บริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน)
Don Muang Tollway Public Company Limited

40/40 ถนนวิภาวดีรังสิต แขวงสนามบิน
เขตดอนเมือง กรุงเทพฯ 10210
โทร: (66) (02) 792-6500
โทรสาร: (66) (02) 552-8065
เลขทะเบียน บมจ. 0107537001129

ISO9001 & ISO14001 CERTIFIED

40/40 ViphavadiRangsit Road,
Sanambin, DonMuang, Bangkok 10210
Tel.: (66) (02) 792-6500
Fax.: (66) (02) 552-8065
Plc Registration No. 0107537001129

ดีเอ็มที/พี/ซีเอส/006/66

วันที่ 4 มกราคม 2566

ประกาศฉบับที่ 4/2566

สำนักกรรมการผู้จัดการ

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศฉบับปรับปรุงครั้งที่ 1/2565

ตามที่ได้มีมติที่ประชุมคณะกรรมการกำกับดูแลเทคโนโลยีสารสนเทศ ครั้งที่ 14/2565 เมื่อวันที่ 12 ธันวาคม 2565 อนุมัติการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศดังมีรายละเอียดดังต่อไปนี้

ในปัจจุบันระบบเทคโนโลยีสารสนเทศได้มีการพัฒนาไปอย่างรวดเร็ว และได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กร จากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคล องค์กร และระดับประเทศ ดังนั้นการป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และความมั่นคงปลอดภัยไบเบอร์จึงเป็นเรื่องสำคัญอย่างยิ่ง เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร มีความมั่นคงปลอดภัยและสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและน่าเชื่อถือ พร้อมกับเป็นแนวทางปฏิบัติสำหรับผู้ปฏิบัติงานขององค์กร เพื่อให้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ และตั้งใจปฏิบัติตามนโยบายอย่างเคร่งครัด โดยครอบคลุมแนวทางปฏิบัติและคำนิยามสำคัญดังต่อไปนี้

1. ผู้ปฏิบัติงาน หมายความว่า พนักงาน ลูกจ้าง และลูกจ้างเหมาบริการขององค์กร
2. สินทรัพย์ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร
3. ความมั่นคงปลอดภัยสารสนเทศ หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

4. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ปฏิบัติงาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
5. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบสารสนเทศขององค์กร ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
6. ศูนย์คอมพิวเตอร์ หมายความว่า ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Data Center), ห้องปฏิบัติการเครือข่ายสื่อสาร (Network Room) และศูนย์ข้อมูลสำรอง (DR Site)
7. การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
8. ภัยคุกคามทางไซเบอร์ หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง
9. โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
10. สำนักงาน หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
11. หน่วยงานควบคุมหรือกำกับดูแล หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

แนวทางปฏิบัติเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศซึ่งอ้างอิงตามมาตรฐานสากล ISO/IEC 27001:2013 มีดังต่อไปนี้

1. **การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ** (Information Security Policy)

วัตถุประสงค์

เพื่อกำหนดทิศทางการดำเนินการและให้การสนับสนุนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ให้สอดคล้องกับการดำเนินงานทางธุรกิจและเป็นไปตามนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ

แนวทางปฏิบัติ

1.1 กำหนดให้มีนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรและนโยบายนี้ต้องได้รับอนุมัติจากผู้บริหารขององค์กร

1.2 มีการทบทวนนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างน้อย 1 ครั้งต่อปี หรือตามความเหมาะสม

2. **โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร** (Organization of Information Security)

วัตถุประสงค์

เพื่อเสริมสร้างการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรให้มีประสิทธิภาพ ต้องมีการกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในการกำกับดูแล ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรไว้อย่างชัดเจน รวมทั้งจะต้องมีมาตรการตรวจสอบหน่วยงาน หรือบุคคลภายนอกที่เกี่ยวข้องทั้งทางตรง และทางอ้อมกับสินทรัพย์สารสนเทศ โดยมีการตรวจสอบอย่างสม่ำเสมอ เพื่อเป็นการรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

แนวทางปฏิบัติ

2.1 กำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน ในการดูแลทางด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรไว้อย่างชัดเจน

2.2 จัดตั้งคณะกรรมการหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ

2.3 กำหนดกระบวนการในการขออนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ และควบคุมให้ถือปฏิบัติตามกระบวนการที่ได้กำหนดขึ้น

