอย่างน้อยปีละ ๑ ครั้ง โดยต้องดำเนินการติดแผ่นสติกเกอร์บนทรัพย์สินด้านเทคโนโลยีสารสนเทศโดยแสดงข้อมูลอย่างน้อย ดังนี้
๓.๒.๑. ชื่อบริษัทผู้รับจ้างในสัญญา
๓.๒.๒. เลขที่สัญญา
๓.๒.๓. ระยะเวลาการบำรุงรักษา
๓.๒.๔. เบอร์โทรศัพท์ของบริษัทผู้รับจ้างในสัญญาที่สามารถติดต่อได้กรณีที่มีปัญหา

๔. การวางแผนจัดหาหรือทดแทนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT assets acquisition plan)
เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ หรือ หน่วยงานที่มีหน้าที่รับผิดชอบในการดูแลและบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ต้องมีการวางแผนจัดหาหรือทดแทนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุและสภาพการใช้งาน

๕. การเรียกคืนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT assets return)
ผู้บริหาร พนักงาน และลูกจ้างของ กปภ. ซึ่งเป็นผู้ที่จะพ้นสภาพการเป็นพนักงานหรือสิ้นสุดสัญญาจ้างงานจะต้องคืนทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กปภ. ที่ตนเองถือครองทั้งหมดให้กับหน่วยงานต้นสังกัดภายในวันสิ้นสุดการจ้างงาน หรือสิ้นสุดสัญญาจ้างงาน

เอกสารอ้างอิง

- ไม่มี -

หมวดที่ ๓
นโยบายการควบคุมการเข้าถึง
(Access control policy)

เพื่อให้ กปภ. มีการกำหนดสิทธิ์ และควบคุมการเข้าถึงระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของ กปภ. เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์
  (Network access control guideline)
- ส่วนที่ ๒ แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
  (Wireless LAN access control guideline)
- ส่วนที่ ๓ แนวทางปฏิบัติการควบคุมการเข้าถึงจากระยะไกล
  (Remote access control guideline)
- ส่วนที่ ๔ แนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง
  (Access rights management guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์
(Network access control guideline)

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ โดยไม่ได้รับอนุญาต

ผู้ปฏิบัติ

- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- ผู้ใช้งานเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. การแบ่งแยกเครือข่ายคอมพิวเตอร์ออกเป็นกลุ่ม (Segregation in network)

ผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องมีการแบ่งแยกเครือข่ายคอมพิวเตอร์ของ กปภ. ออกเป็นกลุ่ม เพื่อป้องกันความปลอดภัยในเครือข่ายคอมพิวเตอร์ ดังนี้

<u>กปภ.สำนักงานใหญ่</u> แบ่งแยกเครือข่ายคอมพิวเตอร์ของ กปภ. ออกเป็น ๖ กลุ่ม คือ

๑.๑. Users Zone เป็นกลุ่มที่ใช้สำหรับพนักงานภายในของ กปภ. โดยแบ่งออกเป็น ๒ ประเภท คือ
- ๑.๑.๑. เครือข่ายคอมพิวเตอร์ภายในแบบมีสาย (LAN)
- ๑.๑.๒. เครือข่ายคอมพิวเตอร์แบบไร้สาย (Wireless LAN)

๑.๒. External Zone เป็นกลุ่มที่ใช้สำหรับติดต่อสื่อสารกับเครือข่ายคอมพิวเตอร์ภายนอก กปภ.

๑.๓. Presentation Zone เป็นกลุ่มที่ใช้สำหรับติดต่อสื่อสารระหว่างเครือข่ายคอมพิวเตอร์ภายนอก กปภ. กับเครื่องแม่ข่ายเพื่อให้บริการเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอก กปภ.

๑.๔. Application Zone เป็นกลุ่มที่ใช้สำหรับเครื่องคอมพิวเตอร์แม่ข่ายโดยเฉพาะระบบที่มีความสำคัญต่อการดำเนินธุรกิจของ กปภ. เพื่อให้บริการเฉพาะภายใน กปภ.

๑.๕. Management Zone เป็นกลุ่มที่ใช้เพื่อบริหารจัดการระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์สำหรับผู้ดูแลเครือข่ายคอมพิวเตอร์และผู้ดูแลระบบสารสนเทศ

๑.๖. Database Zone เป็นกลุ่มที่ใช้สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการฐานข้อมูลโดยเฉพาะโดยมีความสำคัญต่อการดำเนินธุรกิจของ กปภ. ให้บริการเครือข่ายคอมพิวเตอร์เฉพาะภายใน กปภ.

<u>กปภ.เขต</u> แบ่งแยกเครือข่ายคอมพิวเตอร์ของ กปภ. ออกเป็น ๕ กลุ่ม คือ

๑.๑. Internal Zone เป็นกลุ่มที่ใช้สำหรับพนักงานภายในของ กปภ. โดยแบ่งออกเป็น ๒ ประเภท คือ
- ๑.๑.๑. เครือข่ายคอมพิวเตอร์ภายในแบบมีสาย (LAN)
- ๑.๑.๒. เครือข่ายคอมพิวเตอร์แบบไร้สาย (Wireless LAN)

๑.๒. External Zone เป็นกลุ่มที่ใช้สำหรับติดต่อสื่อสารกับเครือข่ายคอมพิวเตอร์ภายนอก กปภ.

๑.๓. DMZ Zone เป็นกลุ่มที่ใช้สำหรับแยกเครื่องคอมพิวเตอร์แม่ข่ายออกมาจากเครื่องคอมพิวเตอร์ลูกข่ายเพื่อให้บริการเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอก กปภ.

๑.๔. Server Zone เป็นกลุ่มที่ใช้สำหรับแยกเครื่องคอมพิวเตอร์แม่ข่ายโดยเฉพาะระบบที่มีความสำคัญต่อการดำเนินธุรกิจของ กปภ. ออกมาจากเครื่องคอมพิวเตอร์ลูกข่ายเพื่อให้บริการเฉพาะภายใน กปภ.

๑.๕. Management Zone เป็นกลุ่มที่ใช้เพื่อบริหารจัดการระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์สำหรับผู้ดูแลเครือข่ายคอมพิวเตอร์และผู้ดูแลระบบสารสนเทศ (Out of band management)

๒. การควบคุมการจัดเส้นทางและการรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ (Network routing and security control)

๒.๑. ต้องมีการควบคุมเส้นทางการเชื่อมต่อระหว่างหมายเลขเครือข่ายคอมพิวเตอร์ต้นทาง (Source network address) กับหมายเลขเครือข่ายคอมพิวเตอร์ปลายทาง (Destination network address)

๒.๒. การเชื่อมต่อและรับส่งข้อมูลผ่านระบบเครือข่ายอินเทอร์เน็ต ระบบเครือข่ายเสมือน (VPN) ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายไร้สาย (Wireless LAN) หรือระบบเครือข่ายอื่นๆ ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ (Firewall) หรือระบบป้องกันการถูกบุกรุก (IPS) ของ กปภ. โดยเปิดเฉพาะพอร์ต (Port) ที่จำเป็นต่อการทำงานเท่านั้น

พร้อมระบุ IP-Address ต้นทางและปลายทางให้ชัดเจน หากต้องการเปิดพอร์ตเพิ่มเติมนอกเหนือจากที่กำหนด ให้ดำเนินการกรอกแบบฟอร์มขอแก้ไข Policy Firewall

๒.๓. ต้องมีการทบทวน Policy Firewall อย่างน้อยปีละ ๑ ครั้ง

๓. การลงทะเบียนเข้าใช้งานเครือข่ายคอมพิวเตอร์

ต้องจัดให้มีการลงทะเบียนก่อนการเข้าใช้งานเครือข่ายคอมพิวเตอร์ของ กปภ. ตามแนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง

๔. การพิสูจน์ตัวตนเข้าใช้งานเครือข่ายคอมพิวเตอร์

๔.๑. ต้องจัดให้มีระบบพิสูจน์ตัวตนก่อนเข้าใช้งานเครือข่ายคอมพิวเตอร์ เช่น ระบบ Active Directory หรือระบบ LDAP หรือระบบพิสูจน์ตัวตนอื่นๆ ที่ กปภ. กำหนด เพื่อให้สามารถระบุตัวตนของผู้ใช้งานเครือข่ายคอมพิวเตอร์ได้ตามแนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง

๔.๒. ต้องกำหนดให้มีการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งานระบบสารสนเทศเครือข่ายคอมพิวเตอร์ด้วยการใช้ Username/Password หรือวิธีการอื่นๆ ตามที่ กปภ. กำหนด ทั้งนี้ระบบที่มีความสำคัญควรพิจารณาการใช้งานระบบพิสูจน์ตัวตนแบบหลายปัจจัย (Multi factor authen)

๕. การกำหนดสิทธิ์เข้าใช้งานเครือข่ายคอมพิวเตอร์

๕.๑. ต้องมีการกำหนดสิทธิ์เข้าใช้งานเครือข่ายคอมพิวเตอร์ตามแนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง

เอกสารอ้างอิง

๑. ขอใช้งานอินเตอร์เน็ตสำหรับหน่วยงาน/บุคคลภายนอก (IT-FM-SC-๐๑)

๒. แบบฟอร์มขอแก้ไข Policy Firewall (IT-FM-NDA-๐๘)

ส่วนที่ ๒
แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN access control guideline)

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการเข้าถึงระบบเครือข่ายไร้สายของ กปภ. ให้มีความมั่นคงปลอดภัย

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- บุคคลภายนอก/ผู้มาชำระค่าน้ำประปาหรือผู้มาติดต่อ

แนวทางการปฏิบัติ

ผู้ดูแลระบบเครือข่ายหรือผู้ที่เกี่ยวข้องต้องดำเนินการ ดังนี้

๑. การลงทะเบียนเข้าใช้งานระบบเครือข่ายไร้สาย
ต้องจัดให้มีการลงทะเบียนก่อนการเข้าใช้งานระบบเครือข่ายไร้สายของ กปภ. ตามแนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง

๒. การพิสูจน์ตัวตนเข้าใช้งานเครือข่ายคอมพิวเตอร์
๒.๑. ต้องจัดให้มีระบบพิสูจน์ตัวตนก่อนเข้าใช้งานระบบเครือข่ายไร้สาย เช่น ระบบ Active Directory หรือระบบ LDAP หรือระบบพิสูจน์ตัวตนอื่นๆ ตามที่ กปภ. กำหนด เพื่อให้สามารถระบุตัวตนของผู้ใช้งานเครือข่ายคอมพิวเตอร์ได้ตามแนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง
๒.๒. ต้องกำหนดให้มีการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งานระบบเครือข่ายไร้สายด้วยการใช้ Username/Password หรือวิธีการอื่นๆ ที่ กปภ. กำหนด

๓. ต้องกำหนดให้มีการเข้ารหัสลับในการติดต่อสื่อสารระหว่าง Wireless LAN Client กับอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless access point) ด้วยวิธีการที่มีความมั่นคงปลอดภัยเพื่อให้ยากต่อการดักจับข้อมูล

๔. ห้ามผู้ใช้งานที่มิได้มีส่วนเกี่ยวข้องกับการดูแลเครือข่ายคอมพิวเตอร์ติดตั้งระบบเครือข่ายไร้สาย (Wireless LAN) ในพื้นที่ปฏิบัติงานของ กปภ.

๕. ห้ามผู้ใช้งานเปิดฟังก์ชัน Share hotspot/Ad-hoc เพื่อกระจายสัญญาณเครือข่ายของ กปภ. ให้กับบุคคลภายนอก

๖. ห้ามเปิดเผยบัญชีผู้ใช้และรหัสผ่านของตนให้ผู้อื่นทราบหากเกิดปัญหาใดๆ ที่ก่อหรืออาจก่อให้เกิดความเสียหายแก่ กปภ. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้นั้นต้องเป็นผู้รับผิดชอบทุกกรณี

๗. หากมีการฝ่าฝืนและก่อหรืออาจก่อให้เกิดความเสียหายแก่ กปภ. จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ใช้งานที่ฝ่าฝืนตามความเหมาะสม

๘. การให้บริการเครือข่ายไร้สายแก่ผู้มาชำระค่าน้ำประปาหรือผู้มาติดต่อ

๘.๑. ต้องปฏิบัติตามข้อที่ ๑ – ๔

๘.๒. ต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานเครือข่ายไร้สาย

๘.๓. ต้องมีการจำกัดการเข้าถึงเครือข่ายภายในของ กปภ. โดยกำหนดให้สามารถใช้งานเฉพาะอินเทอร์เน็ตเท่านั้น

เอกสารอ้างอิง

๑. ขอใช้งานอินเตอร์เน็ตสำหรับหน่วยงาน/บุคคลภายนอก (IT-FM-SC-๐๑)

ส่วนที่ ๓
แนวทางปฏิบัติการควบคุมการเข้าถึงจากระยะไกล
(Remote access control guideline)

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการเข้าถึงระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์จากภายนอกเครือข่ายคอมพิวเตอร์ของ กปภ. ผ่านระบบ Remote access VPN ที่ กปภ. จัดเตรียมให้

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน ของ กปภ.
- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

การเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของ กปภ. จากระยะไกลผ่านระบบ Remote access VPN ที่ กปภ. จัดเตรียมให้ต้องปฏิบัติ ดังนี้

๑. การร้องขอเข้าใช้งานระบบ Remote access VPN
   ๑.๑. ผู้ใช้งานที่ต้องการใช้งานระบบ Remote access VPN ต้องกรอกรายละเอียดพร้อมระบุเหตุผลและความจำเป็นให้ครบถ้วนลงในแบบฟอร์มขอเข้าใช้งานระบบ Remote access VPN เพื่อขออนุมัติจากผู้บังคับบัญชาตามสายงานและต้องได้รับอนุมัติจาก ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษรก่อนเข้าใช้งาน
   ๑.๒. กรณีมีความจำเป็นต้องการใช้งานระบบ Remote access VPN อย่างเร่งด่วนให้ผู้ร้องขอดำเนินการแจ้งต่อผู้บังคับบัญชาในสายงานของตนเองทราบและขออนุมัติจาก ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมาย ผ่านทาง E-mail Address หรือช่องทางอื่น เพื่อพิจารณาอนุมัติใช้งานเร่งด่วนเป็นกรณีพิเศษเป็นรายกรณีไป
๒. การกำหนดสิทธิ์เข้าใช้งานระบบ Remote access VPN
   ๒.๑. การกำหนดสิทธิ์เข้าใช้งานระบบ Remote access VPN ให้กับผู้ใช้งานต้องปฏิบัติตามแนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง
   ๒.๒. ต้องกำหนดให้มีการการพิสูจน์ตัวตน (Authentication) โดยการใช้ Username/Password ก่อนเข้าใช้งานระบบ Remote access VPN
   ๒.๓. ต้องมีการควบคุมพอร์ต สำหรับใช้งานเท่านั้น
   ๒.๔. ต้องกำหนดระยะเวลาตัดการเชื่อมต่อของผู้ใช้งาน (Session Timeout) เมื่อไม่ได้ใช้งานเป็นระยะเวลาดังนี้
      ๒.๔.๑. กำหนดค่า Session Timeout เป็นระยะเวลา ๕ นาที สำหรับหน่วยงานทั่วไป

๒.๔.๒. กำหนดค่า Session Timeout เป็นระยะเวลา ๑๕ นาที สำหรับหน่วยงานที่มีความจำเป็นต้องการใช้งานเกิน ๕ นาที

๒.๕. ต้องมีการกำหนดกลไกการเข้ารหัสลับ (Encryption Algorithm) เพื่อรักษาความมั่นคงปลอดภัยระหว่างการรับส่งข้อมูล เช่น AES-๒๕๖, RSA หรือที่ดีกว่า

๒.๖. ต้องมีการเก็บบันทึกข้อมูล (Log) การเข้าใช้งานระบบ Remote access VPN เพื่อใช้ตรวจสอบและปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ประกาศใช้งาน

๒.๗. ห้ามนำโปรแกรมหรืออุปกรณ์ใดๆ มาใช้งานเพื่อเข้าถึงระบบสารสนเทศและระบบเครือข่ายของ กปภ. จากระยะไกลโดยไม่ได้รับอนุญาตจาก ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษรหากมีการฝ่าฝืนและก่อหรืออาจก่อให้เกิดความเสียหายแก่ กปภ. จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ใช้งานที่ฝ่าฝืนตามความเหมาะสม

เอกสารที่เกี่ยวข้อง

๑. แบบฟอร์มขอเข้าใช้งานระบบ Remote access VPN (IT-FM-NDA-๑๐)

ส่วนที่ ๔
แนวทางปฏิบัติการบริหารจัดการสิทธิ์การเข้าถึง
(Access rights management guideline)

วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ของ กปภ.

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน (User registration)

๑.๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งานใหม่สำหรับการเข้าถึงระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ.

๑.๒. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องส่งมอบบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานโดยตรงหรือวิธีที่มั่นคงปลอดภัยและแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่โดยปฏิบัติตามแนวทางปฏิบัติการบริหารจัดการรหัสผ่าน

๑.๓. ผู้ใช้งานที่ได้รับอนุญาตแต่ละคนต้องมีบัญชีผู้ใช้งานเป็นของตนเองในกรณีที่ต้องการใช้งานบัญชีผู้ใช้งานร่วมกัน (Shared username) ต้องได้รับความเห็นชอบและอนุมัติจาก ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร

๒. การกำหนดสิทธิ์การเข้าถึง (Privileged access rights)

๒.๑. การกำหนดสิทธิ์การเข้าถึงในระดับปกติ

ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ. ตามหน้าที่ความรับผิดชอบและความจำเป็นของผู้ใช้งานเท่านั้น (Least Privilege)

๒.๒. การกำหนดสิทธิ์การเข้าถึงในระดับสิทธิ์พิเศษหรือสิทธิ์สูงสุด

กรณีที่มีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด เช่น Administrator, Root, Superuser เป็นต้น ผู้ใช้งานผู้นั้นจะต้องได้รับความเห็นชอบและอนุมัติจาก ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร

๓. การทบทวนและเพิกถอนสิทธิ์ (Review and removal of access rights)

๓.๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องทบทวนบัญชีผู้ใช้งานและสิทธิ์ของผู้ใช้งานในแต่ละระบบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๓.๒. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องดำเนินการ ถอดถอน หรือยกเลิกสิทธิ์การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของผู้ใช้งานทันทีหลังจากที่ได้รับบันทึกคำสั่งลาออก/เกษียณอายุ/ให้ออก/ไล่ออก จากหน่วยงานที่เกี่ยวข้อง

เอกสารที่เกี่ยวข้อง

๑. แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบงานทั่วไป (IT-FM-AU-๐๑ – ระบบงานทั่วไป)
๒. แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ SAP (IT-FM-AU-๐๑ - SAP)
๓. แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ CIS (IT-FM-AU-๐๑ - CIS)
๔. แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ OIS (IT-FM-AU-๐๑ - OIS)
๕. แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ LIMS (สนญ.) (IT-FM-AU-๐๑ - LIMS (สนญ.))
๖. แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ LIMS (กปภ.ข.) (IT-FM-AU-๐๑ – (กปภ.ข.))
๗. แบบฟอร์ม ขอสิทธิ์ระบบบัตรประชาชน - CIS (IT-FM-AU-๐๒ - CIS)

หมวดที่ ๔
นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
(Information security policy)

เพื่อให้ กปภ. มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดยมีการจัดชั้นความลับของข้อมูลสารสนเทศ การเข้ารหัสลับของข้อมูลที่สำคัญของ กปภ. และการจัดการสื่อที่ใช้บันทึกข้อมูล เพื่อป้องกันข้อมูลสารสนเทศที่สำคัญของ กปภ. รั่วไหล โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการจัดชั้นความลับของข้อมูลสารสนเทศ
  (Information classification guideline)
- ส่วนที่ ๒ แนวทางปฏิบัติการบริหารจัดการการเข้ารหัสลับข้อมูล
  (Cryptography management procedure)
- ส่วนที่ ๓ แนวทางปฏิบัติการจัดการสื่อที่ใช้บันทึกข้อมูล
  (Media handling guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการจัดชั้นความลับของข้อมูลสารสนเทศ
(Information classification guideline)

วัตถุประสงค์

- เพื่อกำหนดแนวทางปฏิบัติในการกำหนดชั้นความลับ การเก็บรักษา การทำสำเนา การทำลาย และการนำข้อมูลสารสนเทศไปใช้งาน ให้สอดคล้องตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม
- เพื่อป้องกันการเปิดเผยและแก้ไขเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- หน่วยงานเจ้าของข้อมูลสารสนเทศ

แนวทางการปฏิบัติ

๑. หน่วยงานเจ้าของข้อมูลสารสนเทศ (Information Owner) ต้องเป็นผู้รับผิดชอบในการกำหนดชั้นความลับและกำหนดสิทธิ์การเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานโดยพิจารณาจากความสำคัญและผลกระทบหากข้อมูลสารสนเทศนั้นถูกเปิดเผยหรือมีการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

๒. ข้อมูลสารสนเทศที่หน่วยงานเจ้าของข้อมูลสารสนเทศพิจารณาแล้วเห็นว่าไม่ส่งผลกระทบหรือสร้างความเสียหายให้กับ กปภ. สามารถเปิดเผยข้อมูลสารสนเทศดังกล่าวต่อสาธารณะได้โดยไม่ต้องระบุชั้นความลับ

<u>การกำหนดชั้นความลับของข้อมูลสารสนเทศ</u>

การกำหนดชั้นความลับของข้อมูลสารสนเทศตามความอ่อนไหวต่อการถูกเปิดเผยหรือถูกแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตแบ่งออกเป็น ๓ ระดับ คือ

คุณลักษณะของข้อมูลสารสนเทศที่อยู่ในแต่ละชั้นความลับ		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ ข้อมูลสารสนเทศลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อ กปภ. อย่างร้ายแรงที่สุด	◆ ข้อมูลสารสนเทศลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อ กปภ. อย่างร้ายแรง	◆ ข้อมูลสารสนเทศลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อ กปภ.
◆ มีความสำคัญและมีผลกระทบต่อความมั่นคงปลอดภัยของ กปภ. สูงมากและไม่อนุญาตให้นำไปใช้งานภายนอก กปภ.	◆ มีความสำคัญและมีผลกระทบต่อความมั่นคงปลอดภัยของ กปภ. สูงและไม่อนุญาตให้นำไปใช้งานภายนอก กปภ.	◆ มีความสำคัญและมีผลกระทบต่อความมั่นคงปลอดภัยของ กปภ. ต่ำและไม่อนุญาตให้นำไปใช้งานภายนอก กปภ.

<u>หลักเกณฑ์ในการบริหารจัดการและใช้งานข้อมูลสารสนเทศโดยแบ่งเป็น ๒ ประเภท ดังนี้</u>

๑. <u>เอกสารตีพิมพ์</u>

๑.๑ การระบุชั้นความลับของข้อมูลสารสนเทศ		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
ระบุคำว่า **“ลับที่สุด”** ◆ ทุกหน้าเอกสารหากเป็นเอกสารแยกแผ่นหรือไม่ได้รับการเข้าเล่ม ◆ เฉพาะปกหรือหน้าแรกของเอกสารหากได้รับการเข้าเล่ม	ระบุคำว่า **“ลับมาก”** ◆ ทุกหน้าเอกสารหากเป็นเอกสารแยกแผ่นหรือไม่ได้รับการเข้าเล่ม ◆ เฉพาะปกหรือหน้าแรกของเอกสารหากได้รับการเข้าเล่ม	ระบุคำว่า **“ลับ”** ◆ ทุกหน้าเอกสารหากเป็นเอกสารแยกแผ่นหรือไม่ได้รับการเข้าเล่ม ◆ เฉพาะปกหรือหน้าแรกของเอกสารหากได้รับการเข้าเล่ม

๑.๒ การเข้าถึง		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)	◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)	◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)

๑.๓ การเก็บรักษา		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ เก็บในตู้เอกสารที่มีกุญแจปิดล็อคและจำกัดการเข้าถึงเป็นรายบุคคล	◆ เก็บในตู้เอกสารที่มีการปิดล็อคและจำกัดการเข้าถึงเป็นรายบุคคล	◆ เก็บในตู้เอกสารที่มีการปิดล็อค

๑.๔ การทำสำเนา		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ ไม่อนุญาตให้ทำสำเนา	◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)	◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)

๑.๕ การทำลาย		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ ใช้เครื่องทำลายเอกสาร	◆ ใช้เครื่องทำลายเอกสาร	◆ ใช้เครื่องทำลายเอกสารหรือฉีกเป็นชิ้นเล็กๆ

๒. <u>ข้อมูลสารสนเทศอิเล็กทรอนิกส์</u>

๒.๑ การระบุชั้นความลับของข้อมูลสารสนเทศ		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ ระบุคำว่า **“ลับที่สุด”** ทุกหน้าเอกสาร	◆ ระบุคำว่า **“ลับมาก”** ทุกหน้าเอกสาร	◆ ระบุคำว่า **“ลับ”** ทุกหน้าเอกสาร

๒.๒ การเข้าถึง		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)	◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)	◆ บุคคลที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศ ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)

๒.๓ การเก็บรักษา		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ เข้ารหัสลับ	◆ เข้ารหัสลับ	◆ เข้ารหัสลับ

๒.๔ การทำสำเนา		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ ไม่อนุญาตให้ทำสำเนา	◆ ต้องขออนุญาตจากเจ้าของหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศก่อน ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)	◆ ต้องขออนุญาตจากเจ้าของหน่วยงานที่เป็นเจ้าของข้อมูลสารสนเทศก่อน ◆ ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูล (NDA : Non disclosure agreement)

๒.๕ การส่งผ่านเครือข่ายสาธารณะ		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ เข้ารหัสลับข้อมูล ◆ ส่งข้อมูลผ่านเครือข่ายที่มีการเข้ารหัสลับ ด้วยโปรโตคอลที่มีความมั่นคงปลอดภัย เช่น HTTPS, SSH, SCP, SFTP,PGP หรืออื่นๆ เป็นต้น	◆ เข้ารหัสลับข้อมูล ◆ ส่งข้อมูลผ่านเครือข่ายที่มีการเข้ารหัสลับ ด้วยโปรโตคอลที่มีความมั่นคงปลอดภัย เช่น HTTPS, SSH, SCP, SFTP,PGP หรืออื่นๆ เป็นต้น	◆ เข้ารหัสลับข้อมูล ◆ ส่งข้อมูลผ่านเครือข่ายที่มีการเข้ารหัสลับ ด้วยโปรโตคอลที่มีความมั่นคงปลอดภัย เช่น HTTPS, SSH, SCP, SFTP,PGP หรืออื่นๆ เป็นต้น

๒.๖ การทำลาย		
ลับที่สุด (Top Secret)	**ลับมาก (Secret)**	**ลับ (Confidential)**
◆ ใช้การทำลายด้วยวิธีที่มั่นคงปลอดภัย (Secure delete) เพื่อไม่ให้สามารถกู้คืนข้อมูลกลับมาได้ เช่น Zero Fill	◆ ใช้การทำลายด้วยวิธีที่มั่นคงปลอดภัย (Secure delete) เพื่อไม่ให้สามารถกู้คืนข้อมูลกลับมาได้ เช่น Zero Fill	◆ ใช้การทำลายด้วยวิธีที่มั่นคงปลอดภัย (Secure delete) เพื่อไม่ให้สามารถกู้คืนข้อมูลกลับมาได้ เช่น Zero Fill

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๒
แนวทางปฏิบัติการบริหารจัดการการเข้ารหัสลับข้อมูล
(Cryptography management guideline)

วัตถุประสงค์

- เพื่อป้องกันการเข้าถึงและเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่สำคัญของ กปภ. โดยไม่ได้รับอนุญาต
- เพื่อป้องกันการแก้ไขปลอมแปลงข้อมูลที่เป็นความลับหรือข้อมูลที่สำคัญของ กปภ. โดยไม่ได้รับอนุญาต
- เพื่อให้การติดต่อสื่อสารที่ใช้รับส่งข้อมูลผ่านช่องทางที่มีความมั่นคงปลอดภัย

ผู้ปฏิบัติ

- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- ผู้ดูแลระบบสารสนเทศ

แนวทางการปฏิบัติ

๑. ต้องมีการเข้ารหัสลับช่องทางการติดต่อสื่อสารที่ใช้รับส่งข้อมูลระหว่าง กปภ. ส่วนกลาง กับ กปภ.ข. กปภ.สาขา ด้วยช่องทางที่มีความมั่นคงปลอดภัย เช่น IPSec-VPN, SSL-VPN, TLS
๒. การคัดเลือกผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ Certification Authority (ถ้ามี) ต้องเป็นผู้ให้บริการที่มีความน่าเชื่อถือ และสามารถขอเพิกถอนและทำลายกุญแจเพื่อไม่ให้สามารถนำกลับมาใช้งานได้อีกในอนาคต
๓. สำหรับระบบสารสนเทศที่มีความสำคัญ ซึ่งมีการรับ-ส่งข้อมูลผ่านระบบเครือข่ายอินเทอร์เน็ต ผู้ดูแลระบบสารสนเทศควรมีการใช้งาน TLS Certificate จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
๔. สำหรับการรับ-ส่งข้อมูล ที่เป็นความลับผ่านอีเมล ให้ใช้วิธีการเข้ารหัสลับแบบ (PGP: Pretty Good Privacy)

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๓
แนวทางปฏิบัติการจัดการสื่อที่ใช้บันทึกข้อมูล
(Media handling guideline)

วัตถุประสงค์

- เพื่อป้องกันการเปิดเผยข้อมูลสารสนเทศของ กปภ. ที่ถูกจัดเก็บบนสื่อบันทึกข้อมูลโดยไม่ได้รับอนุญาต

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.

