



ประกาศบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 มาตรา 5 และมาตรา 7 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ซึ่งเป็นรัฐวิสาหกิจตามพระราชบัญญัติว่าด้วยวิธีการงบประมาณ พ.ศ. 2502 มีหน้าที่ลงทุนก่อสร้างอาคาร บริหารโครงการศูนย์ราชการกรุงเทพมหานคร และบริหารจัดการทรัพย์สินอื่นของรัฐตามนโยบายรัฐบาล ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ และเพื่อให้ระบบเทคโนโลยีดิจิทัล สามารถดำเนินการได้อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย รวมทั้งป้องกันปัญหา และภัยคุกคามต่าง ๆ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) จึงกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีเนื้อหาครอบคลุมตามประกาศ ดังต่อไปนี้

วัตถุประสงค์

1. เพื่อให้เกิดความเชื่อมั่น และความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีดิจิทัลและเครือข่ายคอมพิวเตอร์ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2. เพื่อกำหนดมาตรฐาน นโยบาย และแนวทางปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีดิจิทัลในการดำเนินงาน

3. เพื่อเผยแพร่นโยบายและแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ได้รับทราบ และถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

4. เพื่อให้เกิดการบริหารจัดการความมั่นคงปลอดภัยของระบบเทคโนโลยีดิจิทัล และมีการปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยอย่างต่อเนื่อง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ V 2.0 (ฉบับทบทวนปี 2568)

ขอบเขตการดำเนินงาน

1. การเข้าถึงและการใช้งานสารสนเทศ

- 1.1 การเข้าถึงข้อมูลและการควบคุมการใช้งานสารสนเทศ
- 1.2 การกำหนดประเภทข้อมูล ระดับข้อมูล และระดับชั้นความลับของข้อมูล
- 1.3 ข้อกำหนดการใช้งานตามภารกิจ
- 1.4 การบริหารจัดการการเข้าถึงของผู้ใช้งานระบบสารสนเทศ
- 1.5 การบริหารจัดการ และการใช้งานรหัสผ่าน
- 1.6 การควบคุมสิทธิ์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ที่อยู่ใน ภาวะเสี่ยงต่อการเข้าถึงโดยผู้ที่ไม่ได้สิทธิ
- 1.7 การเข้ารหัสสำหรับข้อมูลที่เป็นความลับ
- 1.8 การควบคุมการเข้าถึงระบบเครือข่าย
 - 1.8.1 การยืนยันตัวบุคคลในการใช้งานเครือข่าย
 - 1.8.2 การป้องกันพอร์ตที่ใช้สำหรับการปรับแต่งระบบ
 - 1.8.3 การควบคุมการเชื่อมต่อเครือข่าย
 - 1.8.4 การควบคุมการจัดเส้นทางบนเครือข่าย
- 1.9 การเข้าถึงระบบปฏิบัติการ
- 1.10 การควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่
- 1.11 การปฏิบัติงานจากภายนอกสำนักงาน
- 1.12 การใช้งานอินเทอร์เน็ต โซเชียลเน็ตเวิร์ก และจดหมายอิเล็กทรอนิกส์
- 1.13 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล
- 1.14 การควบคุมการใช้บริการผู้ให้บริการภายนอก
- 1.15 การจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control)
- 1.16 การจัดการและรักษาความปลอดภัยของดาต้าเซ็นเตอร์
- 1.17 การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศที่สำคัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

- 1.18 การพัฒนาระบบให้มีความมั่นคงปลอดภัย
- 1.19 ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก
- 1.20 การใช้บริการ Cloud Computing
- 2. การสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน
 - 2.1 การสำรองข้อมูล
 - 2.2 การเตรียมความพร้อมกรณีฉุกเฉิน
- 3. การประเมินความเสี่ยง และการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ
 - 3.1 การตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ
 - 3.2 การดำเนินโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศภายในองค์กร

การกำหนดขอบเขตความรับผิดชอบ

แบ่งขอบเขตความรับผิดชอบเป็น 2 ระดับ คือ ระดับนโยบาย และระดับปฏิบัติ ดังต่อไปนี้

1. ระดับนโยบาย

กำหนดให้ผู้บริหารสูงสุด (Managing Director) ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบเทคโนโลยีดิจิทัล หรือข้อมูลสารสนเทศเกิดความเสียหาย หรือผลกระทบแก่องค์กร อันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้อำนวยการอาวุโสฝ่ายดิจิทัล ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด เป็นผู้รับผิดชอบในการสั่งการ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามกำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ และคำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

2. ระดับปฏิบัติ

2.1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ ผู้รับผิดชอบ ได้แก่

- 2.1.1 ฝ่ายดิจิทัล
- 2.1.2 ผู้ดูแลระบบที่ได้รับมอบหมาย
- 2.1.3 เจ้าหน้าที่ที่ได้รับมอบหมาย
- 2.1.4 ผู้ใช้งาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2.2 นโยบายการสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน

2.2.1 ฝ่ายดิจิทัล

2.2.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

2.2.3 เจ้าหน้าที่ที่ได้รับมอบหมาย

2.3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.3.1 ฝ่ายดิจิทัล

2.3.2 ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบจากภายนอก

2.3.3 ผู้ดูแลระบบที่ได้รับมอบหมาย

3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ต้องมีการตรวจสอบ ประเมิน ทบทวน และปรับปรุงนโยบายและแนวปฏิบัติอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ถือเป็นมาตรฐาน โดยอ้างอิงรายละเอียดแนบท้ายประกาศนี้ เพื่อใช้เป็นแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศที่มีความมั่นคง ปลอดภัย และเชื่อถือได้ และเป็นไปตามกฎระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด และผู้ที่เกี่ยวข้อง ต้องถือปฏิบัติตามอย่างเคร่งครัด

การทบทวนนโยบาย : ให้มีการทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง

บทลงโทษ : กรณีผู้บริหาร หรือผู้ปฏิบัติงาน ธพส. ไม่ประพฤติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งก่อให้เกิดผลกระทบต่อบุคคลหรือองค์กร ผู้บริหาร หรือผู้ปฏิบัติงาน ธพส. บุคคลดังกล่าวมีโทษทางวินัยอ้างอิงตามระเบียบข้อบังคับเกี่ยวกับการทำงาน พ.ศ. 2566

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)
คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศนี้ ประกอบด้วย

บริษัท/องค์กร/หน่วยงาน หมายถึง บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ผู้บริหารระดับสูงสุด (Managing Director: MD) หมายถึง ผู้มีอำนาจสูงสุดของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย ตัดสินใจ และแนะนำแนวทางการดำเนินงานของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ฝ่ายดิจิทัล หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุง รักษาระบบเทคโนโลยีสารสนเทศ คอมพิวเตอร์ และเครือข่ายภายใน ธพส.

ผู้อำนวยการอาวุโส ฝ่ายดิจิทัล หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของ ธพส. เป็นผู้มีอำนาจตัดสินใจเกี่ยวกับระบบเทคโนโลยีสารสนเทศ มีบทบาทหน้าที่ และความรับผิดชอบ ในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศคอมพิวเตอร์ และเครือข่าย ของ ธพส.

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือ เป้าหมาย

ผู้ใช้งาน หมายถึง พนักงาน ลูกจ้าง พนักงานจ้างเหมา เจ้าหน้าที่ประจำโครงการต่างๆ ของ ธพส. และบุคคลภายนอก ที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานระบบสารสนเทศ และเครือข่าย ของ ธพส.

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรม คอมพิวเตอร์ หรือข้อมูลอื่นเพื่อการจัดการระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบ คอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

เจ้าหน้าที่ หมายถึง พนักงาน ลูกจ้าง พนักงานจ้างเหมา และเจ้าหน้าที่ประจำโครงการต่างๆ ของ ธพส.

ผู้ให้บริการภายนอก หมายถึง บริษัท หน่วยงาน บุคคลที่รับดำเนินงาน (Outsourcing) ให้กับ ธพส. และได้รับสิทธิการเข้าถึงระบบสารสนเทศ และเครือข่าย ตามที่ ธพส. อนุญาต

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่ ธพส. อนุญาตให้มีสิทธิในการเข้าถึง และใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ ระบบตามอำนาจหน้าที่และ ต้องรับผิดชอบในการรักษาความลับของข้อมูล

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก มาผ่านการประมวลผลให้ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ใน การปฏิบัติงาน บริหาร การวางแผน และการตัดสินใจ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

ระบบเครือข่าย (Network System) หมายถึง คือ กลุ่มของคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่ถูกนำมาเชื่อมต่อกันเพื่อให้ผู้ใช้ในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่างๆ ในเครือข่ายร่วมกันได้

อินเทอร์เน็ต (Internet) หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ ที่มีการเชื่อมต่อระหว่างเครือข่ายหลาย ๆ เครือข่ายทั่วโลกเข้าด้วยกัน โดยใช้โปรโตคอล TCP/IP เป็นมาตรฐานการเชื่อมต่อ

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

ดาต้าเซ็นเตอร์ (Data Center) หมายถึง โครงสร้างพื้นฐานทางกายภาพหรือเสมือนจริง สำหรับจัดวางคอมพิวเตอร์ เซิร์ฟเวอร์ และอุปกรณ์เครือข่าย เพื่อการจัดเก็บ ประมวลผล และให้บริการข้อมูลที่มีความสำคัญแก่องค์กร ทั้งยังเป็นที่อยู่ของอุปกรณ์สำรองข้อมูล และอุปกรณ์รักษาความปลอดภัยบนเครือข่าย

ระบบสารสนเทศที่สำคัญ หมายถึง ระบบบริหารจัดการและวางแผนทรัพยากรองค์กร (SAP-ERP) ระบบบริหารงานบุคคล (HRIS) ระบบสารสนเทศเพื่อสนับสนุนการตัดสินใจของผู้บริหาร (BI) และระบบอนุมัติจัดซื้อจัดจ้าง (i-Process) ที่ใช้งานใน ทรพส.

พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

สินทรัพย์หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารที่มีคุณค่าสำหรับองค์กร

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน
เครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก
ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการ
รับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษร หรืออักขระพิเศษ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการ
ตรวจสอบยืนยันตัว บุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของ
ข้อมูล และระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่ง/โปรแกรมไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์
หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้อง หรือปฏิบัติงานไม่ตรง
ตามคำสั่งที่กำหนดไว้

ล็อก (Logs) หมายถึง รายการลงบันทึก ที่ถูกสร้างโดยอัตโนมัติเมื่อมีการเข้าถึง หรือใช้งาน

เอกสารแนบท้ายประกาศ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท ธนารักษ์พัฒนาสินทรัพย์จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและใช้งานสารสนเทศ

เรื่องที่ 1 การควบคุมการเข้าถึงและใช้งานสารสนเทศ

วัตถุประสงค์

- 1) เพื่อป้องกันการบุกรุกที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงัก
- 2) เพื่อกำหนดมาตรการ การอนุญาต การกำหนดสิทธิ และการมอบอำนาจ ในการเข้าถึงและใช้งานสารสนเทศ
- 3) เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) จัดทำทะเบียนสินทรัพย์ โดยจำแนกเป็นกลุ่มทรัพยากรระบบ การทำงาน และสถานที่เก็บหรือประมวลผล และระบุสิทธิในการเข้าถึงสินทรัพย์นั้น
- 2) กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าใช้งานระบบสารสนเทศ ดังนี้
 - 2.1) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ
 - 2.2) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น
 - 2.3) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้งานโดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ
- 3) ให้มีการกำหนดสิทธิของผู้ใช้งาน ดังนี้
 - 3.1) กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งานแต่ละกลุ่ม ได้แก่
 - 3.1.1) สิทธิอ่านอย่างเดียว
 - 3.1.2) สิทธิการเพิ่มข้อมูล
 - 3.1.3) สิทธิการแก้ไขข้อมูล

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

3.1.4) สิทธิการลบข้อมูล

3.1.5) สิทธิการอนุมัติ/อนุญาต

3.1.6) ไม่มีสิทธิ

3.2) กำหนดการระดับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

3.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย ตามแบบลงทะเบียนผู้ใช้งาน

4) กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ดังนี้

4.1) ผู้ใช้งานจะต้องได้ใบอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

4.2) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

4.3) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้งานโดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ

เอกสารแนบท้ายประกาศ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 2 การกำหนดประเภทข้อมูล ระดับข้อมูล และระดับชั้นความลับของข้อมูล

วัตถุประสงค์

1) เพื่อให้มีความตระหนักถึงความสำคัญของข้อมูล และมีวิธีปฏิบัติที่เหมาะสมในการรักษาความมั่นคงปลอดภัยของข้อมูลแต่ละประเภท ระดับ และชั้นความลับ

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

1) จัดแบ่งประเภทข้อมูลเป็นข้อมูลด้านการบริหาร ข้อมูลด้านการดำเนินงาน และข้อมูลด้านการให้บริการ

1.1) ข้อมูลด้านการบริหาร ได้แก่

- 1.1.1) นโยบาย
- 1.1.2) ข้อมูลยุทธศาสตร์แผน และภารกิจของบริษัท
- 1.1.3) ผลการปฏิบัติงาน
- 1.1.4) กฎหมาย ระเบียบ แนวปฏิบัติ ขั้นตอนปฏิบัติ
- 1.1.5) ข้อมูลบุคลากร
- 1.1.6) งบประมาณ

1.2) ข้อมูลด้านการดำเนินงาน ได้แก่

- 1.2.1) ข้อมูลการเงินและบัญชี
- 1.2.2) ข้อมูลทะเบียนสินทรัพย์
- 1.2.3) ข้อมูลแจ้งซ่อม
- 1.2.4) ข้อมูล Logs
- 1.2.5) ข้อมูลการอนุมัติจัดซื้อจัดจ้าง

1.3) ข้อมูลด้านการให้บริการ ได้แก่

- 1.3.1) ข้อมูลวิชาการและองค์ความรู้
- 1.3.2) ข้อมูลพื้นที่อาคาร
- 1.3.3) ข้อมูลการให้บริการ อื่นๆ

2) การจัดแบ่งระดับชั้นความลับข้อมูลสารสนเทศ ได้แก่

2.1 ลับที่สุด หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากที่สุดต่อการดำเนินงานของบริษัท และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาตจะเกิดความเสียหายแก่บริษัทอย่างร้ายแรงที่สุด

2.2 ลับมาก หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากต่อการดำเนินงานของบริษัทและกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาตจะเกิดความเสียหายแก่บริษัทอย่างร้ายแรง

2.3 ลับ หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่อการดำเนินงานของบริษัท และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่บริษัท

2.4 ใช้ภายใน หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่อการดำเนินงานของบริษัท และเปิดเผยได้เฉพาะภายในบริษัทฯ และบุคคลภายนอกที่มีความสัมพันธ์ทางการค้าเท่านั้น ซึ่งไม่เหมาะที่จะเปิดเผยต่อสาธารณชนเป็นการทั่วไป หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้จะต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานรวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท

2.5 ทั่วไป หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญทั่วไปต่อการดำเนินงานของบริษัท และเป็นข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ อย่างไรก็ดี ข้อมูลสารสนเทศในระดับชั้นนี้จะต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานรวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท

3) จัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภท เป็น 4 ระดับ คือ

3.1) สำคัญมากที่สุด

3.2) สำคัญมาก

3.3) สำคัญ

3.4) ทั่วไป

4) จัดแบ่งระดับชั้นการเข้าถึงข้อมูล คือ

4.1) ระดับชั้นสำหรับผู้บริหาร

4.2) ระดับชั้นสำหรับผู้ใช้ทั่วไป

4.3) ระดับชั้นสำหรับผู้ดูแลระบบ

4.4) ระดับชั้นสำหรับผู้ที่ได้รับมอบหมาย

- 5) ต้องมีวิธีปฏิบัติในการจัดเก็บ และควบคุมการเข้าถึงข้อมูล ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงต้องมีวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- 6) เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- 7) มีวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบมีการกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล
- 8) การรับส่งข้อมูลระดับชั้นความลับ ตั้งแต่ชั้น “ลับ” ขึ้นไปผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ตามนโยบายการเข้าถึงและการใช้งานสารสนเทศ ว่าด้วย การเข้ารหัส สำหรับข้อมูลที่เป็นความลับ
- 9) มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท หรือกรณีส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลและลบข้อมูลสำคัญที่เก็บอยู่ในเครื่องคอมพิวเตอร์ออกก่อน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการทำงานของสารสนเทศ

เรื่องที่ 3 ข้อกำหนดการใช้งานตามภารกิจ

วัตถุประสงค์

- 1) เพื่อควบคุมและป้องกันไม่ให้เกิดการเข้าถึงสารสนเทศโดยผู้ที่ไม่เกี่ยวข้องตามภารกิจ
- 2) เพื่อกำหนดข้อปฏิบัติเพื่อควบคุมการเข้าถึงที่สอดคล้องและเหมาะสมตามภารกิจของผู้ใช้งาน

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

ข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) แบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

- 1) การควบคุมการเข้าถึงสารสนเทศตามภารกิจ
 - 1.1) ติดตั้งโปรแกรมเฉพาะที่เกี่ยวข้องตามภารกิจบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน
 - 1.2) กำหนดสิทธิการเข้าถึงและใช้งานระบบสารสนเทศในฟังก์ชันงานที่เกี่ยวข้องตามภารกิจ
 - 1.3) กำหนดสิทธิการเข้าถึงระดับชั้นข้อมูลตามภารกิจ
 - 1.4) มีการจำกัดระยะเวลาใช้งานระบบเทคโนโลยีสารสนเทศ ตามประเภทภารกิจ
- 2) การปรับปรุงให้สอดคล้องกับข้อกำหนดในการปฏิบัติงานและข้อกำหนดด้านความปลอดภัย
 - 2.1) มีการกำหนดพื้นที่การเข้าดำเนินงานที่สอดคล้องตามภารกิจ
 - 2.2) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงาน
 - 2.3) ทบทวนสิทธิ์ของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิ์เมื่อไม่มีความเกี่ยวข้อง
 - 2.4) การเปลี่ยนรหัสผ่านของผู้ใช้โปรแกรม ให้มีความถี่ที่เหมาะสมตามภารกิจที่เกี่ยวข้องกับ

โปรแกรมอื่น

2.5) การเปลี่ยนรหัสผ่านในการเข้าถึงพื้นที่ทางกายภาพ ให้มีความถี่ที่เหมาะสมกับ
ความสำคัญของพื้นที่ และตามความสำคัญของข้อมูล

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 4 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

- 1) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว
- 2) เพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) ให้มีการสร้างความตระหนัก เรื่องความมั่นคงปลอดภัยสารสนเทศ ดังนี้
 - 1.1) กำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)
 - 1.2) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์
 - 1.3) กำหนดให้มีมาตรการเชิงป้องกันภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศตามความเหมาะสม
- 2) มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้
 - 2.1) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศและให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
 - 2.2) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
 - 2.3) กำหนดชื่อผู้ใช้งาน (Username) จากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น หรือ กำหนดโดยใช้ ID พนักงาน ที่ เป็นเลข หรือ email ที่ไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น
 - 2.4) จัดทำเอกสารที่แสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบตามลำดับชั้นการบริหารงานของ ธพส.
 - 2.5) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการฝ่ายหรือผู้ดูแลระบบที่ได้รับมอบหมาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2.6) ทบทวนสิทธิของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิเมื่อไม่มีความเกี่ยวข้อง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

3) มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

3.1) กำหนดสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ ในฟังก์ชันงานที่เกี่ยวข้องตามภารกิจ

3.2) มีการแยกการกำหนดสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ สำหรับสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่ไม่ใช่สิทธิในการปฏิบัติงานตามปกติ

3.3) ไม่ให้ผู้ดูแลระบบใช้บัญชีผู้ใช้งานที่มีสิทธิในระดับสูง ในการปฏิบัติงานทั่วไป

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 5 การบริหารจัดการ และการใช้งานรหัสผ่าน

วัตถุประสงค์

- 1) เพื่อให้เกิดความรัดกุมในการกำหนดรหัสผ่านในการเข้าถึง และใช้งานสารสนเทศ
- 2) เพื่อให้ผู้ใช้ระมัดระวัง และตระหนักถึงความสำคัญของการบริหารจัดการ และใช้งานรหัสผ่านของตนเองที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- 3) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูล

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่าน ดังนี้
 - 1.1) มีขั้นตอนปฏิบัติสำหรับการตั้ง และเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
 - 1.2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน
 - 1.3) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกัน ในการจัดส่งรหัสผ่าน
 - 1.4) ผู้ใช้งานตอบกลับทันทีหลังจากได้รับรหัสผ่าน ต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และเปลี่ยนให้รหัสผ่านยากต่อการเดา
 - 1.5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (password) ไม่เกิน 90 วันหรือทุกครั้งที่มีการ แจ้งเตือนให้เปลี่ยนรหัสผ่าน
- 2) กำหนดให้มีวิธีปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้
 - 2.1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
 - 2.2) ตั้งรหัสผ่านที่ยากต่อการคาดเดา
 - 2.3) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข เข้าด้วยกัน
 - 2.4) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
 - 2.5) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

