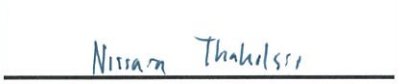
บริษัทนีโอ คอร์ปอเรท จำกัด (มหาชน)
บริษัทนีโอ แฟคทอรี่ จำกัด

นโยบาย
ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ปี 2567

การควมคุมเอกสาร (Document Control)

การอนุมัติเอกสาร (Document Approvals)

เอกสารฉบับนี้ได้รับการทบทวนและอนุมัติโดย

จัดเตรียมเอกสารโดย	เสนอโดย	อนุมัติโดย
ฝ่ายเทคโนโลยีสารสนเทศ	 (คุณธิปพันธ์ ภูริกิตติ) ผู้อำนวยการ ฝ่ายเทคโนโลยีสารสนเทศ	 (คุณณิศรา ถกลศรี) รองประธานเจ้าหน้าที่บริหาร สายปฏิบัติการ

การปรับปรุงแก้ไข (Revision History)

เวอร์ชั่น	วันที่แก้ไข	ผู้แก้ไข	หมายเหตุ
ฉบับปี 2561	8 พ.ค. 61	ฝ่ายเทคโนโลยีสารสนเทศ	จัดทำเพื่อเป็นกรอบการปฏิบัติงานของบริษัท
ฉบับปี 2565	7 ก.ย. 65	ฝ่ายเทคโนโลยีสารสนเทศ	ทบทวนและตรวจสอบความครบถ้วนประจำปี
ฉบับปี 2566	1 พ.ย. 66	ฝ่ายเทคโนโลยีสารสนเทศ	ทบทวนและตรวจสอบความครบถ้วนประจำปี
ฉบับปี 2567	28 มิ.ย. 67	ฝ่ายเทคโนโลยีสารสนเทศ	ทบทวนและตรวจสอบความครบถ้วนประจำปี

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

บทนำ

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) ของกลุ่มบริษัทนีโอ ฉบับนี้จัดทำขึ้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทนีโอ มีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัยถูกต้องเชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง ซึ่งเป็นอำนาจตามได้รับอนุมัติให้ประกาศถือใช้โดยผู้บริหารที่มีอำนาจ มีวัตถุประสงค์เพื่อให้ส่วนงานต่างๆ หรือผู้ที่มีส่วนเกี่ยวข้อง ถือใช้เป็นส่วนหนึ่งในนโยบายหลักของบริษัท เพื่อเป็นแนวทางในการกำหนดวิธีปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยเนื้อหาในส่วนของนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วย

1. นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information security policy)
2. โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of information security)
3. การบริหารจัดการทรัพย์สิน (Asset management)
4. การควบคุมการเข้าถึง (Access control)
5. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)
6. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
7. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
8. การจัดหาการพัฒนาและการบำรุงรักษาระบบ (System acquisition, development and maintenance)
9. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
10. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information security incident management)
11. ประเด็นด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity)
12. การปฏิบัติตามข้อกาหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Compliance)

นโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัทนีโอ แต่ละส่วนที่กล่าวข้างต้นประกอบด้วยวัตถุประสงค์และขอบเขตรายละเอียดของมาตรฐาน แนวปฏิบัติ และขั้นตอนวิธีปฏิบัติ เพื่อให้องค์กรมีมาตรการในด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อยู่ในระดับที่มั่นคงปลอดภัย มีความเชื่อถือได้ ช่วยลดความเสี่ยงที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศต่าง ๆ และให้พนักงานที่ปรึกษาบริษัท คู่สัญญา รวมทั้งผู้รับจ้างทุกราย ได้ตระหนักถึงความสำคัญของระบบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ จึงขอให้ผู้ที่มีส่วนเกี่ยวข้องปฏิบัติตามนโยบายและวิธีปฏิบัติต่าง ๆ อย่างเคร่งครัด

วัตถุประสงค์และขอบเขต

การจัดให้มีนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย โดยอ้างอิงกับมาตรฐานสากลเพื่อให้มาตรฐานด้านความปลอดภัยสอดคล้องกับมาตรฐานสากล