แนวทางการปฏิบัติ

๑. การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้
   ๑.๑. สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ต้องถูกจัดเก็บให้อยู่ในสภาพแวดล้อมที่มีความมั่นคงปลอดภัย เช่น การจัดเก็บในตู้เอกสารที่มีกุญแจปิดล็อค
   ๑.๒. ก่อนการใช้งานสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ต้องมีการสแกนไวรัสคอมพิวเตอร์จากโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ได้รับการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
   ๑.๓. ห้ามนำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ไปใช้เพื่อกิจการอื่นที่ไม่ได้เกี่ยวข้องกับการทำงานของ กปภ.
   ๑.๔. การนำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ออกไปจำหน่ายหรือซ่อมแซมต้องดำเนินการลบข้อมูลสารสนเทศที่เป็นความลับของ กปภ. ออกจากสื่อบันทึกข้อมูลก่อนด้วยวิธีที่มั่นคงปลอดภัย (Secure delete) เพื่อไม่ให้สามารถกู้คืนข้อมูลกลับมาได้ เช่น Zero Fill
๒. การส่งสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ไปนอก กปภ.
   ๒.๑. ต้องมีการเข้ารหัสลับข้อมูลสารสนเทศที่สำคัญของ กปภ. ที่จัดเก็บอยู่ในสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลและการเข้าถึงโดยไม่ได้รับอนุญาต
   ๒.๒. การส่งสื่อบันทึกข้อมูลอาจนำส่งด้วยตัวเองหรืออาจใช้วิธีการขนส่งจากบริษัทที่มีความน่าเชื่อถือและสามารถตรวจสอบสถานะการจัดส่งได้
   ๒.๓. บรรจุภัณฑ์ที่จัดส่งสื่อบันทึกข้อมูลต้องเป็นวัสดุที่สามารถป้องกันความเสียหายระหว่างการจัดส่ง

เอกสารอ้างอิง

๑. แบบฟอร์ม บันทึกการทำลายข้อมูลสารสนเทศบนอุปกรณ์อิเล็กทรอนิกส์และสื่อบันทึก (IT-FM-NDA-๑๑)

หมวดที่ ๕
นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and environmental security policy)

เพื่อให้ กปภ. มีมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าปฏิบัติงานห้องศูนย์คอมพิวเตอร์ของ กปภ. รวมทั้งกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค (Facility) ที่สนับสนุนการทำงานของระบบสารสนเทศภายในห้องศูนย์คอมพิวเตอร์ให้สามารถทำงานได้อย่างต่อเนื่องและมีความมั่นคงปลอดภัย โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการใช้งานห้องศูนย์คอมพิวเตอร์และพื้นที่ใช้งานระบบสารสนเทศ (Data center and IT area working guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการใช้งานห้องศูนย์คอมพิวเตอร์และพื้นที่ใช้งานระบบสารสนเทศ
(Data center and IT area guideline)

วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และมาตรการควบคุมการปฏิบัติงานในห้องศูนย์คอมพิวเตอร์ของ กปภ. ให้มีความมั่นคงปลอดภัย
- เพื่อกำหนดให้มีกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และระบบสาธารณูปโภค (Facility) ของห้องศูนย์คอมพิวเตอร์และพื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

ผู้ปฏิบัติ

- ผู้บริหาร พนักงานของ กปภ.
- ผู้ดูแลห้องศูนย์คอมพิวเตอร์
- บุคคลภายนอก

แนวทางการปฏิบัติ

๑. กำหนดพื้นที่หรือบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยทางกายภาพ โดยมีรายละเอียด ดังนี้
   ๑.๑. ห้องมั่นคง (Strong Room)
   ๑.๒. ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room)
   ๑.๓. ห้องอุปกรณ์เครือข่าย (Network Room)
   ๑.๔. ห้องเครื่องปรับอากาศและระบบควบคุมความชื้น (Precision Air Room)
   ๑.๕. ห้องส่งมอบหรือจัดเตรียมสินทรัพย์ด้านสารสนเทศ (Store Room)

๑.๖. ห้องจัดเตรียมอุปกรณ์ (Staging Room)

๑.๗. ห้อง Facility ต่างๆ เช่น Power Generator, UPS เป็นต้น

๒. การควบคุมการเข้า-ออก และการปฏิบัติงานภายในห้องศูนย์คอมพิวเตอร์

๒.๑. ผู้ดูแลห้องศูนย์คอมพิวเตอร์ต้องกำหนดสิทธิ์ของพนักงานที่มีสิทธิ์ผ่านเข้า-ออก พื้นที่หรือบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยทางกายภาพด้วยการใช้ลายนิ้วมือ หรือบัตร Access Control และต้องมีการเก็บบันทึกเวลาการเข้า-ออก ทั้งนี้จะต้องมีการทบทวนสิทธิ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๒.๒. ผู้ดูแลห้องศูนย์คอมพิวเตอร์ต้องจัดให้มีกล้องโทรทัศน์วงจรปิด (CCTV) ในพื้นที่หรือบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยทางกายภาพ และตรวจสอบความพร้อมใช้งานของกล้องโทรทัศน์วงจรปิดให้สามารถทำงานได้อย่างต่อเนื่องและสามารถบันทึกภาพล่าสุดเพื่อดูย้อนหลังอย่างน้อย ๑ เดือน

๒.๓. ผู้ที่จะเข้ามาปฏิบัติงานจะต้องติดต่อเจ้าหน้าที่ดูแลห้องศูนย์คอมพิวเตอร์เพื่อกรอกแบบฟอร์มต่างๆ ดังนี้

๒.๓.๑. แบบฟอร์ม บันทึกข้อตกลงเรื่อง การรักษาความปลอดภัยของข้อมูลสารสนเทศ

๒.๓.๒. แบบฟอร์ม บันทึกการเข้าปฏิบัติงานในห้องศูนย์คอมพิวเตอร์ กปภ.

ทั้งนี้ในระหว่างการปฏิบัติงานของบุคคลภายนอกจะต้องมีพนักงานของ กปภ. ที่เกี่ยวข้องดูแลและประสานงานด้วยอย่างน้อยจำนวน ๑ ท่าน

๒.๔. การนำอุปกรณ์เข้า-ออก ห้องศูนย์คอมพิวเตอร์ต้องได้รับอนุญาตจากผู้ดูแลห้องศูนย์คอมพิวเตอร์ และต้องกรอกแบบฟอร์ม “บันทึกการนำอุปกรณ์เข้า-ออก ห้องศูนย์คอมพิวเตอร์”

๒.๕. การส่งมอบและจัดเตรียมทรัพย์สินด้านสารสนเทศต้องอยู่ในห้อง Loading Area ซึ่งแยกออกจากห้องศูนย์คอมพิวเตอร์แต่หากมีความจำเป็นต้องติดตั้งในห้องศูนย์คอมพิวเตอร์ให้ผู้ดูแลห้องศูนย์คอมพิวเตอร์หรือผู้ที่เกี่ยวข้องควบคุมการปฏิบัติงานอย่างใกล้ชิด

๒.๖. ต้องติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย หรืออื่นๆ ไว้ในตู้ Rack ที่ได้จัดเตรียมไว้ และต้องปิดล็อคกุญแจตู้ Rack ทุกครั้งเมื่อปฏิบัติงานเสร็จ

๒.๗. ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายคอมพิวเตอร์ และสายสัญญาณสื่อสารที่จะส่งผลกระทบต่อการทำงานของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ. โดยไม่ได้รับอนุญาต

๒.๘. ให้ผู้เข้าปฏิบัติงานสวมรองเท้าที่ได้จัดเตรียมไว้ในห้องศูนย์คอมพิวเตอร์

๒.๙. ห้ามสูบบุหรี่ภายในห้องศูนย์คอมพิวเตอร์

๒.๑๐. ห้ามนำอาหารและเครื่องดื่มเข้าไปภายในห้องศูนย์คอมพิวเตอร์

๒.๑๑. ห้ามถ่ายรูปภายในห้องศูนย์คอมพิวเตอร์เว้นแต่ได้รับอนุญาติจากผู้ดูแลห้องศูนย์คอมพิวเตอร์

๓. ระบบสาธารณูปโภค (Facility)

ต้องจัดให้มีระบบสาธารณูปโภคเพื่อสนับสนุนการให้บริการของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ภายในห้องศูนย์คอมพิวเตอร์ให้สามารถทำงานได้อย่างต่อเนื่องและมีความมั่นคงปลอดภัย ดังนี้

๓.๑. ระบบไฟฟ้า

๓.๒. ระบบสำรองกระแสไฟฟ้า (UPS)

๓.๓. เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Power Generator)

๓.๔. ระบบปรับอากาศและควบคุมความชื้น (Precision Air)

๓.๕. ระบบระบายอากาศ

๓.๖. ระบบป้องกันอัคคีภัย (Fire Protection)

๓.๗. ระบบควบคุมการเข้า-ออก ห้องศูนย์คอมพิวเตอร์ (Access Control)

๓.๘. ระบบกล้องโทรทัศน์วงจรปิด (CCTV)

๔. การเดินสายสัญญาณสื่อสาร

๔.๑. ต้องเดินสายสัญญาณสื่อสารและสายไฟฟ้าออกจากกันเพื่อป้องกันการรบกวนกันของสัญญาณ (Crosstalk)

๔.๒. การเดินสายสัญญาณสื่อสารต้องเดินในราง (Wire way) ที่จัดเตรียมไว้หรือมีการร้อยสายเข้าท่อ Flex ให้เป็นระเบียบเรียบร้อย

๔.๓. ต้องจัดทำป้ายชื่อ (Label) ของสายสัญญาณสื่อสารให้ครบถ้วน

๕. การบำรุงรักษาอุปกรณ์และสภาพแวดล้อมในห้องศูนย์คอมพิวเตอร์

๕.๑. ต้องมีการบำรุงรักษาระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ และระบบสาธารณูปโภคต่างๆ รวมถึงสายสื่อสารสัญญาณ ภายในห้องศูนย์คอมพิวเตอร์ตามรอบระยะเวลาที่กำหนด เพื่อให้มั่นใจว่าระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ของ กปภ. สามารถทำงานได้อย่างต่อเนื่อง

๕.๒. ดูแลความสะอาด และความเป็นระเบียบเรียบร้อยของห้องศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ และต้องไม่เก็บกล่องกระดาษหรือวัตถุที่จะเป็นเชื้อเพลิงไว้ในห้องศูนย์คอมพิวเตอร์

เอกสารอ้างอิง

๑. บันทึกข้อตกลงเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศ (พนักงาน) (IT-FM-NDA-๐๑)

๒. บันทึกข้อตกลงเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศ (บุคคลภายนอก) (IT-FM-NDA-๐๒)

๓. แบบฟอร์ม บันทึกการเข้าปฏิบัติงานในของศูนย์คอมพิวเตอร์ (IT-FM-NDA-๐๓)

๔. แบบฟอร์ม บันทึกการนำอุปกรณ์เข้า-ออก ห้องศูนย์คอมพิวเตอร์ (IT-FM-NDA-๐๔)

หมวดที่ ๖
นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน
(IT Operation security policy)

เพื่อให้ กปภ. มีแนวปฏิบัติในการบริหารจัดการการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ให้มีความมั่นคงปลอดภัยจากภัยคุกคามต่างๆ ที่อาจสร้างความเสียหายต่อการดำเนินธุรกิจของ กปภ. โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการแบ่งแยกอำนาจหน้าที่
  (Segregation of duties guideline)
- ส่วนที่ ๒ แนวทางปฏิบัติการบริหารจัดการขีดความสามารถของระบบสารสนเทศ
  (Capacity management guideline)
- ส่วนที่ ๓ แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ที่ใช้ปฏิบัติงาน
  (Server and endpoint security guideline)
- ส่วนที่ ๔ แนวทางปฏิบัติการสำรองและกู้คืนข้อมูล
  (Data backup and recovery guideline)
- ส่วนที่ ๕ แนวทางปฏิบัติการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์
  (Logging guideline)
- ส่วนที่ ๖ แนวทางปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์
  (Monitoring security guideline)
- ส่วนที่ ๗ แนวทางปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ
  (Vulnerability management and penetration test guideline)
- ส่วนที่ ๘ แนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลง
  (Change management guideline)
- ส่วนที่ ๙ แนวทางปฏิบัติการบริหารจัดการการตั้งค่าระบบและการกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ
  (System configuration and minimum baseline standard management guideline)
- ส่วนที่ ๑๐ แนวทางปฏิบัติการบริหารจัดการ Patch
  (Patch management guideline)
- ส่วนที่ ๑๑ แนวทางปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี
  (Malware protection guideline)

- ส่วนที่ ๑๒ แนวทางปฏิบัติการบริหารจัดการรหัสผ่าน
  (Password management guideline)
- ส่วนที่ ๑๓ แนวทางปฏิบัติการใช้งานอินเทอร์เน็ต
  (Internet guideline)
- ส่วนที่ ๑๔ แนวทางปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
  (E-mail guideline)
- ส่วนที่ ๑๕ แนวทางปฏิบัติการใช้งานระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน
  (Virtual machine system guideline)
- ส่วนที่ ๑๖ แนวทางปฏิบัติการนำอุปกรณ์ส่วนบุคคลเข้ามาใช้งาน
  (BYOD : Bring Your Own Device guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการแบ่งแยกอำนาจหน้าที่
(Segregation of duties guideline)

วัตถุประสงค์

- เพื่อแบ่งแยกอำนาจหน้าที่และความรับผิดชอบให้แก่บุคลากรในแต่ละตำแหน่งอย่างเหมาะสม และจัดทำคู่มือการปฏิบัติงานไว้ให้สมบูรณ์เพียงพอต่อการปฏิบัติงานในระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่มีความสำคัญ

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. กำหนดหน้าที่ และความรับผิดชอบของบุคคลที่เกี่ยวข้องอย่างชัดเจน เช่น หน้าที่และความรับผิดชอบของผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ เป็นต้น
๒. มีการจัดทำคำอธิบายลักษณะงาน ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งานอย่างชัดเจน
๓. กำหนดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีที่จำเป็น

๔. จัดทำ และปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัย อย่างน้อยให้ครอบคลุมระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ หรือระบบอื่นๆ ที่มีความสำคัญ ดังนี้
   ๔.๑. คู่มือการใช้งานระบบสารสนเทศต่างๆ ทั้งในส่วนของผู้ใช้งาน และผู้ดูแลระบบ
   ๔.๒. คู่มือการตรวจสอบสถานะของเครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์
   ๔.๓. คู่มือการสำรองข้อมูล/คู่มือการกู้คืนข้อมูล
   ๔.๔. คู่มือการแก้ไขปัญหาระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
๕. จำกัดการเข้าถึงคู่มือการปฏิบัติงานทั้งในรูปแบบของเอกสารและไฟล์อิเล็กทรอนิกส์โดยอนุญาตให้เฉพาะพนักงานที่มีส่วนเกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๒

แนวทางปฏิบัติการบริหารจัดการขีดความสามารถของระบบสารสนเทศ

(Capacity management guideline)

วัตถุประสงค์

- เพื่อกำหนดแนวทางปฏิบัติสำหรับการตรวจสอบ เฝ้าระวัง การใช้งานทรัพยากรของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ. ให้สามารถรองรับการทำงานในอนาคตได้อย่างต่อเนื่อง

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ ต้องมีการกำหนดค่าเกณฑ์ (Threshold) การใช้งานทรัพยากรของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ เช่น CPU, Memory, Storage, Network Bandwidth เป็นต้น

๒. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ ต้องคอยตรวจสอบการใช้งานทรัพยากรของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่ตนเองดูแล ไม่ให้เกินค่าเกณฑ์ที่กำหนดอย่างสม่ำเสมอหากมีการใช้งานทรัพยากรเกินค่าเกณฑ์ที่กำหนดต้องรายงานให้ผู้บริหารรับทราบ เพื่อวางแผนบริหารการใช้งานทรัพยากรให้รองรับการทำงานในอนาคตได้อย่างต่อเนื่องและเหมาะสม

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๓
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย
และอุปกรณ์ที่ใช้ปฏิบัติงาน
(Server and endpoint security guideline)

วัตถุประสงค์

- เพื่อกำหนดแนวทางปฏิบัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่ใช้ปฏิบัติงาน ให้มีความมั่นคงปลอดภัยและไม่เป็นจุดอ่อนหรือช่องทางที่ทำให้ข้อมูลของ กปภ. รั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- หน่วยงานที่ดูแลอุปกรณ์ที่ใช้ปฏิบัติงาน

แนวทางการปฏิบัติ

๑. เครื่องคอมพิวเตอร์แม่ข่าย (Server)

ผู้ดูแลระบบสารสนเทศที่รับผิดชอบในการดูแลเครื่องคอมพิวเตอร์แม่ข่ายที่เป็นทรัพย์สินของ กปภ. ต้องปฏิบัติ ดังนี้

๑.๑. ต้องมีการจัดทำรายการทะเบียนทรัพย์สินเครื่องคอมพิวเตอร์แม่ข่ายที่ตนเองดูแล และต้องมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๑.๒. ต้องกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ (Minimum baseline standard) ตามแนวทางปฏิบัติการบริหารจัดการการตั้งค่าระบบและการกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ

๑.๓. ต้องติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

๑.๔. ต้องติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายในตู้ Rack หรือสถานที่ที่มีการรักษาความปลอดภัย

๑.๕. การเปลี่ยนแปลงใดๆ บนเครื่องคอมพิวเตอร์แม่ข่ายต้องปฏิบัติตามแนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลงโดยดำเนินการตาม หมวดที่ ๖ ส่วนที่ ๙ แนวทางปฏิบัติการบริหารจัดการการตั้งค่าระบบและการกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ

๒. อุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint) ที่เป็นทรัพย์สินของ กปภ.
หน่วยงานที่ดูแลเครื่องคอมพิวเตอร์ PC เครื่องคอมพิวเตอร์ Laptop หรืออุปกรณ์แบบพกพาชนิดต่างๆ เช่น Tablet, Smart device ที่เป็นทรัพย์สินของ กปภ. ต้องปฏิบัติ ดังนี้

๒.๑. ต้องมีการจัดให้ทำรายการทะเบียนทรัพย์สินเครื่องคอมพิวเตอร์ PC เครื่องคอมพิวเตอร์ Laptop หรืออุปกรณ์แบบพกพาชนิดต่างๆ และต้องมีการทบทวนรายการทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๒.๒. ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์บนเครื่องของผู้ใช้งานและตรวจสอบว่ามีการปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ให้เป็นเวอร์ชันปัจจุบันและพร้อมใช้งานอยู่เสมอ

๒.๓. ต้องมีการปรับปรุง Patch ของระบบปฏิบัติการให้เป็นเวอร์ชันปัจจุบันเพื่อปิดช่องโหว่ตามแนวทางปฏิบัติการบริหารจัดการ Patch

๒.๔. ต้องกำหนดระยะเวลาล็อคหน้าจอ (Screen Saver) เมื่อไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง ดังนี้

๒.๔.๑. กำหนดค่า Screen Saver ๕ นาที สำหรับหน่วยงานทั่วไป

๒.๔.๒. กำหนดค่า Screen Saver ๑๕ นาที สำหรับหน่วยงานที่มีความจำเป็นต้องการใช้งานเกิน ๕ นาที

๒.๕. ต้องมีการกำหนดเพื่อไม่ให้ผู้ใช้งานแก้ไขเปลี่ยนแปลงการตั้งค่าต่างๆ บนอุปกรณ์ ดังนี้

๒.๕.๑. แก้ไขการตั้งค่าที่เกี่ยวกับเครือข่าย เช่น IP Address, DNS, Subnetmask, Default Gateway

๒.๕.๒. แก้ไขการทำงานของ Host-base Firewall

๒.๕.๓. แก้ไขการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์

๒.๕.๔. ติดตั้งหรือถอดถอนโปรแกรมที่อยู่บนเครื่อง

๒.๖. ต้องแจ้งให้ผู้ใช้งานระมัดระวังการใช้งานสื่อบันทึกข้อมูลทุกประเภท เช่น External Hard Drive, Thumb Drive หรือสื่อบันทึกข้อมูลที่อยู่ในรูปแบบอื่นๆ เพื่อป้องกันไม่ให้ข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาต

๒.๗. ต้องแจ้งให้ผู้ใช้งานดูแลรักษาอุปกรณ์ที่ใช้ปฏิบัติงาน อุปกรณ์สำรองไฟฟ้า (UPS) และอุปกรณ์ต่อพ่วงอื่นๆ ให้อยู่ในสภาพพร้อมใช้งานและปิดเครื่องทุกครั้งเมื่อไม่มีการใช้งาน

๒.๘. ต้องแจ้งให้ผู้ใช้งานห้ามใช้อุปกรณ์ที่ใช้ปฏิบัติงานเพื่อดำเนินการ ดังต่อไปนี้

๒.๘.๑. เพื่อกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๒.๘.๒. ห้ามใช้งานโปรแกรมคอมพิวเตอร์ประเภทดักจับข้อมูล (Packet sniffing tools) หรือโปรแกรมประเภททดสอบเจาะระบบ (Penetration testing tools) ยกเว้นเครื่องของผู้ดูแลระบบสารสนเทศและผู้ดูแลเครือข่ายคอมพิวเตอร์ที่มีความจำเป็นต้องใช้สำหรับปฏิบัติงานต้องได้รับอนุญาตจาก ผชด./ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร

๒.๘.๓. เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของ กปภ. หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่ กปภ.

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๔
แนวทางปฏิบัติการสำรองและกู้คืนข้อมูล
(Data backup and recovery guideline)

วัตถุประสงค์

- เพื่อกำหนดให้ระบบสำรองข้อมูล และจัดทำแผนสำรองและแผนกู้คืนสภาพระบบสารสนเทศให้มั่นใจว่าระบบสามารถกลับมาทำงานได้อย่างต่อเนื่อง

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ

แนวทางการปฏิบัติ

๑. การจัดทำบัญชีรายชื่อระบบสารสนเทศและเอกสารคู่มือ
   ๑.๑. ต้องจัดทำบัญชีรายชื่อระบบสารสนเทศที่มีความสำคัญที่อยู่ในความรับผิดชอบของตนเองโดยพิจารณาจากความสำคัญของระบบสารสนเทศและธุรกิจที่ใช้ระบบสารสนเทศนั้นๆ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง
   ๑.๒. ต้องจัดทำเอกสารและคู่มือปฏิบัติงานต่างๆ ที่เกี่ยวข้องให้ครบถ้วนเพื่อความสะดวกต่อการใช้งาน เช่น คู่มือทางด้านเทคนิค คู่มือการปฏิบัติงาน เอกสารลิขสิทธิ์ของซอฟต์แวร์ เป็นต้น

๒. การสำรองระบบสารสนเทศ
   ๒.๑. กำหนดให้มีการสำรองระบบสารสนเทศเป็นประจำ โดยจัดทำตารางเวลาการทำงานเกี่ยวกับการสำรองข้อมูลของแต่ละระบบสารสนเทศ โดยพิจารณาจากความสำคัญของระบบสารสนเทศและธุรกิจที่ใช้ระบบสารสนเทศนั้นๆ
   ๒.๒. กำหนดแผนการสำรองระบบสารสนเทศต่างๆ โดยต้องได้รับความเห็นชอบจากผู้บังคับบัญชาที่รับผิดชอบ ดังนี้
      ๒.๒.๑. ระบบสารสนเทศที่จะทำสำรอง
      ๒.๒.๒. เวลาเริ่มต้นและระยะเวลาในการทำสำรองระบบข้อมูลแต่ละระบบสารสนเทศ
      ๒.๒.๓. ความถี่ในการสำรองระบบข้อมูล
      ๒.๒.๔. ระยะเวลาที่ต้องการจัดเก็บของข้อมูล แต่ละระบบสารสนเทศ
      ๒.๒.๕. เงื่อนไขและข้อจำกัดต่างๆ ของแต่ละระบบสารสนเทศ
   ๒.๓. กำหนดสื่อบันทึกที่ใช้ในการสำรองข้อมูลระบบสารสนเทศ (Backup media) เช่น เทป หรือดิสก์ พื้นที่จัดเก็บข้อมูลบนคลาวด์สตอเรจ เป็นต้น
   ๒.๔. กำหนดผู้รับผิดชอบในการจัดเก็บรักษาสื่อบันทึกที่ใช้ในการสำรองข้อมูลระบบสารสนเทศ
   ๒.๕. จัดทำเอกสารประกอบการสำรองระบบสารสนเทศ ดังนี้
      ๒.๕.๑. แผนการดำเนินงานสำรองระบบสารสนเทศของแต่ละระบบสารสนเทศในแต่ละปี
      ๒.๕.๒. ขั้นตอนการทำงานและผู้ปฏิบัติงานในความรับผิดชอบต่างๆ
      ๒.๕.๓. ขั้นตอนการตรวจสอบผลการสำรองระบบสารสนเทศ

๒.๕.๔. กำหนดสถานที่ จัดเก็บสื่อในการสำรองระบบสารสนเทศ ทั้งภายในและภายนอกสถานที่

๒.๖. ทบทวนเอกสารการสำรองระบบสารสนเทศทุกๆ ๑ ปี หรือเมื่อมีการเพิ่มระบบใหม่เข้ามาในคู่มือ โดยต้องมีการบันทึกผลการเปลี่ยนแปลงทุกครั้ง

๓. แนวทางการกู้คืนสภาพระบบสารสนเทศ

๓.๑. กำหนดระบบสารสนเทศที่จะต้องจัดให้มีแผนการกู้คืนสภาพ โดยพิจารณาจากความสำคัญของระบบสารสนเทศและความสำคัญของธุรกิจที่ใช้ระบบสารสนเทศนั้นๆ เป็นสำคัญ

๓.๒. กำหนดผู้รับผิดชอบระบบรวมทั้งในส่วนของผู้ใช้งานเพื่อร่วมดำเนินการ ดังนี้

๓.๒.๑. การปรับปรุงเปลี่ยนแปลงแผนการดำเนินงาน

๓.๒.๒. การกำหนดขั้นตอนและวิธีการตรวจสอบ

๓.๓.๓. การกำหนดผู้รับผิดชอบในแต่ละขั้นตอนการดำเนินงาน

๓.๓. กำหนดขั้นตอนการกู้คืนสภาพระบบ ดังนี้

๓.๓.๑. การกู้คืนสภาพระบบปฏิบัติการและระบบสารสนเทศ

๓.๓.๒. การเตรียมความพร้อมระบบเครือข่าย

๓.๓.๓. การเตรียมความพร้อมทรัพยากรเครื่องคอมพิวเตอร์แม่ข่าย

๓.๓.๔. การตรวจสอบความถูกต้องในแต่ละขั้นตอน

๓.๔. กำหนดระยะเวลาการทดสอบในแต่ละระบบ

๓.๕. จัดทำบัญชีรายชื่อ ตัวแทนจำหน่ายผลิตภัณฑ์ ที่เกี่ยวข้องพร้อมทั้งช่องทางการสื่อสารที่สามารถติดต่อได้

๓.๖. กำหนดให้มีการทดสอบการกู้คืนสภาพระบบสารสนเทศ โดยพิจารณาจากความสำคัญของระบบสารสนเทศและความสำคัญของธุรกิจที่ใช้ระบบสารสนเทศนั้นๆ เป็นสำคัญ อย่างน้อยปีละ ๑ ครั้ง พร้อมทั้งบันทึกผลการดำเนินงาน และรายงานให้ผู้บังคับบัญชาที่รับผิดชอบทราบ

๔. ในกรณีที่มีการขนย้ายสื่อบันทึกที่ใช้ในการสำรองข้อมูลระบบสารสนเทศไปเก็บรักษาไว้นอก กปภ. สื่อบันทึกข้อมูลฯ ต้องได้รับการติดฉลากที่มีรายละเอียดชัดเจน และต้องมีการควบคุมความมั่นคงปลอดภัยทางกายภาพอย่างเหมาะสม

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๕
แนวทางปฏิบัติการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์
(Logging guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่ถูกต้องครบถ้วนและมีความมั่นคงปลอดภัย และสามารถใช้ติดตามตรวจสอบร่องรอยการเข้าใช้งานระบบหรือข้อมูลของผู้ใช้งานรวมทั้งใช้เป็นหลักฐานในทางกฎหมายได้

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. ต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของเครื่องคอมพิวเตอร์แม่ข่าย ระบบงานสารสนเทศ และอุปกรณ์เครือข่ายที่สำคัญเป็นระยะเวลาอย่างน้อย ๙๐ วัน ตามที่กฎหมายกำหนดเพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคตอย่างน้อย ดังนี้

หลักฐานที่ต้องจัดเก็บ	รายละเอียดขั้นต่ำในการจัดเก็บ	ระยะเวลาจัดเก็บ
๑. หลักฐานการเข้าถึงพื้นที่หรือบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยทางกายภาพ	• ชื่อบัญชีผู้เข้าถึงพื้นที่ • วันเวลาที่ผ่านเข้าออก	ไม่น้อยกว่า ๙๐ วัน
๒. หลักฐานการใช้งานระบบเครือข่ายอินเทอร์เน็ต	• ชื่อบัญชีผู้ใช้งาน • หมายเลข IP Address ของผู้ใช้งาน • บันทึกกิจกรรม (Activity log) • วันเวลาที่เข้าใช้งาน	

๒. ผู้ดูแลระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ต้องกำหนดการตั้งค่าสัญญาณนาฬิกา (Clock Synchronization) ของอุปกรณ์หรือระบบที่ตนเองดูแลให้สอดคล้องกับเครื่องคอมพิวเตอร์แม่ข่าย Time Server ที่ กปภ. กำหนดซึ่งจะมีการอ้างอิงสัญญาณนาฬิกาจากแหล่งที่มีความน่าเชื่อถือ

๓. จัดให้มีระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ โดยสามารถกำหนดการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์เพื่อป้องกันการแก้ไขหรือเปลี่ยนแปลงข้อมูลได้ เช่น Centralized Log Server หรือการทำ Data Archive หรือการทำ Data Hashing เป็นต้น

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๖
แนวทางปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์
(Monitoring security guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. มีกระบวนการที่สามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. ต้องมีกระบวนการและเครื่องมือที่ใช้สำหรับตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่กระทบต่อความปลอดภัยของระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ที่มีความสำคัญได้อย่างทันท่วงที เช่น Firewall หรือ IPS/IDS หรือ SIEM หรือ ผู้ให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (SOC) เป็นต้น

๒. ในกรณีที่พบเหตุการณ์ผิดปกติหรือภัยคุกคามต่อระบบสารสนเทศที่มีความสำคัญต้องรายงานให้ผู้บริหารรับทราบและต้องดำเนินการแก้ไขอย่างเร่งด่วนหากระบบสารสนเทศนั้นเกิดโดนโจมตีหรือโดนยึดครองให้ปฏิบัติตามแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber incident response plan)

เอกสารอ้างอิง

๑. แผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber incident response plan)

<u>หมายเหตุ</u>

สามารถดาวน์โหลดเอกสารอ้างอิง ๑ ได้ที่ https://cybersecurity.pwa.co.th

ส่วนที่ ๗

แนวทางปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ

(Vulnerability management and penetration test guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. ทราบถึงช่องโหว่ด้านการรักษาความมั่นคงปลอดภัย และสามารถดำเนินการปรับปรุงแก้ไขช่องโหว่เพื่อป้องกันความเสี่ยงจากภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้นได้อย่างทันท่วงที
- เพื่อให้ กปภ. มีการแก้ไขและปิดช่องโหว่ที่พบภายในระยะเวลาที่กำหนด

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. การบริหารจัดการช่องโหว่ (Vulnerability management)

๑.๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องคอยติดตามข่าวสารด้านความมั่นคงปลอดภัยและคอยปรับปรุง Security Patch เพื่อปิดช่องโหว่ต่างๆ ที่อาจใช้เป็นช่องทางในการสร้างความเสียหายให้กับ กปภ. จากตัวอย่างเว็บไซต์ ที่เกี่ยวข้อง เช่น