2.4 กำหนดให้มีบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่น สำนักงานตำรวจแห่งชาติ ศูนย์ประสานการรักษาความมั่นคงปลอดภัย ผู้ให้บริการอินเตอร์เน็ต เพื่อติดต่อประสานงานด้านความมั่นคงปลอดภัยสารสนเทศในกรณีที่มีความจำเป็น และดำเนินการปรับปรุงบัญชีรายชื่อ หรือข้อมูลดังกล่าวให้เป็นปัจจุบัน

2.5 กำหนดให้มีการประเมินความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายนอก

3. **การบริหารจัดการสินทรัพย์ขององค์กร** (Asset Management)

วัตถุประสงค์

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อสินทรัพย์สารสนเทศ ซึ่งถือว่าเป็นสิ่งที่สำคัญต้องได้รับการจัดทำบัญชีสินทรัพย์ขององค์กร โดยจัดหมวดหมู่ จำแนกความสำคัญ และมีวิธีการควบคุมดูแล เพื่อให้เกิดความถูกต้องเหมาะสมและปลอดภัย โดยกำหนดให้มีผู้รับผิดชอบชัดเจน

แนวทางปฏิบัติ

3.1 จัดทำบัญชีสินทรัพย์สารสนเทศและปรับปรุงแก้ไขข้อมูลให้มีความถูกต้องอยู่เสมอ

3.2 จัดหมวดหมู่ของสินทรัพย์สารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญต่อองค์กร

3.3 จัดทำป้ายชื่อรายละเอียดและผู้รับผิดชอบตามที่ได้จัดทำบัญชีสินทรัพย์สารสนเทศไว้

3.4 ผู้ปฏิบัติงานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่องค์กร มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ปฏิบัติงานเอง

4. **ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร** (Human Resource Security)

วัตถุประสงค์

เพื่อให้ผู้ปฏิบัติงานขององค์กรได้รับการสรรหาอย่างเหมาะสม สามารถปฏิบัติหน้าที่ความรับผิดชอบได้ตามบทบาทที่ได้รับมอบหมาย รวมถึงความรับผิดชอบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศการอบรมให้ความรู้ที่เหมาะสมกับบทบาทหน้าที่ และหากพ้น หรือเปลี่ยนแปลงบทบาทหน้าที่ควรมีการจัดการอย่างถูกต้องเหมาะสม การละเมิดนโยบาย หรือการละเลยต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ ควรได้รับการพิจารณาดำเนินการอย่างเป็นทางการ และเป็นไปด้วยความยุติธรรม

แนวทางปฏิบัติ

4.1 กำหนดหน้าที่ความรับผิดชอบทางด้านความปลอดภัยสำหรับสารสนเทศให้กับผู้ปฏิบัติงานที่จะปฏิบัติงานให้สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

4.2 กำหนดให้มีการสร้างความตระหนัก ให้ความรู้ หรือจัดอบรมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศให้กับผู้ปฏิบัติงาน

4.3 กำหนดให้ผู้ปฏิบัติงานคืนสินทรัพย์สารสนเทศ ในกรณีที่สิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการทำงาน

4.4 กำหนดให้ดำเนินการถอดถอนสิทธิในการเข้าถึงสารสนเทศและสินทรัพย์สารสนเทศในกรณีที่สิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการทำงาน

4.5 กำหนดให้มีบทลงโทษผู้ปฏิบัติงานที่ฝ่าฝืนนโยบายและแนวทางปฏิบัติ เรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร และทำให้เกิดความเสียหายต่อองค์กร

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

เพื่อป้องกันผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงอุปกรณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ สินทรัพย์สารสนเทศที่มีความสำคัญควรอยู่ในพื้นที่ควบคุมซึ่งมีความมั่นคงปลอดภัย ได้รับการป้องกันและควบคุม อย่างเหมาะสม เพื่อไม่ให้ผู้ไม่มีสิทธิเข้าถึงได้ ตลอดจนความเสียหาย หรือการถูกรบกวนที่อาจเกิดขึ้นได้ อุปกรณ์ที่เกี่ยวข้องรวมถึงอุปกรณ์ที่ใช้นอกสถานที่ หรือสามารถเคลื่อนย้ายได้ ควรได้รับการป้องกันต่อภัยคุกคามต่าง ๆ อย่างเหมาะสม เพื่อลดความเสี่ยงจากการถูกโจรกรรมหรือการเข้าถึงโดยผู้ไม่มีสิทธิ

แนวทางปฏิบัติ

5.1 กำหนดให้มีการออกแบบแนวทางป้องกันการเข้าถึงทางกายภาพสำหรับพื้นที่ปฏิบัติงานที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area)