บริษัทฯ ได้ตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติของพนักงานในองค์กร เพื่อให้พนักงานมีความตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลเทคโนโลยีสารสนเทศของบริษัท และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัท ด้านอื่นๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทให้มีความมั่นคงปลอดภัยในการดำเนินกิจการของบริษัท

การนำมาตรฐาน ISO27001 มาใช้งาน มี 4 องค์ประกอบใหญ่คือ

1. จัดทำระบบ(Establish) การจัดการความมั่นคงปลอดภัยของสารสนเทศ(Information Security Management System -ISMS) คือ การเตรียมการวางแผนเพื่อปกป้องสารสนเทศ
2. นำไปปฏิบัติ(Implement) คือ นาแผนจากขั้นตอนการจัดทาระบบ(Establish) ไปปฏิบัติจริงหน้างานทำตามเอกสารคู่มือและลงบันทึกในแบบฟอร์ม
3. รักษาไว้ (Maintain) คือปฏิบัติควบคู่ไปกับการทำงานปกติ
4. ปรับปรุงอย่างต่อเนื่อง(Continual Improvement) คือ ทบทวนผลการทาระบบและหาจุดปรับปรุงอย่างต่อเนื่อง ไม่ใช่ทำครั้งเดียวจบ

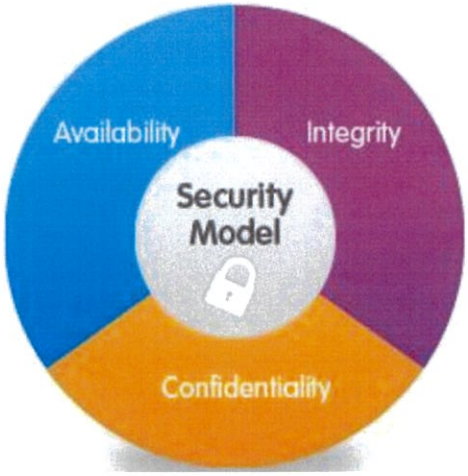
การทำระบบ ISO27001 ให้มีประสิทธิภาพ ท่านต้องทาตาม 4 ข้อข้างต้นให้ครบถ้วน ตั้งแต่ จัดทาระบบ(Establish), นาไปปฏิบัติ(Implement) , รักษาไว้(Maintain) และ Continual Improvement และต้อง มีหลักฐาน(ทั้งเอกสารและผลการปฏิบัติ) ที่น่าเชื่อถือ สะท้อนความเป็นจริงและตรวจสอบย้อนหลังได้

โมเดล CIA ใน ISO27001

Confidential: การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์

Integrity: ปกป้องความถูกต้องสมบูรณ์ของ สารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความ เป็นจริง เช่น การแฮกระบบเพื่อแก้ไขข้อมูล เป็นต้น

Availability: สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน



ขอบเขตของการสร้างความมั่นคงปลอดภัย

เอกสารฉบับนี้มีขอบเขตคลอบคลุมถึงการสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศต่าง ๆ ของบริษัท ดังนี้

- พนักงานและลูกจ้างของบริษัททั้งหมด
- ข้อมูล/สารสนเทศของบริษัท
- เครื่องคอมพิวเตอร์, โน๊ตบุ้ค, เซิร์ฟเวอร์ต่าง ๆ ขององค์กร
- อุปกรณ์เครือข่าย
- ระบบไฟฟ้าสำรอง
- สายสัญญาณเครือข่าย
- ซอฟท์แวร์ระบบ ซอฟท์แวร์จ้างพัฒนา ซอฟท์แวร์พัฒนาเอง ซอฟท์แวร์สำเร็จรูป

1. นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Information Security Policy)

1.1 วัตถุประสงค์และขอบเขต

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นนโยบายในภาพรวมของการรักษาความมั่นคงปลอดภัยของกลุ่มบริษัทนีโอ เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้าน ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

1.2 นโยบายสำหรับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Policies for information security)