- 2.6) เก็บรักษาชื่อผู้ใช้-รหัสผ่านของตนเองไว้เป็นความลับ ไม่แจกจ่ายให้แก่ผู้อื่น และไม่ใช้ชื่อ ผู้ใช้-รหัสผ่านของผู้อื่น
- 2.7) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์
- 2.8) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)
- 2.9) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากความจำเป็นในการปฏิบัติงานหลังจากดำเนินการเรียบร้อยแล้ว ให้เปลี่ยนรหัสผ่านโดยทันที
- 2.10) มีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
- 2.11) ในกรณีที่ผู้ใช้ระบบ Single Sign On ให้หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน
- 2.12) หลีกเลี่ยงการใช้รหัสผ่านเดิม
- 2.13) ผู้ดูแลระบบต้องเปลี่ยนรหัสดีกว่าผู้ใช้งานทั่วไป

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 6 การควบคุมสินทรัพย์สารสนเทศ และการใช้งานระบบคอมพิวเตอร์
ที่อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ์

วัตถุประสงค์

1) เพื่อควบคุม และป้องกันไม่ให้สินทรัพย์สารสนเทศหรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการ เข้าถึง โดยผู้ซึ่งไม่มีสิทธิ์

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

1) กำหนดให้มีข้อปฏิบัติในการป้องกันอุปกรณ์ในขณะที่ไม่ผู้ใช้งานอุปกรณ์ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ดูแล ดังนี้

- 1.1) ต้องล็อกเอาต์ออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน
- 1.2) กำหนดให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้
- 1.3) ต้องล็อกเอาต์ออกจากเครื่องเซิร์ฟเวอร์ อุปกรณ์สำคัญ และเครื่องคอมพิวเตอร์สำคัญ เมื่อไม่ถูกใช้งาน หรือเมื่อปล่อยทิ้งไว้ โดยไม่มีผู้ดูแล
- 1.4) มีการควบคุมพื้นที่ปฏิบัติงาน ให้เข้า-ออกได้เฉพาะผู้ที่มีสิทธิ์ และต้องมีระบบบันทึกการเข้า-ออก
- 1.5) การเข้าพื้นที่ที่ไม่มีสิทธิ์ ต้องได้รับอนุญาต และต้องมีการบันทึกการเข้า-ออก โดยมีผู้ดูแลเท่านั้น

- 2) กำหนดให้มีการจัดการสภาพแวดล้อมทางกายภาพของระบบสารสนเทศ ดังนี้
 - 2.1) จำแนกและกำหนดพื้นที่การใช้งานและระดับ ความสำคัญของระบบเทคโนโลยีสารสนเทศ
 - 2.2) มีระบบป้องกันการบุกรุกติดตั้งครอบคลุมพื้นที่ที่มีความสำคัญ
 - 2.3) มีระบบรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัยดูแลอาคาร และมีการติดตั้งกล้องวงจรปิดเพื่อบันทึกเหตุการณ์ไว้ใช้ในการตรวจสอบภายหลัง
 - 2.4) บุคลากรที่ปฏิบัติงานในพื้นที่ต้องปิดล็อกประตู และหน้าต่างทุกครั้งหลังเลิกงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2.5) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพว่าใช้งานได้ตามปกติอย่างสม่ำเสมอ

3) กำหนดให้มีการควบคุมการเข้าออกพื้นที่ใช้งาน ดังนี้

3.1) จัดทำบันทึกการเข้า-ออกพื้นที่ใช้งานสำหรับ บุคคลภายนอกหรือผู้มาติดต่อ

3.2) มีเจ้าหน้าที่ดูแลบุคคลภายนอกหรือผู้มาติดต่อในพื้นที่ที่มีความสำคัญทุกครั้งจนเสร็จสิ้นภารกิจ

3.3) กรณีบุคคลภายนอกหรือผู้มาติดต่อต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเข้ามาในบริเวณพื้นที่ใช้งาน ต้องบันทึกแบบฟอร์มการเข้า-ออก ในรายการอุปกรณ์ด้วยทุกครั้ง

3.4) มีการควบคุมการเข้าออกสถานที่ตั้งของระบบเทคโนโลยีสารสนเทศอย่างรัดกุม และอนุญาตให้เฉพาะผู้มีสิทธิและความจำเป็นผ่านเข้าถึงพื้นที่ได้ เท่านั้น

3.5) กรณีที่ต้องการนำทรัพย์สินสารสนเทศ ออกจากพื้นที่ใช้งาน ต้องขออนุมัติจากผู้อำนวยการฝ่ายดิจิทัลก่อนทุกครั้ง

3.6) จัดให้มีการทบทวนสิทธิการเข้าถึงพื้นที่ หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

4) กำหนดให้มีการจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดย บุคคลภายนอก (Public Access, Delivery and Loading Areas) ดังนี้

4.1) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.2) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

4.3) จัดพื้นที่หรือบริเวณส่งมอบไว้ต่างๆหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในองค์กร

4.4) ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตราย ก่อนจะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

4.5) ต้องลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขาย หรือผู้ให้บริการภายนอก ให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

5) กำหนดให้มีการจัดวางและป้องกันอุปกรณ์ ดังนี้

5.1) ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของระบบเทคโนโลยีสารสนเทศน้อยที่สุด

5.2) ต้องแยกอุปกรณ์ที่มีความสำคัญเก็บไว้ในที่มีความปลอดภัย

5.3) ไม่นำอาหารและเครื่องดื่ม เข้ามาในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ

5.4) ดำเนินการตรวจสอบ ดูแลสภาพแวดล้อม อุณหภูมิ ความชื้น ภายในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายต่ออุปกรณ์ ภายในบริเวณดังกล่าว

5.5) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรอย่างเพียงพอ ได้แก่ ระบบกระแสไฟฟ้าสำรองและป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการเกิดกระแสไฟฟ้าผิดปกติ ระบบปรับอากาศ ระบบระบายอากาศ และระบบควบคุมความชื้น

5.6) ต้องตรวจสอบหรือทดสอบการทำงานของระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบต่างๆ สามารถทำงานได้ตามปกติ และลดความเสี่ยงจากการทำงานของระบบล้มเหลว

6) กำหนดให้มีการรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่นๆ ดังนี้

6.1) ผู้ใช้งานต้องระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน หรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหาย หรือเสียหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดเชยต่อความเสียหายนั้น

6.2) ผู้ใช้งานต้องเก็บเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลสำคัญไว้ในที่ปลอดภัย เช่น ในตู้หรือ โต๊ะที่สามารถล็อกได้ และแยกเอกสารสำคัญสำหรับทำลายไว้ต่างๆหาก เพื่อความปลอดภัยของทรัพย์สิน

6.3) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

6.4) ต้องไม่ให้ผู้ที่มิได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ และสื่อสารต่างๆ โดยไม่ได้รับอนุญาต

7) กำหนดมาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์ ดังนี้

7.1) ต้องล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนการส่งซ่อมหรือเปลี่ยนอุปกรณ์

7.2) ต้องลบข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำลายหรือจำหน่าย

7.3) ต้องฟอร์แมตฮาร์ดดิสก์และ SSD เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์และ SSD โดย

7.3.1) ใช้วิธีแบบเขียนทับซ้ำจำนวน 1 ครั้ง ตามมาตรฐาน NIST 800-88 สำหรับข้อมูลที่ใช้ภายในและข้อมูลความลับ

7.3.2) เขียนทับซ้ำจำนวน 3 ครั้ง ตามมาตรฐาน DoD 5220.22- M สำหรับข้อมูลที่มีชั้นความลับเป็นลับมาก หรือใช้วิธีการทุบทำลายตามระเบียบที่ ธพส. กำหนด

7.3.3) เขียนทับซ้ำจำนวน 7 ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลลับมากที่สุดหรือใช้วิธีการทุบทำลายตามระเบียบที่ ธพส. กำหนด

7.3.4) ลบข้อมูลการดำเนินงานที่มีอายุตั้งแต่ 5 ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

7.3.5) ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล และเจ้าของข้อมูลในการลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการทำงานของสารสนเทศ

เรื่องที่ 7 การเข้ารหัสสำหรับข้อมูลที่เป็นความลับ

วัตถุประสงค์

- 1) เพื่อให้ข้อมูลและสารสนเทศของ บริษัท ธนารักษ์ พัฒนาสินทรัพย์ จำกัด (ธพส.) มีความมั่นคงปลอดภัย
- 2) เพื่อป้องกันความเสียหายอันเกิดจากการรั่วไหล เปลี่ยนแปลง ทำซ้ำข้อมูล และสารสนเทศที่มีความสำคัญ หรือเป็นความลับ

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทขึ้นความลับทั้งการเข้าถึงโดยตรงและผ่านระบบงานสารสนเทศ
- 2) ผู้ใช้งานกำหนดรหัสผ่านในการเข้าถึงไฟล์ข้อมูลลับ เพื่อป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในคอมพิวเตอร์ที่ใช้งาน
- 3) ต้องมีการเข้ารหัสข้อมูลที่เป็นความลับซึ่งจัดเก็บไว้ในรูปแฟ้มอิเล็กทรอนิกส์ หรือในฐานข้อมูล ด้วยวิธีที่เป็นมาตรฐานสากล
- 4) ผู้ใช้งานต้องนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544
- 5) การรับ-ส่งข้อมูลสำคัญ ข้อมูลที่เป็นความลับผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส ด้วยวิธีที่เป็นมาตรฐานสากลเพื่อความมั่นคงปลอดภัย
- 6) ผู้ใช้งานไม่แชร์ไฟล์ข้อมูลลับบนเครือข่ายเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้
- 7) กำหนดให้ใช้การเข้ารหัสข้อมูลบนระบบเครือข่ายไร้สาย ที่เป็นมาตรฐานสากล เช่น WPA2 WPA-PSK หรือ WPA2-PSK เป็นต้น
- 8) กำหนดให้ใช้ระบบสารสนเทศสำคัญจากภายนอกสำนักงาน (Teleworking) ผ่านช่องทางที่มีการเข้ารหัสที่เป็นมาตรฐานสากล เช่น VPN เพื่อความมั่นคงปลอดภัย
- 9) กำหนดให้ผู้ที่สามารถใช้เครื่องมือวิเคราะห์ข้อมูลการจราจรบนเครือข่ายได้ ต้องได้รับการอนุมัติสิทธิจากผู้อำนวยการอาวุโสฝ่ายดิจิทัลเป็นลายลักษณ์อักษร และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

