การเคหะแห่งชาติ
NATIONAL HOUSING AUTHORITY
คลองจั่น เขตบางกะปิ กทม. ๑๐๒๔๐ โทร.๐-๒๓๕๑-๗๗๗๗

ประกาศการเคหะแห่งชาติ

เรื่อง นโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ

ปัจจุบันระบบสารสนเทศเป็นส่วนสำคัญในการสนับสนุนการดำเนินงานของการเคหะแห่งชาติ ประกอบกับได้มีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ กำหนดมาตรการเพื่อป้องกันและปราบปรามการใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลโดยมิชอบ อันก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม ตลอดจนความมั่นคงของรัฐ

เพื่อให้การดำเนินงานของการเคหะแห่งชาติ ทางด้านระบบเทคโนโลยีสารสนเทศด้วยวิธีอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นไปด้วยความมั่นคงปลอดภัย ตลอดจนมีประสิทธิภาพและประสิทธิผล จึงเห็นควรให้มีนโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ

อาศัยอำนาจตามมาตรา ๒๑ แห่งพระราชบัญญัติการเคหะแห่งชาติ พ.ศ. ๒๕๓๗ ผู้ว่าการการเคหะแห่งชาติ จึงมีคำสั่งดังต่อไปนี้

๑. ให้ยกเลิกประกาศการเคหะแห่งชาติ เรื่อง นโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ ฉบับลงวันที่ ๒๙ กันยายน พ.ศ. ๒๕๖๖

๒. ประกาศนโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ โดยผู้ปฏิบัติงานนำมาใช้เป็นส่วนหนึ่งของการปฏิบัติงานด้านเทคโนโลยีสารสนเทศภายในองค์กร ตามเอกสารแนบท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๒๒ มีนาคม พ.ศ. ๒๕๖๗

(นายทวีพงษ์ วิชัยดิษฐ)
ผู้ว่าการการเคหะแห่งชาติ

นโยบายและแนวทางปฏิบัติ
เรื่อง ความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ

วัตถุประสงค์

ในปัจจุบันระบบเทคโนโลยีสารสนเทศได้มีการพัฒนาไปอย่างรวดเร็ว และได้เข้ามามีบทบาทสำคัญในการดำเนินงานของการเคหะแห่งชาติ จากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคล องค์กร และระดับประเทศ ดังนั้นการป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์จึงเป็นเรื่องสำคัญอย่างยิ่ง เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของการเคหะแห่งชาติ มีความมั่นคงปลอดภัยและสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและน่าเชื่อถือ พร้อมกับเป็นแนวทางปฏิบัติสำหรับผู้ปฏิบัติงานของการเคหะแห่งชาติ เพื่อให้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ และตั้งใจปฏิบัติตามนโยบายอย่างเคร่งครัด

หน้าที่และความรับผิดชอบ

จัดให้มีการประชุมคณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัลของการเคหะแห่งชาติ โดยพิจารณาเรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ เพื่อนำมาปรับปรุงให้เป็นไปตามมาตรฐานสากล และเสริมสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศกับการเคหะแห่งชาติอย่างต่อเนื่องต่อไป

คำนิยาม

1. *ผู้ปฏิบัติงาน* หมายความว่า พนักงาน ลูกจ้าง และลูกจ้างเหมาบริการของการเคหะแห่งชาติ

2. *สินทรัพย์* หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร ตัวอย่างเช่น ข้อมูลที่จำเป็นต่อการดำเนินงานทางธุรกิจขององค์กร ระบบสารสนเทศ ฮาร์ดแวร์ และซอฟต์แวร์ที่สนับสนุนการดำเนินงานทางธุรกิจเป็นต้น ทั้งนี้ ไม่รวมอุปกรณ์ที่ กคช. เช่าใช้

3. *ความมั่นคงปลอดภัยสารสนเทศ* หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

4. *การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ* หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ปฏิบัติงาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

5. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบสารสนเทศของการเคหะแห่งชาติ ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

6. *ศูนย์คอมพิวเตอร์* หมายความว่า ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Data Center), ห้องปฏิบัติการเครือข่ายสื่อสาร (Network Room) และศูนย์ข้อมูลสำรอง (DR Site)

7. *การรักษาความมั่นคงปลอดภัยไซเบอร์* หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

8. *ภัยคุกคามทางไซเบอร์* หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง

9. *โครงสร้างพื้นฐานสำคัญทางสารสนเทศ* หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

10. *สำนักงาน* หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

11. *หน่วยงานควบคุมหรือกำกับดูแล* หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของการเคหะแห่งชาติ