1.2.1นโยบายสำหรับด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต้องมีการจัดทำอนุมัติโดยผู้บริหารเผยแพร่และสื่อสารให้พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ โดยอาจจะเป็นประกาศ หรือ จดหมายที่ได้รับการอนุมัติจากคณะกรรมการ

1.2.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Review of the policies for information security)

นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กรเพื่อให้นโยบายมีความเหมาะสมเพียงพอและได้ผล โดยมีการทบทวนอย่างน้อยปีละ 1 ครั้ง

2. โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
(Organization of information security)

2.1 วัตถุประสงค์และขอบเขต

เพื่อการบริหารจัดการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัทนีโออย่างเป็นระบบนั้น จำเป็นต้องมีการจัดโครงสร้างของหน่วยงานภายใน ที่มีส่วนเกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างเหมาะสมของพนักงาน รวมถึงการกำหนดบทบาทและสิทธิหน้าที่ที่มีต่อข้อมูลของผู้ที่มี ส่วนเกี่ยวข้องในฐานะต่าง ๆ ตลอดจนความเข้าใจและตระหนักถึงหน้าที่ด้านความมั่นคงปลอดภัยของข้อมูล

2.2 โครงสร้างภายในองค์กร (Internal organization)

วัตถุประสงค์เพื่อให้มีการกำหนดกรอบการบริหารจัดการโดยต้องมีการควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภายในองค์กร

2.2.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information security roles and responsibilities)

หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องมีการกำหนดและมอบหมายความรับผิดชอบให้ชัดเจน

2.2.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

หน้าที่และส่วนงานที่รับผิดชอบต้องแบ่งแยกให้ชัดเจนโดยไม่มีการปฏิบัติงานที่ทับซ้อนกัน เพื่อให้เกิดการขัดต่อการปฏิบัติงาน และทำให้เกิดความเสียหายต่อข้อมูลหรือทรัพย์สินขององค์กรโดยเจตนาหรือไม่เจตนาก็ตาม

2.2.3 การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

การติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้องต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.2.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันกลุ่มทมีความเชี่ยวชาญ ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและสมาคมอาชีพต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.2.5 ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตามต้องมีการระบุ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโครงการนั้น

2.3 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

วัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและ ของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

2.3.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาต้องมีการนำมาใช้งานเพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว

2.3.2 การปฏิบัติงานจากระยะไกล (Teleworking)

นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกลต้องมีการนำมาใช้งานเพื่อป้องกันข้อมูลที่มีการเข้าถึงการประมวลผลหรือการจัดเก็บจากสถานที่ดังกล่าว

3. การบริหารจัดการทรัพย์สิน
(Asset management)

3.1 วัตถุประสงค์และขอบเขต

เพื่อการดูแลรักษา ปกป้องสินทรัพย์หรือทรัพย์สิน รวมถึงข้อมูลด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยการกำหนดกฎระเบียบ หรือหลักเกณฑ์ วิธีปฏิบัติ อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานเทคโนโลยีสารสนเทศและทรัพย์สิน ต้องมีการเก็บรักษาทรัพย์สินที่มีความสำคัญต่อกลุ่มบริษัทนีโอ อย่างเป็นระเบียบ ในสถานที่ที่ปลอดภัยให้เหมาะสม พนักงาน บริษัทที่ปรึกษาและคู่สัญญา ต้องทราบถึง การมีอยู่ของทรัพย์สิน และกำหนดให้มีเจ้าของทรัพย์สิน เพื่อรับผิดชอบในทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแล และควบคุมทรัพย์สินแทน อย่างไรก็ดีเจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว

3.2 การจัดการสื่อบันทึกข้อมูล (Media handling)

วัตถุประสงค์เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาตการเปลี่ยนแปลงการขนย้ายการลบหรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

3.2.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการกับสื่อบันทึกข้อมูลที่ถอดแยกได้ต้องมีการจัดทำและปฏิบัติตามโดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

3.2.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media)

สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัยเมื่อหมดความต้องการในการใช้งานโดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ

3.2.3 การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)

สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาตการนำไปใช้ผิดวัตถุประสงค์หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

4. การควบคุมการเข้าถึง
(Access control)