10) ต้องกำหนดให้มีแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสข้อมูล เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ โดยให้มีการควบคุม กำกับ ติดตามให้ครอบคลุมตลอดทั้งวงจรในการนำกุญแจรหัสลับ ไปใช้งาน ได้แก่ การสร้างกุญแจรหัสลับ การจัดเก็บและดูแลรักษากุญแจรหัสลับ การนำกุญแจรหัสลับไปใช้ การกำหนดอายุของกุญแจรหัสลับ ตลอดจนการทำลายกุญแจรหัสลับเมื่อไม่ได้ใช้งาน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการทำงานของสารสนเทศ

เรื่องที่ 8 การเข้าถึงระบบเครือข่าย

วัตถุประสงค์

- 1) เพื่อให้สามารถ ตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่ใช้งานระบบเครือข่ายขององค์กรได้อย่างถูกต้อง
- 2) เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลและสารสนเทศขององค์กรผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) การยืนยันตัวบุคคลในการใช้งานเครือข่าย
 - 1.1) มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนอนุญาตให้เข้าถึงระบบเครือข่าย ด้วยการใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
 - 1.2) ผู้ใช้งานต้องเข้าสู่ระบบเครือข่ายด้วยชื่อผู้ใช้และรหัสผ่าน ที่ได้รับอนุญาตจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล
 - 1.3) ผู้ใช้งานต้องยืนยันตัวบุคคลเพื่อใช้งานเครือข่ายด้วยชื่อผู้ใช้และรหัสผ่านของตัวเองเท่านั้น หากมีปัญหาในการเข้าถึงระบบเครือข่าย ต้องแจ้งให้ผู้ดูแลระบบ หรือเจ้าหน้าที่ที่ได้รับมอบหมายเพื่อทราบ และแก้ไข
 - 1.4) ผู้ใช้งานที่เป็นเจ้าของชื่อผู้ใช้ ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดจากความเสียหายจากการใช้งานเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น และผู้ใช้งานไม่ได้มอบชื่อผู้ใช้ และรหัสผ่านให้แก่ผู้กระทำความผิด
 - 1.5) กำหนดให้เก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ไว้ในสื่อเก็บข้อมูลอย่างน้อย 90 วัน นับตั้งแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ โดยกำหนดชั้นความลับในการเข้าถึงข้อมูลเป็นลับมาก และมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์การเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
 - 1.6) กำหนดให้มีการบันทึกการเข้า-ออกเครือข่าย และความพยายามเข้าสู่เครือข่ายของผู้ใช้งานไว้อย่างน้อย 90 วัน นับตั้งแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2) การป้องกันพอร์ตที่ใช้สำหรับการปรับแต่งระบบ

2.1) มีการติดตั้งไฟร์วอลล์เพื่อควบคุมการรับส่งข้อมูลระหว่างเครือข่ายขององค์กรกับเครือข่ายภายนอก โดยการปิดพอร์ตที่เข้าสู่ระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน

2.2) การเปิดพอร์ตใดๆ บนเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น

2.3) มีการตรวจสอบและทำรายงานหมายเลขพอร์ตบนเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ที่เปิดให้บริการอย่างน้อยเดือนละครั้ง

2.4) ผู้ใช้งานที่ต้องการใช้พอร์ตของเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ บนเครือข่ายขององค์กรจากเครือข่ายภายนอกจะต้องได้รับการอนุมัติสิทธิจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล โดยมีการระบุระยะเวลาการใช้พอร์ตเป็นกรณีๆ

2.5) มีการกำหนดสิทธิบุคคลในการเข้าออก-ห้องคอมพิวเตอร์แม่ข่าย ห้อง Data Center และห้องระบบเครือข่าย

2.6) การเข้าถึงพอร์ตของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายของ Outsource จะต้องได้รับการอนุมัติสิทธิจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล โดยมีการระบุระยะเวลาการใช้พอร์ตเป็นกรณีๆ

3) การควบคุมการเชื่อมต่อเครือข่าย

3.1) มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจจับการโจมตี และตรวจจับการใช้งานในลักษณะที่ผิดปกติ จากเครือข่ายภายนอก

3.2) ต้องมีการป้องกัน IP Address ภายในระบบเครือข่ายมิให้มองเห็นจากการเชื่อมต่อจากภายนอก

3.3) การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ต้องได้รับอนุมัติสิทธิจากผู้อำนวยการอาวุโสฝ่ายดิจิทัลเป็นกรณีไป

3.4) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายดิจิทัล หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการอาวุโสฝ่ายดิจิทัลเท่านั้น

3.5) กำหนดให้มีการจำกัดช่วงระยะเวลาการเชื่อมต่อเครือข่ายแต่ละครั้งไม่เกิน 8 ชั่วโมง และหากไม่มีการใช้งานนานเกิน 30 นาทีต้องยกเลิกการเชื่อมต่อระบบและมีการพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ ยกเว้นสิทธิของผู้ดูแลระบบ

4) การควบคุมการจัดเส้นทางบนเครือข่าย

4.1) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่าย ได้แก่ Internal Zone, Demilitarized Zone และ External Zone รวมทั้ง อุปกรณ์ต่างๆ หมายเลข IP Address ที่ตั้งของอุปกรณ์ต่างๆ และหมายเลข VLAN ให้เป็นปัจจุบันอยู่เสมอ

4.2) กำหนดการแบ่งพื้นที่และเส้นทางบนเครือข่ายดังต่อไปนี้

4.2.1) Internal Zone เป็นส่วนที่ไม่อนุญาตให้มีการเริ่มการเชื่อมต่อจากเครือข่ายภายนอกโดยกำหนดให้เครื่องคอมพิวเตอร์ลูกข่ายทั้งหมดต้องอยู่ในส่วนนี้

4.2.2) Demilitarized Zone (DMZ) เป็นส่วนที่อนุญาตให้มีการเชื่อมต่อจากเครือข่ายภายนอก (External Zone) และเครือข่ายภายใน (Internal Zone) โดยกำหนดให้เครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดต้องอยู่ในส่วนนี้

4.2.3) External Zone เป็นระบบเครือข่ายภายนอกองค์กร รวมทั้งอินเทอร์เน็ต

4.3) กำหนดให้มีวิธีเพื่อจำกัดและควบคุมเส้นทางบนเครือข่ายตามข้อ 4.2

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

4.4) ระบบทั้งหมดที่จะติดตั้งใหม่ใน Demilitarized Zone จะต้องได้รับการอนุญาตจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล อย่างเป็นลายลักษณ์อักษร

4.5) กำหนดให้มีการรับส่งข้อมูลบนเครือข่ายระหว่าง Internal Zone กับ Demilitarized Zone Internal Zone กับ External Zone และ Demilitarized Zone กับ External Zone ผ่าน Firewall และ IDS/IPS ที่ฝ่ายดิจิทัลกำหนดไว้

4.6) ห้ามไม่ให้ผู้ใช้งานเชื่อมต่ออุปกรณ์คอมพิวเตอร์จากระบบเครือข่ายภายนอกองค์กร (External Zone) กับเครือข่ายภายในองค์กร (Internal Zone และ Demilitarized Zone) ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่มีเหตุผลความจำเป็น และจะต้องได้รับอนุญาตจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล อย่างเป็นลายลักษณ์อักษรแล้ว

4.7) ห้ามผู้ที่ไม่มีสิทธิและหน้าที่กระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์เครือข่าย ได้แก่ Router Switch Firewall IDS/IPS Access Point

4.8) กำหนดให้มีการเชื่อมต่อเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์บนเครือข่าย (Router, Switch, Firewall, IDS/IPS, Access Point) เพื่อบริหารจัดการระบบได้เฉพาะชุดไอพีแอดเดรสที่กำหนดเท่านั้น

4.9) ต้องมีการติดตั้งเส้นทางสำรองสำหรับการเชื่อมต่ออินเทอร์เน็ต เพื่อให้สามารถติดต่อสื่อสารได้อย่างต่อเนื่องในกรณีที่ช่องทางการสื่อสารหลักเกิดความเสียหาย

4.10) กำหนดผู้รับผิดชอบในการปรับปรุง แก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของอุปกรณ์เครือข่าย ได้แก่ Router Switch Firewall IDS/IPS Access Point และมีการทบทวนค่าต่างๆ อย่างสม่ำเสมอ

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการทำงานของสารสนเทศ

เรื่องที่ 9 การเข้าถึงระบบปฏิบัติการ

วัตถุประสงค์

- 1) เพื่อป้องกันความเสียหายของข้อมูลและสารสนเทศ ที่อยู่ในเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์คอมพิวเตอร์ของผู้ใช้งาน
- 2) เพื่อป้องกันการละเมิดข้อมูลและสารสนเทศขององค์กร รวมถึงข้อมูลส่วนบุคคลของผู้อื่น ผ่านการใช้งานอุปกรณ์คอมพิวเตอร์ของผู้ใช้งาน
- 3) เพื่อให้ผู้ใช้ตระหนักถึงการรักษาความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ จากการเข้าถึงระบบปฏิบัติการ

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) Laptop Tablet และ Smart Phone ที่ใช้ในการปฏิบัติงาน
- 2) ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ ตามนโยบายการเข้าถึงและการทำงานของสารสนเทศ ว่าด้วยการบริหารจัดการ และการใช้งานรหัสผ่าน
- 3) ผู้ใช้งานต้องล็อกหน้าจอหรือตั้ง Screen Saver เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) Laptop Tablet และ Smart Phone ที่ใช้ในการปฏิบัติงาน เกินกว่า 30 นาที และเมื่อกลับมาใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน
- 4) ผู้ใช้ต้อง Logoff ออกจากระบบปฏิบัติการหรือปิดเครื่องทันทีเมื่อเลิกใช้งาน
- 5) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นนำรหัสผู้ใช้และรหัสผ่านที่เข้าใช้เครื่องคอมพิวเตอร์ส่วนบุคคล (PC), Laptop และ Smart Phone ไปใช้งาน
- 6) ห้ามมิให้ผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากตรวจพบถือเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- 7) ผู้ดูแลระบบต้อง Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมมัลแวร์ประโยชน์ต่างๆ ให้ทันสมัยเพื่อปิดช่องโหว่ในการโจมตี หรือจากภัยคุกคามอื่นๆ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

8) ผู้ดูแลระบบมีสิทธิในการแจ้งเตือนหากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) Laptop Tablet และ Smart Phone ติดไวรัส หรือมีโปรแกรมชุดคำสั่งไม่พึงประสงค์ และห้ามไม่ให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์ที่พบหรือต้องสงสัยเหล่านั้นกับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายไวรัส หรือโปรแกรมไม่พึงประสงค์ไปยังเครื่องอื่นๆ ในเครือข่าย