12. อุปกรณ์พกพา หมายความว่า อุปกรณ์ที่ใช้ในการติดต่อสื่อสาร ประมวลผลข้อมูล และ/หรือจัดเก็บข้อมูล โดยผู้ใช้งานสามารถนำพาและเคลื่อนย้ายได้โดยสะดวก ซึ่งรวมถึงอุปกรณ์พกพาที่เป็นทรัพย์สินของบริษัทฯ และ อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาใช้เองโดยนำมาใช้ภายในเครือข่ายของ กคช. ที่ได้ทำการลงทะเบียนและได้รับอนุญาตจากทาง กคช. ให้ใช้ในการเข้าถึงข้อมูลและระบบสารสนเทศของ กคช. ตัวอย่างอุปกรณ์พกพา เช่น Notebook/Laptop computer, Mobile/Cellular phone, Smartphone, Tablet, Netbook เป็นต้น

นโยบายและแนวทางปฏิบัติ

นโยบายและแนวทางปฏิบัติเรื่อง ความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ ซึ่งอ้างอิงตามมาตรฐานสากล ISO/IEC 27001:2022 มีดังต่อไปนี้

1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดทิศทางการดำเนินการและให้การสนับสนุนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ ให้สอดคล้องกับการดำเนินงานทางธุรกิจและเป็นไปตามนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ

<u>แนวทางปฏิบัติ</u>

1.1 กำหนดให้มีนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรและนโยบายนี้ต้องได้รับอนุมัติจากผู้บริหารของการเคหะแห่งชาติ

1.2 มีการทบทวนนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างน้อย 1 ครั้งต่อปี หรือตามความเหมาะสม

2. โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร (Organization of Information Security)

<u>วัตถุประสงค์</u>

เพื่อเสริมสร้างการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติให้มีประสิทธิภาพ ต้องมีการกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในการกำกับดูแล ด้านความมั่นคงปลอดภัยสารสนเทศของการเคหะแห่งชาติไว้อย่างชัดเจน รวมทั้งจะต้องมีมาตรการตรวจสอบหน่วยงาน หรือบุคคลภายนอกที่เกี่ยวข้องทั้งทางตรง และทางอ้อมกับสินทรัพย์สารสนเทศ โดยมีการตรวจสอบอย่างสม่ำเสมอ เพื่อเป็นการรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

<u>แนวทางปฏิบัติ</u>

2.1 กำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน ในการดูแลทางด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรไว้อย่างชัดเจน

2.2 จัดตั้งคณะกรรมการหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ

2.3 กำหนดกระบวนการในการขออนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ และควบคุมให้ถือปฏิบัติตามกระบวนการที่ได้กำหนดขึ้น

2.4 กำหนดให้มีบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่น สำนักงานตำรวจแห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ผู้ให้บริการอินเตอร์เน็ต เพื่อติดต่อประสานงานด้านความมั่นคงปลอดภัยสารสนเทศในกรณีที่มีความจำเป็น และดำเนินการปรับปรุงบัญชีรายชื่อหรือข้อมูลดังกล่าวให้เป็นปัจจุบัน

2.5 กำหนดให้มีการประเมินความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายนอก

3. การบริหารจัดการสินทรัพย์ขององค์กร (Asset Management)

<u>วัตถุประสงค์</u>

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อสินทรัพย์สารสนเทศ ซึ่งถือว่าเป็นสิ่งที่สำคัญต้องได้รับการจัดทำบัญชีสินทรัพย์ขององค์กร โดยจัดหมวดหมู่ จำแนกความสำคัญ และมีวิธีการควบคุมดูแล เพื่อให้เกิดความถูกต้องเหมาะสมและปลอดภัย โดยกำหนดให้มีผู้รับผิดชอบชัดเจน

<u>แนวทางปฏิบัติ</u>

3.1 จัดทำบัญชีสินทรัพย์สารสนเทศรวมถึงอุปกรณ์เช่าด้านสารสนเทศ และปรับปรุงแก้ไขข้อมูลให้มีความถูกต้อง โดยกำหนดให้มีการทบทวนและปรับปรุงบัญชีสินทรัพย์สารสนเทศ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลง

3.2 จัดหมวดหมู่ของสินทรัพย์สารสนเทศรวมถึงอุปกรณ์เช่าด้านสารสนเทศ ตามระดับชั้นความลับ คุณค่า ข้อกำหนด ทางกฎหมาย และระดับความสำคัญต่อการเคหะแห่งชาติ

3.3 จัดทำป้ายชื่อรายละเอียดและผู้รับผิดชอบตามที่ได้จัดทำบัญชีสินทรัพย์สารสนเทศรวมถึงอุปกรณ์เช่าด้านสารสนเทศ ไว้

3.4 ผู้ปฏิบัติงานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่การเคหะแห่งชาติ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ปฏิบัติงานเอง

3.5 กำหนดให้มีการเข้ารหัสข้อมูลบนสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ ตามระดับชั้นความลับที่กำหนด

3.6 กำหนดให้มีการติดตามและพิจารณาลบข้อมูลสำคัญ ข้อมูลส่วนบุคคล ที่มีการจัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือสื่อบันทึกข้อมูลใด ๆ ด้วยวิธีการที่มั่นคงปลอดภัย ตามระยะเวลาการจัดเก็บข้อมูลที่กำหนด หรือเมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไป พร้อมทั้งจัดเก็บบันทึกการลบข้อมูลนั้นไว้เป็นหลักฐาน