๑.๑.๑. เว็บไซต์ของระบบปฏิบัติการ Windows platform **

- https://portal.msrc.microsoft.com/en-us/security-guidance

๑.๑.๒. เว็บไซต์ของระบบปฏิบัติการ Linux platform **

- https://access.redhat.com/security/security-updates/
- https://www.debian.org/security/
- https://ubuntu.com/security/notices

๑.๑.๓. เว็บไซต์ของระบบปฏิบัติการ Virtualization platform **

- https://www.vmware.com/security/advisories.html

๑.๑.๔. เว็บไซต์ของอุปกรณ์เครือข่าย **

- https://tools.cisco.com/security/center/publicationListing.x
- https://advisory.juniper.net
- https://www.hpe.com/us/en/services/security-vulnerability.html
- https://www.arubanetworks.com/support-services/security-bulletins/
- https://www.checkpoint.com/advisories/

๑.๑.๕. เว็บไซต์ที่เกี่ยวกับการพัฒนาระบบสารสนเทศ **

- https://httpd.apache.org/security/
- https://nginx.org/en/security_advisories.html

- https://www.oracle.com/security-alerts/
- https://mariadb.com/kb/en/security/
- https://wordpress.org/news/category/security/
- https://developer.joomla.org/security-centre.html
- https://www.docker.com/legal/docker-cve-database
- https://aws.amazon.com/security/security-bulletins

๑.๑.๖. เว็บไซต์แจ้งเตือนช่องโหว่และภัยคุกคามต่างๆ **

- http://www.ncsa.or.th (Add ThaiCERT NCSA Line Openchat)
- https://webboard-nsoc.ncsa.or.th/
- https://cve.mitre.org/news/
- https://www.cvedetails.com/
- https://owasp.org/
- https://apwg.org

หมายเหตุ

** เว็บไซต์ข้างต้นอาจมีการเปลี่ยนแปลง URL ได้ในอนาคต (ขึ้นอยู่กับผู้ดูแลเว็บไซต์นั้นๆ)

๑.๒. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องกำหนดให้มีการประเมินหาช่องโหว่ของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ตามระดับความเสี่ยงของระบบงานที่มีความสำคัญหรือระบบที่สามารถเข้าถึงจากภายนอกได้โดยตรง (Public IP) ซึ่งมีความเสี่ยงสูงที่จะโดนโจมตีจากภัยคุกคามทางไซเบอร์โดยผู้เชี่ยวชาญอิสระอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการพัฒนาระบบใหม่ก่อนใช้งานระบบจริง (Golive)

๑.๓. การดำเนินการแก้ไขเพื่อปิดช่องโหว่ที่ตรวจพบในแต่ละครั้งต้องมีการวางแผนการเปลี่ยนแปลง ประเมินผลกระทบและจัดทำแผนกู้คืนตามแนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลงต้องขออนุมัติจากผู้บังคับบัญชาที่รับผิดชอบก่อนดำเนินการเปลี่ยนแปลง เนื่องจากการเปลี่ยนแปลงดังกล่าวอาจเกิดความเสี่ยงหรือส่งผลกระทบต่อการทำงานของระบบได้

๒. การทดสอบเจาะระบบ (penetration test)

๒.๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ ควรพิจารณาให้มีการทดสอบเจาะระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ตามระดับความเสี่ยงของระบบงานที่มีความสำคัญหรือระบบที่สามารถเข้าถึงจากภายนอกได้โดยตรง (Public IP) ซึ่งมีความเสี่ยงสูงที่จะโดนโจมตีจากภัยคุกคามทางไซเบอร์ โดยผู้เชี่ยวชาญอิสระอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการพัฒนาระบบใหม่ก่อนใช้งานระบบจริง (Golive)

๒.๒. การดำเนินการแก้ไขจุดบกพร่องหรือจุดอ่อนของระบบในแต่ละครั้งต้องมีการวางแผนการเปลี่ยนแปลงประเมินผลกระทบและจัดทำแผนกู้คืนตามแนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลงต้องขออนุมัติจากผู้บังคับบัญชาที่รับผิดชอบก่อนดำเนินการเปลี่ยนแปลง เนื่องจากการเปลี่ยนแปลงดังกล่าวอาจเกิดความเสี่ยงหรือส่งผลกระทบต่อการทำงานของระบบได้

๓. ระยะเวลาในการแก้ไขเพื่อปิดช่องโหว่ หรือจุดอ่อนของระบบ

ระยะเวลาในการแก้ไขขึ้นอยู่กับระดับความรุนแรงของช่องโหว่หรือจุดอ่อน (Severity Level) โดยผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ ต้องพิจารณาระยะเวลาในการวางแผนแก้ไข ดังนี้

ระดับความรุนแรง	รายละเอียด	ระยะเวลาวางแผนและแก้ไขช่องโหว่
สูงมาก (Critical)	ผู้บุกรุกสามารถใช้ช่องโหว่ดังกล่าวควบคุมระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของ กปภ. ด้วยสิทธิ์สูงสุด (Admin/Root) เพื่อสร้างความเสียหายต่อระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของ กปภ. ได้ทั้งหมด (Full Control)	๑-๒ สัปดาห์
สูง (High)	ผู้บุกรุกสามารถใช้ช่องโหว่ดังกล่าวทำให้ระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของ กปภ. เสียหายแต่ไม่สามารถควบคุมด้วยสิทธิ์สูงสุด (Admin/Root)	๑ เดือน
ปานกลาง (Medium)	ผู้บุกรุกไม่สามารถใช้ช่องโหว่ดังกล่าวโจมตีหรือสร้างความเสียหายต่อระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของ กปภ. ได้โดยตรง แต่อาจรวบรวมข้อมูลจากช่องโหว่อื่นๆ เพื่อสร้างความเสียหายได้ในอนาคต	๖ - ๑๒ เดือน
ต่ำ (Low)	ผู้บุกรุกไม่สามารถใช้ช่องโหว่ดังกล่าวโจมตีหรือสร้างความเสียหายต่อระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของ กปภ.	พิจารณาตามความเหมาะสม

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๘
แนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลง
(Change management guideline)

วัตถุประสงค์

- เพื่อกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศของ กปภ. เช่น อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และอื่นๆ
- เพื่อให้มีการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
- เพื่อให้มีการจัดทำแผนย้อนกลับหากเกิดความผิดพลาดจากการเปลี่ยนแปลง

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- พนักงานที่มีส่วนเกี่ยวข้องกับการเปลี่ยนแปลงแก้ไขระบบสารสนเทศเครือข่ายคอมพิวเตอร์ของ กปภ.

แนวทางการปฏิบัติ

๑. การบริหารจัดการการเปลี่ยนแปลง เป็นกระบวนการในการ การวางแผน วิเคราะห์ความเสี่ยงในการดำเนินการเพื่อลดผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง โดยแบ่งออกเป็น ๓ ประเภท คือ

๑.๑. Normal Change

เป็นการเปลี่ยนแปลงที่ต้องทำตามกระบวนการปกติที่ต้องมีการวางแผนการเปลี่ยนแปลง ประเมินผลกระทบและจัดทำแผนกู้คืน โดยต้องขออนุมัติจากผู้บังคับบัญชาที่รับผิดชอบก่อนดำเนินการเปลี่ยนแปลงเนื่องจากการเปลี่ยนแปลงดังกล่าวอาจเกิดความเสี่ยงหรือส่งผลกระทบต่อการทำงานของระบบได้

๑.๒. Standard Change

เป็นการเปลี่ยนแปลงที่ได้รับอนุมัติไว้ล่วงหน้าซึ่งการเปลี่ยนแปลงดังกล่าวจะไม่ส่งผลกระทบต่อระบบงานโดยรวมขององค์กร ทั้งนี้สามารถดำเนินการเปลี่ยนแปลงได้โดยไม่ต้องปฏิบัติตามกระบวนการ Normal Change ดังนี้

๑.๒.๑. การติดตั้งหรือถอดถอน ระบบปฏิบัติการ/ซอฟต์แวร์มาตรฐาน

๑.๒.๒. การเพิ่ม-ลบ User Account ในระบบต่างๆ เช่น E-mail, Intranet, Internet, AD เป็นต้น

๑.๒.๓. การซ่อมหรือเปลี่ยนเครื่อง PC/Notebook/UPS

๑.๒.๔. การติดตั้งแก้ไขสาย LAN ของผู้ใช้งาน

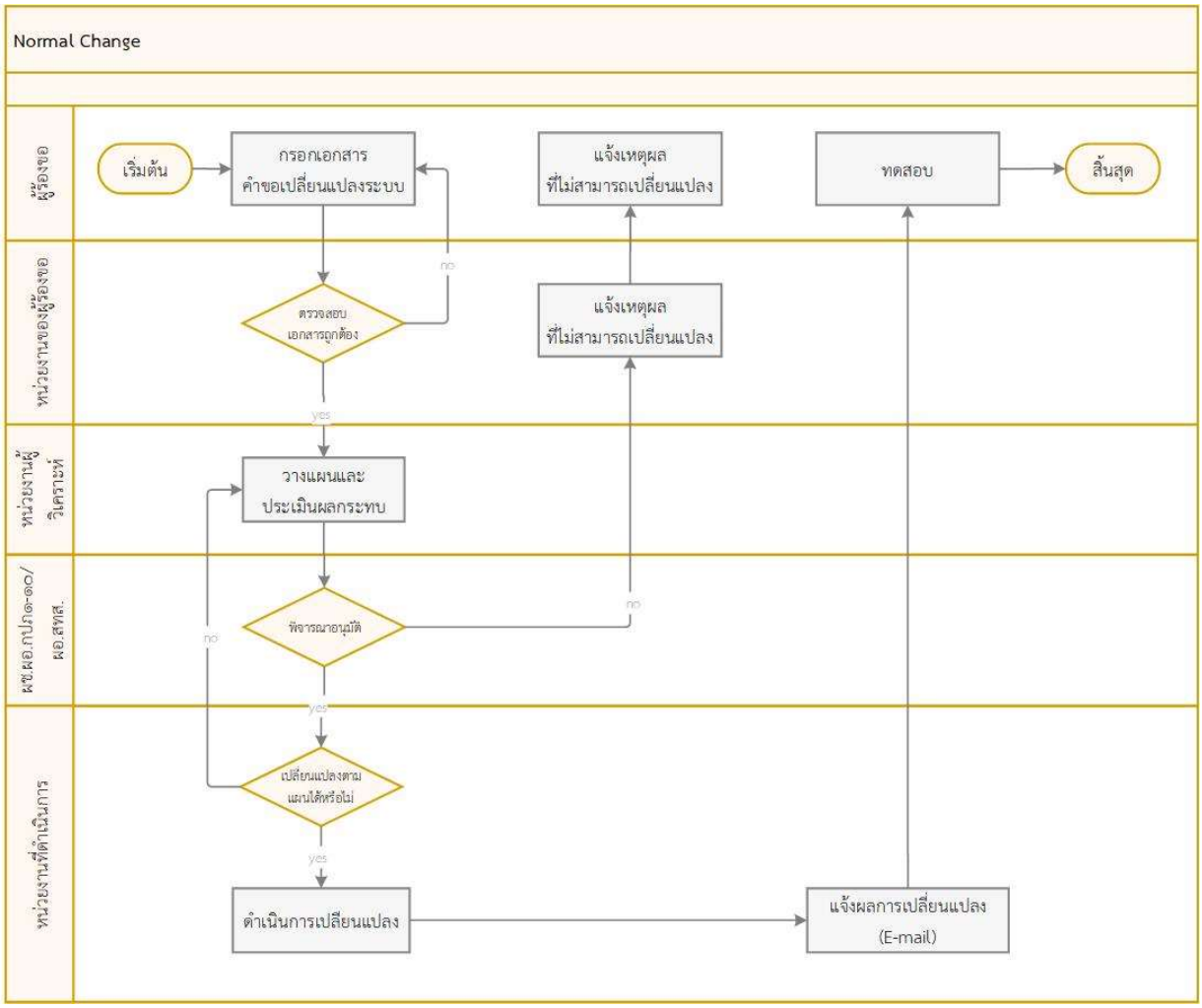
๑.๒.๕. การแก้ไขซ่อมแซมอุปกรณ์ Access switch และ Wireless Access Point

๑.๓. Emergency Change

เป็นการเปลี่ยนแปลงแบบเร่งด่วนต้องทำการแก้ไขโดยทันที หากไม่แก้ไขจะส่งผลกระทบและสร้างความเสียหายโดยรวมขององค์กร เช่น การแก้ไข Major Incident, การปรับเปลี่ยนค่า Configuration หรือการเปลี่ยนอุปกรณ์ที่เสียโดยกระทันหันเพื่อให้ระบบสามารถทำงานกลับคืนได้อย่างรวดเร็วหลังจากนั้นให้ปฏิบัติตามกระบวนการNormal Change ย้อนหลัง

๒. แผนภาพและคำอธิบายขั้นตอนการปฏิบัติงาน

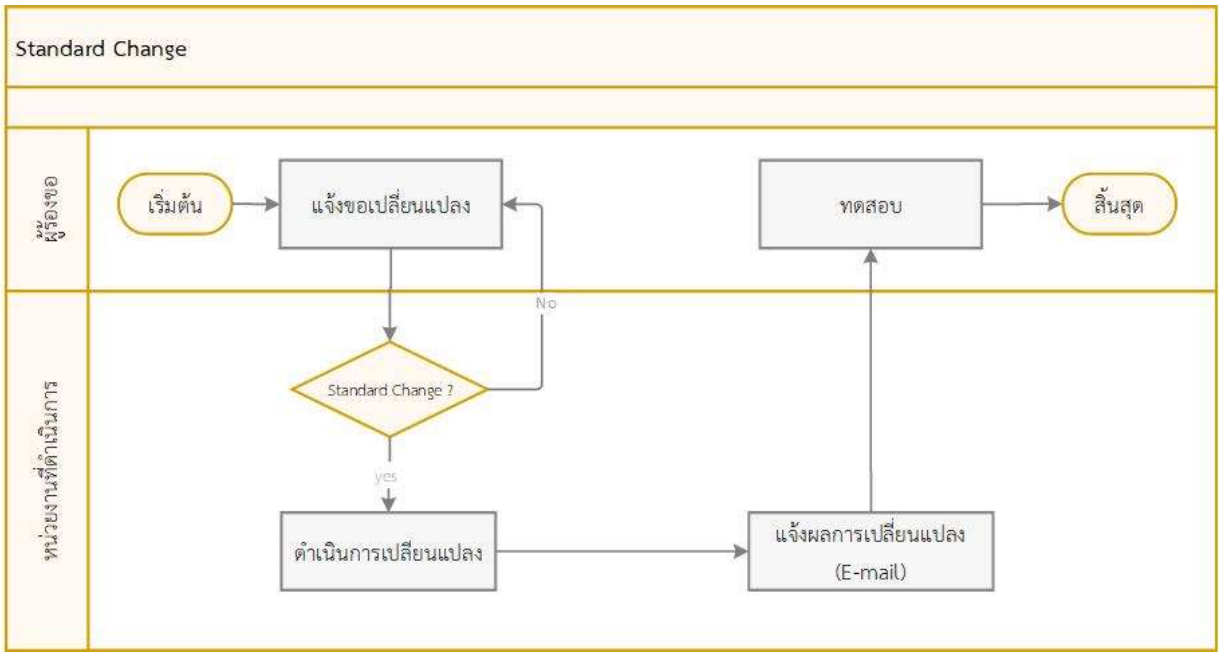
๒.๑. <u>แผนภาพกิจกรรม Normal Change</u>



คำอธิบายกิจกรรม Normal Change

ผู้ปฏิบัติ	กิจกรรม
ผู้ร้องขอ	• ตรวจสอบแล้วพบว่าการเปลี่ยนแปลงนี้มีความซับซ้อนและอาจมีผลกระทบต่อระบบงาน • กรอกแบบฟอร์มคำขอเปลี่ยนแปลงระบบและให้ผู้บังคับบัญชาที่รับผิดชอบตามสายงานตรวจสอบความถูกต้องพร้อมลงนามในแบบฟอร์มหากข้อมูลไม่ถูกต้องจะส่งกลับให้ผู้ร้องขอดำเนินการแก้ไขต่อไป
หน่วยงานผู้วิเคราะห์	• พิจารณารายละเอียดระบุความสำคัญและประเมินผลกระทบของการเปลี่ยนแปลง • วางแผนการเปลี่ยนแปลง/ทรัพยากรที่ต้องใช้ • ระบุแผนการย้อนกลับ (Roll Back Plan) ในกรณีที่ผลของการเปลี่ยนแปลงระบบไม่บรรลุตามวัตถุประสงค์ • ให้ผู้บังคับบัญชาที่รับผิดชอบตามสายงานลงนามเห็นชอบในแบบฟอร์ม
ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐	• พิจารณาและอนุมัติการเปลี่ยนแปลง ทบทวนผลที่ได้จากการวิเคราะห์ว่าคุ้มค่าต่อการเปลี่ยนแปลง และมีความเสี่ยงต่อระบบงานเหมาะสมที่จะทำการเปลี่ยนแปลงตามการร้องขอหรือไม่ • กรณีที่พิจารณาแล้วผลของการเปลี่ยนแปลงมีความเสี่ยง และส่งผลกระทบต่อระบบงานให้หน่วยงานผู้วิเคราะห์ดำเนินการหาแนวทางในการแก้ไขรูปแบบอื่นและขออนุมัติใหม่อีกครั้ง
หน่วยงานที่ดำเนินการ	• ดำเนินการเปลี่ยนแปลงตามการร้องขอ โดยอ้างอิง ขั้นตอนปฏิบัติการจากแผนการเปลี่ยนแปลงที่อนุมัติแล้วหลังจากนั้นแจ้งต่อผู้ร้องขอทดสอบผ่านทาง E-mail • หากดำเนินการตามแผนปกติแล้วไม่บรรลุตามวัตถุประสงค์ให้ดำเนินตามแผนย้อนกลับและแจ้งให้หน่วยงานผู้วิเคราะห์ทราบเพื่อวิเคราะห์ผลลัพธ์ที่ได้จากการแก้ไขในรูปแบบอื่นอีกครั้ง

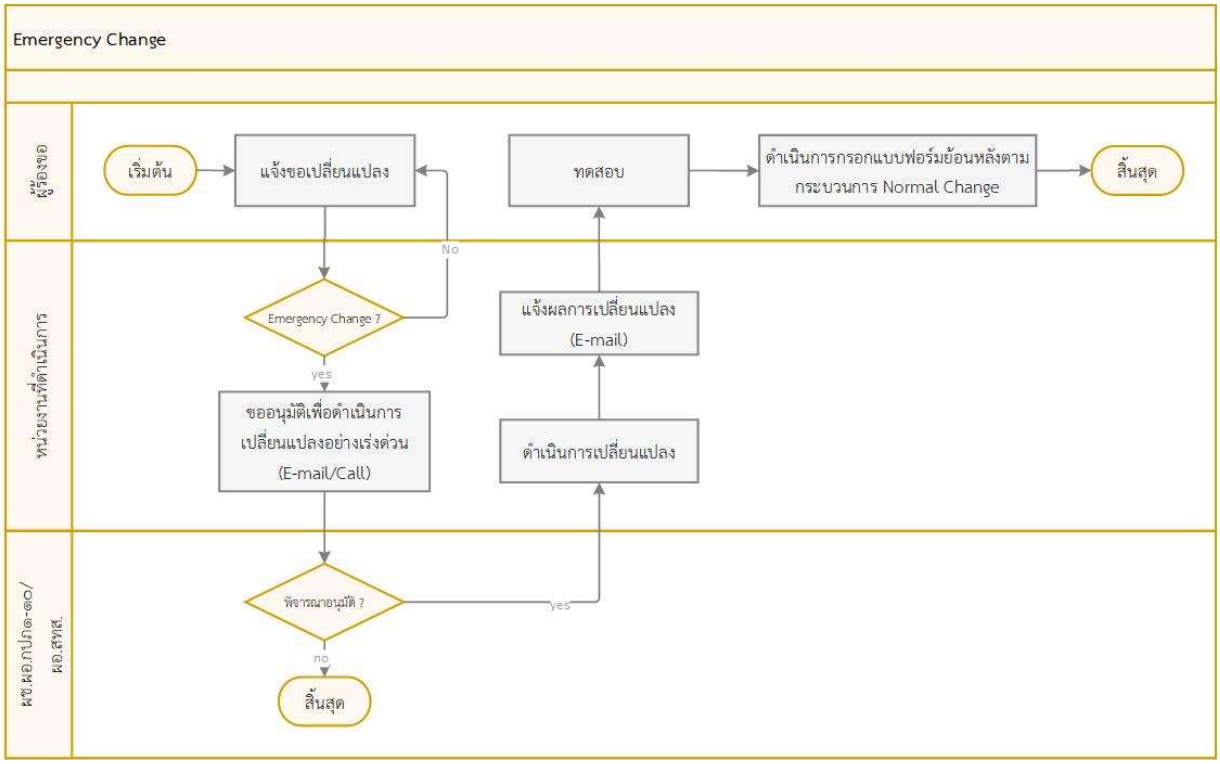
๒.๒. <u>แผนภาพกิจกรรม Standard Change</u>



<u>คำอธิบายกิจกรรม Standard Change</u>

ผู้ปฏิบัติ	กิจกรรม
ผู้ร้องขอ	• ร้องขอการเปลี่ยนแปลง
หน่วยงานที่ดำเนินการ	• ตรวจสอบการเปลี่ยนแปลงว่าเป็น Standard Change หรือไม่ หากเป็น Standard Change ให้ดำเนินการเปลี่ยนแปลงตามการร้องขอ • กรณีไม่ตรงตาม Standard Change ให้แจ้งต่อผู้ร้องขอดำเนินการตามกระบวนการ Normal Change ต่อไป

๒.๓. แผนภาพกิจกรรม Emergency Change



คำอธิบายกิจกรรม Emergency Change

ผู้ปฏิบัติ	กิจกรรม
ผู้ร้องขอ	• ร้องขอการเปลี่ยนแปลงแบบเร่งด่วน
หน่วยงานที่ดำเนินการ	• ตรวจสอบการเปลี่ยนแปลงว่าเป็น Emergency Change หรือไม่ หากเป็น Emergency Change ให้ดำเนินการขออนุมัติเปลี่ยนแปลงแบบเร่งด่วนต่อ ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐ เมื่อได้รับอนุมัติแล้วสามารถแก้ไขได้ทันที • กรณีไม่ตรงตาม Emergency Change ให้แจ้งต่อผู้ร้องขอดำเนินการตามกระบวนการ Normal Change หรือ Standard Change ต่อไป แจ้งต่อผู้ร้องขอทดสอบผ่านทาง E-mail หากทดสอบแล้วสามารถใช้งานได้ตามที่ร้องขอ ให้ผู้ร้องขอดำเนินการกรอกแบบฟอร์มคำขอเปลี่ยนแปลงตามกระบวนการ Normal Change ย้อนหลัง

ผู้ปฏิบัติ	กิจกรรม
ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐	• พิจารณาและอนุมัติการเปลี่ยนแปลง ทบทวนผลที่ได้จากการวิเคราะห์ว่าคุ้มค่าต่อการเปลี่ยนแปลง และมีความเสี่ยงต่อระบบงานเหมาะสมที่จะทำการเปลี่ยนแปลงตามการร้องขอหรือไม่ • กรณีที่พิจารณาแล้วผลของการเปลี่ยนแปลงมีความเสี่ยง และส่งผลกระทบต่อระบบงานให้หน่วยงานผู้วิเคราะห์ดำเนินการหาแนวทางในการแก้ไขรูปแบบอื่นและขออนุมัติใหม่อีกครั้ง

เอกสารอ้างอิง

๑. แบบฟอร์มคำขอเปลี่ยนแปลง – ระบบงานทั่วไป (IT-FM-DEV-๐๘ – ระบบงานทั่วไป)

๒. แบบฟอร์มคำขอเปลี่ยนแปลง – ระบบสารสนเทศด้านปฏิบัติการ (IT-FM-DEV-๐๘ – OIS)

ส่วนที่ ๙
แนวทางปฏิบัติการบริหารจัดการการตั้งค่าระบบและการกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ
(System configuration management and Minimum baseline standard guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. มีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุมปลอดภัย และเป็นไปตามมาตรฐานขั้นต่ำที่ กปภ. กำหนด

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. การบริหารจัดการการตั้งค่าระบบ (System configuration management)

๑.๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ ต้องตั้งค่าระบบและอุปกรณ์ ได้แก่ ระบบปฏิบัติการ ระบบฐานข้อมูล อุปกรณ์เครือข่ายสื่อสารต่างๆ ตามการตั้งค่าระบบตามมาตรฐานขั้นต่ำ (Minimum baseline standard) และต้องจัดให้มีการตรวจสอบการตั้งค่าของระบบอีกครั้ง (Cross Check) โดยหัวหน้างานหรือผู้ที่ได้รับมอบหมาย

๑.๒. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ ต้องเก็บบันทึกข้อมูลต่างๆ รวมถึงการตั้งค่าของระบบหรืออุปกรณ์ทั้งหมดโดยมีรายละเอียดอย่างน้อย ดังนี้

๑.๒.๑. แผนผังการเชื่อมต่อของระบบ (System/Network Diagram)

๑.๒.๒. รายละเอียดของฮาร์ดแวร์ (Hardware Specification)

๑.๒.๓. รายละเอียดของซอฟต์แวร์ (Software Specification)

๑.๒.๔. รายละเอียดของการตั้งค่าต่างๆ ของระบบ (Configuration)

๑.๓. การเปลี่ยนแปลงการตั้งค่าบนระบบต้องมีการวางแผนการเปลี่ยนแปลงประเมินผลกระทบและจัดทำแผนกู้คืนตามแนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลงโดยต้องขออนุมัติจากผู้บังคับบัญชาที่รับผิดชอบก่อนดำเนินการเปลี่ยนแปลงเนื่องจากการเปลี่ยนแปลงดังกล่าวอาจเกิดความเสี่ยงหรือส่งผลกระทบต่อการทำงานของระบบได้

๑.๔. ต้องจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบ ของทุกอุปกรณ์และระบบงาน (System configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมอย่างเพียงพอ

๒. การกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ (Minimum baseline standard)

๒.๑. ระบบปฏิบัติการและซอฟต์แวร์ที่ติดตั้งใช้งาน ต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

๒.๒. ต้องปิดพอร์ต (Ports) หรือ โปรโตคอล (Protocols) ที่ไม่มีความจำเป็นต่อการใช้งานรวมถึงควรหลีกเลี่ยงการใช้งานพอร์ตหรือโปรโตคอลที่มีความปลอดภัยต่ำหรือสุ่มเสี่ยงต่อการโดนโจมตี

๒.๓. ปรับปรุง Patch ของระบบปฏิบัติการ ซอฟต์แวร์ และเฟิร์มแวร์ของอุปกรณ์ โดยปฏิบัติตามแนวทางปฏิบัติการบริหารจัดการ Patch

๒.๔. ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์บนเครื่องคอมพิวเตอร์แม่ข่าย (หากสามารถติดตั้งได้) และตรวจสอบว่ามีการปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ให้เป็นเวอร์ชันปัจจุบันและพร้อมใช้งานอยู่เสมอ

๒.๕. เปลี่ยนค่ารหัสผ่านตั้งต้น (Default Password) และตั้งค่าใหม่ให้มีความซับซ้อนยากต่อการคาดเดา

๒.๖. ปิดการใช้งานหรือถอดถอนบัญชีผู้ใช้ที่ไม่ได้ใช้งานในระบบหรืออุปกรณ์

๒.๗. บัญชีผู้ใช้งานต้องได้รับการพิจารณาสิทธิ์ในการเข้าถึงและสิทธิ์การใช้งานตามความจำเป็นเท่านั้น (Least Access Privilege)

๒.๘. เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายต้องมีการกำหนดค่าให้เชื่อมต่อกับ Time Server ของ กปภ.

๒.๙. การแบ่งแยกหน้าที่ (Separation of Duties) โดยดำเนินการตาม หมวดที่ ๖ ส่วนที่ ๑ แนวทางปฏิบัติการแบ่งแยกอำนาจหน้าที่ (Segregation of duties guideline)

๒.๑๐. การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๑๐
แนวทางปฏิบัติการบริหารจัดการ Patch
(Patch management guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. มีการบริหารจัดการ Patch ของระบบปฏิบัติการ ซอฟต์แวร์ และเฟิร์มแวร์ของอุปกรณ์ โดยมีการควบคุมการติดตั้ง Patch ได้อย่างเหมาะสมทันการณ์

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องคอยตรวจสอบว่ามีการแจ้งเตือนปรับปรุง Patch จากเจ้าของผลิตภัณฑ์อย่างสม่ำเสมอ

๒. การปรับปรุงแก้ไข Patch ควรปรับปรุงให้เป็นเวอร์ชันปัจจุบันหรือเวอร์ชันที่มีความเสถียรและต้องดำเนินการทดสอบ Patch ที่ออกใหม่ทุกครั้งก่อนใช้งานบนระบบจริง ทั้งนี้ต้องมีการวางแผนการเปลี่ยนแปลง ประเมินผลกระทบและจัดทำแผนกู้คืนตามแนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลง โดยต้องขออนุมัติจากผู้บังคับบัญชาที่รับผิดชอบก่อนดำเนินการเปลี่ยนแปลงเนื่องจากการเปลี่ยนแปลงดังกล่าวอาจเกิดความเสี่ยงหรือส่งผลกระทบต่อการทำงานของระบบได้

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๑๑
แนวทางปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี
(Malware protection guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. สามารถจัดการกับโปรแกรมไม่ประสงค์ดีที่อาจจะสร้างความเสียหายต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ.