9) ไม่อนุญาตให้ผู้ใช้งานทั่วไปเข้าถึงหน้าจอเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) Laptop Tablet และ Smart Phone จากระยะไกล (Remote) ยกเว้นผู้ดูแลระบบ เจ้าหน้าที่ที่ได้รับมอบหมาย หรือผู้ให้บริการภายนอกที่ได้รับมอบหมาย

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 10 การควบคุมอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

วัตถุประสงค์

1) เพื่อป้องกันความเสียหายต่อองค์กรที่อาจเกิดขึ้นจากการใช้งานอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) ฝ่ายดิจิทัล ต้องกำหนดรายการโปรแกรมที่ต้องติดตั้ง และโปรแกรมที่ห้ามติดตั้งลงใน คอมพิวเตอร์แบบพกพาที่จะนำมาใช้ปฏิบัติงานที่เชื่อมต่อกับระบบสารสนเทศและเครือข่ายของ ธพส.
- 2) ผู้ใช้งานต้องตรวจสอบคอมพิวเตอร์แบบพกพาที่นำมาใช้ปฏิบัติงานว่าได้ติดตั้งโปรแกรมตามที่ฝ่ายดิจิทัลกำหนดไว้หรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งผู้ดูแลระบบ หรือเจ้าหน้าที่ที่ได้รับมอบหมาย เพื่อขอรับการติดตั้งก่อนการใช้งาน
- 3) ผู้ใช้งานต้องตรวจสอบคอมพิวเตอร์แบบพกพาที่นำมาใช้ปฏิบัติงานว่าไม่ได้ติดตั้งโปรแกรมที่ห้ามติดตั้งตามที่ฝ่ายดิจิทัลกำหนด
- 4) ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากคอมพิวเตอร์แบบพกพา
- 5) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กร ต้องเป็นโปรแกรมที่ลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น
- 6) หากมีการนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินขององค์กรมาใช้งานกับระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากฝ่ายดิจิทัลก่อนการใช้งาน
- 7) กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์แบบพกพาที่นำมาปฏิบัติงานภายในองค์กร ทั้งที่เป็นทรัพย์สินส่วนตัวและขององค์กร
- 8) ผู้ใช้ต้องมีการสำรองข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์แบบพกพาอย่างสม่ำเสมอ
- 9) ฝ่ายดิจิทัล ต้องจัดเตรียมอุปกรณ์หรือพื้นที่ที่สามารถใช้สำรองข้อมูลออกมาจากเครื่องคอมพิวเตอร์แบบพกพา
- 10) ผู้ใช้ต้องมีการเข้ารหัสข้อมูลสำคัญ และข้อมูลที่เป็นความลับก่อนจะสำรองข้อมูลออกมาจากเครื่องคอมพิวเตอร์แบบพกพา

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 11 การปฏิบัติงานจากภายนอกสำนักงาน

วัตถุประสงค์

- 1) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต รวมทั้งการโจมตีระบบสารสนเทศขององค์กรจากภายนอก
- 2) เพื่อให้เกิดประสิทธิภาพในการตรวจติดตามเหตุการณ์ไม่พึงประสงค์

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) การเข้าสู่เครื่องคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ซึ่งเป็นช่องทางที่มีความเสี่ยงสูงต่อความมั่นคงปลอดภัย ต้องได้รับอนุมัติสิทธิ์จากผู้อำนวยการอาวุโสฝ่ายดิจิทัลทุกครั้ง และเมื่อเลิกใช้งานแล้วต้องยกเลิกสิทธิ์ดังกล่าวทันที
- 2) การเข้าสู่เครื่องคอมพิวเตอร์ขององค์กรจากระยะไกล ต้องมีการจำกัดเวลาในการได้รับสิทธิ์ในการเข้าถึงตามระดับสิทธิ์หรือตามความจำเป็น
- 3) ต้องมีการพิสูจน์ตัวตนก่อนเข้าสู่เครื่องคอมพิวเตอร์ขององค์กรจากระยะไกล
- 4) ไม่อนุญาตให้ครอบครัว หรือผู้อื่น เข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลขององค์กรจากภายนอกสำนักงาน
- 5) มีการอัปเดตซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่ใช้งานจากระยะไกลให้เป็นเวอร์ชันปัจจุบัน
- 6) ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัส หรือป้องกันชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ และอุปกรณ์ที่ใช้เชื่อมต่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกล
- 7) ซอร์สโค้ด และสารสนเทศของ ธพส. ถือเป็นทรัพย์สินทางปัญญา ห้ามมิให้ผู้ปฏิบัติงานจากระยะไกล คัดลอก แก้ไข เผยแพร่ โดยไม่ได้รับอนุญาต

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 12 การใช้งานอินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ และโซเชียลเน็ตเวิร์ก

วัตถุประสงค์

- 1) เพื่อให้ใช้งานอินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ และโซเชียลเน็ตเวิร์ก สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ
- 2) เพื่อให้เกิดความมั่นคงปลอดภัยในการใช้งานอินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ และโซเชียลเน็ตเวิร์ก

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) ไม่ใช้อินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม หรือเว็บไซต์ที่ละเมิดลิขสิทธิ์
- 2) ห้ามเปิดเผยข้อมูลลับรวมทั้งข้อมูลที่ยังไม่ได้ประกาศอย่างเป็นทางการของหน่วยงานผ่านอินเทอร์เน็ต และโซเชียลเน็ตเวิร์ก
- 3) การดาวน์โหลด และการอัปเดตโปรแกรมต่างๆ จากอินเทอร์เน็ตต้องกระทำโดยไม่ละเมิดลิขสิทธิ์
- 4) ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่อรับส่งข้อความ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
- 5) ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กรโดยไม่แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ ในเชิงธุรกิจจากการใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร
- 6) ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Mail Box) ของตนเองทุกวัน
- 7) ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป
- 8) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้
 - 8.1) จดหมายขยะ (Spam Mail)
 - 8.2) จดหมายลูกโซ่ (Chain Letter)
 - 8.3) จดหมายที่ละเมิดสิทธิของบุคคลอื่น
 - 8.4) จดหมายที่มีเนื้อหาขัดต่อศีลธรรม
- 9) ต้องจำกัดผู้รับจดหมายอิเล็กทรอนิกส์ เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

10) ต้องไม่เผยแพร่ข้อความที่ร้ายอันจะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน และบุคคลอื่น

11) ห้ามเผยแพร่ภาพ หรือข้อความใดๆ อันก่อให้เกิดความเสียหายต่อองค์กร รวมทั้งละเมิดสิทธิของบุคคลอื่น ผ่านช่องทางอินเทอร์เน็ต และโซเชียลเน็ตเวิร์ค

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 13 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

วัตถุประสงค์

- 1) เพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล ของผู้ใช้บริการ และบุคลากรของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด
- 2) เพื่อสร้างความมั่นใจในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ให้แก่ผู้ใช้บริการและบุคลากรของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) หน่วยงานต้องจัดเก็บข้อมูลส่วนบุคคลในรูปอิเล็กทรอนิกส์อย่างจำกัดเท่าที่จำเป็นต้องใช้งาน
- 2) หน่วยงานต้องระบุนโยบายการรวบรวมและจัดเก็บข้อมูลส่วนบุคคลในรูปอิเล็กทรอนิกส์ โดยต้องแจ้งให้เจ้าของข้อมูลทราบทุกครั้งที่มีการให้ข้อมูล
- 3) ห้ามหน่วยงานนำข้อมูลส่วนบุคคลไปใช้งานนอกเหนือจากที่ระบุไว้ในวัตถุประสงค์
- 4) ต้องมีการเข้ารหัสข้อมูลส่วนบุคคลซึ่งจัดเก็บไว้ในรูปแฟ้มอิเล็กทรอนิกส์ หรือในฐานข้อมูลด้วยวิธีที่เป็นมาตรฐานสากล และมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์การเข้าถึงข้อมูลเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
- 5) แต่งตั้งผู้รับผิดชอบในการเข้าถึง และแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล
- 6) หน่วยงานต้องไม่จัดเก็บข้อมูลเกี่ยวกับพฤติกรรมทางเพศ ประวัติอาชญากรรม หรือการกระทำความผิดหรือได้รับโทษใด ๆ ประวัติสุขภาพ แหล่งกำเนิดของเผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในทางศาสนา ยกเว้นเพื่อวัตถุประสงค์ในการแพทย์หรือการรักษาพยาบาล และความมั่นคง
- 7) หน่วยงานต้องไม่จัดเก็บข้อมูลที่อาจเป็นผลร้าย หรือทำให้เสียชื่อเสียง หรืออาจก่อให้เกิดการเลือกปฏิบัติโดยไม่เป็นธรรม หรือเกิดความไม่เท่าเทียมกันแก่บุคคลใดๆ
- 8) หน่วยงานต้องไม่เปิดเผยเลขบัตรประจำตัวประชาชนของบุคคลใดๆ ผ่านทางสื่อสาธารณะ

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการทำงานของงานสารสนเทศ

เรื่องที่ 14 การควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก

วัตถุประสงค์

- 1) เพื่อให้เกิดความมั่นคงปลอดภัยแก่ข้อมูลและสารสนเทศจากการปฏิบัติงานโดยผู้ให้บริการภายนอก
- 2) เพื่อสร้างความมั่นใจว่าผู้ให้บริการภายนอกจะปฏิบัติตามข้อตกลงการให้บริการที่ทำไว้กับองค์กร