3.7 กำหนดให้มีมาตรการควบคุมเพื่อป้องกันข้อมูลรั่วไหล สำหรับระบบเครือข่าย และอุปกรณ์ที่ใช้ในการประมวลผล จัดเก็บ และรับส่งข้อมูลสำคัญ

4. ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (Human Resource Security)

<u>วัตถุประสงค์</u>

เพื่อให้ผู้ปฏิบัติงานของการเคหะแห่งชาติได้รับการสรรหาอย่างเหมาะสม สามารถปฏิบัติหน้าที่ความรับผิดชอบได้ตามบทบาทที่ได้รับมอบหมาย รวมถึงความรับผิดชอบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ การอบรมให้ความรู้ที่เหมาะสมกับบทบาทหน้าที่ และหากพ้น หรือเปลี่ยนแปลงบทบาทหน้าที่ควรมีการจัดการอย่างถูกต้องเหมาะสม การละเมิดนโยบาย หรือการละเลยต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ ควรได้รับการพิจารณาดำเนินการอย่างเป็นทางการ และเป็นไปด้วยความยุติธรรม

<u>แนวทางปฏิบัติ</u>

4.1 กำหนดหน้าที่ความรับผิดชอบทางด้านความปลอดภัยสำหรับสารสนเทศให้กับผู้ปฏิบัติงานที่จะปฏิบัติงานให้สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

4.2 กำหนดให้มีการสร้างความตระหนัก ให้ความรู้ หรือจัดอบรมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศให้กับผู้ปฏิบัติงาน โดยกำหนดเป็นแผนการสร้างความตระหนักด้านความมั่นคงปลอดภัย และกำหนดให้มีการทบทวนแผนดังกล่าว อย่างน้อยปีละ 1 ครั้ง

4.3 กำหนดให้ผู้ปฏิบัติงานคืนสินทรัพย์สารสนเทศ ในกรณีที่สิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการทำงาน

4.4 กำหนดให้ดำเนินการถอดถอนสิทธิในการเข้าถึงสารสนเทศและสินทรัพย์สารสนเทศในกรณีที่สิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการทำงาน

4.5 กำหนดให้มีบทลงโทษผู้ปฏิบัติงานที่ฝ่าฝืนนโยบายและแนวทางปฏิบัติ เรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ และทำให้เกิดความเสียหายต่อการเคหะแห่งชาติ

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

<u>วัตถุประสงค์</u>

เพื่อป้องกันผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงอุปกรณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ สินทรัพย์สารสนเทศที่มีความสำคัญควรอยู่ในพื้นที่ควบคุมซึ่งมีความมั่นคงปลอดภัย ได้รับการป้องกันและควบคุม อย่างเหมาะสม เพื่อไม่ให้ผู้ไม่มีสิทธิเข้าถึงได้ ตลอดจนความเสียหาย หรือการถูกรบกวนที่อาจเกิดขึ้นได้ อุปกรณ์ที่เกี่ยวข้องรวมถึงอุปกรณ์ที่ใช้นอกสถานที่ หรือสามารถเคลื่อนย้ายได้ควรได้รับการป้องกันต่อภัยคุกคามต่าง ๆ อย่างเหมาะสม เพื่อลดความเสี่ยงจากการถูกโจรกรรมหรือการเข้าถึงโดยผู้ไม่มีสิทธิ

<u>แนวทางปฏิบัติ</u>

5.1 กำหนดให้มีการออกแบบแนวทางป้องกันการเข้าถึงทางกายภาพสำหรับพื้นที่ปฏิบัติงานที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area)

5.2 กำหนดให้มีมาตรการควบคุมการเข้า-ออก ในบริเวณ หรือพื้นที่ที่ต้องรักษาความปลอดภัยและอนุญาตให้ผ่านเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

5.3 กำหนดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหวหรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์ และธรรมชาติ

5.4 กำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบ และอุปกรณ์สนับสนุนต่าง ๆ เช่น ระบบกระแสไฟฟ้า ระบบปรับอากาศ และระบบกระแสไฟฟ้าสำรอง

5.5 กำหนดให้มีการบำรุงรักษาอุปกรณ์ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

5.6 กำหนดให้มีการรักษาความปลอดภัยในพื้นที่ปฏิบัติงาน โดยจะต้องหลีกเลี่ยงการละทิ้งเอกสารที่มีความสำคัญ และสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ เช่น อุปกรณ์เก็บข้อมูลพกพา (Flash Drive) ไว้ในพื้นที่ปฏิบัติงานเมื่อไม่ได้ใช้งาน โดยจะต้องมีการบริหารจัดการตามระดับชั้นความลับของข้อมูล

5.7 กำหนดให้มีการรักษาความปลอดภัยให้กับเครื่องคอมพิวเตอร์เมื่อไม่มีการใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

5.8 กำหนดให้มีข้อปฏิบัติในการใช้งานศูนย์คอมพิวเตอร์

6. การบริหารจัดการด้านการสื่อสารและดำเนินงาน (Communication and Operations Management)