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันโปรแกรมไม่ประสงค์ดี (Malware) และไวรัสคอมพิวเตอร์ (Antivirus Server) ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอและต้องปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ให้เป็นปัจจุบัน
๒. ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์บนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายเพื่อให้ทำงานในลักษณะทันทีทันใด (Real-time Scan) เมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน
๓. ตรวจสอบว่าโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายได้มีการปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์จากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัสคอมพิวเตอร์ให้เป็นเป็นปัจจุบัน

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๑๒
แนวทางปฏิบัติการบริหารจัดการรหัสผ่าน
(Password management guideline)

วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และควบคุมการใช้งานรหัสผ่านที่คาดเดายากในการเข้าใช้งานระบบสารสนเทศของ กปภ. ให้มีความมั่นคงปลอดภัย

ผู้ปฏิบัติ

- ผู้บริหาร พนักงานและลูกจ้างของ กปภ.
- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. การตั้งค่าและใช้งานรหัสผ่าน

๑.๑. ผู้ใช้งานต้องตั้งรหัสผ่านที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร ซึ่งประกอบด้วย

๑.๑.๑. ตัวอักษรที่เป็นตัวพิมพ์ปกติ

๑.๑.๒. ตัวอักษรที่เป็นตัวพิมพ์ใหญ่

๑.๑.๓. ตัวเลข และอักขระพิเศษ

๑.๒. ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่าน ดังนี้

๑.๒.๑. ชื่อ-สกุล ของตนเองหรือบุคคลในครอบครัว

๑.๒.๒. วัน/เดือน/ปีเกิด และเบอร์โทรศัพท์ของตนเองหรือบุคคลในครอบครัว

๑.๒.๓. คำที่ใช้ในพจนานุกรม และคำที่ง่ายต่อการคาดเดา

๑.๓. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทุกๆ ๙๐ วันหรือตามระยะเวลาที่ระบบสารสนเทศกำหนด และจะต้องไม่นำรหัสผ่านที่หมดอายุแล้วมาใช้ซ้ำอีก รวมถึงควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ

๑.๔. ผู้ใช้งานต้องปกปิดและรักษารหัสผ่านของตนอย่างดีที่สุดโดยไม่จดหรือบันทึกรหัสผ่าน ไม่เปิดเผยรหัสผ่านของตนเองให้บุคคลอื่นรับรู้ หากรหัสผ่านถูกเปิดเผยต้องเปลี่ยนใหม่โดยเร็ว

๑.๕. ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง หากระบบสารสนเทศนั้นสามารถกำหนดได้ และต้องไม่แสดงรหัสผ่านที่พิมพ์ลงไปหรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

๒. การส่งมอบรหัสผ่าน

๒.๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องส่งมอบบัญชีชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานโดยตรงหรือวิธีที่มั่นคงปลอดภัย และแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทันทีหลังจากที่ได้รับมอบรหัสผ่านชั่วคราว

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๑๓
แนวทางปฏิบัติการใช้งานอินเทอร์เน็ต
(Internet guideline)

วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และควบคุมการใช้งานอินเทอร์เน็ตของ กปภ. ให้เป็นไปอย่างถูกต้องไม่ก่อให้เกิดความเสียหายต่อ กปภ. และปฏิบัติตามกฎหมาย หรือ ระเบียบข้อบังคับอื่นๆ ที่เกี่ยวข้อง

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- บุคคลภายนอก

แนวทางการปฏิบัติ

๑. ผู้ใช้งานอินเทอร์เน็ต จะต้องเป็นพนักงาน ลูกจ้าง หรือบุคคลภายนอก ที่ กปภ. อนุมัติให้ใช้งานอินเทอร์เน็ตของ กปภ.

๒. การแบ่งกลุ่มของผู้ใช้งานอินเทอร์เน็ต

กลุ่มที่ ๑ : พนักงานของ กปภ.

จะต้องเป็นพนักงาน ของ กปภ. โดยมีรหัสพนักงานและได้สมัครเป็นสมาชิกเข้าใช้งานเว็บไซต์อินทราเน็ต (Intranet) และอีเมล (E-mail) ของ กปภ. แล้วเท่านั้น จึงจะสามารถลงทะเบียนขอใช้งานอินเทอร์เน็ตได้ที่เว็บไซต์ https://computer.pwa.co.th และเลือกหัวข้อ “ระบบลงทะเบียน Internet”

กลุ่มที่ ๒ : พนักงานของ กปภ. ที่ยังไม่มีรหัสพนักงาน ลูกจ้างของ กปภ. และบุคคลภายนอก

พนักงานของ กปภ. ที่ยังไม่มีรหัสพนักงาน ลูกจ้างของ กปภ. และบุคคลภายนอกจะต้องกรอกแบบฟอร์มขอใช้งานอินเทอร์เน็ตสำหรับบุคคลภายนอกผ่านหน่วยงานต้นสังกัดหรือหน่วยงานเจ้าของโครงการของ กปภ. โดยต้องได้รับอนุมัติจาก ผอ.สปท./ผช.ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมายจึงจะมีสิทธิ์เข้าใช้งานระบบอินเทอร์เน็ตของ กปภ.

๓. การใช้งานอินเทอร์เน็ตของ กปภ. จะมีการจัดเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานเพื่อปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีการประกาศใช้งาน

๔. ข้อห้ามการใช้งานอินเทอร์เน็ตของ กปภ.

๔.๑. ห้ามดาวน์โหลดและใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ และซอฟต์แวร์ที่อาจจะสร้างความเสียหายต่อระบบสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์ของ กปภ.

๔.๒. ห้ามผู้ใช้งานกดหน้าต่างโฆษณาแบบป๊อบอัพที่แสดงขึ้นมาโดยอัตโนมัติจากเว็บไซต์ที่ไม่มีความน่าเชื่อถือหรือเว็บไซต์ที่สุ่มเสี่ยงตามข้อ ๔.๔ เพื่อป้องกันความเสียหายจากการติดมัลแวร์

๔.๓. ห้ามเล่นเกม หรือดู Streaming Content ที่ไม่เกี่ยวข้องกับการปฏิบัติงาน ในวันและเวลาทำงาน

๔.๔. ห้ามใช้อินเทอร์เน็ตของ กปภ. เพื่อเข้าเว็บไซต์ที่อยู่ในประเภทดัง ต่อไปนี้

๔.๔.๑. เว็บไซต์การพนัน

๔.๔.๒. เว็บไซต์ที่มีการวิพากษ์วิจารณ์ที่เกี่ยวกับ ชาติ ศาสนา และ พระมหากษัตริย์

๔.๔.๓. เว็บไซต์ลามก อนาจาร

๔.๔.๔. เว็บไซต์อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๔.๕. ห้ามใช้อินเทอร์เน็ตของ กปภ. เพื่อส่ง กระจาย หรือแจกจ่ายข้อมูล ดังต่อไปนี้

๔.๕.๑. ข้อมูลที่เป็นความลับของ กปภ. ไปยังบุคคลที่ไม่ได้รับอนุญาต

๔.๕.๒. ใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

๔.๕.๓. ข้อมูลที่เข้าข่ายลามก อนาจาร

๔.๕.๔. ข้อมูลอื่นๆ ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ

๕. การใช้งานเว็บไซต์ เว็บบอร์ด เว็บบล็อก หรือ Social Network ต้องปฏิบัติ ดังนี้

๕.๑. ห้ามพิมพ์ข้อความที่เปิดเผยข้อมูลอันเป็นความลับของ กปภ. หรือแสดงความคิดเห็นอันจะก่อให้เกิดความเสียหายต่อ กปภ.

๕.๒. ห้ามสร้างกลุ่มผู้ใช้งานเพื่อวัตถุประสงค์ในการปลุกระดมพนักงานไปในทางที่ผิด

๕.๓. ไม่ควรให้ข้อมูลส่วนบุคคลบนระบบ Social network ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์

๖. หากผู้ใดพบเห็นการใช้อินเทอร์เน็ตในเครือข่ายของ กปภ. ไปในทางที่ไม่เหมาะสมหรืออาจจะส่งผลกระทบต่อ กปภ. ต้องรายงานผู้บังคับบัญชาในสายงานทราบทันที

เอกสารอ้างอิง

๑. ขอใช้งานอินเตอร์เน็ตสำหรับหน่วยงาน/บุคคลภายนอก (IT-FM-SC-๐๑)

ส่วนที่ ๑๔
แนวทางปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
(E-mail guideline)

วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ของ กปภ. ให้เป็นไปอย่างถูกต้องไม่ก่อให้เกิดความเสียหายต่อ กปภ. และปฏิบัติตามกฎหมาย หรือ ระเบียบข้อบังคับอื่นๆ ที่เกี่ยวข้อง

ผู้ปฏิบัติ

- ผู้บริหาร และพนักงานของ กปภ.

แนวทางการปฏิบัติ

๑. ผู้ใช้งาน E-mail จะต้องเป็นพนักงาน ของ กปภ. โดยมีรหัสพนักงานและได้สมัครเป็นสมาชิกเข้าใช้งานเว็บไซต์ https://intranet.pwa.co.th แล้วเท่านั้น

๒. การแบ่งกลุ่มของผู้ใช้งาน E-mail

กลุ่มที่ ๑ : E-mail สำหรับผู้บริหารและพนักงาน

เป็น E-mail ส่วนตัวของผู้บริหารและพนักงาน กปภ. ทุกระดับชั้น โดยพนักงานที่ต้องการใช้งานจะต้องลงทะเบียนขอใช้งาน E-mail ที่เว็บไซต์ https://pwamail.pwa.co.th และเลือกหัวข้อ “ลงทะเบียนเป็นผู้ใช้งานระบบ”

กลุ่มที่ ๒ : E-mail สำหรับหน่วยงาน

เป็น E-mail ของหน่วยงานระดับกอง หรือเทียบเท่าขึ้นไป โดยหน่วยงานที่ต้องการใช้งานให้หัวหน้าหน่วยงานแจ้งความต้องการใช้งานตาม “แบบฟอร์ม ขอใช้/ยกเลิก/ขยายพื้นที่ อีเมล” หากผู้แจ้งความต้องการไม่ได้เป็นผู้ใช้งาน E-mail ดังกล่าวเอง สามารถมอบหมายให้พนักงานในหน่วยงานเป็นผู้ใช้งานแทน

กลุ่มที่ ๓ : E-mail สำหรับกรณีพิเศษ

เป็น E-mail ที่หัวหน้าโครงการหรือหัวหน้างานขอใช้งานเป็นกรณีพิเศษ เพื่อใช้งานเฉพาะด้าน โดยให้แจ้งความต้องการใช้งานตาม “แบบฟอร์ม ขอใช้/ยกเลิก/ขยายพื้นที่ อีเมล” หากผู้แจ้งความต้องการไม่ได้เป็นผู้ใช้งาน E-mail ดังกล่าวเอง สามารถมอบหมายให้ผู้ใต้บังคับบัญชาเป็นผู้ใช้งานแทน

๓. เงื่อนไขและข้อจำกัดในการให้บริการของระบบ E-mail

๓.๑. การใช้งานรหัสผ่าน E-mail ผู้ใช้งานต้องปฏิบัติตามขั้นตอน และแนวทางปฏิบัติการบริหารจัดการรหัสผ่าน

๓.๒. กรณีที่ผู้ใช้งานใส่รหัสผ่าน E-mail ผิดเกิน ๑๐ ครั้งใน ๑ นาที ระบบจะระงับบัญชีผู้ใช้งานเพื่อป้องกันการโจมตีแบบ Brute Force ทั้งนี้ผู้ใช้งานจะต้องแจ้งผู้ดูแลระบบ E-mail เพื่อทำการเปิดบัญชีผู้ใช้งานต่อไป

๓.๓. ผู้ใช้งาน E-mail จะได้รับจัดสรรเนื้อที่เมลขนาด ๑ GB และสามารถแนบไฟล์ได้สูงสุด ๒๕ MB หากเนื้อที่ที่ได้รับจัดสรรไม่เพียงพอต่อการใช้งาน สามารถแจ้งความต้องการเนื้อที่เมลเพิ่มได้ตาม “แบบฟอร์ม ขอใช้/ยกเลิก/ขยายพื้นที่ อีเมล”

๓.๔. ผู้ใช้งาน E-mail จะได้รับพื้นที่จัดเก็บข้อมูลบนระบบ Cloud Drive ขนาด ๑ GB ต่อผู้ใช้งาน

๓.๕. ผู้ใช้งานต้องระมัดระวังในการใช้ E-mail เพื่อไม่ให้เกิดความเสียหายต่อ กปภ. หรือละเมิดสิทธิ์หรือสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาผลประโยชน์หรืออนุญาต ให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้ E-mail ของ กปภ.

๓.๖. ผู้ใช้งานต้องรับผิดชอบในข้อความ รูปภาพ เสียง หรือแฟ้มข้อมูลที่ส่งออกจาก E-mail ของตนเอง

๓.๗. ผู้บริหารระดับผู้อำนวยการฝ่ายหรือเทียบเท่าขึ้นไป หรือพนักงานที่ได้รับมอบหมายให้ดูแลระบบ E-mail มีสิทธิ์ส่ง E-mail ถึงพนักงานทุกคนใน กปภ.

๓.๘. การให้บริการ E-mail นี้ผู้ดูแลระบบได้ปฏิบัติตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ประกาศใช้งาน ดังนั้นผู้ดูแลระบบจะไม่รับผิดชอบต่อความสูญหายหรือความเสียหายของข้อมูลหรือแฟ้มข้อมูลของผู้ใช้งานกรณีเกิดความเสียหายอันเนื่องมาจากผู้ใช้งาน

๓.๙. ผู้ดูแลระบบขอสงวนสิทธิ์ระงับการให้บริการระบบ E-mail หากตรวจพบในกรณี ดังต่อไปนี้

๓.๙.๑. การใช้งานของผู้ใช้งานที่ฝ่าฝืนหรือละเมิด กฎหมาย ระเบียบข้อบังคับและเงื่อนไขการให้บริการ

๓.๙.๒. การใช้งานของผู้ใช้งานที่ก่อให้เกิดผลกระทบต่อภาพรวมการให้บริการของระบบ E-mail ของ กปภ. หรือปัญหาด้านความมั่นคงปลอดภัย

๓.๙.๓. กรณีที่ผู้ใช้งานไม่มีการเข้าใช้งานระบบเกิน ๖ เดือน

๓.๙.๔. กรณีที่มีเหตุจำเป็นต้องบำรุงรักษาหรือแก้ไขระบบ E-mail ของ กปภ.

เอกสารอ้างอิง

๑. แบบฟอร์ม ขอใช้/ยกเลิก/ขยายพื้นที่ อีเมล (IT-FM-Mail-๐๑)

ส่วนที่ ๑๕
แนวทางปฏิบัติการใช้งานระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน
(Virtual machine system guideline)

วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และควบคุมการใช้งานระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Machine) ของ กปภ. สำหรับผู้ดูแลระบบสารสนเทศของ กปภ. ให้เป็นไปอย่างถูกต้องไม่ก่อให้เกิดความเสียหายต่อ กปภ. และปฏิบัติตามกฎหมาย หรือระเบียบข้อบังคับอื่นๆ ที่เกี่ยวข้อง

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ

แนวทางการปฏิบัติ

๑. ผู้ขอใช้บริการระบบ Virtual Machine
   ๑.๑. ผู้ดูแลระบบสารสนเทศ สังกัดผู้ช่วยผู้ว่าการ (ดิจิทัลและสารสนเทศ) สามารถขอใช้บริการได้โดยการกรอกแบบฟอร์มขอใช้บริการเครื่อง Virtual Machine และจัดทำบันทึกขออนุมัติการใช้งานตามสายงาน เมื่อได้รับอนุมัติแล้ว ผู้ให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือนจะดำเนินการสร้างเครื่อง Virtual Machine ให้
   ๑.๒. ผู้ดูแลระบบสารสนเทศ สังกัดกองเทคโนโลยีสารสนเทศ ๑-๑๐ สามารถขอใช้บริการได้โดยการกรอกแบบฟอร์มขอใช้บริการเครื่อง Virtual Machine โดยมีผู้เกี่ยวข้อง ดังนี้
      ๑.๒.๑. นักวิชาการคอมพิวเตอร์ ผู้พัฒนา/ผู้ดูแล ระบบสารสนเทศที่สร้างขึ้นบน Virtual Machine
      ๑.๒.๒. หัวหน้างานบริการคอมพิวเตอร์ ผู้พิจารณาการขอใช้งานของ นักวิชาการคอมพิวเตอร์
      ๑.๒.๓. ผู้อำนวยการกองเทคโนโลยีสารสนเทศ ๑-๑๐ ผู้พิจารณา/อนุมัติ การขอใช้งานของหัวหน้างานผู้ให้บริการเครื่อง Virtual Machine จะส่งมอบวิธีการใช้งานระบบ PWA Private Cloud ซึ่งระบบฯ จะสร้างเครื่อง Virtual Machine ให้อัตโนมัติ

๒. ผู้ให้บริการจะจัดเตรียมเครื่อง Virtual Machine โดยจัดสรรทรัพยากรหน่วยประมวลผลกลางเสมือน (vCPU), หน่วยความจำเสมือน (vRAM), พื้นที่จัดเก็บข้อมูล (Storage) ให้กับผู้ขอใช้บริการ รวมถึงระบบปฏิบัติการตามรูปแบบที่กำหนดหากผู้ใช้บริการต้องการเปลี่ยนแปลงรูปแบบบริการ หรือต้องการให้จัดสรรทรัพยากรเพิ่ม ผู้ใช้บริการต้องดำเนินการร้องขอตามที่ผู้ให้บริการกำหนดและระบุรูปแบบบริการที่ต้องการใหม่ ทั้งนี้ผู้ให้บริการจะพิจารณาเปลี่ยนแปลงการให้บริการหรือจัดสรรทรัพยากรตามความเหมาะสม

๓. ผู้ให้บริการจะดำเนินการสร้างเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่มีระบบปฏิบัติการ (OS) และโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (สำหรับระบบปฏิบัติการ Microsoft Windows Server), ระบบสำรองข้อมูล พร้อมทั้งทำการตั้งค่าระบบต่างๆ เบื้องต้นสำหรับระบบปฏิบัติการ (OS) และกรณีที่ผู้ใช้บริการมีความจำเป็นต้องใช้ซอฟต์แวร์นอกเหนือจากที่ผู้ให้บริการจัดเตรียมให้ ผู้ใช้บริการต้องเป็นผู้จัดหาและดำเนินการติดตั้งและตั้งค่าอื่นๆ เองรวมถึงรับผิดชอบค่าลิขสิทธิ์ที่เกิดขึ้นด้วย

๔. การบริการระบบเครือข่ายเครื่อง Virtual Machine จะให้หมายเลข IP Address เครือข่าย Intranet เท่านั้น หากผู้ใช้บริการต้องการใช้งานเครือข่ายอื่นจะต้องประสานงานกับงานควบคุมระบบเครือข่าย กคค. เพื่อขอหมายเลข IP Address ให้กับเครื่องคอมพิวเตอร์แม่ข่ายเสมือนและขอเปิดPolicy Firewall ในกรณีที่ต้องการใช้ Ports พิเศษที่นอกเหนือจาก Port ๘๐, ๔๔๓

๕. ผู้ใช้บริการสามารถแจ้งความต้องการให้ผู้ดูแลระบบ Virtual Machine ทำการ Snapshot Guest VM ก่อนดำเนินการปรับปรุงโปรแกรม หรือปรับปรุงระบบปฏิบัติการ (Update OS) เพื่อใช้ในการกู้คืนระบบหากระบบสารสนเทศเกิดขัดข้อง

๖. ผู้ใช้บริการเครื่อง Virtual Machine จะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ. ทุกประการที่สำคัญ ดังต่อไปนี้

๖.๑. แนวทางปฏิบัติการบริหารการจัดการรหัสผ่าน (Password management guideline)

๖.๒. แนวทางปฏิบัติการบริหารจัดการขีดความสามารถของระบบสารสนเทศ (Capacity management guideline)

๗. ผู้ใช้บริการจะต้องไม่ใช้บริการระบบ PWA Private Cloud ไปในทางที่ผิดกฎหมายหรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รวมทั้งต้องไม่กระทำการอย่างหนึ่งอย่างใด ดังต่อไปนี้

๗.๑. เป็นแหล่งกระจายหรือเผยแพร่มัลแวร์หรือเป็นแหล่งที่ใช้ในการเจาะหรือโจมตีระบบอื่นๆ

๗.๒. เป็นแหล่งที่ใช้ในการทำ Phishing เพื่อแอบขโมยข้อมูลของผู้อื่น

๗.๓. ให้บริการในลักษณะที่เป็น Peer to Peer BitTorrent และ BitCoins

๗.๔. ให้บริการระบบเว็บไซต์ที่นำเสนอสิ่งผิดกฎหมาย, การพนัน, ผิดศีลธรรม หรือขัดต่อระเบียบของ กปภ. ในที่นี้รวมถึงสื่อลามกอนาจาร การทำให้ผู้อื่นเสียหาย รวมถึงการเชื่อมต่อไปยังเว็บไซต์ลักษณะนี้ด้วย

๗.๕. ห้ามพัฒนาระบบการให้บริการ Video Streaming สำหรับเผยแพร่สื่อลามกอนาจาร รวมถึงการกระทำที่ไม่เหมาะสมต่างๆ

๗.๖. เป็นแหล่งเผยแพร่รูปภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการตัดต่อหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

๗.๗. เป็นแหล่งที่ใช้ในการทำ Commercial Mass E-mailing หรือ "Spamming" ไม่ว่ากรณีใดๆ ทั้งสิ้น การส่งโฆษณาไปยังอีเมลผู้อื่นโดยผู้อื่นไม่ได้ขอ หรือ ส่งไปยัง Groups Mail User การส่งอีเมลโดยใช้ที่อยู่ส่งกลับที่ไม่มีจริงทางด้านธุรกิจ การส่งข้อความลูกโซ่เพื่อจะทำให้เกิดการตอบกลับจำนวนมากและการส่ง ข้อความซ้ำๆ เดิมๆ ไปยังผู้อื่น เป็นต้น

๗.๘. ห้ามพัฒนาให้บริการที่เกี่ยวข้องกับซอฟต์แวร์ผิดกฎหมายทุกประเภทรวมไปถึงนามสกุลไฟล์ อื่นๆ ที่พยายามหลบเลี่ยงด้วยการใช้อุปกรณ์ โปรแกรมหรือข้อมูลที่ไม่ได้รับอนุญาตจากเจ้าของ ผลิตภัณฑ์และการละเมิดสิทธิทรัพย์สินทางปัญญา

๗.๙. เป็นแหล่งทำกิจกรรมใดๆ ที่ก่อให้เกิดการฝ่าฝืนกฎหมายไทย หรือกฎหมายระหว่างประเทศ หรือทำให้เกิด ความวุ่นวายต่อสถาบัน ชาติ ศาสนา พระมหากษัตริย์ หรือ สังคมทั่วไป

๗.๑๐. ไม่รองรับเว็บไซต์ที่ทำการแจกหรือให้บริการ Free Hosting, Free Image Hosting, Free File Hosting, Free Blog และ Backup Server ที่ทำให้ประสิทธิภาพของ Server ลดลง

๗.๑๑. เว็บไซต์ที่นำทรัพยากรของผู้ให้บริการ ไปแจกจ่ายแก่สาธารณะชนโดยทั่วไป โดยไม่ได้รับอนุญาต เช่น E-mail, Web Space, Database, download, proxy

๗.๑๒. เว็บไซต์ซึ่งนำมาถึงความเสื่อมเสียให้แก่ กปภ.

๘. ผู้ใช้งานต้องปฏิบัติตามกฎหมาย นโยบาย ระเบียบ คำสั่ง ขั้นตอนและแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ. หากผู้ใช้งานฝ่าฝืนและก่อหรืออาจก่อให้เกิดความเสียหายแก่ กปภ. หรือบุคคลหนึ่งบุคคลใด กปภ. จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ใช้งานที่ฝ่าฝืนตามความเหมาะสม

เอกสารที่เกี่ยวข้อง

๑. แบบฟอร์มขอใช้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (IT-FM-VM-๐๑)

๒. แบบฟอร์มขอเปลี่ยนแปลงทรัพยากร เครื่องคอมพิวเตอร์แม่ข่ายเสมือน (IT-FM-VM-๐๒)

ส่วนที่ ๑๖
แนวทางปฏิบัติการนำอุปกรณ์ส่วนบุคคลเข้ามาใช้งาน
(BYOD : Bring Your Own Device guideline)

วัตถุประสงค์

- เพื่อลดความเสี่ยงจากภัยคุกคามต่างๆ อันจะก่อให้เกิดความเสียหายจากการนำอุปกรณ์ส่วนบุคคลเข้ามาใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กปภ.

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- บุคคลภายนอก

แนวทางการปฏิบัติ

ผู้บริหาร พนักงาน ลูกจ้างของ กปภ. และบุคคลภายนอกที่นำอุปกรณ์ส่วนบุคคล ได้แก่ Laptop หรืออุปกรณ์แบบพกพาชนิดต่างๆ เช่น Tablet, Smart device เป็นต้น เข้ามาใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของ กปภ. ต้องปฏิบัติ ดังนี้

๑. ต้องมีการปรับปรุง Patch ของระบบปฏิบัติการ หรือ Firmware ให้เป็นเวอร์ชันปัจจุบัน
๒. ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (หากอุปกรณ์นั้นสามารถติดตั้งได้) และต้องอัปเดตให้เป็นเวอร์ชันปัจจุบันและพร้อมใช้งานอยู่เสมอ
๓. ห้ามใช้อุปกรณ์ส่วนบุคคลเชื่อมต่อเข้ากับเครือข่ายคอมพิวเตอร์ของ กปภ. เพื่อดำเนินการ ดังต่อไปนี้
   ๓.๑. เพื่อกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
   ๓.๒. เพื่อดักจับข้อมูล (Packet sniffing) สแกนเครือข่ายคอมพิวเตอร์ (Network Scan) หรือเจาะระบบ (Hacking)
๔. หากตรวจสอบพบว่าอุปกรณ์ส่วนบุคคลที่นำมาใช้งานส่งผลกระทบหรือก่อให้เกิดความเสียหายในการเข้าใช้งานระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของ กปภ. บุคคลที่ใช้งานอุปกรณ์ดังกล่าวจะต้องเป็นผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมดตามความเหมาะสม

เอกสารที่เกี่ยวข้อง

- ไม่มี -

หมวดที่ ๗
นโยบายการบริหารจัดการการรักษาความมั่นคงปลอดภัยในการติดต่อสื่อสาร
(Communications security policy)

เพื่อให้ กปภ. มีแนวปฏิบัติในการบริหารจัดการการรักษาความมั่นคงปลอดภัยในการติดต่อสื่อสาร โดยมีการแบ่งแยกเครือข่ายคอมพิวเตอร์ตามความสำคัญของระบบ และมีการเฝ้าระวังการใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์ของ กปภ. ให้มีความพร้อมใช้ได้อย่างต่อเนื่องอีกทั้งยังมีมาตรการควบคุมการถ่ายโอนข้อมูลระหว่างหน่วยงานเพื่อป้องกันข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการบริหารจัดการเครือข่ายคอมพิวเตอร์ (Computer network management guideline)
- ส่วนที่ ๒ แนวทางปฏิบัติการถ่ายโอนข้อมูลสารสนเทศ (Information transfer guideline)
- ส่วนที่ ๓ แนวทางปฏิบัติการแบ่งบันหรือเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber security information sharing)

ส่วนที่ ๑
แนวทางปฏิบัติการบริหารจัดการเครือข่ายคอมพิวเตอร์
(Computer network management guideline)

วัตถุประสงค์

- เพื่อบริหารจัดการเครือข่ายคอมพิวเตอร์ของ กปภ. ให้มีความมั่นคงปลอดภัย
- เพื่อเฝ้าระวังการใช้ทรัพยากรเครือข่ายคอมพิวเตอร์ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

ผู้ปฏิบัติ

- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. ผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องดำเนินการออกแบบเครือข่ายคอมพิวเตอร์โดยแบ่งแยกเครือข่ายคอมพิวเตอร์ออกเป็นกลุ่มๆ (Segregation in network) ตามลักษณะการใช้งานและความสำคัญของระบบสารสนเทศที่อาจส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร โดยให้ปฏิบัติตามแนวทางปฏิบัติการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์

๒. ผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องดำเนินการควบคุมการจัดเส้นทางและการรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ (Network routing and security control) โดยให้ปฏิบัติตามแนวทางปฏิบัติการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์

๓. ผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องมีการควบคุมการเชื่อมต่อเพื่อเข้าไปบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อจะต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบสารสนเทศและผู้ดูแลเครือข่ายคอมพิวเตอร์หรือผู้ที่มีส่วนเกี่ยวข้องเท่านั้น

๔. ผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องดำเนินการจัดทำรายการทะเบียนหมายเลข IP Address เพื่อใช้สำหรับระบุเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย หรืออุปกรณ์ต่อพ่วงอื่นๆ (Equipment Identification in network)

๕. ผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องจัดทำแผนผังการเชื่อมต่อเครือข่ายคอมพิวเตอร์ (Network Diagram) และต้องมีการปรับปรุงทบทวนให้เป็นปัจจุบัน

๖. ผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องมีการเฝ้าระวังเครือข่ายคอมพิวเตอร์ (Network monitor) เพื่อให้มั่นใจว่าเครือข่ายคอมพิวเตอร์ของ กปภ. สามารถให้บริการได้อย่างต่อเนื่อง

๗. ห้ามพนักงานที่มิได้มีส่วนเกี่ยวข้องกับการดูแลเครือข่ายคอมพิวเตอร์ติดตั้งระบบเครือข่ายอินเทอร์เน็ต (Internet), ระบบเครือข่ายไร้สาย (Wireless LAN), ระบบเครือข่ายเสมือน (VPN) และห้ามนำระบบเครือข่ายอื่นมาติดตั้งและเชื่อมต่อเข้ากับเครือข่ายคอมพิวเตอร์ของ กปภ.

๘. ห้ามตั้งโปรแกรมคอมพิวเตอร์ประเภทดักจับข้อมูล (Packet sniffing tools) หรือโปรแกรมประเภททดสอบเจาะระบบ (Penetration testing tools) ยกเว้นเครื่องของผู้ดูแลระบบสารสนเทศและผู้ดูแลเครือข่ายคอมพิวเตอร์ที่มีความจำเป็นต้องใช้สำหรับปฏิบัติงานโดยต้องได้รับอนุญาตจาก ผชด./ผอ.กปภ.ข.๑-๑๐ หรือผู้ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร

๙. หากมีการฝ่าฝืนข้อห้ามที่ ๗-๘ และก่อหรืออาจก่อให้เกิดความเสียหายแก่ กปภ. จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ใช้งานที่ฝ่าฝืนตามความเหมาะสม

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๒
แนวทางปฏิบัติการถ่ายโอนข้อมูลสารสนเทศ
(Information transfer guideline)

วัตถุประสงค์

- เพื่อป้องกันการเปิดเผยข้อมูลสารสนเทศที่เป็นความลับของ กปภ.

ผู้ปฏิบัติ

- เจ้าของข้อมูล

แนวทางการปฏิบัติ

๑. เอกสาร ซอฟต์แวร์ ไฟล์อิเล็กทรอนิกส์ และข้อมูลสารสนเทศที่อยู่ในรูปแบบอื่นๆ ที่เป็นความลับของ กปภ. ต้องไม่ถูกส่งต่อให้กับบุคคลหรือหน่วยงานภายนอกเพื่อวัตถุประสงค์อื่นใดนอกเหนือจากการทำงานหรือการดำเนินธุรกิจที่ได้รับอนุญาตหรือมอบหมายจากผู้บังคับบัญชา

๒. การรับ-ส่งข้อมูล เอกสาร ซอฟต์แวร์ หรือไฟล์อิเล็กทรอนิกส์ และข้อมูลสารสนเทศที่อยู่ในรูปแบบอื่นๆ ที่เป็นความลับของ กปภ. ต้องได้รับการเข้ารหัสลับ โดยปฏิบัติตามแนวทางปฏิบัติการบริหารจัดการการเข้ารหัสลับข้อมูล และต้องได้รับอนุมัติจากผู้บังคับบัญชาที่มีอำนาจอนุมัติอย่างเป็นลายลักษณ์อักษร

๓. ต้องลงนามในบันทึกข้อตกลงเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศ (NDA) ระหว่าง กปภ. กับบุคคลหรือหน่วยงานภายนอกก่อนการแลกเปลี่ยนเอกสาร ซอฟต์แวร์ ไฟล์อิเล็กทรอนิกส์ และข้อมูลสารสนเทศที่อยู่ในรูปแบบอื่นๆ ที่เป็นความลับของ กปภ. เพื่อป้องกันการเปิดเผยข้อมูลที่สำคัญของ กปภ.