5.2 กำหนดให้มีมาตรการควบคุมการเข้า-ออก ในบริเวณ หรือพื้นที่ที่ต้องรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

5.3 กำหนดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือหายนะอื่น 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 กำหนดให้มีการรักษาความปลอดภัยให้กับเครื่องคอมพิวเตอร์เมื่อไม่มีการใช้งานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

5.8 กำหนดให้มีข้อปฏิบัติในการใช้งานศูนย์คอมพิวเตอร์

6. การบริหารจัดการด้านการสื่อสารและดำเนินงาน (Communication and Operations Management)

วัตถุประสงค์

การสื่อสารและการดำเนินการอันเกี่ยวข้องกับสินทรัพย์สารสนเทศ ต้องได้รับการควบคุมดูแลโดยมีการเฝ้าตรวจสอบและทดสอบอย่างเหมาะสม พร้อมทั้งมีการสำรองข้อมูลที่สำคัญ มีการควบคุมสื่อบันทึกข้อมูล มีการควบคุมการแลกเปลี่ยนข้อมูลให้เป็นไปตามนโยบายและข้อกำหนด พร้อมทั้งมีการระบุหน้าที่ความรับผิดชอบตามกระบวนการบริหารจัดการอย่างชัดเจน

แนวทางปฏิบัติ

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 กำหนดให้มีขั้นตอนการตรวจสอบการใช้งานของระบบ การใช้งานสินทรัพย์สารสนเทศอย่างสม่ำเสมอ

6.7 กำหนดให้มีการติดตามและตรวจสอบการทำงานของผู้ให้บริการภายนอก

6.8 กำหนดให้มีการจัดการสื่อบันทึกข้อมูลที่เหมาะสม

6.9 กำหนดให้มีการจัดการการแลกเปลี่ยนข้อมูลสารสนเทศอย่างปลอดภัย โดยต้องมีการจัดทำขั้นตอนปฏิบัติในการแลกเปลี่ยนสารสนเทศ และในกรณีที่มีการแลกเปลี่ยนสารสนเทศกับผู้ให้บริการภายนอกจะต้องจัดทำข้อตกลงไม่เปิดเผยความลับของข้อมูล

6.10 กำหนดให้มีการวางแผนความต้องการการใช้งานทรัพยากรสารสนเทศเพิ่มในอนาคตเพื่อรองรับการใช้งานระบบสารสนเทศที่เพิ่มขึ้น

6.11 กำหนดให้มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ

6.12 กำหนดให้มีการตั้งค่าเวลาของระบบและอุปกรณ์จากแหล่งเวลาที่เชื่อถือได้

7. **การควบคุมการเข้าถึง** (Access Control)

<u>วัตถุประสงค์</u>

การเข้าถึงข้อมูล ระบบสารสนเทศ เครือข่าย หรือสิ่งอื่นใดที่มีอยู่ในสินทรัพย์สารสนเทศ จะต้องได้รับการควบคุม เพื่อให้มั่นใจว่าเฉพาะผู้มีสิทธิเท่านั้นที่ได้รับอนุญาต โดยมีกระบวนการลงทะเบียน การยกเลิก

การอนุมัติสิทธิ และการทบทวนสิทธิอย่างเหมาะสม รวมทั้งการจัดทำ การใช้ การจัดเก็บ และการทำลายสำหรับเอกสารสำคัญและสื่อบันทึกข้อมูล เพื่อลดความเสี่ยงที่อาจเกิดขึ้น

<u>แนวทางปฏิบัติ</u>

7.1 กำหนดให้มีการควบคุมและจำกัดสิทธิในการเข้าถึงสารสนเทศ ตามความจำเป็นในการใช้งาน

7.2 กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่าน (Password) สำหรับผู้ปฏิบัติงานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ปฏิบัติงาน

7.3 กำหนดให้มีมาตรการป้องกันช่องทางการสื่อสารระหว่างคอมพิวเตอร์ (Port) ที่ใช้สำหรับตรวจสอบ และการปรับแต่งระบบ

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 และมาตรการด้านการเข้ารหัส เพื่อป้องกันความผิดพลาด สูญหาย การเปลี่ยนแปลงแก้ไข หรือการใช้ในทางที่ผิด นอกจากนี้ควรมีการทบทวน ตรวจสอบระบบรักษาความมั่นคงปลอดภัย โดยมีการบริหารจัดการช่องโหว่ทางเทคนิคอย่างมีประสิทธิผล