<u>วัตถุประสงค์</u>

การสื่อสารและการดำเนินการอันเกี่ยวข้องกับสินทรัพย์สารสนเทศ ต้องได้รับการควบคุมดูแลโดยมีการเฝ้าตรวจสอบและทดสอบอย่างเหมาะสม พร้อมทั้งมีการสำรองข้อมูลที่สำคัญ มีการควบคุมสื่อบันทึกข้อมูล มีการควบคุมการแลกเปลี่ยนข้อมูลให้เป็นไปตามนโยบายและข้อกำหนด พร้อมทั้งมีการระบุหน้าที่ความรับผิดชอบตามกระบวนการบริหารจัดการอย่างชัดเจน

<u>แนวทางปฏิบัติ</u>

6.1 กำหนดให้มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ ให้มีสภาพพร้อมใช้งาน เพื่อให้ผู้ปฏิบัติงานสามารถนำไปปฏิบัติงานได้อย่างถูกต้อง

6.2 กำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืน เพื่อป้องกันสินทรัพย์สารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี

6.3 กำหนดให้มีการสำรองข้อมูลที่สำคัญและทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.4 กำหนดมาตรการ เพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่ายคอมพิวเตอร์ และดูแลโปรแกรมประยุกต์ (Application) ที่ใช้งานบนเครือข่าย

6.5 กำหนดให้บันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบและเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างสม่ำเสมอ

6.6 กำหนดให้มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ

6.7 กำหนดให้มีการตั้งค่าเวลาของระบบและอุปกรณ์จากแหล่งเวลาที่เชื่อถือได้

6.8 กำหนดให้มีขั้นตอนการตรวจสอบการใช้งานของระบบ การใช้งานสินทรัพย์สารสนเทศอย่างสม่ำเสมอ

6.9 กำหนดให้มีการติดตามและตรวจสอบการทำงานของผู้ให้บริการภายนอก

6.10 กำหนดให้มีการจัดการสื่อบันทึกข้อมูลที่เหมาะสม

6.11 กำหนดให้มีการจัดการการแลกเปลี่ยนข้อมูลสารสนเทศอย่างปลอดภัย โดยต้องมีการจัดทำขั้นตอนปฏิบัติในการแลกเปลี่ยนสารสนเทศ และในกรณีที่มีการแลกเปลี่ยนสารสนเทศกับผู้ให้บริการภายนอกจะต้องจัดทำข้อตกลงไม่เปิดเผยความลับของข้อมูล

6.12 กำหนดให้มีการวางแผนความต้องการการใช้งานทรัพยากรสารสนเทศเพิ่มในอนาคตเพื่อรองรับการใช้งานระบบสารสนเทศที่เพิ่มขึ้น

6.13 กำหนดให้มีการประเมินช่องโหว่ (Vulnerability Assessment) ของบริการที่สำคัญของการเคหะแห่งชาติ ก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding new application module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี โดยกำหนดขอบเขตของการประเมินช่องโหว่ครอบคลุมถึง

6.14 ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของการเคหะแห่งชาติ อย่างน้อย 1 ครั้งตามความจำเป็น ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding new application module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing)

6.15 กำหนดให้มีการตรวจสอบว่าผู้ทดสอบเจาะระบบ (Penetration testers) มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบ และการทดสอบเจาะระบบโดยผู้ให้บริการภายนอก ดำเนินการภายใต้การดูแลของหน่วยงาน

6.16 กำหนดให้มีการติดตามและจัดการกับช่องโหว่ที่ระบุในการประเมินช่องโหว่ และในการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

6.17 กำหนดให้มีการจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายของบริการที่สำคัญของการเคหะแห่งชาติ และให้มีการทบทวนมาตรฐานดังกล่าวอย่างน้อยปีละ 1 ครั้ง

6.18 กำหนดให้ผู้ดูแลระบบตั้งค่าความมั่นคงปลอดภัย สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายของบริการที่สำคัญของการเคหะแห่งชาติ ตามมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) ก่อนที่จะมีการเชื่อมต่อ การเปลี่ยนแปลง หรือปรับปรุงระบบสารสนเทศ และกำหนดรอบการตรวจสอบการตั้งค่าความมั่นคงปลอดภัยอย่างน้อยปีละ 1 ครั้ง

7. การควบคุมการเข้าถึง (Access Control)

<u>วัตถุประสงค์</u>

การเข้าถึงข้อมูล ระบบสารสนเทศ เครือข่าย หรือสิ่งอื่นใดที่มีอยู่ในสินทรัพย์สารสนเทศ จะต้องได้รับการควบคุม เพื่อให้มั่นใจว่าเฉพาะผู้มีสิทธิเท่านั้นที่ได้รับอนุญาต โดยมีกระบวนการลงทะเบียน การยกเลิกการอนุมัติสิทธิ และการทบทวนสิทธิอย่างเหมาะสม รวมทั้งการจัดทำ การใช้ การจัดเก็บ และการทำลายสำหรับเอกสารสำคัญและสื่อบันทึกข้อมูล เพื่อลดความเสี่ยงที่อาจเกิดขึ้น