เอกสารอ้างอิง

๑. บันทึกข้อตกลง เรื่อง การรักษาความปลอดภัยของข้อมูลสารสนเทศ (สำหรับบุคคลภายนอก) (IT-FM-NDA-๐๒)

ส่วนที่ ๓

แนวทางปฏิบัติการแบ่งบันหรือเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์

(Cyber security information sharing)

วัตถุประสงค์

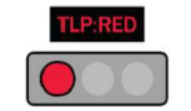
- เพื่อกำหนดข้อตกลงสำหรับการแบ่งปันหรือเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภายในและภายนอก กปภ. ได้อย่างถูกต้องตามมาตรฐานสากล

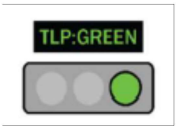
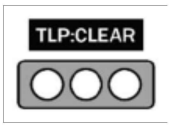
ผู้ปฏิบัติ

- ผู้ที่แบ่งปันข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์

แนวทางการปฏิบัติ

๑. การกำหนดข้อตกลงสำหรับการแบ่งปันหรือเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (Traffic Light Protocol: TLP) จะมีการแบ่งลำดับชั้นความลับหรือความละเอียดอ่อนของข้อมูล ซึ่งแบ่งตามประเภทของสี ๔ ประเภท ดังนี้

สี	รายละเอียด	การเผยแพร่/การส่งต่อ
สีแดง 	- เป็นข้อมูลที่ไม่สามารถเปิดเผยหรือเผยแพร่ได้อย่างจำกัด โดยกำหนด ให้เฉพาะผู้ที่มีสิทธิ์ได้รับข้อมูลทราบเท่านั้น ซึ่งข้อมูลดังกล่าวมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล หรือส่งผลกระทบต่อการดำเนินงาน ความเป็นส่วนตัว และชื่อเสียงขององค์กร หากข้อมูลดังกล่าวหลุดรั่วออกไป	- ผู้รับข้อมูลต้องไม่เผยแพร่หรือส่งต่อข้อมูลให้กับบุคคลใดๆ นอกเหนือจากที่ผู้ส่งข้อมูลได้ระบุไว้
สีเหลือง 	- เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ได้อย่างจำกัด โดยกำหนดให้เฉพาะองค์กร หน่วยงาน หรือกลุ่มบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลทราบเท่านั้น ซึ่งข้อมูลดังกล่าวถูกใช้สำหรับการแก้ไข หรือป้องกันภัยคุกคามทางไซเบอร์ แต่อาจมีผลกระทบต่อการดำเนินงาน ความเป็นส่วนตัว และชื่อเสียงขององค์กร หากข้อมูลดังกล่าวหลุดรั่วออกไป	- ผู้ได้รับข้อมูลสามารถเผยแพร่หรือส่งต่อข้อมูลให้กับองค์กร หน่วยงาน หรือกลุ่มบุคคลที่จำเป็นต้องรู้เท่านั้น (Need to know basis) เพื่อให้สามารถป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานตนเอง และต้องปฏิบัติตามข้อจำกัดที่ผู้ส่งได้ระบุไว้อย่างเคร่งครัด

สี	รายละเอียด	การเผยแพร่/การส่งต่อ
สีเขียว 	- เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ได้อย่างจำกัด โดยกำหนดให้เฉพาะหน่วยงานภายใน หรือระหว่างหน่วยงานที่ทำข้อตกลงร่วมกันทราบเท่านั้น ซึ่งข้อมูลดังกล่าวถูกใช้สำหรับสร้างความตระหนัก หรือการป้องกันภัยไซเบอร์	- ผู้ได้รับข้อมูลสามารถเผยแพร่ หรือส่งต่อข้อมูลให้กับหน่วยงานภายในหรือระหว่างหน่วยงานที่ทำข้อตกลงร่วมกันเท่านั้น
สีขาว/โปร่งใส 	- เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่สู่สาธารณะได้ ซึ่งข้อมูลดังกล่าวจะต้องไม่ส่งผลกระทบต่อ การดำเนินงาน ความเป็นส่วนตัว รวมถึงชื่อเสียงขององค์กร และบุคคล	- ผู้ได้รับข้อมูลสามารถเผยแพร่หรือส่งต่อข้อมูลให้กับสาธารณะได้ แต่ต้องอยู่ภายใต้หลักกฎหมายระหว่างประเทศและกฎหมายภายในประเทศที่เกี่ยวข้อง

๒. ช่องทางสำหรับการแบ่งปันหรือเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์

ช่องทางการแจ้งเตือน	รายละเอียด
๑. จดหมายอิเล็กทรอนิกส์	๑.๑. ควรกำหนดเครื่องหมาย (Label) สำหรับ TLP ไว้ในชื่อเรื่อง (Subject) และเนื้อหา (Body) ของ E-mail โดยใช้ตัวอักษรตัวใหญ่ เช่น TLP:RED, TLP:AMBER, TLP:GREEN, TLP:CLEAR เป็นต้น ๑.๒. ข้อมูลใน E-mail ประเภท TLP:RED และ TLP AMBER ต้องได้รับการเข้ารหัสแบบ PGP (Pretty Good Privacy) หรือการเข้ารหัสลับในรูปแบบอื่นๆที่มีความปลอดภัย เพื่อป้องกันข้อมูลที่เป็นความลับรั่วไหล
๒. ไฟล์เอกสาร	๒.๑. ควรกำหนดเครื่องหมาย (Label) สำหรับ TLP ไว้ใน Header โดยวางไว้ที่มุมขวาของเอกสาร และในส่วนของ Footer ให้วางไว้ที่จุดกึ่งกลางของเอกสาร 

ช่องทางการแจ้งเตือน	รายละเอียด
	 ๒.๒ ไฟล์ข้อมูลอิเล็กทรอนิกส์ ประเภท TLP:RED และ TLP AMBER ต้องได้รับการเข้ารหัสลับแบบ PGP (Pretty Good Privacy) หรือการเข้ารหัสลับในรูปแบบอื่นๆ ที่มีความปลอดภัย เพื่อป้องกันข้อมูลที่เป็นความลับรั่วไหล ๒.๓ ข้อมูลในรูปแบบของกระดาษ ประเภท TLP:RED, TLP AMBER และ TLP:GREEN จะต้องมีการป้องกันการเข้าถึง เช่น ใส่ซองปิดผนึกและต้องจัดเก็บในสภาพแวดล้อมที่มีการรักษาความปลอดภัย

เอกสารอ้างอิง

- ไม่มี -

หมวดที่ ๘
นโยบายการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ
(IT system acquisition and development policy)

เพื่อให้ กปภ. มีแบบแผน มาตรฐานในการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศและเว็บไซต์ให้มีความมั่นคงปลอดภัย โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศ (IT system acquisition and development guideline)
- ส่วนที่ ๒ แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเว็บไซต์ (Website security guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศ
(IT system acquisition and development policy)

วัตถุประสงค์

- เพื่อให้มั่นใจว่ากระบวนการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศของ กปภ. มีความมั่นคงปลอดภัย

ผู้ปฏิบัติ

- พนักงานหรือหน่วยงานที่มีส่วนเกี่ยวข้องในการจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศของ กปภ.

แนวทางการปฏิบัติ

๑. การจัดหาระบบ (System acquisition)

๑.๑. ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยโดยระบุลงในข้อกำหนด (TOR) ซึ่งมีรายละเอียดอย่างน้อย ดังนี้

๑.๑.๑. ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยที่ กปภ. กำหนด เช่น ในกรณีที่ผู้รับจ้างเข้าถึงพื้นที่สำคัญ ต้องดำเนินการตามหมวดที่ ๕ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security policy), หรือในกรณีที่ผู้รับจ้างเข้าถึงเครือข่ายและการเชื่อมต่อเครือข่าย ต้องดำเนินการตามหมวดที่ ๓ นโยบายการควบคุมการเข้าถึง (Access control policy) เป็นต้น

๑.๑.๒. ต้องลงนามในบันทึกข้อตกลง เรื่อง การรักษาความปลอดภัยของข้อมูลสารสนเทศ (Non-Disclosure Agreement : NDA) เพื่อป้องกันการเปิดเผยข้อมูลของ กปภ.

๑.๑.๓. ต้องกำหนดให้มีการปิดช่องโหว่ของระบบ (Hardening) เพื่อปกป้องให้ระบบมีความมั่นคงปลอดภัย

๑.๑.๔. ต้องรับทราบและยอมรับปฏิบัติตามนโยบาย มาตรการ ระเบียบวิธีปฏิบัติและคู่มือการปฏิบัติงาน ด้านการรักษาความมั่นคงปลอดภัยของ กปภ. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้องที่มีอยู่ในปัจจุบันหรือจะมีใช้ในอนาคต

๑.๒. ต้องกำหนดคุณสมบัติของผู้รับจ้างโดยระบุลงในข้อกำหนด (TOR) ซึ่งมีรายละเอียดอย่างน้อย ดังนี้

๑.๒.๑. คุณสมบัติตามที่กรมบัญชีกลาง หรือ กปภ. กำหนด

๑.๒.๒. มีประสบการณ์และมีความเชี่ยวชาญในเรื่องที่ว่าจ้าง

๑.๒.๓. มีใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศ (Certification) ที่ได้รับการยอมรับโดยทั่วไป

๑.๒.๔. มีผลงานการทำงานให้กับหน่วยงานราชการ รัฐวิสาหกิจ หรือ เอกชน ในงานที่ว่าจ้าง

๑.๓. การพิจารณาหลักเกณฑ์การจัดซื้อ-จัดจ้างหรือการใช้บริการ Cloud Service จากภายนอกองค์กร ในกรณีที่มีความจำเป็นในการจัดซื้อ-จัดจ้าง Cloud Service จากภายนอกองค์กร ผู้ร้องขอจะต้องมีการกำหนดในสัญญาการจ้างให้ครอบคลุมรายละเอียดความมั่นคงปลอดภัยของการจัดจ้าง โดยพิจารณาหัวข้อ ดังนี้

๑.๓.๑. การลักษณะการจัดจ้าง (ตัวอย่าง เช่น เช่าใช้หรือเช่าซื้อ เป็นต้น)

๑.๓.๒. การใช้บริการ (ยกตัวอย่างเช่น วัตถุประสงค์เพื่อนำไปจัดเก็บหรือประมวลผลข้อมูลของระบบสารสนเทศที่สำคัญหรือระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ)

๑.๓.๓. การบริหารจัดการบริการหรือความมั่นคงปลอดภัยของผู้ให้บริการ

๑.๓.๔. การยกเลิกบริการ ที่ควรระบุในสัญญาการจ้าง หรือเอกสารอื่น ๆ เช่น MOU

๒. การพัฒนาระบบเทคโนโลยีสารสนเทศ (IT system Development)

๒.๑. การรวบรวมความต้องการของระบบ (System requirement)

เก็บรวบรวมความต้องการของระบบจากผู้ที่เกี่ยวข้องทั้งหมดเพื่อให้ได้ความต้องการที่ครอบคลุมและสร้างความเข้าใจตรงกันระหว่างผู้ใช้งานและผู้พัฒนาระบบซึ่งอาจใช้วิธีการรวบรวมความต้องการที่หลากหลาย ดังนี้

๒.๑.๑. การสัมภาษณ์บุคคล (Personal interview)

๒.๑.๒ การวิเคราะห์เอกสาร (Document analysis)

๒.๑.๓. การเข้าไปดูลักษณะการทำงานจริง (Site survey)

๒.๒. การออกแบบระบบ (System Design)

การออกแบบระบบต้องมีการออกแบบฟังก์ชันและเงื่อนไขต่างๆ ด้านประสิทธิภาพที่ตรงตามความต้องการของผู้ใช้งานและหน่วยธุรกิจ (Business unit requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามที่ กปภ. กำหนด

๒.๓. การพัฒนาระบบ (System Development)

๒.๓.๑. มีการแบ่งแยกสภาพแวดล้อมของระบบสารสนเทศที่มีความสำคัญ โดยแยกสภาพแวดล้อมที่ใช้สำหรับการพัฒนาและการทดสอบ (Develop and Testing) ออกจากระบบที่ให้บริการจริง (Production) เพื่อลดผลกระทบที่อาจเกิดขึ้นจากการนำขึ้นระบบที่ให้บริการจริง

๒.๓.๒. ควบคุมการเข้าถึงเครื่องที่มีระบบที่ให้บริการจริง (Production) และเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (Non-production) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๓. มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชันของชุดคำสั่งที่ใช้ในการพัฒนาระบบ (Source code version control)

๒.๓.๔. มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือที่ใช้ในการพัฒนาระบบ (Development tools) และเครื่องมือแปลโปรแกรม (Compilers) ไว้บนระบบที่ให้บริการจริง

๒.๔. การทดสอบระบบ (System testing)

๒.๔.๑. ต้องมีการสอบทานชุดคำสั่งในการเขียนโปรแกรม (Source code review)

๒.๔.๒. ต้องมีการทดสอบฟังก์ชันและกระบวนการสอบทาน (Test case) ของระบบให้ครอบคลุมและตรงตามความต้องการของผู้ใช้งาน

๒.๔.๓. ต้องมีการทดสอบประสิทธิภาพ (Performance testing) เพื่อให้มั่นใจว่าระบบที่พัฒนามีประสิทธิภาพและสามารถรองรับการใช้งานจากผู้ใช้งานพร้อมๆ กันเป็นจำนวนมากได้

๒.๔.๔. ต้องมีการทำ Data masking เพื่อป้องกันการรั่วไหลของข้อมูลที่สำคัญที่นำไปใช้ในการทดสอบ

๒.๔.๕. ต้องมีการทดสอบการนำเข้าของข้อมูล (Input validation) รวมถึงตรวจสอบช่องโหว่หรือจุดอ่อนของระบบที่พัฒนาและดำเนินการปรับปรุงแก้ไขก่อนนำไปให้บริการบนระบบที่ใช้งานจริง

๒.๔.๖. มีการจัดทำคู่มือและจัดอบรมให้ผู้ใช้งานมีความเข้าใจฟังก์ชันการทำงานและการใช้งานระบบอย่างปลอดภัย

๒.๔.๗. มีการจัดทำคู่มือและจัดอบรมด้านเทคนิคให้ผู้ดูแลระบบให้สามารถใช้งานและแก้ไขเมื่อระบบเกิดปัญหาได้

๒.๕. การนำระบบขึ้นใช้งานจริง (System Deployment)

ต้องมีกระบวนการต่างๆ ในการนำระบบขึ้นใช้งานจริงอย่างน้อย ดังนี้

๒.๕.๑. การนำระบบขึ้นใช้งานจริงต้องมีการวางแผนการเปลี่ยนแปลงประเมินผลกระทบตามแนวทางปฏิบัติการบริหารจัดการการเปลี่ยนแปลงโดยต้องขออนุมัติจากผู้บังคับบัญชาที่รับผิดชอบก่อนดำเนินการเปลี่ยนแปลงเนื่องจากการเปลี่ยนแปลงดังกล่าวอาจเกิดความเสี่ยงหรือส่งผลกระทบต่อการทำงานของระบบได้

๒.๕.๒. ต้องมีการแจ้งให้ผู้ใช้งานหรือผู้ที่มีส่วนเกี่ยวข้องกับระบบทราบทุกครั้งก่อนดำเนินการเปลี่ยนแปลงใดๆ ที่ส่งผลกระทบต่อการใช้งานของระบบ

๒.๕.๓. มีการควบคุมเวอร์ชันของชุดคำสั่งและไลบรารี่ต้นฉบับของระบบที่พัฒนา (Version control) โดยต้องกำหนดสิทธิ์การเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

เอกสารอ้างอิง

๑. แนวทางปฏิบัติในการพัฒนาระบบงานสารสนเทศ ของสายงานเทคโนโลยีสารสนเทศ
๒. แบบฟอร์ม พัฒนาระบบงานใหม่ (IT-FM-DEV-๐๑)
๓. แบบฟอร์ม พัฒนาระบบงานใหม่ - กบข. (IT-FM-DEV-๐๑ – กบข.)
๔. แบบฟอร์ม เอกสารความต้องการผู้ใช้งาน (IT-FM-DEV-๐๒)
๕. แบบฟอร์ม ออกแบบระบบงาน (IT-FM-DEV-๐๓)
๖. แบบฟอร์ม ทดสอบโปรแกรม (IT-FM-DEV-๐๔)
๗. แบบฟอร์ม ขอใช้งาน User/แจ้งรับการ Transport/Deployระบบ/Upload Reporting เปลี่ยนแปลง database/เพิ่ม Role ให้ user (IT-FM-DEV-๐๕)
๘. แบบฟอร์ม ปรับปรุงเอกสารคู่มือ (IT-FM-DEV-๐๖)
๙. แบบฟอร์ม ส่งเอกสารยืนยัน (IT-FM-DEV-๐๗)
๑๐. แบบฟอร์ม คำขอเปลี่ยนแปลง - ระบบทั่วไป (IT-FM-DEV-๐๘ - ระบบทั่วไป)
๑๑. แบบฟอร์ม คำขอเปลี่ยนแปลง - OIS (IT-FM-DEV-๐๘ - OIS)
๑๒. แบบฟอร์ม ปรับปรุงโปรแกรม (IT-FM-DEV-๐๙)
๑๓. แบบฟอร์ม ปรับปรุงโปรแกรม – กบข. (IT-FM-DEV-๐๙ – กบข.)

ส่วนที่ ๒
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเว็บไซต์
(Website security guideline)

วัตถุประสงค์

- เพื่อให้การพัฒนาเว็บไซต์ของ กปภ. มีความมั่นคงปลอดภัยตามมาตรฐานสากล

ผู้ปฏิบัติ

- พนักงานหรือหน่วยงานที่มีส่วนเกี่ยวข้องในการพัฒนาเว็บไซต์ของ กปภ.

แนวทางการปฏิบัติ

๑. การพัฒนาเว็บไซต์ตั้งแต่กระบวนการการรวบรวมความต้องการของระบบ (System requirement) การออกแบบระบบ (System Design), การพัฒนาระบบ (System Development), การทดสอบระบบ (System test), การนำระบบขึ้นใช้งานจริง (System Deployment) ให้ปฏิบัติตามแนวทางปฏิบัติการจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศ

๒. การพัฒนาเว็บไซต์ให้มีความมั่นคงปลอดภัย (Secure Coding) ต้องมีวิธีการป้องกันและรับมือภัยคุกคามในรูปแบบต่างๆ อย่างน้อยครอบคลุมประเด็น ดังนี้
   ๒.๑. การป้องกันการโจมตีในรูปแบบ SQL Injection
   ๒.๒. การป้องกันการโจมตีในรูปแบบ Session Hijacking
   ๒.๓. การป้องกันการโจมตีในรูปแบบ Cross-Site Script
   ๒.๔. การป้องกันการโจมตีจากปัญหาข้อมูลลับรั่วไหล (Sensitive data exposure)

เอกสารอ้างอิง

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์
๒. มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ
๓. คู่มือ How to Secure Your Website ของสำนักงานส่งเสริมเทคโนโลยีสารสนเทศประเทศญี่ปุ่น

<u>หมายเหตุ</u>
สามารถดาวน์โหลดเอกสารอ้างอิง ๑-๓ ได้ที่ https://intranet.pwa.co.th/help

หมวดที่ ๙
นโยบายการบริหารจัดการผู้ให้บริการภายนอก
(Third party management policy)

เพื่อให้ กปภ. มีแนวทางป้องกันข้อมูลที่มีความสำคัญของ กปภ. รั่วไหลออกสู่ภายนอก และเป็นไปตามข้อตกลงเรื่องการเก็บรักษาความลับที่จัดทำไว้ระหว่าง กปภ. กับผู้ให้บริการภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก
  (Third party management guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก
(Third party management guideline)

วัตถุประสงค์

- เพื่อกำหนดข้อตกลงและป้องกันข้อมูลที่มีความสำคัญของ กปภ. รั่วไหลในระหว่างการปฏิบัติงานของบุคคลภายนอกหรือบริษัทที่เป็นคู่สัญญากับ กปภ.

ผู้ปฏิบัติ

- พนักงานของ กปภ. ที่เป็นผู้ประสานงานในโครงการ
- บุคคลภายนอก

แนวทางการปฏิบัติ

๑. บุคคลภายนอก หรือบริษัทที่เป็นคู่สัญญากับ กปภ. ต้องลงนามใน บันทึกข้อตกลงเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศ (NDA) เพื่อป้องกันการเปิดเผยข้อมูลของ กปภ.

๒. บุคคลภายนอก หรือบริษัทที่เป็นคู่สัญญากับ กปภ. ต้องรับทราบและปฏิบัติตามระเบียบ ข้อบังคับ และวิธีการปฏิบัติงานต่างๆ ของ กปภ. อย่างเคร่งครัด

๓. ระหว่างการปฏิบัติงานของบุคคลภายนอก หรือบริษัทที่เป็นคู่สัญญากับ กปภ. ต้องมีพนักงานของ กปภ. ที่เป็นผู้ประสานงานในโครงการคอยควบคุมการปฏิบัติงานทุกครั้ง

๔. หากบุคคลภายนอก หรือบริษัทที่เป็นคู่สัญญากับ กปภ. มีความจำเป็นต้องเข้าใช้งานระบบสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์ของ กปภ. ให้แจ้งความจำนงต่อพนักงานของ กปภ. ที่เป็นผู้ประสานงานในโครงการเพื่อดำเนินการขออนุมัติจากผู้บริหารที่มีอำนาจอนุมัติต่อไป

๕. กปภ. ขอสงวนสิทธิ์ในการตรวจสอบการทำงานของบุคคลภายนอก หรือบริษัทที่เป็นคู่สัญญากับ กปภ. รวมถึงการเพิกถอนสิทธิ์ต่างๆ ในการเข้าใช้งานระบบสารสนเทศ หรือระบบเครือข่ายคอมพิวเตอร์ของ กปภ. หากพบความผิดปกติโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

๖. การกระทำใดๆ ของบุคคลภายนอก หรือบริษัทที่เป็นคู่สัญญากับ กปภ. ที่ก่อให้เกิดความเสียหาย หรือละเมิดข้อตกลง หรือสัญญาต่างๆ ที่ได้ทำร่วมกับ กปภ. บุคคลภายนอก หรือบริษัทที่เป็นคู่สัญญากับ กปภ. ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด

เอกสารอ้างอิง

๑. บันทึกข้อตกลง เรื่อง การรักษาความปลอดภัยของข้อมูลสารสนเทศ (สำหรับบุคคลภายนอก) (IT-FM-NDA-๐๒)

หมวดที่ ๑๐
นโยบายการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ
(IT incident and problem management policy)

เพื่อให้ กปภ. มีแนวทางปฏิบัติในการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถจัดการแก้ไขปัญหาให้กลับสู่ในสภาพปกติได้อย่างรวดเร็วและสามารถหาสาเหตุของปัญหาเพื่อป้องกันการเกิดขึ้นซ้ำในอนาคต โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT incident management guideline)
- ส่วนที่ ๒ แนวทางปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT problem management guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ
(IT incident management guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อการทำงานของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้อย่างทันท่วงที

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- กองความมั่นคงปลอดภัยไซเบอร์

แนวทางการปฏิบัติ

๑. เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (Security Incident)

หมายถึง เหตุการณ์ใดๆ ที่เกิดขึ้นหรือมีความเกี่ยวข้องกับระบบสารสนเทศ เครือข่ายคอมพิวเตอร์ ระบบสาธารณูปโภคพื้นฐานด้านสารสนเทศ ที่ส่งผลกระทบต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) หรือส่งผลกระทบต่อการให้บริการด้านสารสนเทศในวงกว้าง ดังนี้

๑.๑. เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่**ไม่ได้เกิดจาก**ภัยคุกคามไซเบอร์

- ระบบ/อุปกรณ์ ที่เกี่ยวกับเทคโนโลยีสารสนเทศ (System/Hardware, Software/) ไม่สามารถให้บริการได้ตามปกติ
- ระบบ/อุปกรณ์ ที่เกี่ยวกับสาธารณูปโภคพื้นฐานด้านสารสนเทศ มีปัญหา เช่น ระบบไฟฟ้า ระบบปรับอากาศ ระบบอัคคีภัย เป็นต้น
- ความผิดพลาดจากการกระทำของมนุษย์
- เหตุการณ์จากภัยพิบัติหรือภัยธรรมชาติ
- การชุมนุมประท้วง/การก่อจลาจล
- การฝ่าฝืน ละเมิด และไม่ปฏิบัติตามกฎหมาย หรือระเบียบข้อบังคับขององค์กร
- อื่นๆ

๑.๒. เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่**เกิดจาก**ภัยคุกคามไซเบอร์

- โปรแกรมมุ่งร้าย (Malicious code) เช่น Virus Computer, Ransomware, Trojan, Worm, APT ฯลฯ เป็นต้น
- การเข้าถึงระบบสารสนเทศ ข้อมูล โดยไม่ได้รับอนุญาต (Unauthorized access) เช่น SSH Access from Suspicious IP, Inbound Communication With Blacklist IP Addressเป็นต้น
- การรบกวนและทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ (Denial of services)
- การหลอกลวงจากผู้ไม่ประสงค์ดี (Phishing) เช่น E-mail Phishing, Web Phishing เป็นต้น
- การเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement)
- การค้นหาข้อมูลบนเครือข่ายคอมพิวเตอร์เพื่อใช้ในการโจมตีระบบ (Reconnaissance)
- เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)
- การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
- การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
- การบุกรุกในระดับผู้ควบคุม (Root Level Intrusion)
- การดำเนินการที่ไม่เป็นไปตามมาตรฐานความมั่นคงปลอดภัยที่หน่วยงานกำหนด (Non Compliance Activity)
- อื่นๆ

๒. ระดับความรุนแรงของเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (Security Level)

ระดับความรุนแรงของเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ จะถูกใช้เป็นเกณฑ์ในการกำหนดวิธีการรับมือที่เหมาะสมสำหรับแต่ละเหตุการณ์ โดยได้กำหนดระดับความรุนแรงไว้ 5 ระดับ ดังนี้

ระดับความรุนแรง	รายละเอียด	ระดับความรุนแรงตาม พ.ร.บ. ไซเบอร์ฯ
Extreme (๕)	■ ระบบสารสนเทศหรือสาธารณูปโภคพื้นฐานด้านสารสนเทศเสียหายไม่สามารถให้บริการได้ ■ มีผลกระทบต่อการปฏิบัติงานของพนักงาน หรือการให้บริการประชาชนทั้งหมด หรือส่งผลกระทบต่อชีวิตของประชาชน หรือก่อให้เกิดความสูญเสียอย่างใหญ่หลวงในทางการเงิน ชื่อเสียง หรือทำให้สูญเสียโอกาสทางธุรกิจหรือลูกค้าอย่างถาวร	วิกฤติ
High (๔)	■ ระบบสารสนเทศหรือสาธารณูปโภคพื้นฐานด้านสารสนเทศเสียหายไม่สามารถให้บริการได้ ■ มีผลกระทบต่อการปฏิบัติงานของพนักงาน หรือการให้บริการประชาชนในวงกว้าง หรือก่อให้เกิดความสูญเสียอย่างใหญ่หลวงในทางการเงิน ชื่อเสียง หรือทำให้สูญเสียโอกาสทางธุรกิจหรือลูกค้าอย่างถาวร	ร้ายแรง
Medium (3)	■ ระบบสารสนเทศหรือสาธารณูปโภคพื้นฐานด้านสารสนเทศเสียหายส่งผลทำให้ประสิทธิภาพในการให้บริการลดลง ■ มีผลกระทบต่อการปฏิบัติงานของพนักงานตั้งแต่ 10 คนขึ้นไป และไม่ส่งผลกระทบต่อการให้บริการประชาชน	ไม่ร้ายแรง
Low (2)	■ ระบบสารสนเทศหรือสาธารณูปโภคพื้นฐานด้านสารสนเทศเสียหายส่งผลทำให้ประสิทธิภาพในการให้บริการลดลง ■ มีผลกระทบต่อการปฏิบัติงานของพนักงานไม่เกิน 10 คน และไม่ส่งผลกระทบต่อการให้บริการประชาชน	
Insignificant (1)	■ ระบบสารสนเทศหรือสาธารณูปโภคพื้นฐานด้านสารสนเทศเสียหายแต่ยังสามารถให้บริการได้ตามปกติ ■ ไม่มีผลกระทบต่อการปฏิบัติงานของพนักงานและการให้บริการประชาชน	

๓. กระบวนการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Security Incident Management Framework)

กระบวนการ	รายละเอียด
การเตรียมความพร้อม (Preparation)	ต้องกำหนดทีมรับมือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ พร้อมทั้งกำหนดหน้าที่ และความรับผิดชอบ เพื่อให้สามารถรับมือต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม
การระบุเหตุและการแจ้งเหตุ (Identification and Reporting)	จัดให้มีระบบหรือกระบวนการในการตรวจจับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศในแต่ละประเภท และสร้างกระบวนการและความตระหนักของพนักงานในการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ โดยพนักงาน รวมถึงบุคคลภายนอกทุกคนที่พบเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศหรือจุดอ่อนด้านความมั่นคงปลอดภัย (Security weakness) มีหน้าที่ต้องรายงานเหตุไปยังพนักงานที่เป็นผู้ติดต่อประสานงาน และ/หรือ พนักงานด้านเทคโนโลยีสารสนเทศของ กปภ. เพื่อทำการบันทึกเหตุ (Record the incident) ลงในแบบฟอร์ม บันทึกเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ และดำเนินการในขั้นต่อไป
การประเมินสถานการณ์ (Assessment)	เมื่อได้รับการแจ้งเหตุ พนักงานด้านเทคโนโลยีสารสนเทศ ต้องทำการระบุหมายเลขกำกับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (Incident No. เช่น ๐๒/๒๕๕๒) ประเมินสถานการณ์เบื้องต้น โดยวิเคราะห์ขอบเขต ประเภทของเหตุการณ์ ระดับความรุนแรง ผลกระทบที่เกิดขึ้นจากเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศนั้น เพื่อให้สามารถดำเนินการรับมือได้อย่างถูกต้องและส่งต่อไปยังทีมที่เกี่ยวข้องเพื่อดำเนินการขั้นต่อไป ทั้งนี้ เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่มีระดับความรุนแรง ๔ (High) ขึ้นไปต้องรายงานไปยังผู้บริหารระดับสูงของ กปภ. (CIO) ภายใน ๓๐ นาที และหากเป็นเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นจากภัยคุกคามไซเบอร์ให้รายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานกำกับดูแล เพื่อทราบผ่านคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. หรือผู้ที่ได้รับมอบหมาย และให้ดำเนินการตามแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ ของ กปภ. (Cyber Incident Response Plan) ที่ประกาศใช้งาน
การควบคุมเหตุ (Containment)	ให้ผู้ดูแลระบบสารสนเทศ, ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือผู้ที่เกี่ยวข้องดำเนินการควบคุมเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้น เพื่อจำกัดขอบเขตและผลกระทบต่อการดำเนินธุรกิจของ กปภ. ให้น้อยที่สุด และป้องกันไม่ให้มีการลุกลามหรือขยายวงไปยังจุดอื่นๆ โดยต้องมีการจัดเก็บรักษาหลักฐานของเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นเพื่อนำไปใช้วิเคราะห์หาสาเหตุที่แท้จริง