แนวทางปฏิบัติ

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

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

8.3 กำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ และดำเนินการตรวจสอบทดสอบช่องโหว่ในระบบต่าง ๆ ที่ใช้งานเพื่อป้องกันความเสี่ยงที่จะเกิดขึ้น

8.4 กำหนดให้มีมาตรการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูลที่มีความสำคัญ

8.5 ระบบสารสนเทศที่สำคัญจะต้องมีการแบ่งแยกระบบที่ใช้ในการพัฒนา ทดสอบ และใช้งาน

8.6 กำหนดให้ข้อมูลที่ใช้ในการทดสอบระบบ จะต้องไม่เป็นข้อมูลที่ใช้งานอยู่จริงหรือกระทบต่อข้อมูลส่วนบุคคล

8.7 กำหนดให้ผู้พัฒนาระบบต้องจัดทำคำขออนุมัติการขอพัฒนาระบบใหม่ หรือปรับปรุงระบบเดิมโดยมีการระบุรายละเอียดและให้ผู้มีอำนาจพิจารณา

8.8 กำหนดให้ผู้พัฒนาระบบ ทั้งการพัฒนาภายในองค์กรและการพัฒนาโดยผู้ให้บริการภายนอก พัฒนาโดยปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย ได้แก่ การรักษาความลับของ

ข้อมูล การรักษาความถูกต้องสมบูรณ์ของข้อมูล ความพร้อมใช้ของข้อมูล การระบุตัวตนผู้ปฏิบัติงาน การพิสูจน์ตัวตนผู้ปฏิบัติงาน การกำหนดสิทธิ การเก็บบันทึกปูมเหตุการณ์และความต่อเนื่องของการให้บริการระบบเทคโนโลยีสารสนเทศ

8.9 กำหนดให้มีความต้องการหรือเงื่อนไขการจ้างด้านความมั่นคงปลอดภัยขั้นพื้นฐาน (Security Requirement) สำหรับการว่าจ้างผู้ให้บริการภายนอกดำเนินงานเกี่ยวกับการพัฒนาระบบใหม่หรือพัฒนาเพิ่มเติมจากระบบเดิม การจัดซื้ออุปกรณ์ประมวลผล อุปกรณ์เครือข่าย และอุปกรณ์รักษาความมั่นคงปลอดภัย

8.10 กำหนดให้มีการควบคุมการส่งข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction)

9. **การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดขององค์กร** (Information Security Incident Management)

วัตถุประสงค์

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

แนวทางปฏิบัติ

9.1 กำหนดให้มีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้น และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2 กำหนดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดที่เกิดขึ้น

9.3 กำหนดให้มีบุคลากรและโปรแกรม/ชุดคำสั่ง (Software) เพื่อเฝ้าระวังการละเมิดความมั่นคงปลอดภัยสำหรับสารสนเทศ

10. **การบริหารความต่อเนื่องในการดำเนินงานขององค์กร** (Business Continuity Management)

วัตถุประสงค์

เพื่อป้องกันการหยุดชะงักของกิจกรรมต่าง ๆ ขององค์กร และป้องกันความล้มเหลวของระบบสารสนเทศที่สำคัญ ต้องมีการจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อลดผลกระทบที่อาจเกิดขึ้นกับองค์กร โดยต้องได้รับการทดสอบและปรับปรุงอย่างสม่ำเสมอ

แนวทางปฏิบัติ

10.1 ประเมินความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินธุรกิจอย่างต่อเนื่อง อันจะทำให้ธุรกิจเกิดการหยุดชะงัก หรือล้มเหลว

10.2 จัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าธุรกิจสามารถดำเนินการต่อไปได้ หากระบบสารสนเทศหยุดชะงัก หรือล้มเหลว

10.3 กำหนดให้มีการซ้อมแผนการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าธุรกิจสามารถดำเนินการต่อไปได้หากระบบสารสนเทศหยุดชะงักหรือล้มเหลว

10.4 กำหนดให้มีการจัดเตรียมทรัพยากรให้เพียงพอต่อการความพร้อมใช้ ในกรณีที่จำเป็นต้องใช้ แผนการดำเนินธุรกิจอย่างต่อเนื่อง

11. **การปฏิบัติตามข้อกำหนด** (Compliance)

วัตถุประสงค์

เพื่อป้องกันการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร กฎเกณฑ์ และสัญญาต่าง ๆ อันเกี่ยวข้องกับสินทรัพย์สารสนเทศ ควรได้รับการพิจารณาจัดทำให้เหมาะสม โดยมีกระบวนการตรวจสอบการปฏิบัติตามข้อกำหนดและกฎหมายอย่างเหมาะสม รวมถึงการควบคุมการตรวจสอบและควบคุมเครื่องมือที่ใช้ในการตรวจสอบ