<u>แนวทางปฏิบัติ</u>

7.1 กำหนดให้มีการควบคุมและจำกัดสิทธิในการเข้าถึงสารสนเทศ และบริการที่สำคัญของการเคหะแห่งชาติ ตามความจำเป็นในการใช้งาน

7.2 กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่าน (Password) สำหรับผู้ปฏิบัติงานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ปฏิบัติงาน

7.3 กำหนดให้มีมาตรการป้องกันช่องทางการสื่อสารระหว่างอินเทอร์เฟซ (Interface) ที่ใช้สำหรับตรวจสอบการปรับแต่งระบบ และการเข้าถึงบริการที่สำคัญ

7.4 กำหนดให้มีมาตรการทบทวนสิทธิการการเข้าถึงหรือควบคุมการใช้งานสารสนเทศตามรอบที่กำหนด

7.5 กำหนดให้มีการบริหารจัดการสิทธิสูงสุดของระบบ โดยจะต้องใช้สิทธิสูงสุดเมื่อมีความจำเป็นเท่านั้น

8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

<u>วัตถุประสงค์</u>

เพื่อให้การดำเนินงานจัดหา พัฒนา และบำรุงรักษาระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพ รวมทั้งการดำเนินงานที่เกี่ยวข้องกับการพัฒนาระบบมีความมั่นคงปลอดภัยตลอดทั้งวงจรของการพัฒนาระบบ จะต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัย โดยมีข้อกำหนด เกณฑ์การพิจารณาจัดซื้อ หรือจัดจ้างที่ชัดเจน รวมถึงความมั่นคงปลอดภัยในกระบวนการสนับสนุน การพัฒนาระบบ และมาตรการด้านการเข้ารหัสเพื่อป้องกันความผิดพลาด สูญหาย การเปลี่ยนแปลงแก้ไข หรือการใช้ในทางที่ผิด นอกจากนี้ควรมีการทบทวนตรวจสอบระบบรักษาความมั่นคงปลอดภัย โดยมีการบริหารจัดการช่องโหว่ทางเทคนิคอย่างมีประสิทธิผล

<u>แนวทางปฏิบัติ</u>

8.1 กำหนดกระบวนการตรวจสอบข้อมูลนำเข้า (Input Data Validation) และข้อมูลนำออก (Output Data Validation) ของโปรแกรมประยุกต์ (Application) ว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผล

8.2 จำกัดการเข้าถึงรหัสต้นฉบับ (Source Code) ของโปรแกรมประยุกต์ (Application) ที่ใช้ภายในองค์กร เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต

8.3 กำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งาน เพื่อป้องกันความเสี่ยงที่จะเกิดขึ้น

8.4 กำหนดให้มีมาตรการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูลที่มีความสำคัญ

8.5 ระบบสารสนเทศที่สำคัญจะต้องมีการแบ่งแยกระบบที่ใช้ในการพัฒนา ทดสอบ และใช้งาน

8.6 กำหนดให้ข้อมูลที่ใช้ในการทดสอบระบบ จะต้องไม่เป็นข้อมูลที่ใช้งานอยู่จริงหรือกระทบต่อข้อมูลส่วนบุคคล

8.7 กำหนดให้ผู้พัฒนาระบบต้องจัดทำคำขออนุมัติการขอพัฒนาระบบใหม่ หรือปรับปรุงระบบเดิมโดยมีการระบุรายละเอียดและให้ผู้มีอำนาจพิจารณา

8.8 กำหนดให้ผู้พัฒนาระบบ ทั้งการพัฒนาภายในองค์กรและการพัฒนาโดยผู้ให้บริการภายนอกพัฒนาโดยปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย ได้แก่ การรักษาความลับของข้อมูล การรักษาความถูกต้องสมบูรณ์ของข้อมูล ความพร้อมใช้ของข้อมูล การระบุตัวตนผู้ปฏิบัติงาน การพิสูจน์ตัวตนผู้ปฏิบัติงาน การกำหนดสิทธิ การเก็บบันทึกปูมเหตุการณ์ และความต่อเนื่องของการให้บริการระบบเทคโนโลยีสารสนเทศ

8.9 กำหนดให้มีความต้องการหรือเงื่อนไขการจ้างด้านความมั่นคงปลอดภัยขั้นพื้นฐาน (Security Requirement) สำหรับการว่าจ้างผู้ให้บริการภายนอกดำเนินงานเกี่ยวกับการพัฒนาระบบใหม่หรือพัฒนาเพิ่มเติมจากระบบเดิม การจัดซื้ออุปกรณ์ประมวลผล อุปกรณ์เครือข่าย และอุปกรณ์รักษาความมั่นคงปลอดภัย

8.10 กำหนดให้มีการควบคุมการส่งข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction)