กระบวนการ	รายละเอียด
การกำจัดเหตุ (Eradication)	ให้ผู้ดูแลระบบสารสนเทศ ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือผู้ที่เกี่ยวข้องกับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ แก้ไขปัญหาให้ระบบสารสนเทศ เครือข่ายคอมพิวเตอร์ หรือระบบที่เกี่ยวกับสาธารณูปโภคพื้นฐานด้านสารสนเทศให้สามารถใช้งานได้ตามปกติ
การฟื้นฟู (Recovery)	หากไม่สามารถดำเนินการแก้ไขให้ระบบสารสนเทศ เครือข่ายคอมพิวเตอร์ หรือระบบที่เกี่ยวกับสาธารณูปโภคพื้นฐานด้านสารสนเทศ กลับมาใช้งานได้ตาม SLA ให้ดำเนินการกู้คืนให้ระบบเทคโนโลยีสารสนเทศกลับมาใช้งานได้ตามปกติ ตามแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) และแผนสำรองและกู้คืนระบบสารสนเทศ (DRP) ของ กปภ. ที่มีการประกาศใช้งาน

๔. ขั้นตอนการรับแจ้งและรายงาน

๔.๑. เมื่อได้รับการแจ้งเหตุ พนักงานด้านเทคโนโลยีสารสนเทศ ต้องทำการระบุหมายเลขกำกับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (Incident No. เช่น ๐๒/๒๕๕๒) ประเมินสถานการณ์เบื้องต้นโดยวิเคราะห์ขอบเขต ประเภทของเหตุการณ์ ระดับความรุนแรง ผลกระทบที่เกิดขึ้นจากเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศนั้น เพื่อให้สามารถดำเนินการรับมือได้อย่างถูกต้อง และส่งต่อไปยังทีมที่เกี่ยวข้องเพื่อดำเนินการขั้นต่อไป

๔.๒. ผู้ดูแลเครือข่ายคอมพิวเตอร์ ผู้ดูแลระบบสารสนเทศ ดำเนินการแก้ไขเพื่อให้ระบบกลับคืนสู่สภาวะปกติได้อย่างเร็วที่สุด

๔.๓. เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่มีระดับความรุนแรง ๔ (High) ขึ้นไปต้องรายงานไปยังผู้บริหารระดับสูงของ กปภ. (CIO) ภายใน ๓๐ นาที และหากเป็นเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นจากภัยคุกคามไซเบอร์ให้ผู้ดูแลระบบสารสนเทศและผู้ดูแลเครือข่ายคอมพิวเตอร์รวบรวมข้อมูลต่างๆ ที่เกิดขึ้นกับระบบ และแจ้งมาที่กองความมั่นคงปลอดภัยไซเบอร์เพื่อรายงานข้อมูลที่เกี่ยวข้องให้สอดคล้องตามแบบฟอร์มเอกสารแนบท้ายประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่องหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ..ศ. ๒๕๖๖

เอกสารอ้างอิง

๑. แบบฟอร์ม บันทึกเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT-FM-NDA-๐๕)

๒. แผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber incident response plan)

<u>หมายเหตุ</u>

สามารถดาวน์โหลดเอกสารอ้างอิง ๒ ได้ที่ https://cybersecurity.pwa.co.th

ส่วนที่ ๒
แนวทางปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ
(IT problem management guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. มีกระบวนการติดตามหาสาเหตุที่แท้จริงเพื่อป้องกันการเกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศซ้ำ

ผู้ปฏิบัติ

- ผู้ดูแลระบบสารสนเทศ
- ผู้ดูแลเครือข่ายคอมพิวเตอร์

แนวทางการปฏิบัติ

๑. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเครือข่ายคอมพิวเตอร์ต้องมีการนำเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident) ที่ยังไม่ทราบสาเหตุที่แท้จริง (Unknown root cause) หรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นซ้ำมาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง

๒. จัดให้มีระบบรับแจ้งปัญหาเกี่ยวกับเทคโนโลยีสารสนเทศ เพื่อให้มีการบันทึก การจัดลำดับความสำคัญ และการติดตามปัญหา (Ticket) เพื่อให้สามารถติดตามสถานะของการแก้ไขปัญหา

๓. จัดให้มีการบันทึกรายละเอียดการแก้ไขปัญหาเพื่อใช้เป็นแหล่งข้อมูลในการสืบค้นแนวทางการแก้ไขปัญหาได้ในภายหลังได้อย่างรวดเร็วและมีประสิทธิภาพ

เอกสารอ้างอิง

- ไม่มี -

หมวดที่ ๑๑
นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(IT contingency plan policy)

เพื่อให้มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจของ กปภ. สามารถดำเนินการต่อไปได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้ โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

ส่วนที่ ๑
แนวทางปฏิบัติการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้ กปภ. มีระบบสารสนเทศพร้อมใช้งานอย่างต่อเนื่องในภาวะวิกฤติหรือเกิดเหตุการณ์ฉุกเฉิน สามารถตอบสนองลูกค้าและความต้องการทางธุรกิจอย่างมีประสิทธิผล

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.
- หน่วยงานเจ้าของระบบสารสนเทศที่สำคัญของ กปภ.
- คณะกรรมการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของ กปภ.

แนวทางการปฏิบัติ

๑. ต้องแต่งตั้งคณะกรรมการโดยกำหนดให้มีหน้าที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่างๆ ที่เกี่ยวข้องร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น

๒. ต้องดำเนินการประเมินความเสี่ยง (Risk assessment) โดยระบุเหตุการณ์ความเสี่ยง ซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ ดังนี้

๒.๑. ระบุเหตุการณ์ความเสี่ยง (Risk identification) ที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ ความผิดพลาดของเจ้าหน้าที่ เป็นต้น

๒.๒. ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง

๒.๓. จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๓. ต้องวิเคราะห์ผลกระทบธุรกิจ (Business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบสารสนเทศที่มีผลต่อการดำเนินธุรกิจของ กปภ. รวมถึงผลกระทบจากการหยุดชะงักและความเชื่อมโยงของการดำเนินธุรกิจกับระบบสารสนเทศ โดยมีแนวทางการดำเนินการ ดังนี้

๓.๑. ระบุระบบสารสนเทศที่สำคัญของ กปภ. และทรัพยากรที่มีความเชื่อมโยงพึ่งพาระหว่างกัน (Dependency)

๓.๒. วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD)

๓.๓. กำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO)

๔. ต้องจัดลำดับความสำคัญของระบบงาน โดยคำนึงถึงทรัพยากร ระยะเวลาในการกู้คืนระบบ เป้าหมายของระบบงานและข้อมูลที่ควรกู้ได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้คืนระบบ ทั้งนี้ ต้องพิจารณาให้ระบบการชำระเงินหรือระบบที่มีผลกระทบกับระบบของ กปภ. เป็นวงกว้างเป็นระบบที่มีความสำคัญสูงสุด

๕. ต้องกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแนวทางจัดเตรียมทรัพยากรระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามการจัดลำดับความสาคัญของระบบงาน โดยพิจารณาอย่างน้อยครอบคลุม ดังนี้

๕.๑. เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ เช่น RTO, RPO เป็นต้น

๕.๒. ปัจจัยสำคัญที่สนับสนุนให้แผนเป็นไปตามกลยุทธ์ เช่น เทคโนโลยีในการสำรองและกู้คืนข้อมูล ความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง เป็นต้น เพื่อให้ กปภ. มีทิศทางในการพัฒนาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่กำหนดไว้

๕.๓. ทรัพยากรและงบประมาณ เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามแผนกลยุทธ์และกิจกรรมที่ต้องดำเนินการทั้งหมด

๖. แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมีการระบุกระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น โดยต้องระบุรายละเอียดครอบคลุมหัวข้ออย่างน้อย ดังนี้

๖.๑. ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่นๆ ที่เกี่ยวข้อง

๖.๒. ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบและผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผน

๖.๓. รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบเครือข่ายสื่อสาร เป็นต้น

๖.๔. ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การตอบสนองต่อเหตุการณ์ฉุกเฉินและแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ

๖.๕. ขั้นตอนในการดำเนินการกู้คืนระบบ ต้องระบุรายละเอียดอย่างชัดเจนและเพียงพอ เพื่อให้สามารถใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ ทั้งนี้ กปภ. ต้องจัดทำเอกสารหรือคู่มือประกอบการกู้คืนในแต่ละระบบ ในกรณีที่มีการปรับปรุง หรือเพิ่มเติมขั้นตอน

นอกเหนือจากที่ระบุในแผนขณะปฏิบัติงานจริง ต้องมีกระบวนการรายงานและขออนุมัติจากผู้บริหารตามที่กำหนดในโครงสร้างการบังคับบัญชา พร้อมทั้งนำ ขั้นตอนดังกล่าวมาปรับปรุงแผนให้เป็นปัจจุบัน

๖.๖. ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๖.๗. แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง

๗. ต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้อง

๗.๑. ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางสื่อสารที่ชัดเจนให้บุคลากรทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน

๗.๒. จัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ ๑ ครั้ง โดยอย่างน้อยควรครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงานและการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น

๘. การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๘.๑. จัดทำแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียดอย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ทั้งนี้แผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีในภาพรวมต้องได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

๘.๒. จัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศทั้งในระดับหน่วยงานและระดับองค์กรอย่างน้อยปีละ ๑ ครั้ง โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการลูกค้าหรือต่อ กปภ. ทั้งระบบ เช่น ระบบเงินฝาก ระบบการโอนและชำระเงินระหว่าง กปภ. เป็นต้น นอกจากนี้อาจพิจารณาการทดสอบระบบสำรองในลักษณะเสมือนจริง (DR live test) เพื่อให้มั่นใจว่าระบบสำรองสามารถรองรับให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง

๘.๓. กรณีระบบงานมีการเชื่อมโยงเครือข่ายสื่อสารหรือใช้บริการจากหน่วยงานภายนอก กปภ. ต้องมีการทดสอบแผนฉุกเฉินร่วมกับหน่วยงานภายนอกที่เกี่ยวข้องด้วย เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศของ กปภ. มีความพร้อมใช้งานร่วมกับระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

๘.๔. รายงานผลการทดสอบต่อคณะกรรมการของ กปภ. โดยมีรายละเอียดอย่างน้อยครอบคลุมวัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข

๘.๕. กปภ. ควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน

๘.๖. กปภ. อาจจัดให้มีการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอกหรือภายในที่มีความเป็นอิสระ เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่างๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง

เอกสารอ้างอิง

- ไม่มี -

หมวดที่ ๑๒
นโยบายการปฏิบัติตามข้อกำหนด
(Compliance policy)

เพื่อให้ กปภ. มีการควบคุมการปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้สอดคล้องตามกฎหมาย ระเบียบข้อบังคับของ กปภ. โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการปฏิบัติตามข้อกำหนด
  (Compliance guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการปฏิบัติตามข้อกำหนด
(Compliance guideline)

วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และควบคุมการปฏิบัติงานของพนักงานให้เป็นไปอย่างถูกต้องไม่ก่อให้เกิดความเสียหายต่อ กปภ. และปฏิบัติตามกฎหมาย หรือ ระเบียบข้อบังคับอื่นๆ ที่เกี่ยวข้อง

ผู้ปฏิบัติ

- ผู้บริหาร พนักงาน และลูกจ้างของ กปภ.

แนวทางการปฏิบัติ

๑. การระบุกฎหมายที่บังคับใช้และข้อกำหนดทางสัญญา (Identification of applicable legislation and contractual requirement)

๑.๑. ผู้บริหาร พนักงาน และลูกจ้างของ กปภ. ต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เช่น

๑.๑.๑. พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ประกาศใช้งาน

๑.๑.๒. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ที่ประกาศใช้งาน

๑.๑.๓. พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑.๑.๔. พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ที่ประกาศใช้งาน

๑.๑.๕. พ.ร.บ. ลิขสิทธิ์ที่ประกาศใช้งาน

๑.๑.๖. นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ กปภ.

๑.๑.๗. ประกาศ กปภ. เรื่องนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

๑.๑.๘ ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์

๑.๒. สิทธิและทรัพย์สินทางปัญญา (Intellectual property rights)

ผู้บริหารและพนักงานของ กปภ. ต้องใช้งานซอฟต์แวร์ที่ถูกต้องตามกฎหมาย ในกรณีที่มีความจำเป็นต้องใช้งานซอฟต์แวร์อื่นนอกจากที่ กปภ. กำหนด และยังไม่มี License ให้ดำเนินการ ดังนี้

๑.๒.๑. ประสานงานกับหน่วยงานที่รับผิดชอบในการดูแลเรื่องซอฟต์แวร์ของ กปภ. เพื่อจัดหา License ที่ถูกต้องตามกฎหมาย

๑.๒.๒. ในกรณีที่ไม่อาจดำเนินการตามข้อ ๑.๒.๑ ให้ดำเนินการลบซอฟต์แวร์ดังกล่าวออกจากเครื่องคอมพิวเตอร์โดยเร็ว

๑.๒.๓. หากมีการละเมิดลิขสิทธิ์ของซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของ กปภ. พนักงานผู้นั้นต้องเป็นผู้รับผิดชอบต่อการละเมิดลิขสิทธิ์ดังกล่าว

๑.๓. การป้องกันข้อมูล (Protection of record)

ต้องมีการป้องกันมิให้ข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับของ กปภ. รั่วไหลหรือถูกแก้ไขเปลี่ยนแปลง

๑.๔. การคุ้มครองข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

การเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลให้ถือปฏิบัติตามประกาศ กปภ. เรื่อง นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

๒. การทบทวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information security reviews)

กำหนดให้มีการทบทวนนโยบายและขั้นตอนแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงตามบริบทขององค์กร

๓. การกำกับ ดูแลการปฏิบัติงานให้เป็นไปตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ กปภ. (Regulation of Information security)

๓.๑. ให้ผู้บังคับบัญชาเป็นผู้กำกับดูแลผู้ใต้บังคับบัญชาในการปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ กปภ. อย่างเคร่งครัด

๓.๒. หากพนักงานจงใจฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ กปภ. โดยการกระทำนั้นเป็นเหตุที่ทำให้เกิดความเสียหายต่อ กปภ. หรือบุคคลหนึ่งบุคคลใด กปภ. จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสมต่อไป

เอกสารอ้างอิง

๑. แบบฟอร์มขอใช้งานซอฟต์แวร์ (IT-FM-SW-๐๑)

หมวดที่ ๑๓
นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT risk management policy)

เพื่อให้ กปภ. มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจส่งผลกระทบต่อการทำงานของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT risk management guideline)

วัตถุประสงค์

- เพื่อให้ กปภ. การกำหนดโครงสร้างและบทบาทหน้าที่ของผู้มีส่วนเกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านภัยคุกคามไซเบอร์ และความเสี่ยงอื่นๆ ที่เกิดขึ้นจากปัจจัยภายในและภายนอกที่อาจส่งผลกระทบต่อการดำเนินธุรกิจของ กปภ.
- เพื่อให้มั่นใจได้ว่าความเสี่ยงที่พบมีการดำเนินการแก้ไข และควบคุมด้วยวิธีการที่เหมาะสม
- เพื่อให้ผู้บริหารรับทราบความเสี่ยงที่มีอยู่ และตัดสินใจดำเนินการกับความเสี่ยงเหล่านั้นได้อย่างเหมาะสม

ผู้ปฏิบัติ

- ผู้บริหาร พนักงานที่ได้รับมอบหมายหรือมีส่วนเกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset owner)
- เจ้าของความเสี่ยง (Risk owner)
- กองความมั่นคงปลอดภัยไซเบอร์

แนวทางการปฏิบัติ

๑. โครงสร้างและบทบาทหน้าที่
ต้องมีการกำหนดโครงสร้างและบทบาทหน้าที่ของผู้มีส่วนเกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๒. การกำหนดรายละเอียดข้อมูลเพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Areas)
เจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset owner) และเจ้าของความเสี่ยง (Risk owner) จะต้องกำหนด IT Risk Areas เพื่อทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยพิจารณาจากหัวข้อดังต่อไปนี้

๒.๑. การเปลี่ยนแปลงภายในองค์กร

๒.๒. การเปลี่ยนแปลงวัตถุประสงค์ หรือกระบวนการทางธุรกิจ

๒.๓. การเปลี่ยนแปลงเทคโนโลยี หรือมีการนำเทคโนโลยีใหม่ เข้ามาใช้งาน

๒.๔. ภัยคุกคามที่เกิดขึ้น หรือแนวโน้มภัยคุกคามที่คาดว่าจะเกิด

๒.๕. ภัยที่เกิดจากช่องโหว่ต่างๆ

๓. ประเภทและกลุ่มของทรัพย์สินด้านเทคโนโลยีสารสนเทศที่จะนำมาประเมินความเสี่ยง

๓.๑ ประเภทของทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Type of asset)

ลำดับ	ทรัพย์สินด้านเทคโนโลยีสารสนเทศ
๑	ฮาร์ดแวร์ (Hardware)
๒	ซอฟต์แวร์ (Software)
๓	ข้อมูล (Information/Data)
๔	บุคลากร (People)
๕	บริการ (Service)

๔. การประเมินความเสี่ยง (Risk assessment)

๔.๑. การระบุความเสี่ยง (Risk identification)

เจ้าของทรัพย์สินฯ และเจ้าของความเสี่ยงจะต้องระบุเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยคุกคามไซเบอร์ รวมถึงเหตุการณ์ความเสี่ยงอื่นๆ จากปัจจัยภายในและภายนอกที่เป็นไปได้ทั้งหมดที่อาจส่งผลกระทบต่อการดำเนินธุรกิจของ กปภ.

เหตุการณ์ความเสี่ยง (IT Risk Event) = ภัยคุกคาม (Threat) x ช่องโหว่ (Vulnerability)

๔.๒. การประเมินค่าความเสี่ยง (Risk analysis and evaluation)

เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีต่อ กปภ. ว่าจะก่อให้เกิดความเสี่ยงในระดับใด ดังนี้

๔.๒.๑. กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาส (Likelihood) และผลกระทบ (Impact)

๔.๒.๑.๑. เจ้าของทรัพย์สินฯ และเจ้าของความเสี่ยง ต้องดำเนินการประเมินโอกาสที่ภัยคุกคามจะสามารถเข้ามากระทำความ เสียหายแก่ทรัพย์สินผ่านช่องโหว่ที่มีอยู่ตามตาราง ดังต่อไปนี้

โอกาสเกิด (Likelihood)	รายละเอียด (Description)
Almost Certain (5)	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้สูงมาก อาจเกิดขึ้นได้ทุกสัปดาห์หรือบ่อยกว่า
Likely (4)	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้สูง อาจเกิดขึ้นได้ประมาณเดือนละครั้ง
Possible (3)	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้ปานกลาง อาจเกิดขึ้นได้ประมาณปีละครั้ง
Unlikely (2)	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้ต่ำ ในรอบ 2-3 ปี อาจเกิดขึ้น 1-2 ครั้ง
Rare (1)	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้ต่ำมาก ในรอบ 4-5 ปี อาจเกิดขึ้นได้สักครั้ง หรือแทบเป็นไปไม่ได้ที่จะเกิดขึ้น

๔.๒.๑.๒. เจ้าของทรัพย์สินฯ และเจ้าของความเสี่ยง ต้องดำเนินการทบทวนและประเมินผลกระทบ (Impact) ของภัยคุกคามกลุ่มของทรัพย์สิน (Group Assets Value) โดยพิจารณาถึงเหตุการณ์ความเสี่ยงว่ามีผลกระทบต่อความสูญเสีย C,I,A ในด้านใดและพิจารณาถึง มาตรการควบคุม (Existing Control) และช่องโหว่ที่มีอยู่ โดยจะแบ่งผลกระทบจะแบ่งออกเป็น ๕ ระดับ ตามตาราง ดังนี้

Asset Value	ผลกระทบหากสูญเสีย C, I, A ไป				
	ด้านการเงิน *	ด้านผลกระทบต่อชื่อเสียงขององค์กร	ผลกระทบต่อร่างกาย อนามัย หรือชีวิตผู้ใช้บริการ **	ผลกระทบอื่น ๆ ต่อผู้ใช้บริการ **	ผลกระทบต่อรัฐ
Very High (๕)	ความเสียหายเป็นจำนวนเงินตั้งแต่ ๑,๐๐๐,๐๐๐ บาท ขึ้นไป	มีข่าวเชิงลบในสื่อระดับประเทศ เช่น หนังสือพิมพ์ วิทยุ โทรทัศน์หรือสื่อต่างประเทศ มากกว่า ๒ วัน ติดต่อกันขึ้นไป	มีผู้ใช้บริการเสียชีวิตตั้งแต่ ๑ คน ขึ้นไป	ขอบเขตระบบงาน : มีผู้ใช้บริการได้รับผลกระทบเกินกว่า ๑๐๐,๐๐๐ คน ขอบเขต Infrastructure : ระบบในขอบเขตไม่สามารถให้บริการทั้งหมดได้ สามารถให้บริการได้ทั้งหมด และระบบงานสำคัญไม่สามารถให้บริการได้ทั้งหมด ต้องใช้หน่วยงานภายนอกดำเนินการแก้ไข	มีผลกระทบต่อความมั่นคงของรัฐ หรือส่งผลกระทบต่อกฎหมายของประเทศไทย (พ.ร.บ. ไซเบอร์, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล, พ.ร.บ. กระทำผิดทางคอมพิวเตอร์)
High (๔)	ความเสียหายเป็นจำนวนเงินน้อยกว่า ๑,๐๐๐,๐๐๐ บาท	มีข่าวเชิงลบในสื่อระดับประเทศ เช่น หนังสือพิมพ์ วิทยุ โทรทัศน์ หรือสื่อต่างประเทศ ๑-๒ วัน	มีผู้ใช้บริการได้รับผลกระทบต่อร่างกาย หรืออนามัยตั้งแต่ ๑,๐๐๐ คน แต่ไม่มีผู้เสียชีวิต	ขอบเขตระบบงาน : ผู้ใช้บริการได้รับผลกระทบเกินกว่า ๕๐,๐๐๐ คน แต่ไม่เกิน ๑๐๐,๐๐๐ คน ขอบเขต Infrastructure : ระบบโครงสร้างพื้นฐานล้มเหลวไม่สามารถให้บริการได้บางส่วน และระบบงานสำคัญไม่สามารถให้บริการบางส่วน ต้องใช้หน่วยงานภายนอกดำเนินการแก้ไข	ส่งผลกระทบต่อกฎ ระเบียบ ข้อบังคับ คำสั่งการของหน่วยงานโครงการสร้างพื้นฐานที่กำกับดูแล
Medium (๓)	ความเสียหายเป็นจำนวนเงินน้อยกว่า ๕๐๐,๐๐๐ บาท	มีข้อร้องเรียนผ่านช่องทางการร้องเรียนมากกว่า ๒๐ ครั้ง : ผู้ใช้บริการ ๑,๐๐๐ ราย	มีผู้ใช้บริการได้รับผลกระทบต่อร่างกาย หรืออนามัยตั้งแต่ ๕๐๐ คน แต่ไม่เกิน ๑,๐๐๐ คน	ขอบเขตระบบงาน : ผู้ใช้บริการได้รับผลกระทบเกินกว่า ๑๐,๐๐๐ คน แต่ไม่เกิน ๕๐,๐๐๐ คน ขอบเขต Infrastructure : ระบบโครงสร้างพื้นฐานล้มเหลวไม่สามารถให้บริการได้บางส่วน ไม่กระทบกับระบบงาน อาจจะต้องใช้หน่วยงานอื่นในดำเนินการแก้ไข	ส่งผลกระทบต่อกฎ ระเบียบ ข้อบังคับ คำสั่งการขององค์กร

Asset Value	ผลกระทบหากสูญเสีย C, I, A ไป				
	ด้านการเงิน *	ด้านผลกระทบต่อชื่อเสียงขององค์กร	ผลกระทบต่อร่างกาย อนามัย หรือชีวิตผู้ใช้บริการ **	ผลกระทบอื่น ๆ ต่อผู้ใช้บริการ **	ผลกระทบต่อรัฐ
Low (๒)	ความเสียหายเป็นจำนวนเงินน้อยกว่า ๒๐๐,๐๐๐ บาท	มีข้อร้องเรียนผ่านช่องทางการร้องเรียนมากกว่า ๑๐-๒๐ ครั้ง : ผู้ใช้บริการ ๑,๐๐๐ ราย	มีผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ ๑ คน แต่ไม่เกิน ๕๐๐ คน	ขอบเขตระบบงาน : ผู้ใช้บริการได้รับผลกระทบเกินกว่า ๑,๐๐๐ คน แต่ไม่เกิน ๑๐,๐๐๐ คน ขอบเขต Infrastructure : ระบบโครงสร้างพื้นฐานไม่สามารถให้บริการได้เลยน้อย ไม่กระทบกับระบบการให้บริการระบบงาน หน่วยงานภายในดำเนินการแก้ไข	ส่งผลกระทบต่อกฎ ระเบียบ ข้อบังคับ คำสั่งการของหน่วยงาน
Very Low (๑)	ความเสียหายเป็นจำนวนเงินน้อยกว่า ๑๐๐,๐๐๐ บาท	มีข้อร้องเรียนผ่านช่องทางการร้องเรียน ไม่เกิน ๑๐ ครั้ง : ผู้ใช้บริการ ๑,๐๐๐ ราย	ไม่มีผู้ใช้บริการได้รับผลกระทบต่อชีวิตร่างกายหรืออนามัย	ขอบเขตระบบงาน : ผู้ใช้บริการได้รับผลกระทบไม่เกิน ๑,๐๐๐ คน หรือผู้ใช้บริการไม่ได้รับผลกระทบ ขอบเขต Infrastructure : ระบบโครงสร้างพื้นฐานไม่เสถียรภาพเกิดปัญหาเล็กน้อย ไม่กระทบกับระบบการให้บริการระบบงาน หน่วยงานภายในดำเนินการแก้ไข	ไม่มีผลกระทบต่อความมั่นคงของรัฐ และไม่มีผลต่อกฎ ระเบียบ ข้อบังคับ คำสั่ง หรือกฎหมาย

๔.๒.๒. กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

ระดับความเสี่ยง		กิจกรรมที่ต้องกระทำ
Extreme (สูงมาก)	25	ความเสี่ยงในระดับสูงมาก ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง หรือดำเนินการภายใน 1 สัปดาห์
High (สูง)	15-24	ความเสี่ยงในระดับสูง ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง หรือดำเนินการภายใน 2 สัปดาห์
Medium (ปานกลาง)	8-14	ความเสี่ยงในระดับปานกลาง • องค์กรยอมรับได้โดยต้องมีมาตรการควบคุม (Existing Control) ปัจจุบัน • ในกรณีไม่มีมาตรการควบคุม (Existing Control) องค์กรไม่สามารถยอมรับได้ ต้องพิจารณาแก้ไขความเสี่ยง หรือดำเนินการภายใน 3 เดือน
Low (ต่ำ)	1-7	ความเสี่ยงระดับต่ำ สามารถยอมรับได้โดยไม่ต้องดำเนินการใด ๆ เพิ่มเติม

๔.๒.๓. กำหนดระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงของกลุ่มทรัพย์สินด้านเทคโนโลยีสารสนเทศ

Impact		Likelihood				
		Rare	Unlikely	Possible	Likely	Almost Certain
		1	2	3	4	5
Very High	5	Low (5)	Medium (10)	High (15)	High (20)	Extreme (25)
High	4	Low (4)	Medium (8)	Medium (12)	High (16)	High (20)
Medium	3	Low (3)	Low (6)	Medium (9)	Medium (12)	High (15)
Low	2	Low (2)	Low (4)	Low (6)	Medium (8)	Medium (10)
Very Low	1	Low (1)	Low (2)	Low (3)	Low (4)	Low (5)
Low 1 – 7 Medium 8 – 14 High 15 – 24 Extreme 25						

๕. การจัดการความเสี่ยง (Risk treatment)

๕.๑. กำหนดแนวทางในการจัดการและควบคุมและป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือกแนวทางในการจัดการและควบคุมความเสี่ยงซึ่งควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสม ดังนี้

๕.๑.๑. การลดระดับความเสี่ยง (Risk reduce)

๕.๑.๒. การโอนความเสี่ยง (Risk transfer)

๕.๑.๓. การหลีกเลี่ยงความเสี่ยง (Risk avoid)

๕.๑.๔. การยอมรับความเสี่ยง (Risk accept)

๕.๒. ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ และระยะเวลาที่ใช้ในการดำเนินการ

๕.๓. ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (Residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้และเสนออนุมัติความเสี่ยงที่เหลืออยู่ (Actual Residual Risk) ต่อผู้บังคับบัญชาที่กำกับดูแล พร้อมทั้งรายงานการระดับความเสี่ยง ต่อผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายอย่างน้อยปีละ ๑ ครั้ง

๕.๔. จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญในการดำเนินการ

๕.๕. นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๕.๖. ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และควรมีการจัดทำตัวชี้วัดให้สอดคล้องกับความสำคัญของงานแต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

๖. การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

๖.๑. ติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

๖.๒. ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานการณ์ดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น ในกรณีที่แผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่สามารถดำเนินการได้ตามรอบระยะเวลาที่กำหนด โดยระดับค่าความเสี่ยงที่เหลืออยู่ (Residual risk) อยู่ในระดับดังต่อไปนี้

- ระดับสีส้มหรือสีแดง ผู้รับผิดชอบต้องดำเนินการแจ้งให้ กองความมั่นคงปลอดภัยไซเบอร์เพื่อรวบรวมและแจ้งให้ต่อผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมาย เพื่อรับทราบและให้คำแนะนำสำหรับการบริหารจัดการความเสี่ยง
- ระดับสีเหลือง ผู้รับผิดชอบแจ้งต่อผู้บังคับบัญชาที่กำกับดูแลเพื่อรับทราบและให้คำแนะนำสำหรับการบริหารจัดการความเสี่ยง
- ระดับสีเขียว ผู้รับผิดชอบแจ้งต่อผู้บังคับบัญชาที่กำกับดูแลเพื่อรับทราบ

๖.๓. ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับ กปภ.