4.1 วัตถุประสงค์และขอบเขต

เป็นการกำหนดวิธีปฏิบัติมาตรการควบคุมการเข้าถึงของบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงซึ่งระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทนีโอ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ และภัยคุกคามต่าง ๆ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศ ได้อย่างถูกต้อง

4.2 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

วัตถุประสงค์เพื่อจำกัดการเข้าถึงเทคโนโลยีสารสนเทศและอุปกรณ์ประมวลผลเทคโนโลยีสารสนเทศ

4.2.1 นโยบายควบคุมการเข้าถึง (Access control policy)

นโยบายควบคุมการเข้าถึงต้องมีการกำหนดจัดทำเป็นลายลักษณ์อักษรและทบทวนตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

4.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

4.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

วัตถุประสงค์เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตและป้องกัน การเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

4.3.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

กระบวนการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการให้สิทธิการเข้าถึง

4.3.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)

กระบวนการจัดการสิทธิการเข้าถึงของผู้ใช้งานต้องมีการปฏิบัติตามทั้งให้และถอดถอนสิทธิการเข้าถึงสำหรับผู้ใช้งานทุกประเภทและทุกระบบและบริการทั้งหมดขององค์กร

4.3.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

การให้และใช้สิทธิการเข้าถึงตามระดับสิทธิต้องมีการจำกัดและควบคุม

4.3.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)

การมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับต้องมีการควบคุมโดยผ่านกระบวนการบริหารจัดการที่เป็นทางการ

4.3.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้อย่างน้อยปีละ 1 ครั้ง

4.3.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)

สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อเทคโนโลยีสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงานหมดสัญญาหรือสิ้นสุดข้อตกลงการจ้างหรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน

4.4 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

4.4.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information)

ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูลการพสูจน์ตัวตนซึ่งเป็นข้อมูลลับ

4.5 การควบคุมการเข้าถึงระบบ (System and application access control)

วัตถุประสงค์เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

4.5.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

4.5.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log on procedures)

กรณีมีการกำหนดโดยนโยบายควบคุมการเข้าถึงการเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

4.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)

ระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ

4.5.4 การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

5. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

5.1 วัตถุประสงค์และขอบเขต

นโยบายความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม เป็นนโยบายเพื่อกำหนดระเบียบ วิธีปฏิบัติในการป้องกันพื้นที่ควบคุมและพื้นที่ควบคุมพิเศษความมั่นคงปลอดภัยภายในกลุ่มบริษัทนีโอ และแนวทางการแก้ไขปัญหาที่เกิดขึ้นจากการสูญหาย การรั่วไหลของระบบสารสนเทศ ในส่วนที่เกี่ยวข้องกับสิ่งซึ่งเป็นรูปธรรมจับต้องได้ในระบบ เช่น อุปกรณ์และสื่อจัดเก็บข้อมูล อาคารที่ตั้งของระบบบริหารจัดการตลอดจนระบบข้อมูลและเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เป็นต้น และเพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

5.2 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

วัตถุประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตความเสียหายและการแทรกแซงการทำงานที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

5.2.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

ขอบเขตหรือบริเวณโดยรอบพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัยต้องมีการกำหนดขึ้นมาเพื่อใช้ในการป้องกันพื้นที่สำคัญดังกล่าวอันประกอบไปด้วยสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศที่มีความสำคัญ

5.2.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัยต้องมีการป้องกันโดยมีการควบคุมการเข้าออกอย่างเหมาะสมโดยกำหนดให้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถเข้าถึงพื้นที่สำคัญได้

5.2.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงานห้องทำงานและอุปกรณ์ (Securing office, room and facilities)

ความมั่นคงปลอดภัยทางกายภาพของสำนักงานห้องทำงานและอุปกรณ์ต่างๆต้องมี การออกแบบและดำเนินการ

5.2.4 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external end environmental threats)

การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติการโจมตีหรือการบุกรุกหรืออุบัติเหตุต้องมีการออกแบบและดำเนินการ

5.2.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

ขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัยต้องมีการจัดทำและปฏิบัติตามดังกล่าวควรแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