แนวทางปฏิบัติ

11.1 กำหนดให้ผู้บังคับบัญชากำกับดูแลและควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชา ของตน ให้ปฏิบัติตามนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

11.2 กำหนดมาตรการป้องกันไม่ให้ผู้ปฏิบัติงานใช้อุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ หรือโดยไม่ได้รับอนุญาต

11.3 กำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

11.4 กำหนดให้มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

12. **การเข้ารหัสและการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส** (Cryptographic and Key Management)

วัตถุประสงค์

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิผลในการปกป้องความลับ ป้องกันการปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

แนวทางปฏิบัติ

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)

วัตถุประสงค์

เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์สื่อสารประเภทพกพา และการปฏิบัติงานจากภายนอกหน่วยงานขององค์กร มีความมั่นคงปลอดภัย

แนวทางปฏิบัติ

13.1 กำหนดให้มีการควบคุมการใช้งานอุปกรณ์พกพาภายในองค์กร โดยมีมาตรการควบคุมการเข้าถึงระบบเครือข่ายขององค์กร เช่น การลงทะเบียน เพื่อขอใช้งานระบบเครือข่าย

13.2 องค์กรอนุญาตให้ใช้อุปกรณ์พกพาส่วนบุคคลเชื่อมต่อเข้ากับระบบสารสนเทศและเครือข่ายที่มีมาตรการพิสูจน์ตัวตนเท่านั้น

13.3 การใช้อุปกรณ์พกพาส่วนบุคคล เพื่อปฏิบัติงานจากภายนอกองค์กร ต้องปฏิบัติตามแนวทางปฏิบัติการควบคุมการเข้าถึง (Access Control) และจะต้องเชื่อมต่อเข้ากับระบบสารสนเทศขององค์กร โดยใช้ช่องทางที่เจ้าของระบบจัดเตรียมไว้ให้เท่านั้น

13.4 กำหนดให้มีการสร้างความตระหนักให้กับผู้ปฏิบัติงานในการใช้งานอุปกรณ์พกพาส่วนตัวอันได้แก่ โทรศัพท์มือถือสมาร์ทโฟน แท็บเล็ต เครื่องคอมพิวเตอร์พกพา (Notebook)

13.5 กำหนดให้มีการจำกัดการเข้าถึงจากระยะไกล โดยผู้ที่สามารถเข้าถึงจากระยะไกลได้นั้นจะต้องได้รับการอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศ

13.6 กำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กร สามารถเข้าใช้งานเครือข่ายคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศขององค์กร

14. **การบริหารผู้ให้บริการภายนอก** (Supplier Management)

วัตถุประสงค์

เพื่อให้มีการป้องกันสินทรัพย์ขององค์กร ที่สามารถเข้าถึงได้โดยผู้ให้บริการภายนอก และเพื่อให้ระดับการให้บริการของผู้บริการภายนอกเป็นไปตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

แนวทางปฏิบัติ

14.1 กำหนดให้ผู้ให้บริการภายนอกที่จะต้องเข้าถึงข้อมูลสำคัญขององค์กร ต้องลงนามสัญญาให้เก็บรักษาความลับของข้อมูล

14.2 กำหนดให้มีการติดตามการดำเนินงานของผู้ให้บริการภายนอก เพื่อให้เป็นไปตามข้อตกลงระดับการให้บริการ

14.3 กำหนดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่เกี่ยวข้องกับการดำเนินงานของผู้ให้บริการภายนอก

15. การจัดการความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management)

วัตถุประสงค์

เพื่อป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์ และกำหนดแนวทางการตอบสนองและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

แนวทางปฏิบัติ

15.1 จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละ 1 ครั้ง

15.2 กำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อตอบสนองต่อภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

15.3 กำหนดหน่วยงานที่มีหน้าที่ความรับผิดชอบในการเฝ้าระวัง และตอบสนองต่อภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

15.4 กำหนดให้มีการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

15.5 เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบขององค์กร ให้รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามแผนที่กำหนด

15.6 ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบขององค์กร ให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแผนการรับมือภัยคุกคามทางไซเบอร์ และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลโดยเร็ว

15.7 ประสานงานความร่วมมือกับสำนักงาน ในการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ประกาศ ณ วันที่ 4 มกราคม 2566

(ดร.ศักดิ์ดา พรรณไวย)

กรรมการผู้จัดการ