๖.๔. รายงานความคืบหน้าของแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามรอบที่กำหนด

๗. การรายงานความเสี่ยง (Risk report)

๗.๑. ต้องมีการนำเสนอผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศพร้อมทั้งรายงานผลการประเมินและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเชื่อมโยงกับความเสี่ยงในระดับองค์กรต่อผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายอย่างน้อยปีละ ๑ ครั้ง โดยครอบคลุมประเด็น ดังนี้

๗.๑.๑. รายงานสถานะ ผลลัพธ์การดำเนินงาน และความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๗.๑.๒. รายงานผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงระดับองค์กร

๗.๑.๓. ในกรณีเป็นการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องจัดส่งผลสรุปรายงานการบริหารความเสี่ยงต่อ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ

๗.๒. ต้องจัดให้มีการทบทวนกระบวนการในการบริหารความเสี่ยงและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

เอกสารอ้างอิง

- ไม่มี -

หมวดที่ ๑๔
นโยบายการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ
(Information security audit policy)

เพื่อให้ กปภ. มีกระบวนการตรวจสอบการดำเนินงานตามนโยบายและขั้นตอนแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. และมีมาตรการในการคัดเลือกผู้ตรวจประเมินได้อย่างมีประสิทธิภาพ โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ
  (Information Security Audit guideline)

ส่วนที่ ๑
แนวทางปฏิบัติการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ
(Information security audit guideline)

วัตถุประสงค์

- เพื่อให้มีการวางแผน กำหนดหน้าที่ในการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศได้อย่างมีประสิทธิภาพ
- เพื่อให้มีแนวทางในการคัดเลือกผู้ตรวจประเมินภายนอก

ผู้ปฏิบัติ

- สายงาน ผชด. หรือหน่วยงานที่ได้รับมอบหมาย
- ผู้บริหารระดับสูง (ผชด./ผอ.กปภ.ข.๑-๑๐)
- หน่วยงานผู้ตรวจประเมิน
- หน่วยงานผู้รับการตรวจประเมิน

แนวทางการปฏิบัติ

๑. การจัดทำแผน ขอบเขต และกำหนดเกณฑ์ของการตรวจประเมิน

๑.๑. หน่วยงานผู้ตรวจประเมินต้องจัดทำแผน ขอบเขต และเกณฑ์การตรวจประเมินประจำปีโดยขอบเขตการตรวจประเมินขึ้นอยู่กับวัตถุประสงค์ในการเข้าตรวจประเมินแต่ละครั้ง ซึ่งหน่วยงานผู้ตรวจประเมินจะดำเนินการแจ้งก่อนเข้าตรวจประเมิน เช่น ขอบเขตการตรวจประเมินระบบบริหารจัดการตามมาตรฐานสากล ขอบเขตการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ขอบเขตการตรวจประเมินการปฏิบัติตามกฎหมายหรือระเบียบของ กปภ. เป็นต้น

๑.๒. ต้องจัดให้มีการตรวจประเมินภายใต้ขอบเขตที่กำหนดอย่างน้อยปีละ ๑ ครั้ง ซึ่งการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะต้องมีขอบเขตการตรวจประเมิน ดังนี้

๑.๒.๑. กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

๑.๒.๒. ระบบสารสนเทศของ กปภ. ที่ให้บริการที่สำคัญของ กปภ. ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ตามผลการวิเคราะห์ BIA ในข้อ ๑.๒.๑

๑.๒.๓. การปฏิบัติตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ และประมวลแนวทางปฏิบัติ

๒. การรายงานผลการตรวจประเมินและคุณสมบัติของผู้ตรวจประเมิน

๒.๑. หน่วยงานผู้ตรวจประเมินต้องสรุปผลการตรวจประเมินและออกรายงานประเด็นการตรวจประเมินที่ไม่เป็นไปตามข้อกำหนด (ถ้ามี) ให้หน่วยงานผู้รับการตรวจประเมินทราบและนำไปดำเนินการแก้ไข

๒.๒. หน่วยงานผู้รับการตรวจประเมินต้องดำเนินการแก้ไขประเด็นตรวจสอบและรายงานผลการแก้ไขให้สายงานรับทราบ

๒.๓. ในกรณีที่เป็นการตรวจประเมินในขอบเขตการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. จัดส่งผลสรุปรายงานการดำเนินการของ กปภ. ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๓๐ วันนับตั้งแต่วันที่ดำเนินการแล้วเสร็จ โดยผู้ตรวจประเมินต้องมีคุณสมบัติ ดังนี้

๒.๓.๑. ต้องเป็นผู้ที่มีความรู้ความสามารถและประสบการณ์โดยผ่านการอบรมหลักสูตรการตรวจประเมินด้านเทคโนโลยีสารสนเทศ (IT Audit)

๒.๓.๒. ต้องได้รับใบรับรอง (Certification) ในระดับสากล เช่น ISMS Lead Auditor (ISO๒๗๐๐๑) หรือ CISA หรือ CISM เป็นต้น

๒.๓.๓. ต้องเป็นหน่วยงานอิสระที่ไม่มีความเกี่ยวข้องกับหน่วยงานผู้รับตรวจประเมิน

๒.๓.๔. ต้องมีความเป็นกลางและมีความเที่ยงธรรม

๒.๔. ในกรณีที่การตรวจสอบพบความไม่สอดคล้องตามข้อ ๑.๒ ให้หน่วยงานผู้รับการตรวจประเมินส่งข้อมูลแจ้งต่อคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. โดยมีรายละเอียด ดังนี้

๒.๔.๑. แผนการดำเนินการแก้ไข (Corrective Action Plan) เพื่อจัดการกับความไม่สอดคล้อง

๒.๔.๒. กำหนดระยะเวลาสำหรับการแก้ไขความไม่สอดคล้องดังกล่าวเสนอต่อคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลเพื่ออนุมัติและขอความเห็นชอบในการแก้ไขปัญหา การจัดการการแก้ไข ผ่านคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. หรือผู้ประสานงานที่ได้รับมอบหมาย

เอกสารอ้างอิง

- ไม่มี -

หมวดที่ ๑๕
นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber security policy)

เพื่อให้ กปภ. มีกระบวนการในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจสร้างความเสียหายต่อการดำเนินธุรกิจของ กปภ. โดยมีแนวทางปฏิบัติ ดังนี้

- ส่วนที่ ๑ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber security Framework)
- ส่วนที่ ๒ มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ
- ส่วนที่ ๓ มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ
- ส่วนที่ ๔ แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑
แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber security guideline)

วัตถุประสงค์

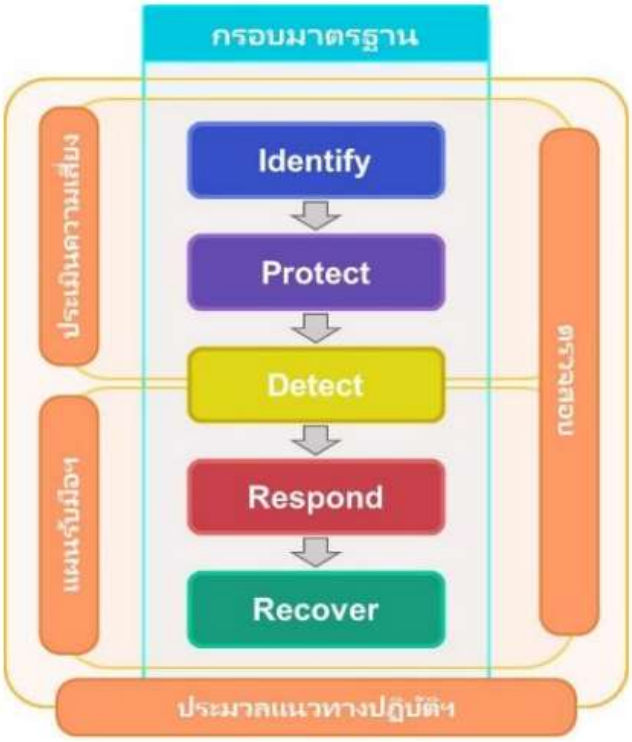
- เพื่อให้มีการบูรณาการเกี่ยวกับการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ กปภ. ให้สอดคล้องตามที่กฎหมายกำหนด
- เพื่อสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- เพื่อสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
- เพื่อประสานและให้ความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศในการการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น เข้าร่วมซักซ้อมการรับมือภัยคุกคามทางไซเบอร์ที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) กำหนด
- เพื่อสนับสนุนการวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- เพื่อพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจัดให้มีการอบรมสร้างความรู้และความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- เพื่อทบทวนปรับปรุงนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปภ. เมื่อมีการเปลี่ยนแปลงทั้งจากปัจจัยภายในและปัจจัยภายนอก

ผู้ปฏิบัติ

- ผู้บริหาร พนักงานและหน่วยงานที่เกี่ยวข้อง
- คณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

แนวทางการปฏิบัติ

แนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ๓ องค์ประกอบ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย ๕ หัวข้อหลัก เพื่อให้ใช้เป็นแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังรูป



๑. องค์ประกอบของการรักษาความมั่นคงปลอดภัยไซเบอร์ ๓ องค์ประกอบ

๑.๑. องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กปภ. ต้องจัดให้มีการทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับระบบงานหรือระบบโครงสร้างพื้นฐานที่มีความสำคัญของ กปภ. อย่างเป็นลายลักษณ์อักษร โดยดำเนินการตามหมวดที่ ๑๔ นโยบายการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒. องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
กปภ. ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับระบบงานหรือระบบโครงพื้นฐานที่มีความสำคัญของ กปภ. โดยดำเนินการตาม หมวดที่ ๑๓ นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑.๓. องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์
กปภ. ต้องจัดให้มีแผนการรับมือภัยคุกคามทางไซเบอร์ สำหรับระบบงาน หรือระบบโครงพื้นฐานที่มีความสำคัญของ กปภ. โดยดำเนินการตาม หมวดที่ ๑๐ นโยบายการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ

๒. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย ๕ หัวข้อหลัก ดังนี้

๒.๑ การระบุความเสี่ยง (Identify)

๒.๑.๑. การจัดการทรัพย์สิน (Asset Management) ให้ดำเนินการตาม หมวดที่ ๒ นโยบายการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

๒.๑.๒. การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Management Strategy) ให้ดำเนินการตาม หมวดที่ ๑๓ นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๑.๓. การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ให้ดำเนินการตาม หมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน (IT Operation security policy) ส่วนที่ ๗ การประเมินช่องโหว่และการทดสอบเจาะระบบ

๒.๑.๔. การจัดการผู้ให้บริการภายนอก (Third Party Management) ให้ดำเนินการตามหมวดที่ ๙ นโยบายการบริหารจัดการผู้ให้บริการภายนอก

๒.๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๒.๑. การควบคุมการเข้าถึง (Access Control) ให้ดำเนินการตาม หมวดที่ ๓ นโยบายการควบคุม การเข้าถึง ส่วนที่ ๑ แนวทางปฏิบัติการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ และหมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ส่วนที่ ๕ แนวทางปฏิบัติการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

๒.๒.๒. การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ให้ดำเนินการตาม หมวดที่ ๘ นโยบายการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ และหมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ส่วนที่ ๙ แนวทางปฏิบัติการบริหารจัดการการตั้งค่าระบบ และการกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ

๒.๒.๓. การเชื่อมต่อระยะไกล (Remote Connection) ให้ดำเนินการตาม หมวดที่ ๓ นโยบายการควบคุมการเข้าถึง ส่วนที่ ๓ แนวทางปฏิบัติการควบคุมการเข้าถึงจากระยะไกล

๒.๒.๔. สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) ให้ดำเนินการตาม หมวดที่ ๔ นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศส่วนที่ ๓ แนวทางปฏิบัติการจัดการสื่อที่ใช้บันทึกข้อมูล

๒.๒.๕. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ให้ดำเนินการตาม หมวดที่ ๑ นโยบายความมั่นคงปลอดภัยด้านทรัพยากรบุคคล

๒.๒.๖. การแบ่งปันข้อมูล (Information Sharing) ให้ดำเนินการตาม หมวดที่ ๗ นโยบายการบริหารจัดการการรักษาความมั่นคงปลอดภัยในการติดต่อสื่อสาร ส่วนที่ ๓ แนวทางปฏิบัติการแบ่งปันหรือเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์

๒.๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๒.๓.๑. การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้ดำเนินการตาม หมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ส่วนที่ ๖ แนวทางปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์

๒.๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๒.๔.๑. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ต้องมีการจัดทำ สื่อสาร ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้งเพื่อให้แน่ใจว่าแผนรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพ

๒.๔.๒. การฝึกซ้อมรับมือเหตุการณ์ภัยคุกคามทางภัยไซเบอร์ (Cybersecurity Exercise) ต้องเข้าร่วมฝึกซ้อมรับมือเหตุการณ์ภัยคุกคามทางภัยไซเบอร์ เมื่อได้รับหนังสือเชิญจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๒.๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) โดยดำเนินการตามหมวดที่ ๑๑ นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

เอกสารอ้างอิง

- ไม่มี -

ส่วนที่ ๒
มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

วัตถุประสงค์

- เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการกำหนดคุณลักษณะความมั่นคงปลอดภัยให้แก่ข้อมูลหรือระบบสารสนเทศ สอดคล้องตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

ผู้ปฏิบัติ

- ผู้บริหาร พนักงานและหน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- กองความมั่นคงปลอดภัยไซเบอร์

แนวทางการปฏิบัติ

กองความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศร่วมพิจารณา ดังนี้

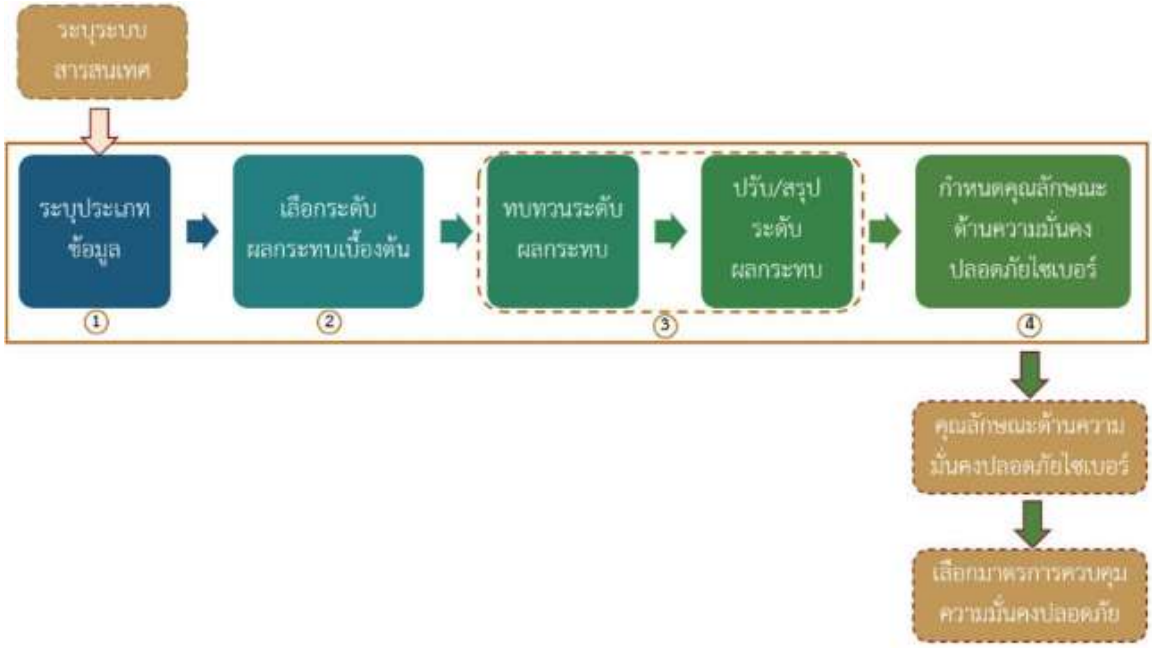
๑. กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objectives) ในเรื่อง ดังนี้ ด้านความลับ (Confidentiality) ด้านความถูกต้อง (Integrity) และด้านความพร้อมใช้ (Availability)

๒. ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นโดยพิจารณาผลกระทบในแต่ละด้าน ดังนี้
   - ผลกระทบต่อมูลค่าความเสียหายทางการเงินหรือทรัพย์สิน หรือต่อชื่อเสียงของหน่วยงาน
   - ผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด
   - ผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน
   - ผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

   ในกรณีที่หน่วยงานควบคุมหรือกำกับดูแลมีการกำหนดแนวทางการประเมินผลกระทบหรือเปลี่ยนแปลง กปภ. จะมีการทบทวนภายหลังการรับทราบข้อมูล

๓. ทบทวนความถูกต้องของการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยทุก ๓ ปี หรือทบทวนเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๔. กระบวนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ประกอบด้วยสี่ขั้นตอน ดังนี้



๔.๑. การระบุประเภทข้อมูลมีการดำเนินการ

ผู้ดำเนินการประเมินระบุประเภทข้อมูลทั้งหมดของข้อมูลที่ถูกนำเข้า จัดเก็บ ประมวลผลหรือเป็นผลลัพธ์ของแต่ละระบบสารสนเทศ โดยจัดเก็บไว้เป็นอนุกรมวิธานประเภทข้อมูล หรือบัญชีรายชื่อประเภทข้อมูล ทั้งนี้ แนวทางนี้ได้แบ่งสายการดำเนินงานหลักออกเป็น ๔ สายการดำเนินงาน ได้แก่

๔.๑.๑. การดำเนินงานสนับสนุนการส่งมอบบริการที่จำเป็น

๔.๑.๒. การบริหารจัดการทรัพยากรของรัฐเพื่อสนับสนุนการดำเนินงาน

๔.๑.๓. บริการสำหรับประชาชน

๔.๑.๔. กลไกที่หน่วยงานใช้ส่งมอบบริการเพื่อให้บรรลุวัตถุประสงค์ของการบริการ

๔.๒. ขั้นตอนการเลือกระดับผลกระทบเบื้องต้น

เจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบสารสนเทศเลือกระดับผลกระทบเบื้องต้นและคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเภทข้อมูลที่หน่วยงานได้ระบุจากขั้นตอนที่ ๔.๑ พร้อมกับจัดทำในรูปแบบเอกสาร

ปัจจัยสำหรับการจัดระดับผลกระทบ

ผู้ดำเนินการประเมินควรพิจารณาปัจจัยต่อไปนี้ในการดำเนินการจัดระดับผลกระทบด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลแต่ละประเภท

๔.๒.๑. ปัจจัยด้านการรักษาความลับ

๔.๒.๒. ปัจจัยด้านการรักษาความถูกต้องครบถ้วน

๔.๒.๓. ปัจจัยด้านการรักษาสภาพพร้อมใช้งาน

๔.๓. ขั้นตอนการทบทวนระดับผลกระทบเบื้องต้น ปรับและสรุประดับผลกระทบที่อาจเกิดขึ้น

เจ้าหน้าที่ระดับอาวุโสด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Senior information security officer) เจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบสารสนเทศ เจ้าของสายการดำเนินงาน และเจ้าของสารสนเทศควรรับหน้าที่ทบทวน และปรับระดับผลกระทบที่ได้จัดระดับไว้ เบื้องต้นในขั้นตอนที่ ๒ สำหรับข้อมูลแต่ละประเภท

๔.๔. ขั้นตอนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์

เมื่อเลือกตรวจทานและปรับระดับผลกระทบในขั้นตอนที่ ๒ และ ๓ แล้ว หน่วยงานสามารถดำเนินการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศตามประเภทข้อมูลทั้งหมดที่มีในระบบสารสนเทศนั้น โดยดำเนินการต่อไปนี้

๔.๔.๑. ทบทวนคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลทุกประเภทในระบบสารสนเทศ

๔.๔.๒. กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศโดยใช้หลักการเครื่องหมายระดับน้ำสูงสุดตามแต่ละวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (การรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน) โดยพิจารณาระดับผลกระทบสำหรับประเภทข้อมูลทุกประเภทในระบบสารสนเทศนั้นและใช้ระดับผลกระทบสูงสุดตามแต่ละวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์

รูปแบบทั่วไปสำหรับการระบุคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศ คือ

คุณลักษณะ$_{\text{ชื่อระบบสารสนเทศ}}$ = {(การรักษาความลับ, ผลกระทบ), (การรักษาความถูกต้องครบถ้วน, ผลกระทบ), (การรักษาสภาพพร้อมใช้งาน, ผลกระทบ)}

๔.๔.๓. ปรับระดับผลกระทบที่ได้จากหลักการเครื่องหมายระดับน้ำสูงสุดตามความจำเป็น

๔.๔.๔. กำหนดระดับผลกระทบของระบบสารสนเทศโดยรวมตามระดับผลกระทบสูงสุดตามแต่ละวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศ

๔.๔.๕. บันทึกการกำหนดและเหตุผลการตัดสินใจในการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ทั้งหมด

๕. จัดระดับผลกระทบที่อาจเกิดขึ้นกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยแบ่งเป็น ๓ ระดับ ระดับต่ำ ระดับกลาง ระดับสูง ของทั้ง ๓ ด้าน ประกอบด้วย ด้านความลับ (Confidentiality) ด้านความถูกต้อง (Integrity) และด้านความพร้อมใช้ (Availability) ดังนี้

ระดับ	ด้านความลับ* (Confidentiality)	ด้านความถูกต้อง (Integrity)	ด้านความพร้อมใช้ (Availability)
ระดับต่ำ	ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด	ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงาน หรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด	ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงาน หรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด
ระดับกลาง	ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรง	ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงาน หรือบุคคลอย่างร้ายแรง	ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงาน หรือบุคคลอย่างร้ายแรง
ระดับสูง	ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก	ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงาน หรือบุคคลอย่างร้ายแรงมาก	ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงาน หรือบุคคลอย่างร้ายแรงมาก

* หมายเหตุ ด้านความลับ อาจพิจารณาจาก หมวดที่ ๔ นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information security policy) ส่วนที่ ๑ แนวทางปฏิบัติการจัดชั้นความลับของข้อมูลสารสนเทศ (Information classification guideline) ตามตารางคุณลักษณะของข้อมูลสารสนเทศที่อยู่ในแต่ละชั้นความลับ

๖. หน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการจัดทำ ตามส่วนที่ ๓ มาตรฐาน ขั้นต่ำของข้อมูลหรือระบบสารสนเทศ และดำเนินการตามระดับชั้นที่มีการจัดระดับผลกระทบตามส่วนที่ ๔ แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

เอกสารอ้างอิง

๑. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

๒. ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๗

ส่วนที่ ๓
มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ

วัตถุประสงค์

- เพื่อให้หน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถดำเนินการตามมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศได้ตามกฎหมายกำหนด

ผู้ปฏิบัติ

- ผู้บริหาร พนักงานและหน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- กองความมั่นคงปลอดภัยไซเบอร์

แนวทางการปฏิบัติ

หน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการตามระดับชั้นที่มีการจัดระดับผลกระทบ ดังนี้

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ			อ้างอิงการดำเนินการของ กปภ.
	ระดับต่ำ	ระดับกลาง	ระดับสูง	
ประมวลแนวปฏิบัติ				
องค์ประกอบที่ ๑ แผนการตรวจสอบ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)		●	●	หมวดที่ ๑๔ นโยบายการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)	●	●	●	หมวดที่ ๑๓ นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	●	●	●	หมวดที่ ๑๐ นโยบายการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ			อ้างอิงการดำเนินการของ กปภ.
	ระดับต่ำ	ระดับกลาง	ระดับสูง	
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์				
๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)				
๑.๑ การจัดการทรัพย์สิน (Asset Management)	●	●	●	หมวดที่ ๒ นโยบายการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	●	●	●	หมวดที่ ๑๓ นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			●	หมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน (IT Operation security policy) ส่วนที่ ๗ การประเมินช่องโหว่ และการทดสอบเจาะระบบ
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)			●	หมวดที่ ๙ นโยบายการบริหารจัดการผู้ให้บริการภายนอก
๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)				
๒.๑ การควบคุมการเข้าถึง (Access Control)	●	●	●	หมวดที่ ๓ นโยบายการควบคุมการเข้าถึง ส่วนที่ ๑ แนวทางปฏิบัติการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ และหมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ส่วนที่ ๕ แนวทางปฏิบัติการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ			อ้างอิงการดำเนินการของ กปภ.
	ระดับต่ำ	ระดับกลาง	ระดับสูง	
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	●	●	●	หมวดที่ ๘ นโยบายการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศและ หมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ส่วนที่ ๙ แนวทางปฏิบัติการบริหารจัดการการตั้งค่าระบบและการกำหนดการตั้งค่าระบบตามมาตรฐานขั้นต่ำ
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)		●	●	หมวดที่ ๓ นโยบายการควบคุมการเข้าถึง ส่วนที่ ๓ แนวทางปฏิบัติการควบคุมการเข้าถึงจากระยะไกล
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		●	●	หมวดที่ ๔ นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ส่วนที่ ๓ แนวทางปฏิบัติการจัดการสื่อที่ใช้บันทึกข้อมูล
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	●	●	●	หมวดที่ ๑ นโยบายความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
๒.๖ การแบ่งปันข้อมูล (Information Sharing)			●	หมวดที่ ๗ นโยบายการบริหารจัดการการรักษาความมั่นคงปลอดภัยในการติดต่อสื่อสาร ส่วนที่ ๓ แนวทางปฏิบัติการแบ่งปันหรือเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ			อ้างอิงการดำเนินการของ กปภ.
	ระดับต่ำ	ระดับกลาง	ระดับสูง	
๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)				
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	●	●	●	หมวดที่ ๖ นโยบายการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ส่วนที่ ๖ แนวทางปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์
๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)				
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	●	●	●	หมวดที่ ๑๐ นโยบายการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ และหมวดที่ ๑๑ นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT contingency plan policy)
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	●	●	●	
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	●	●	●	
๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)				
๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)			●	หมวดที่ ๑๑ นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

เอกสารอ้างอิง

๑. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

ส่วนที่ ๔
แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์

- เพื่อดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้เป็นไปตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในหัวข้อที่ ๓ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ผู้ปฏิบัติ

- ผู้บริหาร พนักงานและหน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- กองความมั่นคงปลอดภัยไซเบอร์

แนวทางการปฏิบัติ

๑. ผู้บริหาร พนักงานและหน่วยงานที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการจัดทำ แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีแผน การรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยควรประกอบด้วยรายละเอียด ๓ หัวข้อ ได้แก่

หัวข้อที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง
หัวข้อที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์
หัวข้อที่ ๓ การบริหารแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. กองความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดเก็บ รวบรวมและจัดส่งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามการร้องขอ

ส่วนที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง ประกอบด้วย ๑๑ หัวข้อ ดังนี้

๑. ชื่อและหมายเลขอ้างอิงระบบสารสนเทศ โดยต้องกำหนดชื่อและหมายเลขอ้างอิงเฉพาะระบบ (Unique Identifier) ให้แก่ระบบสารสนเทศทุกระบบ

๒. คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ ได้แก่ คำอธิบาย การทำงาน (Function) และวัตถุประสงค์ของระบบสารสนเทศ

๓. เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยสารสนเทศ (Senior Information Security Officer) ให้ระบบรายละเอียดของผู้บริหารระดับสูงซึ่งเป็นผู้มีหน้าที่และอำนาจบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO หรือ Head Of Information Security) หรือผู้ที่ได้รับมอบหมายให้รับผิดชอบในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยสารสนเทศเป็นผู้มีหน้าที่และอำนาจจัดทำและทบทวนแผนการรักษา

ความมั่นคงปลอดภัยไซเบอร์ โดยประสานงานกับกองความมั่นคงปลอดภัยไซเบอร์ และตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่มีการใช้งานร่วมกันโดยต้องมีรายละเอียดอย่างน้อย ดังนี้

๓.๑. ชื่อ

๓.๒. ตำแหน่ง

๓.๓. หน่วยงาน/ส่วนงาน

๓.๔. ที่อยู่สำหรับการติดต่อ

๓.๕. หมายเลขโทรศัพท์

๓.๖. อีเมลแอดเดรส

๔. เจ้าของระบบสารสนเทศ (Information System Owner) ให้ระบบรายละเอียดของผู้รับผิดชอบระบบสารสนเทศ ซึ่งทำหน้าที่เกี่ยวกับการจัดซื้อ พัฒนา บูรณาการ เปลี่ยนแปลงหรือแก้ไข ดำเนินงาน และบำรุงรักษาระบบสารสนเทศในภาพรวม โดยเจ้าของระบบสารสนเทศเป็นผู้มีส่วนในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับเจ้าหน้าที่อาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศในการช่วยระบุและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ รวมถึงดำเนินการตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ และหากมีการเปลี่ยนแปลงที่สำคัญที่เกี่ยวข้องกับระบบสารสนเทศเกิดขึ้น เจ้าของระบบสารสนเทศต้องดำเนินการแจ้งเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศทราบ โดยต้องมีรายละเอียดอย่างน้อย ดังนี้

๔.๑. ชื่อ

๔.๒. ตำแหน่ง

๔.๓. หน่วยงาน/ส่วนงาน

๔.๔. ที่อยู่สำหรับการติดต่อ

๔.๕. หมายเลขโทรศัพท์

๔.๖. อีเมลแอดเดรส

๕. เจ้าของสารสนเทศ (Information Owner) ให้ระบุรายละเอียดของผู้มีอำนาจโดยกฎหมายหรือโดยการได้รับมอบหมายให้ดำเนินงานเกี่ยวกับสารสนเทศนั้น หรือรายละเอียดของผู้มีหน้าที่รับผิดชอบกำหนดมาตรการควบคุมสำหรับการสร้าง การรวบรวม การประมวลผล การเผยแพร่ และการทำลายสารสนเทศดังกล่าว โดยเจ้าของสารสนเทศควรมีส่วนในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ ในการให้ข้อมูลเกี่ยวกับความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศ และร่วมพิจารณากำหนดหรืออนุญาตสิทธิและประเภทของสิทธิในการเข้าถึงสารสนเทศให้แก่บุคคล (หรือผู้ดำรงตำแหน่ง) หรือหน่วยงาน รวมทั้งช่วยในการระบุและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ โดยต้องมีรายละเอียดอย่างน้อย ดังนี้