8.11 กำหนดให้มีการพิจารณามาตรการปิดบังข้อมูล (Data Masking) สำหรับข้อมูลสำคัญหรือข้อมูลส่วนบุคคล สอดคล้องกับนโยบายการควบคุมการเข้าถึง (Access Control) ความต้องการทางธุรกิจ กฎหมาย และกฎระเบียบที่เกี่ยวข้อง ด้วยการทำเครื่องหมายหรือแทนที่ข้อมูลเพื่อไม่ให้สามารถอ้างถึงข้อมูลตัวตนของบุคคลได้

8.12 กำหนดให้ผู้พัฒนาระบบ พัฒนาระบบตามหลักการพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย (Secure Coding Practices) เพื่อลดจุดอ่อนหรือช่องโหว่ที่เกิดขึ้นจากการพัฒนาระบบ

9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดขององค์กร (Information Security Incident Management)

<u>วัตถุประสงค์</u>

เพื่อให้สามารถแก้ไขเหตุการณ์สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้อย่างมีประสิทธิผล ควรมีช่องทางการรายงาน แจ้งเหตุ และแก้ไขอย่างเป็นระบบ ทันต่อเวลา โดยมีการวางแผน การกำหนดหน้าที่และขั้นตอนวิธีการในการแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อให้สามารถแก้ไขเหตุการณ์ได้อย่างเหมาะสม ตลอดจนสอดคล้องกับระเบียบ ข้อบังคับ หรือกฎหมาย และมีกระบวนการในการปรับปรุงเพื่อป้องกันไม่ให้เหตุการณ์เกิดขึ้นภายหลัง

<u>แนวทางปฏิบัติ</u>

9.1 กำหนดให้มีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้น และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2 กำหนดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดที่เกิดขึ้น

9.3 กำหนดให้มีบุคลากรและโปรแกรม/ชุดคำสั่ง (Software) เพื่อเฝ้าระวังการละเมิดความมั่นคงปลอดภัยสำหรับสารสนเทศ

9.4 กำหนดให้มีการเก็บรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีอยู่ในปัจจุบันหรือมีแนวโน้มที่จะเกิดขึ้น เพื่อจัดทำข้อมูลข่าวกรองภัยคุกคามเชิงลึก และกำหนดแนวทางการป้องกันและลดผลกระทบจากภัยคุกคาม

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

<u>วัตถุประสงค์</u>

เพื่อป้องกันการหยุดชะงักของกิจกรรมต่าง ๆ ของการเคหะแห่งชาติ และป้องกันความล้มเหลวของระบบสารสนเทศที่สำคัญ ต้องมีการจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อลดผลกระทบที่อาจเกิดขึ้นกับการเคหะแห่งชาติ โดยต้องได้รับการทดสอบและปรับปรุงอย่างสม่ำเสมอ

<u>แนวทางปฏิบัติ</u>

10.1 กำหนดหน้าที่และความรับผิดชอบในการจัดทำและการทบทวนแผนความต่อเนื่องทางธุรกิจ (BCP) การดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบสำรองข้อมูล

10.2 ประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่มีความสำคัญ และกำหนดมาตรการเพื่อลดความเสี่ยง ที่อาจส่งผลกระทบต่อการดำเนินธุรกิจอย่างต่อเนื่อง อันจะทำให้ธุรกิจเกิดการหยุดชะงัก หรือล้มเหลว

10.3 จัดทำแผนความต่อเนื่องทางธุรกิจ และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแผนรับมือภัยคุกคามทางไซเบอร์เพื่อให้มั่นใจได้ว่าธุรกิจสามารถดำเนินการต่อไปได้ หากระบบสารสนเทศหยุดชะงัก หรือล้มเหลว

10.4 กำหนดให้มีการซ้อมแผนการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าธุรกิจสามารถดำเนินการต่อไปได้หากระบบสารสนเทศหยุดชะงักหรือล้มเหลว อย่างน้อยปีละ 1 ครั้ง

10.5 กำหนดให้มีการจัดเตรียมทรัพยากรให้เพียงพอต่อการความพร้อมใช้ ในกรณีที่จำเป็นต้องใช้แผนการดำเนินธุรกิจอย่างต่อเนื่อง

11. การปฏิบัติตามข้อกำหนด (Compliance)

<u>วัตถุประสงค์</u>

เพื่อป้องกันการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร กฎเกณฑ์ และสัญญาต่าง ๆ อันเกี่ยวข้องกับสินทรัพย์สารสนเทศ ควรได้รับการพิจารณาจัดทำให้เหมาะสม โดยมีกระบวนการตรวจสอบการปฏิบัติตามข้อกำหนดและกฎหมายอย่างเหมาะสม รวมถึงการควบคุมการตรวจสอบและควบคุมเครื่องมือที่ใช้ในการตรวจสอบ

<u>แนวทางปฏิบัติ</u>

11.1 กำหนดให้ผู้บังคับบัญชากำกับดูแลและควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

11.2 กำหนดมาตรการป้องกันไม่ให้ผู้ปฏิบัติงานใช้อุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต

11.3 กำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

11.4 กำหนดให้มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลของการเคหะแห่งชาติ

12. การเข้ารหัสและการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส (Cryptographic and Key Management)

<u>วัตถุประสงค์</u>

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิผลในการปกป้องความลับ ป้องกันการปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

<u>แนวทางปฏิบัติ</u>

12.1 กำหนดให้มีมาตรการในการเข้ารหัสข้อมูลอิเล็กทรอนิกส์ขององค์กรที่มีความสำคัญ

12.2 กำหนดให้ใช้ขั้นตอนวิธี (Algorithm) ในการเข้ารหัสที่เป็นมาตรฐานสากล หลีกเลี่ยงการใช้รูปแบบการเข้ารหัสที่พัฒนาขึ้นเอง เพื่อให้มั่นใจว่าขั้นตอนวิธี (Algorithm) ที่ใช้ในการเข้ารหัสนั้นมีความมั่นคงปลอดภัย

12.3 กำหนดให้มีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อย 1 ครั้งต่อปี เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย

12.4 กำหนดให้มีกระบวนการในการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส โดยครอบคลุมการสร้างการจัดเก็บ การจัดส่ง และการเปลี่ยนแปลง

13. การใช้งานอุปกรณ์พกพา และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Device and Teleworking)

<u>วัตถุประสงค์</u>

เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์พกพา และการปฏิบัติงานจากภายนอกหน่วยงานของการเคหะแห่งชาติ มีความมั่นคงปลอดภัย

<u>แนวทางปฏิบัติ</u>

13.1 กำหนดให้มีการควบคุมการใช้งานอุปกรณ์พกพาภายในองค์กร โดยมีมาตรการควบคุมการเข้าถึงระบบเครือข่ายขององค์กร เช่น กรอกแบบฟอร์ม เพื่อลงทะเบียนใช้งานระบบเครือข่าย

13.2 การเคหะแห่งชาติอนุญาตให้ใช้อุปกรณ์พกพาส่วนบุคคลเชื่อมต่อเข้ากับระบบสารสนเทศและเครือข่ายที่มีการพิสูจน์ตัวตนเท่านั้น

13.3 อุปกรณ์พกพาต่าง ๆ ที่นำมาเชื่อมต่อระบบสารสนเทศ ประมวลผล หรือจัดเก็บข้อมูลของ กคช. ต้องดำเนินการตามข้อกำหนดหรือแนวปฏิบัติที่ กคช. ได้กำหนดไว้เพื่อให้เกิดความมั่นคงปลอดภัยต่อข้อมูล

13.4 การใช้อุปกรณ์พกพาส่วนบุคคล เพื่อปฏิบัติงานจากภายนอกการเคหะแห่งชาติ ต้องปฏิบัติตามแนวทางปฏิบัติการควบคุมการเข้าถึง (Access Control) และจะต้องเชื่อมต่อเข้ากับระบบสารสนเทศของการเคหะแห่งชาติ โดยใช้ช่องทางที่เจ้าของระบบจัดเตรียมไว้ให้เท่านั้น

13.5 กำหนดให้มีการสร้างความตระหนักให้กับผู้ปฏิบัติงานในการใช้งานอุปกรณ์พกพาส่วนตัว อันได้แก่ โทรศัพท์มือถือสมาร์ทโฟน แท็บเล็ต เครื่องคอมพิวเตอร์พกพา (Notebook) และผู้ปฏิบัติงานต้องรับผิดชอบหากเกิดความเสียหายใด ๆ จากการรั่วไหลของข้อมูลหรือผลกระทบต่อองค์กรจากการเชื่อมต่อของอุปกรณ์พกพานั้น ทั้งอุปกรณ์พกพาที่ กคช. จัดเตรียมให้และอุปกรณ์พกพาส่วนตัวที่ผู้ปฏิบัติงานนำมาใช้เองโดยนำมาใช้ภายในเครือข่ายของ กคช.

13.6 กำหนดให้มีการจำกัดการเข้าถึงจากระยะไกล โดยผู้ที่สามารถเข้าถึงจากระยะไกลได้นั้นจะต้องได้รับการอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศ

13.7 กำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กร สามารถเข้าใช้งานเครือข่ายคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศของการเคหะแห่งชาติ

13.8 กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของการเคหะแห่งชาติ

13.9 หากผู้ปฏิบัติงานทำอุปกรณ์พกพาของ กคช. ชำรุด สูญหาย ถูกขโมย ต้องแจ้งต่อหน่วยงานต้นสังกัดให้เร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

14. การบริหารผู้ให้บริการภายนอก (Supplier Management)

<u>วัตถุประสงค์</u>

เพื่อให้มีการป้องกันสินทรัพย์ของการเคหะแห่งชาติ ที่สามารถเข้าถึงได้โดยผู้ให้บริการภายนอก และเพื่อให้ระดับการให้บริการของผู้บริการภายนอกเป็นไปตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