5.3 อุปกรณ์ (Equipment)

วัตถุประสงค์เพื่อป้องกันการสูญหายการเสียหายการขโมยหรือการเป็นอันตรายต่อทรัพย์สินและป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

5.3.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

อุปกรณ์ต้องมีการจัดตั้งและป้องกันเพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายด้านสภาพแวดล้อม และจากโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

5.3.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

อุปกรณ์ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่นๆที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ

5.3.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

การเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคมซึ่งส่งข้อมูลหรือสนับสนุนบริการสารสนเทศต้องมีการป้องกันจากการขัดขวางการทำงานการแทรกแซงสัญญาณหรือการทำให้เสียหาย

5.3.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้องเพื่อให้มีสภาพความพร้อมใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง

5.3.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of assets)

อุปกรณ์สารสนเทศหรือซอฟต์แวร์ต้องไม่มีการนำออกนอกสำนักงานโดยปราศจากการขออนุญาตก่อน

5.3.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off- premises)

ทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยโดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกสำนักงาน

5.3.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องมีการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัยก่อนการกำจัดอุปกรณ์หรือก่อนการนำอุปกรณ์ไปใช้งานอย่างอื่น

5.3.8 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

6. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน
(Operations security)

6.1 วัตถุประสงค์และขอบเขต

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย เป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัยธรรมชาติ ระบบเสียหาย ฯลฯ โดยมีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน และเพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบ ลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ และมีกระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

6.2 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedures and responsibilities)

วัตถุประสงค์เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

6.2.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

ขั้นตอนการปฏิบัติงานต้องมีการจัดทำเป็นลายลักษณ์อักษรและต้องสามารถเข้าถึงได้โดยผู้ที่จำเป็นต้องใช้งาน

6.2.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)

การเปลี่ยนแปลงต่อองค์กรกระบวนการทางธุรกิจอุปกรณ์ประมวลผลสารสนเทศและระบบที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศต้องมีการควบคุมการดำเนินการ

6.2.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

การใช้ทรัพยากรของระบบต้องมีการติดตามปรับปรุงและคาดการณ์ความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ

6.2.4 การแยกสภาพแวดล้อมสำหรับการพัฒนาการทดสอบและการให้บริการออกจากกัน (Separation of development, testing and operational environments)

สภาพแวดล้อมสำหรับการพัฒนาการทดสอบและการให้บริการต้องมีการจัดทำแยกกันเพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

6.3 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from malware)

วัตถุประสงค์เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

6.3.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

มาตรการตรวจหาการป้องกันและการกู้คืนจากโปรแกรมไม่ประสงค์ดีต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

6.4 การสำรองข้อมูล (Backup)

วัตถุประสงค์เพื่อป้องกันการสูญหายของข้อมูล

6.4.1 การสำรองข้อมูล (Information backup)

ข้อมูลสำรองสำหรับสารสนเทศซอฟต์แวร์และอิมเมจของระบบต้องมีการดำเนินการสำรองไว้และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้

6.5 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)

วัตถุประสงค์เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

6.5.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)

ข้อมูลล็อกแสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งานการทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติความผิดพลาดในการทำงานของระบบและเหตุการณ์ความมั่นคงปลอดภัยต้องมีการบันทึกไว้จัดเก็บและทบทวนอย่างสม่ำเสมอ

6.5.2 การป้องกันข้อมูลล็อก (Protection of log information)

อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต

6.5.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อกข้อมูลดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ

6.5.4 การตั้งนาฬิกาให้ถูกต้อง (Clock synchronization)

นาฬิกาของระบบที่เกี่ยวข้องทั้งหมดภายในองค์กรหรือในขอบเขตหนึ่งต้องมีการตั้งให้ตรงและถูกต้องเทียบกับแหล่งอ้างอิงเวลาแห่งหนึ่ง

6.6 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

วัตถุประสงค์เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

6.6.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

ขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมี การปฏิบัติตามให้สอดคล้อง

6.7 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical vulnerability management)