๕.๑. ชื่อ

๕.๒. ตำแหน่ง

๕.๓. หน่วยงาน/ส่วนงาน

๕.๔. ที่อยู่สำหรับการติดต่อ

๕.๕. หมายเลขโทรศัพท์

๕.๖. อีเมลแอดเดรส

๖. เจ้าหน้าที่ที่มีอำนาจ (Authorizing Official) ให้ระบุรายละเอียดของผู้บริหารระดับสูงซึ่งมีหน้าที่รับผิดชอบในการดำเนินงานระบบสารสนเทศในระดับความเสี่ยงด้านการดำเนินการ ภารกิจ หน้าที่ ภาพลักษณ์ หรือทรัพย์สินของหน่วยงานหรือของบุคคล ที่ยอมรับได้และมีอำนาจอนุมัติหรือรับรองแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือผู้ที่ได้รับมอบหมาย โดยต้องมีรายละเอียดอย่างน้อย ดังนี้

๖.๑. ชื่อ

๖.๒. ตำแหน่ง

๖.๓. หน่วยงาน/ส่วนงาน

๖.๔. ที่อยู่สำหรับการติดต่อ

๖.๕. หมายเลขโทรศัพท์

๖.๖. อีเมลแอดเดรส

เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคนให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด

๗. ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ (Other designated contact) ให้ระบบรายละเอียดของบุคคลที่มีความเกี่ยวข้องกับระบบสารสนเทศ ดังนี้

๗.๑. ผู้ที่สามารถให้ข้อมูลเกี่ยวกับการดำเนินการและคุณลักษณะของระบบสารสนเทศ

๗.๒. ผู้ที่มีส่วนร่วมในการดำเนินการพัฒนาและปรับปรุงแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

๗.๓. ผู้ที่ได้รับมอบหมายจากบุคคลตาม ๗.๑ หรือ ๗.๒ ให้กระทำการแทน

๗.๔. รายละเอียดของบุคคลตาม ๗.๑ ต้องมีรายละเอียดอย่างน้อย ดังนี้

๗.๔.๑. ชื่อ

๗.๔.๒. ตำแหน่ง

๗.๔.๓. หน่วยงาน/ส่วนงาน

๗.๔.๔. ที่อยู่สำหรับการติดต่อ

๗.๔.๕. หมายเลขโทรศัพท์

๗.๔.๖. อีเมลแอดเดรส

๘. การกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ ให้ระบุรายละเอียดเกี่ยวกับการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ (Security Category) ให้แก่ระบบสารสนเทศจากการประเมินและจัดระดับผลกระทบต่อการดำเนินงานของ กปภ. ทรัพย์สินหรือความปลอดภัยของผู้ใช้บริการ บุคลากร หรือประชาชน ในกรณีที่มีเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือเหตุภัยคุกคามทางไซเบอร์เกิดขึ้น โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ของระบบย่อยแต่ละระบบภายใต้ระบบสารสนเทศในเรื่อง การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) และใช้ระดับผลกระทบของประเภทข้อมูลตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละเรื่องที่มีระดับผลกระทบมากที่สุด

การกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศตามวรรคหนึ่ง ให้ดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

๙. สถานะของระบบสารสนเทศ ให้ระบุสถานะของระบบโดยเลือกจากสถานะ ดังต่อไปนี้
   ๙.๑. สถานะอยู่ระหว่างการพัฒนา หมายถึง ระบบใหม่ที่อยู่ระหว่างขั้นตอนการออกแบบ พัฒนา หรือทดสอบการใช้งาน
   ๙.๒. สถานะดำเนินการ หมายถึง ระบบดำเนินการหรือใช้งานในปัจจุบัน
   ๙.๓. สถานะอยู่ระหว่างการปรับปรุง หมายถึง ระบบอยู่ระหว่างการปรับปรุง แก้ไข หรือเปลี่ยนแปลง และไม่มีการใช้งาน

๑๐. การเชื่อมต่อระบบสารสนเทศและการใช้งานข้อมูลร่วมกัน ให้ระบุรายละเอียดที่เกี่ยวข้องกับการเชื่อมต่อกับระบบสารสนเทศอื่นในเรื่อง ดังนี้
   ๑๐.๑. ชื่อระบบสารสนเทศที่เชื่อมต่อ ชื่อหน่วยงานของระบบสารสนเทศที่เชื่อมต่อและชนิดของการเชื่อมต่อ เช่น ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น
   ๑๐.๒. รายละเอียดการให้สิทธิในการเชื่อมต่อ ได้แก่ วันที่ การกำหนดคุณลักษณะของระบบสารสนเทศที่เชื่อมต่อ การรับรองมาตรฐานด้านความมั่นคงปลอดภัยและสถานะการรับรองมาตรฐานด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่เชื่อมต่อ และชื่อและตำแหน่งของผู้ได้รับมอบอำนาจของระบบสารสนเทศที่เชื่อมต่อ

๑๑. นโยบาย ระเบียบ หรือกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ ให้ระบุนโยบาย ระเบียบหรือกฎหมายที่ส่งผลโดยตรงกับการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

ส่วนที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์

ให้ระบุรายละเอียดการดำเนินการที่เป็นมาตรฐานขั้นต่ำสำหรับการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ (Minimum Security Control) ตามหลักเกณฑ์ที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ เพื่อให้เหมาะสมกับการกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศตามข้อ ๘ ในส่วนที่ ๑

ส่วนที่ ๓ การบริหารงานแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. วันที่ที่จัดทำและลายมือชื่อผู้จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์
๒. วันที่ที่อนุมัติและลายมือชื่อผู้อนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์
๓. กำหนดเวลาทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์และชื่อผู้รับผิดชอบในการติดตามการทบทวนแผน
๔. สาเหตุการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเลือกจากสาเหตุดังต่อไปนี้

๔.๑. จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับแรก หมายถึง การจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นใหม่เป็นครั้งแรก หรือจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นใหม่ทั้งฉบับแทนฉบับเดิม

๔.๒. ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามรอบที่กำหนด หมายถึง การทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กำหนดไว้ในแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับที่ใช้บังคับอยู่ในขณะนั้น

๔.๓. ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เนื่องจากมีการเปลี่ยนแปลง หมายถึง การทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เนื่องจากมีการเปลี่ยนแปลงที่สำคัญ โดยต้องระบุความเปลี่ยนแปลงดังกล่าวด้วย

ทั้งนี้ กระบวนการทบทวนแผนควรดำเนินการทุกปี หรือดำเนินการก่อนรอบหนึ่งปี หากมีการเปลี่ยนแปลงที่สำคัญ เช่น มีการเปลี่ยนแปลงระดับความเสี่ยงเพิ่มขึ้นเกินกว่าระดับความเสี่ยงที่ยอมรับได้ กฎหมายที่เกี่ยวข้องกับการจัดทำหรือดำเนินการตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์มีการเปลี่ยนแปลงในสาระสำคัญ มีการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์ มีการเปลี่ยนแปลงเกี่ยวกับบุคคลที่เกี่ยวข้องกับแผนการรักษาความมันคงปลอดภัยไซเบอร์ เช่น การเปลี่ยนแปลงเจ้าของระบบสารสนเทศ ผู้ที่เกี่ยวข้องกับระบบสารสนะเทศ หรือเจ้าหน้าที่ที่มีอำนาจ เป็นต้น ระบบสารสนเทศมีการเปลี่ยนแปลง สถานะของระบบสารสนเทศมีการเปลี่ยนแปลง หรือการเชื่อมต่อระบบสารสนเทศมีการเปลี่ยนแปลง เป็นต้น

เอกสารอ้างอิง

๑. แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ ท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

๒. แบบฟอร์มแผนรักษาความมั่นคงปลอดภัยไซเบอร์

ภาคผนวก

อภิธานศัพท์

คำศัพท์	ความหมาย
การเข้ารหัสข้อมูล	การแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านเข้าใจได้ เพื่อปกป้องเนื้อหาของข้อมูลจากการเข้าถึงโดยผู้ไม่ได้รับอนุญาต ข้อมูลที่ได้รับการเข้ารหัสจะสามารถเปิดอ่านได้โดยผู้ที่มีรหัสผ่าน หรือกุญแจอิเล็กทรอนิกส์ที่ใช้ในการถอดรหัสเท่านั้น
ความเสี่ยง	ความเสี่ยง คือ โอกาสที่ภัยคุกคามจะเข้าทำอันตรายหรือก่อให้เกิดผลกระทบหรือความเสียหายต่อทรัพย์สินหรือองค์กรผ่านทางจุดอ่อนหรือข้อบกพร่อง
คอมไพเลอร์ (Compiler)	โปรแกรมที่ใช้ในการแปลง Source Code เป็น Executable ไฟล์ที่สามารถนำไปใช้งาน (run) ได้ โดยกระบวนการแปลงดังกล่าว เรียกว่าการคอมไพล์
ชั้นความลับของข้อมูล	การจำแนกประเภทของข้อมูลตามระดับความสำคัญของเนื้อหา เช่น ลับ ลับมาก หรือลับที่สุด ซึ่งข้อมูลในแต่ละชั้นความลับต้องได้รับการปกป้อง และใช้งานอย่างเหมาะสม
ซอฟต์แวร์สำเร็จรูป	ซอฟต์แวร์ที่พัฒนาโดยผู้ผลิตซอฟต์แวร์ ซึ่งสามารถซื้อมาใช้งานได้ทันที โดยไม่ต้องเขียนภาษาโปรแกรมมิ่ง หรือคอมไพล์เพิ่มเติม เช่น โปรแกรม Microsoft Office เป็นต้น
ซอร์สโค้ด (Source Code)	โปรแกรมที่อยู่ในรูปของภาษาโปรแกรมมิ่ง ซึ่งยังไม่ถูกคอมไพล์หรือแปลงให้กลายเป็น Executable ไฟล์
บริการเครือข่าย	บริการสารสนเทศต่างๆ ที่ให้บริการผ่านเครือข่าย เช่น อีเมล อินทราเน็ต การแชร์ไฟล์ ฯลฯ
บัญชีผู้ใช้งาน (User Account)	บัญชีเฉพาะบุคคลที่ใช้ในการพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบสารสนเทศขององค์กร
บัญชีผู้ใช้งานร่วมกัน	บัญชีที่ใช้งานร่วมกันหลายบุคคล เพื่อใช้งานระบบสารสนเทศขององค์กร เช่น บัญชีอีเมลแอดเดรสที่ใช้งานร่วมกันของส่วนงานใดส่วนงานหนึ่ง เป็นต้น
ประเมินความเสี่ยง	การระบุและวิเคราะห์ความเสี่ยง เพื่อให้ทราบถึงภัยคุกคาม (Threat) จุดอ่อน (Vulnerability) ผลกระทบ (Impact) และโอกาส (Probability) ที่ความเสี่ยงนั้นจะเกิดขึ้น โดยในที่นี้มุ่งเน้นไปที่ความเสี่ยงด้านความมั่นคงปลอดภัยเป็นหลัก

คำศัพท์	ความหมาย
พิสูจน์ตัวตน (Authentication)	การตรวจสอบยืนยันตัวบุคคลโดยอาศัยข้อมูลหรือสิ่งยืนยันเฉพาะ เพื่อให้มั่นใจว่าบุคคลนั้นคือตัวตนที่แท้จริง และมีสิทธิถูกต้อง ก่อนที่จะอนุญาตให้เข้าใช้งานระบบสารสนเทศขององค์กรต่อไป
ฟรีแวร์ (Freeware)	ซอฟต์แวร์ที่อนุญาตให้ผู้ใช้งานใช้งานได้โดยไม่มีค่าใช้จ่าย ทั้งนี้ ฟรีแวร์อาจแบ่งเป็นประเภทย่อยๆ ได้อีก ๒ ประเภทคือ ฟรีแวร์ที่อนุญาตให้บุคคลทั่วไปใช้ได้ฟรี และฟรีแวร์ที่อนุญาตให้องค์กร ใช้ในการดำเนินธุรกิจได้ฟรี
ไฟร์วอลล์ (Firewall)	ระบบรักษาความมั่นคงปลอดภัย ที่ทำงานโดยการวิเคราะห์รูปแบบของการเชื่อมต่อทางเครือข่าย (Pattern) เทียบกับกฎ (Rule) ที่องค์กรกำหนดไว้ หากการเชื่อมต่อทางเครือข่ายนั้นไม่เป็นไปตามกฎ ก็จะทำการตัดหรือขัดขวางการเชื่อมต่อเพื่อไม่ให้สามารถกระทำได้ นอกจากนี้ยังมีไฟร์วอลล์ที่ทำงานในลักษณะ Host-based หรือ ไฟล์วอลล์ที่ติดตั้งลงบนระบบปฏิบัติการเพื่อปกป้องความมั่นคงปลอดภัยของระบบปฏิบัติการ ตลอดจนแอพลิเคชั่นที่เกี่ยวข้องอีกด้วย
ยูทิลิตี้ (Utility)	ซอฟต์แวร์อรรถประโยชน์ที่ใช้ในการปรับแต่งระบบ เช่น Control Panel ของ Windows เป็นต้น
สิทธิ (Privilege / Right)	ระดับการเข้าที่ระบบสารสนเทศขององค์กรที่กำหนดให้แก่บุคคลใดบุคคลหนึ่ง ซึ่งสิทธิดังกล่าวจะถูกผูกไว้กับบัญชีผู้ใช้งาน
ห้องศูนย์คอมพิวเตอร์	ศูนย์คอมพิวเตอร์ หรือ Data Center ของ กปภ.
เหตุละเมิดความมั่นคง	เหตุการณ์ใด ๆ ที่ส่งผลกระทบหรือเป็นภัยคุกคามต่อความมั่นคงปลอดภัยขององค์กร ซึ่งเหตุนั้นอาจเกิดขึ้นโดยตั้งใจ โดยอุบัติเหตุ หรือโดยความประมาทเลินเล่อของพนักงาน และมีได้หลายรูปแบบ ทั้งในเชิงกายภาพ เชิงเทคนิค และเชิงกระบวนการ
Bandwidth	ความกว้างของช่องทางในการรับ - ส่งข้อมูล
Download	การดึงข้อมูลจากคอมพิวเตอร์อีกเครื่องหนึ่งซึ่งเป็นต้นทางมาเก็บไว้ยังเครื่องของเรา โดยผ่านเครือข่ายคอมพิวเตอร์
IP Address	หมายเลขประจำเครื่องคอมพิวเตอร์ ซึ่งประกอบด้วยตัวเลข ๔ ชุด มีเครื่องหมายจุดขั้นระหว่างชุด เช่น ๑๙๒.๑๖๘.๒๓๒.๑

คำศัพท์	ความหมาย
Least Privilege	หลักพื้นฐานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยการกำหนดสิทธิในการใช้งานระบบสารสนเทศให้แก่บุคคลให้น้อยที่สุดและเพียงพอต่อการปฏิบัติงานเท่านั้น
Peer to Peer software	ซอฟต์แวร์ที่เมื่อได้ติดตั้งลงในเครื่องคอมพิวเตอร์แล้ว จะทำงานเชื่อมต่อกับเครื่องคอมพิวเตอร์เครื่องอื่นที่ได้รับการติดตั้งซอฟต์แวร์แบบเดียวกันผ่านเครือข่าย เพื่อการแชร์ไฟล์และทรัพยากรระบบ
PGP	Pretty Good Privacy (PGP) นั้นเป็นวิธีเข้ารหัสและยืนยันตัวตนโดยมากนิยมใช้เข้าและถอดรหัส และลงลายมือชื่อ
Secure Delete / Sanitization	การลบข้อมูลแบบมั่นคงปลอดภัย โดยข้อมูลที่ถูกลบด้วยวิธีการในลักษณะนี้จะไม่สามารถถูกกู้คืนกลับมาได้อีก
Segregation of Duties	หลักพื้นฐานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยการแบ่งแยกหน้าที่ความรับผิดชอบของแต่ละบุคคล เพื่อป้องกันไม่ให้บุคคลใดบุคคลหนึ่งรับผิดชอบการดำเนินงานที่สำคัญตลอดกระบวนการ ซึ่งอาจก่อให้เกิดการทุจริตหรือประพฤติมิชอบได้
TOR (Term of Reference)	เอกสารระบุข้อกำหนดด้านราคาและ/หรือด้านเทคนิคของการ จัดซื้อ-จัดจ้างอุปกรณ์หรือบริการจากผู้ให้บริการ ผู้ผลิต หรือ ผู้จัดจำหน่าย
Web Browser	โปรแกรมคอมพิวเตอร์ ที่ผู้ใช้สามารถดูข้อมูลและโต้ตอบกับข้อมูลสารสนเทศที่จัดเก็บในหน้าเว็บที่สร้างด้วยภาษาเฉพาะ เช่น ภาษา HTML ที่จัดเก็บไว้ที่ระบบบริการเว็บหรือเว็บเซิร์ฟเวอร์หรือระบบคลังข้อมูลอื่นๆ โดยโปรแกรมค้นดูเว็บเปรียบเสมือนเครื่องมือในการติดต่อกับเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เรียกว่า www.
Web Site	ศูนย์รวบรวมความรู้และแหล่งข้อมูลต่างๆ จากอินเตอร์เน็ตได้ทั่วโลก อาทิเช่น ข่าวสาร ประชาสัมพันธ์ บันเทิง กีฬา เป็นต้น
Mobile Device	อุปกรณ์พกพาที่สามารถเข้าถึงเครือข่ายไร้สาย ได้ อาทิเช่น โทรศัทพ์มือถือสมาร์ทโฟน (Smart Phone) แท็บเล็ต (Tablet) และอุปกรณ์สมาร์ทดีไวซ์ (Smart Devices) เป็นต้น

คำศัพท์	ความหมาย
Multimedia	สื่อประสมที่รวมรวมสื่อประเภทต่างๆ เข้าด้วยกัน เช่น ข้อความ (Text) กราฟิก (Graphic) ภาพเคลื่อนไหว (Animation) เสียง (Sound) และวีดิทัศน์ (Video) เป็นต้น
Streaming Content	เป็นไฟล์หรือข้อมูลแบบ Multimedia ที่สามารถดูหรือดาวน์โหลดผ่านทางระบบเครือข่ายอินเทอร์เน็ต โดยมีผู้ให้บริการ Streaming Content เช่น Youtube, Facebook, Netflix เป็นต้น
Cloud Drive	เป็นพื้นที่สำหรับจัดเก็บข้อมูลแบบออนไลน์ ซึ่งผู้ใช้งานสามารถอัปโหลด ดาวน์โหลด, แก้ไขเปลี่ยนแปลง และสามารถจำกัดสิทธิ์การเข้าถึงไฟล์หรือข้อมูลประเภทต่างๆ ได้โดยง่าย
ธรรมาภิบาลข้อมูล (Data Governance)	เป็นการกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานไปใช้มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย
MOU (Memorandum of Understanding)	หนังสือซึ่งฝ่ายหนึ่งแสดงความสมัครใจจะปฏิบัติอย่างหนึ่งอย่างใดตามเงื่อนไขที่ปรากฏในหนังสือนั้นกับอีกฝ่ายหนึ่งที่ได้ร่วมกันลงนามไว้

A-๒

คำสั่งการประปาส่วนภูมิภาค
ที่ ๒๖๓ /๒๕๖๘
เรื่อง แต่งตั้งคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์
และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

โดยที่เป็นการสมควรปรับปรุงคำสั่งแต่งตั้งคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. เพื่อกำกับดูแลให้คำแนะนำเกี่ยวกับการใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของ กปภ. ให้เป็นไปอย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย

อาศัยอำนาจตามความในมาตรา ๒๒ แห่งพระราชบัญญัติการประปาส่วนภูมิภาค พ.ศ. ๒๕๒๒ จึงมีคำสั่ง ดังนี้

๑. ยกเลิกคำสั่ง กปภ. ที่ ๑๘/๒๕๖๗ ลงวันที่ ๑๐ มกราคม ๒๕๖๗ เรื่อง แต่งตั้งคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

๒. แต่งตั้งคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. ประกอบด้วย

๑) ผู้ช่วยผู้ว่าการ (ดิจิทัลและสารสนเทศ)	ประธานกรรมการ
๒) ผู้อำนวยการสำนักตรวจสอบกระบวนการสนับสนุน	ที่ปรึกษา
๓) ผู้อำนวยการกองตรวจสอบเทคโนโลยีสารสนเทศ	ที่ปรึกษา
๔) ผู้ช่วยผู้ว่าการ (วิชาการ)	กรรมการ
๕) ผู้ช่วยผู้ว่าการ (แผนยุทธศาสตร์)	กรรมการ
๖) ผู้ช่วยผู้ว่าการ (การเงิน)	กรรมการ
๗) ผู้ช่วยผู้ว่าการ (ควบคุมน้ำสูญเสีย)	กรรมการ
๘) ผู้อำนวยการสำนักดิจิทัลและพัฒนาสารสนเทศ	กรรมการ
๙) ผู้อำนวยการสำนักปฏิบัติการเทคโนโลยีดิจิทัล	กรรมการ
๑๐) ผู้อำนวยการฝ่ายกฎหมาย	กรรมการ
๑๑) ผู้อำนวยการฝ่ายบริหารความเสี่ยง	กรรมการ
๑๒) ผู้อำนวยการฝ่ายการเงินและบัญชี	กรรมการ
๑๓) ผู้อำนวยการฝ่ายวิศวกรรม	กรรมการ
๑๔) ผู้อำนวยการฝ่ายอำนวยการ	กรรมการ
๑๕) ผู้อำนวยการฝ่ายบริหารทรัพยากรบุคคล	กรรมการ
๑๖) ผู้อำนวยการกองคอมพิวเตอร์และเครือข่าย	กรรมการ
๑๗) ผู้อำนวยการกองความมั่นคงปลอดภัยไซเบอร์	กรรมการและเลขานุการ
๑๘) หัวหน้างานมาตรฐานความมั่นคงปลอดภัยสารสนเทศ กคช.	กรรมการและผู้ช่วยเลขานุการ

โดยให้คณะกรรมการ...

โดยให้คณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. มีหน้าที่ อำนาจและความรับผิดชอบ ดังนี้

๑. กำกับและติดตามให้เป็นไปตามอำนาจหน้าที่ที่กำหนดไว้ในระเบียบการประปาส่วนภูมิภาคว่าด้วยการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัย พ.ศ. ๒๕๕๘

๒. กำกับและติดตามการดำเนินงานของ กปภ. ให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่มีการประกาศในราชกิจจานุเบกษา

๓. กำกับและติดตามการดำเนินงานของ กปภ. ให้สอดคล้องตามมาตรฐาน ISO/IEC 27001 ว่าด้วยระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล (ISMS)

๔. ดำเนินการอื่นๆ ตามที่ผู้ว่าการมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๘

(นายจักรพงศ์ คำจันทร์)
ผู้ว่าการการประปาส่วนภูมิภาค

A-m

คำสั่งการประปาส่วนภูมิภาค
ที่ ๔๘๑. /๒๕๖๘
เรื่อง แต่งตั้งคณะทำงานทบทวนปรับปรุงนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

โดยที่เป็นการสมควรปรับปรุงคำสั่งแต่งตั้งคณะทำงานทบทวนปรับปรุงนโยบายและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. ให้สอดคล้องตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ ซึ่งระบุไว้ว่าหน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และหน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

อาศัยอำนาจตามความในมาตรา ๒๒ แห่งพระราชบัญญัติการประปาส่วนภูมิภาค พ.ศ.๒๕๒๒ จึงมีคำสั่ง ดังนี้

๑. ยกเลิกคำสั่ง กปภ. ที่ ๑๙/๒๕๖๗ ลงวันที่ ๑๐ มกราคม ๒๕๖๗ เรื่อง แต่งตั้งคณะทำงานทบทวนปรับปรุงนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

๒. แต่งตั้งคณะทำงานทบทวนปรับปรุงนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. ประกอบด้วย

๑) ผู้อำนวยการสำนักปฏิบัติการเทคโนโลยีดิจิทัล	ประธานคณะทำงาน
๒) ผู้อำนวยการสำนักดิจิทัลและพัฒนาสารสนเทศ	คณะทำงาน
๓) ผู้อำนวยการกองเทคโนโลยีสารสนเทศ ๑-๑๐	คณะทำงาน
๔) ผู้อำนวยการกองบริหารระบบข้อมูลสารสนเทศ	คณะทำงาน
๕) ผู้อำนวยการกองพัฒนาระบบงานสารสนเทศ	คณะทำงาน
๖) ผู้อำนวยการกองพัฒนาระบบสารสนเทศบริการ	คณะทำงาน
๗) ผู้อำนวยการกองแผนกลยุทธ์เทคโนโลยีดิจิทัล	คณะทำงาน
๘) ผู้อำนวยการกองคอมพิวเตอร์และเครือข่าย	คณะทำงาน
๙) ผู้อำนวยการกองเทคโนโลยีสารสนเทศระบบประปา	คณะทำงาน
๑๐) ผู้อำนวยการกองความมั่นคงปลอดภัยไซเบอร์	คณะทำงานและเลขานุการ
๑๑) หัวหน้างานมาตรฐานความมั่นคงปลอดภัยสารสนเทศ กคช.	คณะทำงานและผู้ช่วยเลขานุการ

ให้คณะทำงาน...

ให้คณะทำงานทบทวนปรับปรุงนโยบายและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. มีหน้าที่ อำนาจและความรับผิดชอบ ดังนี้

๑. ทบทวน/ปรับปรุง นโยบายความมั่นคงปลอดภัยด้านสารสนเทศและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.

๒. นำเสนอนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. ตามข้อ ๑ ต่อคณะกรรมการกำกับดูแลการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ. เพื่อพิจารณาให้ความเห็นชอบ

๓. ดำเนินการอื่น ๆ ตามที่คณะกรรมการกำกับฯ มอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๙ พฤษภาคม พ.ศ. ๒๕๖๘

(นายจักรพงศ์ คำจันทร์)
ผู้ว่าการการประปาส่วนภูมิภาค

A-ഭ

แบบฟอร์มการใช้งาน

ลำดับ	ชื่อแบบฟอร์ม	รหัสเอกสาร
๑.	บันทึกข้อตกลงเรื่อง การรักษาความปลอดภัยของข้อมูลสารสนเทศ (สำหรับพนักงาน)	IT-FM-NDA-๐๑
๒.	บันทึกข้อตกลงเรื่อง การรักษาความปลอดภัยของข้อมูลสารสนเทศ (บุคคลภายนอก)	IT-FM-NDA-๐๒
๓.	แบบฟอร์มบันทึกการเข้าปฏิบัติงานในห้องศูนย์คอมพิวเตอร์ กปภ.	IT-FM-NDA-๐๓
๔.	แบบฟอร์มบันทึกการนำอุปกรณ์ เข้า-ออก ห้องศูนย์คอมพิวเตอร์	IT-FM-NDA-๐๔
๕.	แบบฟอร์ม บันทึกเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ	IT-FM-NDA-๐๕
๖.	แบบฟอร์มขอแก้ไข กฎของระบบรักษาความปลอดภัย (Policy Firewall)	IT-FM-NDA-๐๘
๗.	แบบฟอร์มขอเข้าใช้งานระบบ Remote Access VPN	IT-FM-NDA-๑๐
๘.	แบบฟอร์มบันทึกการทำลายข้อมูลสารสนเทศบนอุปกรณ์อิเล็กทรอนิกส์และสื่อบันทึกต่างๆ	IT-FM-NDA-๑๑
๙.	แบบฟอร์มขอใช้/ยกเลิก/ขยายพื้นที่ อีเมล	IT-FM-Mail-๐๑
๑๐.	แบบฟอร์มขอใช้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน	IT-FM-VM-๐๑
๑๑.	แบบฟอร์มขอเปลี่ยนแปลงทรัพยากร เครื่องคอมพิวเตอร์แม่ข่ายเสมือน	IT-FM-VM-๐๒

ลำดับ	ชื่อแบบฟอร์ม	รหัสเอกสาร
๑๒.	แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบงานทั่วไป	IT-FM-AU-๐๑ - ระบบงานทั่วไป
๑๓.	แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ SAP	IT-FM-AU-๐๑ - SAP
๑๔.	แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ CIS	IT-FM-AU-๐๑ - CIS
๑๕.	แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ OIS	IT-FM-AU-๐๑ - OIS
๑๖.	แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ LIMS (สนญ.)	IT-FM-AU-๐๑ - LIMS (สนญ.)
๑๗.	แบบฟอร์ม คำขอเพิ่ม/แก้ไข/ยกเลิก สิทธิ์การใช้งาน - ระบบ LIMS (กปภ.ข.)	IT-FM-AU-๐๑ - (กปภ.ข.)
๑๘.	แบบฟอร์ม ขอสิทธิ์ระบบบัตรประชาชน - CIS	IT-FM-AU-๐๒ - CIS
๑๙.	แบบฟอร์ม พัฒนาระบบงานใหม่	IT-FM-DEV-๐๑
๒๐.	แบบฟอร์ม พัฒนาระบบงานใหม่ - กบข.	IT-FM-DEV-๐๑ – กบข.
๒๑.	แบบฟอร์ม เอกสารความต้องการผู้ใช้งาน	IT-FM-DEV-๐๒
๒๒.	แบบฟอร์ม ออกแบบระบบงาน	IT-FM-DEV-๐๓
๒๓.	แบบฟอร์ม ทดสอบโปรแกรม	IT-FM-DEV-๐๔
๒๔.	แบบฟอร์ม ขอใช้งาน User/แจ้งรับการ Transport/Deployระบบ/Upload Reporting เปลี่ยนแปลง database/เพิ่ม Role ให้ user	IT-FM-DEV-๐๕
๒๕.	แบบฟอร์ม ปรับปรุงเอกสารคู่มือ	IT-FM-DEV-๐๖
๒๖.	แบบฟอร์ม ส่งเอกสารยืนยัน	IT-FM-DEV-๐๗

ลำดับ	ชื่อแบบฟอร์ม	รหัสเอกสาร
๒๗.	แบบฟอร์ม คำขอเปลี่ยนแปลง - ระบบทั่วไป	IT-FM-DEV-๐๘ - ระบบทั่วไป
๒๘.	แบบฟอร์ม คำขอเปลี่ยนแปลง - OIS	IT-FM-DEV-๐๘ - OIS
๒๙.	แบบฟอร์ม ปรับปรุงโปรแกรม	IT-FM-DEV-๐๙
๓๐.	แบบฟอร์ม ปรับปรุงโปรแกรม – กบข.	IT-FM-DEV-๐๙ – กบข.
๓๑.	แบบฟอร์มขอใช้งานซอฟต์แวร์	IT-FM-SW-๐๑
๓๒.	แบบฟอร์ม ขอใช้งานอินเตอร์เน็ตสำหรับหน่วยงาน/บุคคลภายนอก	IT-FM-SC-๐๑

ดาวน์โหลดแบบฟอร์มการใช้งาน