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อปฏิบัติ

- 1) ต้องกำหนดประเภทของการให้บริการที่ต้องการ ระดับการให้บริการที่พึงประสงค์ และมาตรการความมั่นคงปลอดภัย ไว้ในข้อตกลงการให้บริการ (Service Level Agreement) ให้เป็นส่วนหนึ่งของสัญญาจ้างระหว่าง ธพส. กับผู้ให้บริการภายนอก
- 2) ต้องกำหนดให้มีการวางแผนการถ่ายโอนงานก่อนที่จะมีการถ่ายโอนงานให้กับผู้ให้บริการภายนอก
- 3) ต้องกำหนดให้มีแผนการควบคุมเข้าถึงข้อมูลและระบบงานสำคัญ หรือเป็นความลับขององค์กรจากผู้ให้บริการภายนอก
- 4) กำหนดให้ผู้ให้บริการภายนอกต้องจัดส่งแผนการสร้างความต่อเนื่องในการปฏิบัติงาน เพื่อให้สามารถ ช่วยกู้คืนข้อมูลและสารสนเทศให้กลับมาใช้งานได้อย่างรวดเร็ว หลังจากเกิดเหตุการณ์ขัดข้องจากการเรียกใช้บริการ ผู้ให้บริการภายนอก
- 5) กำหนดให้ผู้ให้บริการภายนอกต้องรายงานเหตุการณ์ความมั่นคงปลอดภัย หรือจุดอ่อนในระบบสารสนเทศที่พบ
- 6) กำหนดให้ผู้ให้บริการภายนอกต้องจัดการ และแก้ไขเหตุการณ์ความมั่นคงปลอดภัย หรือจุดอ่อนที่พบ ซึ่งเกี่ยวข้องกับบริการที่จ้าง
- 7) เมื่อพบว่าผู้ให้บริการภายนอกไม่สามารถให้บริการได้ตามระดับการให้บริการที่ตกลงไว้ ธพส. ต้องกำหนดให้ผู้ให้บริการภายนอกต้องนำเสนอแผนการปรับปรุงตามความจำเป็น
- 8) ต้องควบคุมให้มีการจัดทำข้อตกลงด้านการรักษาความลับของข้อมูล (Non-disclosure agreement - NDA) กับผู้ให้บริการภายนอก รวมทั้งการกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศในขอบเขตงานและเงื่อนไขในการให้บริการ (Service level agreement - SLA)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

9) ต้องกำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่องค์กร ตามที่อ้าง ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัยสารสนเทศ

10) ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสียด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอกที่ให้บริการด้านสารสนเทศ และบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการทำงานของสารสนเทศ

เรื่องที่ 15 การจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control)

วัตถุประสงค์

- 1) เพื่อให้เกิดความต่อเนื่องในการให้บริการสารสนเทศ โดยไม่เกิดการติดขัดจากการพัฒนาหรือปรับปรุงระบบสารสนเทศขององค์กร
- 2) เพื่อป้องกันความเสียหายต่อข้อมูลและสารสนเทศจากการพัฒนาหรือปรับปรุงระบบสารสนเทศ โดยผู้ให้บริการภายนอก หรือโดยบุคลากรของ ธพส. เอง

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้พัฒนาหรือปรับปรุงระบบ

ข้อปฏิบัติ

- 1) กำหนดให้มีแผนการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control) ในเอกสารข้อกำหนดของโครงการ (TOR) หรือในเอกสารโครงการพัฒนาหรือปรับปรุงระบบสารสนเทศ ทั้งจากการจัดจ้างผู้ให้บริการภายนอก หรือเจ้าหน้าที่ของ ธพส. เอง
- 2) แผนการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์อย่างน้อยต้องปฏิบัติตามข้อกำหนดต่อไปนี้
 - 2.1) จะต้องจัดเก็บซอร์สโค้ด เอกสาร รูปภาพ และคลิปวิดีโอ ทั้งหมดที่เกี่ยวข้องกับโครงการพัฒนาหรือปรับปรุงระบบสารสนเทศ ไว้ในระบบการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control System) ที่เป็นที่รู้จักและยอมรับจากผู้พัฒนาซอฟต์แวร์ในภาคเอกชน
 - 2.2) ระบบการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ประเภทซอร์สโค้ด ที่ใช้งานจะต้องสามารถแยก Branch และผสาน Branch ได้
 - 2.3) ในแต่ละ Branch จะต้องสามารถกำหนดสิทธิ์การเข้าใช้งานได้
 - 2.4) ในแต่ละ Branch จะต้องสามารถ Commit และ Rollback ได้
 - 2.5) ระบบที่จัดเก็บไฟล์ประเภทซอร์สโค้ด ต้องเป็นระบบการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์แบบกระจาย (Distributed Version Control System) ซึ่งมีความคล่องตัวกับการพัฒนาด้วยทีมงานขนาดใหญ่
 - 2.6) ระบบที่ใช้เพื่อการจัดเก็บการเปลี่ยนแปลง ต้องสามารถค้นหา และแสดงประวัติการเปลี่ยนแปลงของไฟล์ได้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

- 2.7) กำหนดให้มีการเข้าถึงคลังข้อมูล (Repository) ได้เฉพาะทีมพัฒนาที่เกี่ยวข้องเท่านั้น
- 2.8) ต้องกำหนดลำดับงาน (Work Flow) ของการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ที่

ชัดเจน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 16 การจัดการและรักษาความปลอดภัยของดาต้าเซ็นเตอร์

วัตถุประสงค์

- 1) เพื่อให้เกิดความมั่นคงปลอดภัยต่ออุปกรณ์และระบบงานภายในห้องดาต้าเซ็นเตอร์

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ให้บริการภายนอกของ ธพส. (Outsourcing)

ข้อปฏิบัติ

- 1) ต้องจัดทำทะเบียนสินทรัพย์ในดาต้าเซ็นเตอร์ และระบุสิทธิ์ในการเข้าถึงสินทรัพย์นั้น
- 2) กำหนดให้ผู้เข้าใช้งานดาต้าเซ็นเตอร์ จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล ตามความจำเป็นต่อการเข้าใช้งาน
- 3) ต้องมีการบันทึกเวลาเข้า-ออก ดาต้าเซ็นเตอร์ และระบุภารกิจ ทุกครั้ง
- 4) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงาน
- 5) ทบทวนสิทธิ์ของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิ์เมื่อไม่มีความเกี่ยวข้อง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- 6) ต้องขออนุญาต และจดบันทึกรายละเอียดการนำอุปกรณ์เข้า-ออก จากดาต้าเซ็นเตอร์
- 7) ต้องไม่นำอุปกรณ์ที่อาจจะทำให้เครื่องแม่ข่ายติดโปรแกรมที่ไม่พึงประสงค์ เข้าไปในพื้นที่ดาต้าเซ็นเตอร์
- 8) ต้องล็อกเอาต์จากอุปกรณ์และเครื่องคอมพิวเตอร์ เมื่อไม่ได้ถูกใช้งานหรือเมื่อต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว
- 9) กำหนดให้มีการจัดการสภาพแวดล้อมทางกายภาพ ดังนี้
 - 9.1) กำหนดพื้นที่การเข้าถึงอุปกรณ์ตามระดับความสำคัญของระบบงาน
 - 9.2) มีระบบรักษาความปลอดภัยทางกายภาพป้องกันการบุกรุก ติดตั้งครอบคลุมพื้นที่ของดาต้าเซ็นเตอร์
 - 9.3) บุคลากรที่เข้าปฏิบัติงานในพื้นที่ต้องปิดล็อกประตู ทุกครั้งหลังเลิกงาน
 - 9.4) ดำเนินการทดสอบรักษาความปลอดภัยทางกายภาพอย่างสม่ำเสมอ เพื่อให้ใช้งานได้ตามปกติ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

- 10) กำหนดให้มีการจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดย บุคคลภายนอก (Public Access, Delivery and Loading Areas) ดังนี้
- 10.1) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น
 - 10.2) บุคคลภายนอกที่ได้รับอนุญาตให้เข้าปฏิบัติงานในดาต้าเซ็นเตอร์ ต้องแลกบัตรประจำตัวที่บริเวณทางเข้า-ออกอาคาร และลงบันทึกการเข้าปฏิบัติงานในดาต้าเซ็นเตอร์ทุกครั้ง
 - 10.3) ต้องตรวจสอบวัสดุหรือส่วนประกอบในการผลิตที่เป็นอันตราย ก่อนจะโอนย้ายวัสดุ นั้นไปยังพื้นที่ที่มีการใช้งาน
 - 10.4) ต้องลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขาย หรือผู้ให้บริการภายนอก ให้ สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร
- 11) กำหนดให้มีการจัดวางและป้องกันอุปกรณ์ไว้ในพื้นที่หรือบริเวณที่เหมาะสม
 - 12) การนำสิ่งของ หรืออุปกรณ์เข้าภายในดาต้าเซ็นเตอร์ ต้องได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร จากผู้อำนวยการอาวุโสฝ่ายดิจิทัลทุกครั้ง
 - 13) ไม่นำอาหารและเครื่องดื่ม เข้ามาในบริเวณพื้นที่ดาต้าเซ็นเตอร์
 - 14) ดำเนินการตรวจสอบ ดูแลสภาพแวดล้อม อุณหภูมิ ความชื้น อย่างสม่ำเสมอทุกๆ เดือนภายใน บริเวณพื้นที่ของดาต้าเซ็นเตอร์ เพื่อป้องกันความเสียหายต่ออุปกรณ์ต่างๆ
 - 15) มีการระบุชนิดของงาน และภารกิจ ที่ไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล
 - 16) การเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายภายในดาต้าเซ็นเตอร์จากระยะไกล (Remote Access) ต้อง ได้รับอนุมัติสิทธิจากผู้อำนวยการอาวุโสฝ่ายดิจิทัลทุกครั้งตามภารกิจ และระยะเวลาที่กำหนด
 - 17) ไม่อนุญาตให้มีการลบ Logs การบันทึกเข้า-ออก Logs ของเครื่องแม่ข่าย และ Logs ของอุปกรณ์ ใน ห้องดาต้าเซ็นเตอร์ ยกเว้นการลบตามระยะเวลาที่กำหนด หรือลบโดยผู้ที่รับผิดชอบ
 - 18) หากมีการละเมิดข้อปฏิบัติในข้อ (2) (3) (6) (7) (9.3) (12) (16) หรือ (17) ให้มีการตั้งคณะกรรมการ ภายใน เพื่อสอบสวนความผิด

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและใช้งานสารสนเทศ

เรื่องที่ 17 การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศที่สำคัญ

วัตถุประสงค์

- 1) เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศที่สำคัญของบริษัท ธนารักษ์ พัฒนาสินทรัพย์ จำกัด และป้องกันการบุกรุกที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศที่สำคัญให้หยุดชะงัก
- 2) เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบสารสนเทศที่สำคัญของบริษัท ธนารักษ์ พัฒนาสินทรัพย์ จำกัด ได้อย่างถูกต้อง
- 3) เพื่อกำหนดมาตรการ การอนุญาต การกำหนดสิทธิ์ และการมอบอำนาจ ในการเข้าถึงและใช้งานสารสนเทศที่สำคัญ

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

เพื่อให้เกิดการควบคุมการเข้าถึงและใช้งานสารสนเทศให้มีความมั่นคงปลอดภัย กำหนดให้มีข้อปฏิบัติดังนี้