วัตถุประสงค์เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

6.7.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้งานต้องมีการติดตามอย่างทันกาลจุดอ่อนต่อช่องโหว่ดังกล่าวขององค์กรต้องมีการประเมินและมาตรการที่เหมาะสมต้องถูกนำมาใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง

6.7.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

กฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม

6.8 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information systems audit considerations)

วัตถุประสงค์เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ

6.8.1 มาตรการการตรวจประเมินระบบ (Information systems audit controls)

ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการต้องมีการวางแผนและตกลงร่วมกันอย่างระมัดระวังเพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ

7. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล
(Communications security)

7.1 วัตถุประสงค์และขอบเขต

เพื่อเป็นแนวทางในการป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของกลุ่มบริษัทนีโอ ให้มีวิธีการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กรและถ่ายโอนข้อมูลกับภายนอกหน่วยงาน

7.2 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network security management)

วัตถุประสงค์เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ

7.2.1 มาตรการเครือข่าย (Network controls) เครือข่ายต้องมีการบริหารจัดการและควบคุมเพื่อป้องกันสารสนเทศในระบบต่างๆ

7.2.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services) กลไกด้านความมั่นคงปลอดภัยระดับการให้บริการและความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมดต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่ายไม่ว่าบริการเหล่านี้จะมีการให้บริการโดยองค์กรเองหรือจ้างการให้บริการก็ตาม

7.2.3 การแบ่งแยกเครือข่าย (Segregation in networks) กลุ่มของบริการสารสนเทศผู้ใช้งานและระบบต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด

7.3 การถ่ายโอนสารสนเทศ (Information transfer)

วัตถุประสงค์เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

7.3.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

นโยบายขั้นตอนปฏิบัติและมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการต้องมีการปฏิบัติเพื่อป้องกันสารสนเทศที่มีการถ่ายโอนโดยผ่านทางการใช้อุปกรณ์การสื่อสารทุกประเภท

7.3.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

ข้อตกลงสำหรับการถ่ายโอนสารสนเทศทางธุรกิจให้มีความมั่นคงปลอดภัยต้องมี การระบุระหว่างองค์กรกับหน่วยงานภายนอก

7.3.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)

สารสนเทศที่เกี่ยวข้องกับการส่งข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม

7.3.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

ความต้องการในการรักษาความลับหรือการไม่เปิดเผยความลับซึ่งสะท้อนถึงความจำเป็นขององค์กรในการป้องกันสารสนเทศต้องมีการระบุทบทวนอย่างสม่ำเสมอและบันทึกไว้อย่างเป็นลายลักษณ์อักษร

8. การจัดหาการพัฒนาและการบำรุงรักษาระบบ
(System acquisition, development and maintenance)

8.1 วัตถุประสงค์และขอบเขต

เป็นข้อกำหนดเพื่อให้มั่นใจได้ว่าการพัฒนาระบบงานสนับสนุนธุรกิจของกลุ่มบริษัทนีโอ ได้คำนึงถึงความมั่นคงปลอดภัย และการควบคุมที่เพียงพอ จำเป็นต้องกำหนดให้มีการพิจารณาถึงความต้องการด้านความมั่นคงปลอดภัยของระบบงาน ก่อนที่จะมีการพัฒนาระบบ รวมถึงการกำหนดให้มีการควบคุมภายในระบบงาน เช่น การตรวจสอบความถูกต้องของข้อมูลตั้งแต่การนำเข้าข้อมูลสู่ระบบการประมวลผลจนกระทั่งการตรวจสอบผลลัพธ์ที่ได้จากระบบ เป็นต้น

8.2 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

วัตถุประสงค์เพื่อให้ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

8.2.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information security requirements analysis and specification)

ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องมีการรวมเข้ากับ ความต้องการสำหรับระบบใหม่หรือการปรับปรุงระบบที่มีอยู่แล้ว

8.2.2 ความมั่นคงปลอดภัยของบริการเทคโนโลยีสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

สารสนเทศที่เกี่ยวข้องกับบริการเทคโนโลยีสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันจากการฉ้อโกงการโต้เถียงและการเปิดเผยและการเปลี่ยนแปลงเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