<u>แนวทางปฏิบัติ</u>

14.1 กำหนดให้ผู้ให้บริการภายนอกที่จะต้องเข้าถึงข้อมูลสำคัญขององค์กร ต้องลงนามในแบบฟอร์มบันทึกข้อตกลงการไม่เปิดเผยข้อมูลสำหรับผู้ให้บริการภายนอก

14.2 กำหนดให้มีการติดตามการดำเนินงานของผู้ให้บริการภายนอก เพื่อให้เป็นไปตามข้อตกลงระดับการให้บริการ และข้อตกลงด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา

14.3 กำหนดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่เกี่ยวข้องกับการดำเนินงานของผู้ให้บริการภายนอก

14.4 กำหนดข้อตกลงด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอก ในข้อตกลงตามเงื่อนไขของสัญญากับผู้ให้บริการภายนอก

15. นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy)

<u>วัตถุประสงค์</u>

เพื่อป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์ และกำหนดแนวทางการตอบสนองและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

<u>แนวทางปฏิบัติ</u>

15.1 จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละ 1 ครั้ง

15.2 กำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อตอบสนองต่อภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และกำหนดให้มีการทบทวนดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญ

15.3 กำหนดหน่วยงานที่มีหน้าที่ความรับผิดชอบในการเฝ้าระวัง และตอบสนองต่อภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

15.4 กำหนดให้มีการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

15.5 เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของการเคหะแห่งชาติ ให้รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามแผนที่กำหนด

15.6 ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของการเคหะแห่งชาติ ให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามแผนการรับมือภัยคุกคามทางไซเบอร์ และแจ้งไปยังหน่วยงานกำกับหรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยเร็ว

15.7 ประสานงานความร่วมมือกับหน่วยงานกำกับหรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

16. การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Personal Data Security)

<u>วัตถุประสงค์</u>

จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย ข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

<u>แนวทางปฏิบัติ</u>

16.1 ผู้ปฏิบัติงาน ต้องจัดให้มีการควบคุม และรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ครอบคลุมตั้งแต่ขั้นตอนการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าข้อมูลดังกล่าวจะอยู่ในรูปแบบเอกสารหรืออิเล็กทรอนิกส์

16.2 กำหนดมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยพิจารณาจากมาตรการดังต่อไปนี้ประกอบเข้าด้วยกัน

16.2.1 มาตรการเชิงองค์กร (organizational measures) ได้แก่ การแบ่งแยกบทบาทหน้าที่ของผู้ปฏิบัติงาน การจัดลำดับความสำคัญของข้อมูลตามระดับชั้นความลับ และการกำหนดกฎระเบียบ ขั้นตอน หรือกระบวนการ ที่ใช้ในการควบคุมความมั่นคงปลอดภัย

16.2.2 มาตรการเชิงเทคนิค (technical measures) ได้แก่ การเข้ารหัสข้อมูล การจำกัดสิทธิการเข้าถึงข้อมูลและระบบงาน การพิสูจน์ตัวตน และการปิดบังข้อมูล (Data Masking)

16.2.3 มาตรการทางกายภาพ (physical measures) ได้แก่ การควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล และอุปกรณ์ประมวลผลสารสนเทศทางกายภาพ การจำกัดสิทธิการเข้าถึงพื้นที่ และการเฝ้าระวังความมั่นคงปลอดภัยทางการภาพ

16.3 การกำหนดมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล จะต้องคำนึงถึงการดำเนินการตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญ (information assets) การป้องกันความเสี่ยงที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวัง การเผชิญเหตุ และการฟื้นฟูความเสียหาย เมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล เท่าที่จำเป็นและเหมาะสมตามระดับความเสี่ยง

16.4 การกำหนดมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ จะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศ ได้แก่ ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) ระบบเครือข่าย ซอฟต์แวร์และแอปพลิเคชัน โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น

16.5 มาตรการที่เกี่ยวกับการควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้ <u>และเป็นไปตามนโยบายการควบคุมการเข้าถึง (Access Control)</u>

16.5.1 การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) ที่มีการพิสูจน์และยืนยันตัวตน (authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิน้อยที่สุดเท่าที่จำเป็นต่อการปฏิบัติงาน

16.5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งครอบคลุมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน การทบทวนสิทธิการเข้าถึง และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึงเมื่อมีการเปลี่ยนแปลง

16.5.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

16.5.4 การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

16.6 กำหนดให้มีการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย ให้กับผู้ปฏิบัติงาน ทราบและถือปฏิบัติ อย่างน้อยปีละ 1 ครั้ง

16.7 กำหนดให้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล เมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป หรือเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

16.8 จัดให้มีข้อตกลงระหว่างการเคหะแห่งชาติและผู้ประมวลผลข้อมูลส่วนบุคคล พิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย เป็นไปตามมาตรฐานขั้นต่ำตามนโยบายการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล รวมทั้งแจ้งให้การเคหะแห่งชาติทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น