- 1) จัดทำทะเบียนสินทรัพย์ โดยจำแนกกลุ่มทรัพยากรระบบ การทำงาน และสถานที่เก็บหรือประมวลผล โดยระบุสิทธิ์ในการเข้าถึงสินทรัพย์นั้น
- 2) กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศสำคัญ ดังนี้
 - 2.1) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน
 - 2.2) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะ ในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น
 - 2.3) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้งานโดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ ERP-SAP, ระบบสารสนเทศเพื่อสนับสนุนการตัดสินใจของผู้บริหาร (BI) และกำหนดให้มีการลงนามอนุมัติ
- 3) ให้มีการกำหนดสิทธิ์ของผู้ใช้งาน ดังนี้
 - 3.1) กำหนดสิทธิ์ผู้ใช้งานแต่ละคนในการเข้าถึงข้อมูล ตามกลุ่มงานหรือภาระหน้าที่ที่ผู้ใช้งานรับผิดชอบ
 - 3.2) กำหนดการระงับสิทธิ์ การมอบอำนาจ เป็นลายลักษณ์อักษร

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

3.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย ตามแบบลงทะเบียนผู้ใช้งาน

4) ให้มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) ดังนี้

- 4.1) กำหนดสิทธิการเข้าถึงและใช้งานระบบสารสนเทศในฟังก์ชันงานที่เกี่ยวข้องตามภารกิจ
- 4.2) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงาน
- 4.3) ทบทวนสิทธิ์ของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิ์เมื่อไม่มีความเกี่ยวข้อง
- 4.4) ในกรณีมีความจำเป็นต้องให้สิทธิ์สูงสุดกับผู้ใช้งาน ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน
- 4.5) สิทธิ์สูงสุดสำหรับผู้ใช้งาน ต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาที่ขออนุญาต หรือพ้นจากตำแหน่ง
- 4.6) กรณีที่มีการกำหนดสิทธิพิเศษ ต้องกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้ชื่อผู้ใช้งานต่างจากชื่อผู้ใช้งานตามปกติ

5) ให้มีข้อกำหนดเกี่ยวกับการบริหารจัดการผู้ใช้งาน ดังนี้

5.1) การกำหนดชื่อผู้ใช้งาน (username) กำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น หรือ กำหนดโดยใช้ ID พนักงาน ที่เป็นเลข หรือ email ที่ไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

5.2) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบตามลำดับชั้นการบริหารงานของ ธพส.

5.3) มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) ตาม 41 ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

6) กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่าน ดังนี้

- 6.1) มีขั้นตอนปฏิบัติสำหรับการตั้ง และเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
- 6.2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน
- 6.3) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการให้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกัน ในการจัดส่งรหัสผ่าน
- 6.4) ผู้ใช้งานตอบกลับทันทีหลังจากได้รับรหัสผ่าน ต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และเปลี่ยนให้รหัสผ่านยากต่อการเดา
- 6.5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (password) ไม่เกิน 90 วันหรือทุกครั้งที่มีการ แจ้งเตือนให้เปลี่ยนรหัสผ่าน

7) กำหนดให้มีวิธีปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

- 7.1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
- 7.2) ตั้งรหัสผ่านที่ยากต่อการคาดเดา
- 7.3) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข เข้าด้วยกัน
- 7.4) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

- 7.5) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน
- 7.6) เก็บรักษาชื่อผู้ใช้-รหัสผ่านของตนเองไว้เป็นความลับ ไม่แจกจ่ายให้แก่ผู้อื่น และไม่ใช้ชื่อผู้ใช้รหัสผ่านของผู้อื่น
- 7.7) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์
- 7.8) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)
- 7.9) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากความจำเป็นในการปฏิบัติงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้เปลี่ยนรหัสผ่านโดยทันที
- 7.10) มีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
- 7.11) ในกรณีที่ผู้ใช้ระบบ Single Sign On ให้หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน
- 7.12) หลีกเลี่ยงการใช้รหัสผ่านเดิม
- 7.13) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถัดจากผู้ใช้งานทั่วไป
- 8) กำหนดให้ระบบงานต้องมีการล็อกเอาต์อัตโนมัติ (Session Time-out) เมื่อผู้ใช้งานไม่ได้ใช้งาน
- 9) ไม่อนุญาตให้มีการลบ Logs การเข้า-ออกระบบ และการใช้งาน ระบบสารสนเทศที่สำคัญ ยกเว้นการลบตามระยะเวลาที่กำหนด หรือลบโดยผู้ที่รับผิดชอบ
- 10) หากมีการละเมิดข้อปฏิบัติในข้อ (2) (3.3) (7.6) (7.10) หรือ (9) ให้มีการตั้งคณะกรรมการภายในเพื่อสอบสวนความผิด
- 11) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้
- 11.1) ต้องกำหนดมาตรการป้องกันสินทรัพย์ขององค์กรให้ครอบคลุมเรื่องต่าง ๆ โดยควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น การจัดการบริเวณล้อมรอบ การควบคุมการเข้า-ออก การจัดการบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก การวางอุปกรณ์ ระบบ และอุปกรณ์สนับสนุนการทำงาน เป็นต้น
- 11.2) การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้
- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
 - กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
 - วัฒนธรรมองค์กร
- 11.3) ต้องกำหนดให้มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน และต้องกำหนดให้ผู้ใช้งาน ออกจากระบบโดยทันทีเมื่อเสร็จสิ้นงาน

11.4) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ผู้ใช้งานต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันสินทรัพย์ขององค์กร
- ผู้ใช้งานต้องลงชื่อออกจากระบบทันที เมื่อไม่ได้ใช้งาน หรือจำเป็นต้องปล่อยทิ้งโดยไม่มี

ผู้ดูแล

- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัยที่สามารถควบคุมการเข้าถึงได้
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต เช่น กล้องดิจิทัล โทรศัพท์มือถือ

เครื่องถ่ายเอกสาร เครื่องสแกนเอกสาร เป็นต้น

- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

11.5) มีมาตรการทำลายสื่อบันทึกข้อมูล และข้อมูลอิเล็กทรอนิกส์ ดังนี้

- ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรืออุปกรณ์บันทึกข้อมูลอื่นโดยการฟอร์แมตอุปกรณ์ดังกล่าวด้วยวิธีการที่ไม่ให้สามารถเรียกข้อมูลคืนกลับมาใหม่ได้ ก่อนทำการเปลี่ยน ทดแทนทำลาย หรือจำหน่าย หากไม่ต้องการนำกลับมาใช้งานซ้ำอีก ให้ใช้วิธีการทุบทำลาย

- การทำลายสื่อบันทึกข้อมูลที่จัดเก็บข้อมูลแต่ละระดับชั้นความลับให้ดำเนินการตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับ การระบุชั้นความลับ และการจัดการกับระบบสารสนเทศ โดยระดับชั้นความลับขึ้นไปต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายอุปกรณ์บันทึกข้อมูล

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 18 ความสัมพันธ์กับผู้ให้บริการภายนอก

วัตถุประสงค์

- 1) เพื่อบริหารจัดการความสัมพันธ์กับผู้ให้บริการภายนอก เช่น เงื่อนไขที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอกการประเมินผลผู้ให้บริการภายนอก
- 2) เพื่อให้มั่นใจว่าทรัพย์สินขององค์กรที่สามารถเข้าถึงได้โดยหน่วยงานภายนอกได้รับการป้องกันอย่างเหมาะสม
- 3) เพื่อจัดทำและรักษาระดับความปลอดภัยของการปฏิบัติงานของหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่กำหนด

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) ความปลอดภัยข้อมูลกับความสัมพันธ์ของผู้ให้บริการ (Information security in supplier relationships)
 - 1.1) นโยบายความปลอดภัยข้อมูลสำหรับความสัมพันธ์ของผู้ให้บริการ (Information security policy for supplier relationships)
 - 1.1.1) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและเจ้าของข้อมูลสารสนเทศ ต้องประเมินความเสี่ยงและกำหนดข้อตกลงในการรักษาความมั่นคงปลอดภัยสารสนเทศ ก่อนอนุญาตให้บุคคลหรือหน่วยงานภายนอกเข้าถึงข้อมูลสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กรโดยการประเมินความเสี่ยงควรครอบคลุมถึงประเด็นดังต่อไปนี้เป็นอย่างน้อย
 - ประเภทของทรัพย์สินสารสนเทศ
 - ระดับชั้นความลับของข้อมูลสารสนเทศ
 - การควบคุมเพื่อป้องกันข้อมูลสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
 - ขั้นตอนการปฏิบัติงานเมื่อเกิดเหตุการณ์ผิดปกติด้านความปลอดภัยสารสนเทศ
 - ภัยคุกคามที่อาจเกิดขึ้นได้กับทรัพย์สินสารสนเทศและผลกระทบที่เกิดขึ้นกับ

องค์กร

1.2) การระบุข้อกำหนดด้านความปลอดภัยในข้อตกลงกับผู้ให้บริการ (Addressing security within supplier agreements)

1.2.1) เจ้าของข้อมูลสารสนเทศหรือระบบสารสนเทศ ต้องระบุความต้องการการรักษาความมั่นคงปลอดภัยสารสนเทศ ให้ผู้ให้บริการที่ต้องการใช้ทรัพยากรสารสนเทศขององค์กร

1.2.2) หน่วยงานที่รับผิดชอบด้านกฎหมาย ต้องจัดทำข้อตกลงหรือสัญญาซึ่งระบุข้อกำหนดฯ ระหว่างองค์กรและผู้ให้บริการภายนอก ก่อนอนุญาตให้เข้าถึงข้อมูลสารสนเทศหรือทรัพยากรสารสนเทศขององค์กรตั้งแต่รับขอบเขตงานของผู้ว่าจ้าง (Term of Reference) ให้ครอบคลุมถึงก่อนลงนามในสัญญาจัดจ้าง

1.2.3) หน่วยงานที่รับผิดชอบด้านการจัดจ้างงานด้านสารสนเทศ ต้องแนบสำเนาสัญญาการไม่เปิดเผยความลับในข้อกำหนดว่าจ้าง เพื่อให้บริษัทที่สนใจเข้าร่วมเสนองาน ประมูลตามระเบียบกระทรวงการคลัง พิจารณาและลงนามในสัญญาการไม่เปิดเผยความลับเมื่อนำเสนอข้อเสนอเสนองานตามข้อกำหนดขององค์กรตั้งแต่รับขอบเขตงานของผู้ว่าจ้าง (Term of Reference) ให้ครอบคลุมถึงก่อนลงนามในสัญญาจัดจ้าง

1.2.4) เจ้าของข้อมูลสารสนเทศ ต้องจัดให้บุคคลหรือหน่วยงานภายนอกลงนามในสัญญาการไม่เปิดเผยความลับก่อนการใช้ข้อมูลสารสนเทศ ในกรณีที่ข้อมูลที่ต้องการเข้าถึงจัดอยู่ในระดับข้อมูลใช้ภายในขึ้นไป