8.2.3 การป้องกันธุรกรรมของบริการเทคโนโลยีสารสนเทศ (Protecting application services transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการเทคโนโลยีสารสนเทศต้องได้รับการป้องกันจาก การรับส่งข้อมูลที่ไม่สมบูรณ์การส่งข้อมูลผิดเส้นทางการเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาตการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตการส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

8.3 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

วัตถุประสงค์เพื่อให้ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

8.3.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการพัฒนาระบบขององค์กร

8.3.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบต้องมีการควบคุมโดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ

8.3.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบระบบสำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร

8.3.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

การเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปต้องไม่อนุญาตการดำเนินการจำกัดการเปลี่ยนแปลงเท่าที่จำเป็นและต้องมีการควบคุมอย่างรัดกุม

8.3.5 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

องค์กรต้องจัดทำและป้องกันอย่างเหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัยทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

8.3.6 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

องค์กรต้องกำกับดูแลเฝ้าระวังและติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ

8.3.7 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่ระบบอยู่ในช่วงการพัฒนา

8.3.8 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

แผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบต้องมีการจัดทำสำหรับระบบใหม่ระบบที่ปรับปรุงและระบบเวอร์ชั่นใหม่

8.4 ข้อมูลสำหรับการทดทดสอบ (Test data)

วัตถุประสงค์เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

8.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

ข้อมูลสำหรับการทดสอบระบบต้องมีการคัดเลือกอย่างระมัดระวังมีการปองกันและควบคุมการ

นำมาใช้งาน

9. ความสัมพันธ์กับผู้ให้บริการภายนอก
(Supplier relationships)

9.1 วัตถุประสงค์และขอบเขต

เพื่อให้มีการป้องกันสินทรัพย์ของกลุ่มบริษัทนีโอ ที่ผู้ให้บริการภายนอกสามารถเข้าถึงได้ และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

9.2 ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)

วัตถุประสงค์เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

9.2.1 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

ความต้องการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับ การเข้าถึงทรัพย์สินขององค์กรโดยผู้ให้บริการภายนอกต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกและจัดทำเป็นลายลักษณ์อักษร

9.2.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)

ความต้องการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึงการประมวลผลการจัดเก็บการสื่อสารและ การให้บริการโครงสร้างพื้นฐานของระบบสำหรับเทคโนโลยีสารสนเทศขององค์กรโดยผู้ให้บริการภายนอก

9.3 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

9.3.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services)

องค์กรต้องมีการติดตามทบทวนและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

9.3.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)

การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบายขั้นตอนปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการโดยต้องนำระดับความสำคัญของเทคโนโลยีสารสนเทศระบบและกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วยและต้องทบทวนการประเมินความเสี่ยงใหม่

10. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security incident management)

10.1 วัตถุประสงค์และขอบเขต

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทนีโอ ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

10.2 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้ได้รับทราบ

10.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการต้องมีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็วได้ผลและตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

10.2.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Reporting information security events)

สถานการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องมีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

10.2.3 การรายงานจุดอ่อนความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Reporting information security weaknesses)

พนักงานและผู้ที่ทำสัญญาจ้างซึ่งใช้ระบบและบริการเทคโนโลยีสารสนเทศขององค์กรต้องสังเกตและรายงานจุดอ่อนความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศในระบบหรือบริการที่สังเกตพบหรือที่สงสัย

10.2.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Assessment of and decision on information security events)

สถานการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่เหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

10.2.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Response to information security incidents)

เหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

10.2.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Learning from information security incidents)

ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศต้องถูกนำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

10.2.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)

องค์กรต้องกำหนดและประยุกต์ใช้ขั้นตอนปฏิบัติสำหรับการระบุการรวบรวมการจัดหาและการจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐาน

11. การบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ
(Information security-aspects of business continuity management)

11.1 วัตถุประสงค์และขอบเขต

เพื่อป้องกันการหยุดชะงักในการดำเนินงานที่เกิดจากความล้มเหลวหรือระบบหยุดทำงาน และเพื่อจัดเตรียมสภาพความพร้อมใช้งานของข้อมูลและอุปกรณ์ประมวลผลระบบเทคโนโลยีสารสนเทศ โดยครอบคลุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบเทคโนโลยีสารสนเทศ

11.2 ความต่อเนื่องด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information security continuity)

11.2.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Planning information security continuity)

องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้นเช่นในช่วงที่เกิดวิกฤตหรือภัยพิบัติหนึ่ง

11.2.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Implementing information security continuity)

องค์กรต้องกำหนดจัดทำเป็นลายลักษณ์อักษรปฏิบัติและปรับปรุงกระบวนการขั้นตอนปฏิบัติและมาตรการเพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

11.2.3 การตรวจสอบการทบทวนและการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Verify, review and evaluate information security continuity)

องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมการไว้ตามรอบระยะเวลาที่กำหนดไว้เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้องและได้ผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น

11.3 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลเทคโนโลยีสารสนเทศ

11.3.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

12. การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Compliance)

12.1 วัตถุประสงค์และขอบเขต

เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมาย ทรัพย์สินทางปัญญา ที่เกี่ยวข้องกับการดำเนินธุรกิจ พนักงานทุกคนต้องทราบถึงข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศ เป็นการสร้างความตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น รวมทั้งวางมาตรการควบคุมที่เหมาะสมได้เพื่อป้องกันความเสียหายต่อการกระทำความผิดทางกฎหมายต่าง ๆ และสอดคล้องกับนโยบายและวิธีปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกลุ่มบริษัทนีโอ

12.2 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

วัตถุประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมายระเบียบข้อบังคับหรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและที่เป็นความต้องการด้านความมั่นคงปลอดภัย

12.2.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)

ความต้องการทั้งหมดที่เกี่ยวข้องกับกฎหมายระเบียบข้อบังคับและสัญญาจ้างรวมทั้งวิธีการขององค์กรเพื่อให้สอดคล้องกับความต้องการดังกล่าวต้องมีการระบุอย่างชัดเจนจัดทำเป็นลายลักษณ์อักษรและปรับปรุงให้ทันสมัยสำหรับแต่ละระบบและสำหรับองค์กร

12.2.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

ขั้นตอนปฏิบัติที่เหมาะสมต้องได้รับการปฏิบัติอย่างสอดคล้องเพื่อให้มั่นใจว่ามีความสอดคล้องกับความต้องการของกฎหมายระเบียบข้อบังคับและสัญญาจ้างที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์

12.2.3 การป้องกันข้อมูล (Protection of records)

ข้อมูลขององค์กรต้องได้รับการป้องกันจากการสูญหายการถูกทำลายการปลอมแปลงการเข้าถึงโดยไม่ได้รับอนุญาตและการเผยแพร่โดยไม่ได้รับอนุญาตโดยต้องสอดคล้องกับความต้องการของกฎหมายระเบียบข้อบังคับสัญญาจ้างและความต้องการทางธุรกิจ

12.2.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)

ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลต้องมีการดำเนินการให้สอดคล้องกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

12.2.5 ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic

controls)

มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลงกฎหมายและระเบียบข้อบังคับทั้งหมดที่เกี่ยวข้อง

12.3 การทบทวนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information security reviews)

วัตถุประสงค์เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

12.3.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Independent review of information security)

วิธีการในการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการปฏิบัติขององค์กร (กล่าวคือวัตถุประสงค์มาตรการนโยบายกระบวนการและขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ) ต้องมีการทบทวนอย่างอิสระตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงองค์กรที่มากเกิดขึ้น

12.3.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

ผู้จัดการต้องดำเนินการทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลสารสนเทศและขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเองโดยเทียบกับนโยบายมาตรฐานและความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

12.3.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

ระบบต้องได้รับการทบทวนอย่างสม่ำเสมอเพื่อพิจารณาความสอดคล้องกับนโยบายและมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

เอกสารอ้างอิง

1. พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
2. พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
3. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4. พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
5. พ.ร.บ. ข้อมูลข่าวสาร พ.ศ. 2540