1.2.5) เจ้าของข้อมูลสารสนเทศ ต้องกำกับการนำข้อมูลสารสนเทศและสื่อเก็บข้อมูลที่จัดอยู่ในระดับข้อมูลใช้ภายในขึ้นไปที่จะนำออกจากองค์กร โดยบุคคลหรือหน่วยงานภายนอกให้เป็นไปอย่างเหมาะสม

1.2.6) หน่วยงานที่จ้างบุคคลหรือหน่วยงานภายนอก ต้องติดตามตรวจสอบ และประเมินผลการดำเนินงานของหน่วยงานภายนอกตลอดอายุสัญญาการบริการ

1.2.7) องค์กรไม่ยินยอมให้ผู้ให้บริการภายนอกมีสิทธิในการเข้าถึงระบบสารสนเทศ ผ่านทางระบบโทรศัพท์ (Dial-up) เครือข่ายอินเทอร์เน็ต หรือเครือข่ายเสมือนส่วนตัว (VPN) จนกว่าเจ้าของข้อมูลสารสนเทศ และผู้ควบคุมดูแลระบบสารสนเทศจะพิจารณาเห็นชอบว่าหน่วยงานภายนอกนั้นมีสิทธิโดยชอบด้วยกฎหมายตามความต้องการของธุรกิจ โดยมีเงื่อนไขจะต้องพิจารณาเป็นกรณีไป และมีการกำหนดช่วงเวลาสำหรับสิทธิอื่นๆ

1.3 การบริหารจัดการความเปลี่ยนแปลงของบริการของผู้ให้บริการ (Managing changes to supplier services)

1.3.1) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบสารสนเทศ ต้องพัฒนาระบบยืนยันตัวตนอีกครั้ง (Two-Factor Authentication) ก่อนดำเนินการทำธุรกรรมที่สำคัญ

1.3.2) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบและหน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ ต้องควบคุมการรับส่งข้อมูลสารสนเทศ เพื่อป้องกันไม่ให้เกิด

- ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
- การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
- การเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- การเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- การทำสำเนาข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยไม่ได้รับอนุญาต

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

1.3.3) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ หน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ และหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องให้มีกลไกการตรวจสอบที่สามารถยืนยันตัวตนผ่านระบบสารสนเทศ เพื่อยืนยันว่าเป็นผู้ดำเนินการจริง ซึ่งไม่สามารถปฏิเสธความรับผิดชอบนั้นได้ (Non repudiation)

2) ความปลอดภัยในกระบวนการพัฒนาและการสนับสนุน (Security in development and support process)

2.1) การกำกับดูแลและสอบทานการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)

2.1.1) เจ้าของข้อมูลหรือระบบสารสนเทศต้องประเมินผลการให้บริการของหน่วยงานภายนอกที่เกี่ยวข้องในหน่วยงาน

2.1.2) หน่วยงานที่รับผิดชอบการจัดจ้างงานด้านสารสนเทศ ต้องตรวจสอบการให้บริการของบุคคลหรือหน่วยงานภายนอก เพื่อให้มั่นใจว่าได้ปฏิบัติตามข้อกำหนดหรือข้อตกลงการรักษาความปลอดภัยสารสนเทศที่กำหนด

2.1.3) หน่วยงานผู้ดูแลระบบและอุปกรณ์ ต้องรวบรวมผลการประเมินการให้บริการของผู้ให้บริการแต่ละราย

2.2) การบริหารจัดการความเปลี่ยนแปลงในการให้บริการ (Managing changes to supplier services)

2.2.1) หน่วยงานผู้ดูแลระบบและอุปกรณ์ ต้องพิจารณาทบทวนเงื่อนไขการให้บริการ เมื่อองค์กร บุคคลหรือหน่วยงานภายนอกมีการเปลี่ยนแปลงที่สำคัญที่อาจมีผลกระทบต่อระบบสารสนเทศหรือกระบวนการที่เกี่ยวข้องกับการให้บริการ

2.2.2) หน่วยงานผู้ดูแลระบบและอุปกรณ์ ต้องควบคุม กำกับให้มีการดูแลให้ องค์กร บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่จ้างปฏิบัติตามสัญญาหรือข้อตกลง ให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 19 การพัฒนาระบบให้มีความมั่นคงปลอดภัย

วัตถุประสงค์

- 1) เพื่อให้มั่นใจว่ามีการระบุข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เหมาะสมต่อระบบงาน ตั้งแต่เริ่มต้นจัดหาหรือพัฒนาระบบ
- 2) เพื่อให้มั่นใจว่าระบบงานและข้อมูลสารสนเทศได้รับการควบคุมและดูแลอย่างเหมาะสม
- 3) เพื่อให้มั่นใจว่าข้อมูลที่ใช้ในการทดสอบได้รับการปกป้อง

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

- 1) ข้อกำหนดด้านความปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)
 - 1.1) การวิเคราะห์และการระบุข้อกำหนดทางด้านความปลอดภัย (Security requirements analysis and specification)
 - 1.1.1) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องกำหนดความต้องการด้านความปลอดภัยสารสนเทศในขอบเขตงานของผู้ว่าจ้าง (Term of Reference)
 - 1.1.2) คณะกรรมการตรวจรับงาน ต้องกลั่นกรองขอบเขตงานของผู้ว่าจ้าง (Term of Reference) เพื่อให้มั่นใจว่ามีการกำหนดความต้องการด้านความปลอดภัยสารสนเทศในรายละเอียดสำหรับระบบสารสนเทศ
 - 1.1.3) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องประเมินวิเคราะห์ และรายงานผลการปฏิบัติงานการกำหนดความต้องการด้านความปลอดภัยสารสนเทศ โครงการต่างๆ ตามความเหมาะสม
 - 1.1.4) องค์กรจะต้องเลือกใช้ผลิตภัณฑ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ได้รับการทดสอบ อย่างเป็นทางการมากกว่าผลิตภัณฑ์ที่ไม่ได้รับการทดสอบ

1.2) ความปลอดภัยในใช้บริการแอปพลิเคชันบนเครือข่ายสาธารณะ (Securing application services on public networks)

1.2.1) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องทดสอบความปลอดภัยระบบสารสนเทศก่อนนำระบบจริง (Production) ของแอปพลิเคชันขึ้นใช้งานผ่านเครือข่ายสาธารณะ

1.2.2) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องสื่อสารและสร้างความเข้าใจเรื่องพัฒนาระบบ แอปพลิเคชันบนเครือข่ายสาธารณะ ให้มีความปลอดภัย โดยอ้างอิงมาตรฐานสากลหรือมาตรฐานอุตสาหกรรม

1.2.3) ข้อมูลของผู้ใช้งานระบบ จะต้องได้รับการป้องกันอย่างเหมาะสมหากมีการเก็บข้อมูลเหล่านี้ไว้ในสารสนเทศซึ่งสามารถเข้าถึงได้ทางระบบเครือข่ายอินเทอร์เน็ต

1.3) การป้องกันธุรกรรมของบริการบนแอปพลิเคชัน (Protecting application services transactions)

1.3.1) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบสารสนเทศ ต้องพัฒนาระบบให้มีการยืนยันตัวตน

1.3.2) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบและหน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ ต้องควบคุมการรับส่งข้อมูลสารสนเทศ เพื่อป้องกันไม่ให้เกิด

- ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
- การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
- การเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- การเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- การทำสำเนาข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยไม่ได้รับอนุญาต

1.3.3) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ หน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ และหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องจัดให้มีกลไกการตรวจสอบที่สามารถยืนยันตัวตนผ่านระบบสารสนเทศ เพื่อยืนยันว่าเป็นผู้ดำเนินการจริง ซึ่งไม่สามารถปฏิเสธความรับผิดชอบนั้นได้ (Non repudiation)

2) ความปลอดภัยในกระบวนการพัฒนาและการสนับสนุน (Security in development and support process)

2.1) นโยบายการพัฒนาระบบอย่างปลอดภัย (Secure development policy)

2.1.1) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องกำหนดวิธีการพัฒนาระบบสารสนเทศให้มีความปลอดภัย ให้ครอบคลุมด้านระบบและแอปพลิเคชัน โดยต้องสอดคล้องแนวปฏิบัติของกฎหมาย และหน่วยงานควบคุม

2.2) ขั้นตอนการปฏิบัติงานสำหรับการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบงาน (System change control procedures)

2.2.1) ผู้จัดการการเปลี่ยนแปลง ต้องกำหนดกำหนดวิธีการในการขอเปลี่ยนแปลงสำหรับการแก้ไขระบบงาน ซึ่งควรครอบคลุมการประเมินความเสี่ยง การวิเคราะห์ผลกระทบและความต้องการในการรักษาความปลอดภัยที่จำเป็น โดยมีแนวทางดังต่อไปนี้

- การปรับปรุงแก้ไขระบบงานต่างๆ ต้องจัดทำเป็นเอกสาร และต้องได้รับอนุมัติโดยเจ้าของสารสนเทศหรือระบบสารสนเทศ

- เอกสารการเปลี่ยนแปลงระบบงาน ควรระบุถึง
- รายละเอียดของระบบที่จะต้องเปลี่ยนแปลง
- การป้องกันผลกระทบที่อาจเกิดขึ้นกับการทำงาน
- การสำรองข้อมูลก่อนการปรับปรุงแก้ไขหรือบำรุงรักษาระบบ
- การจัดทำบันทึกประกอบการเปลี่ยนแปลง และเพื่อการตรวจสอบการแก้ไข

(Audit Trail)

- การควบคุมเวอร์ชันของซอฟต์แวร์ที่เปลี่ยนแปลง

2.3) การตรวจสอบการทำงานของระบบงานภายหลังการเปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)

2.3.1) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ และ หน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ จะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบที่อาจเกิดขึ้นเมื่อต้องการที่จะเปลี่ยนแปลงหรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชัน และการแก้ไขข้อบกพร่องด้านความปลอดภัย เป็นต้น โดยจะต้องมีการทดสอบบนเครื่องทดสอบ (Test Environment) จนมั่นใจว่าระบบงานต่างๆ ที่ประมวลผลบนเครื่องดังกล่าวสามารถทำงานได้ตามปกติ จึงจะทำการเปลี่ยนแปลงหรือปรับปรุงบนเครื่อง สภาพการณ์ที่ใช้งานจริง (Production Environment)

2.3.2) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ และ หน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ ต้องทบทวนและทดสอบการทำงานของระบบงานที่มีความสำคัญภายหลังการเปลี่ยนแปลงระบบทุกครั้ง และแจ้งการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องทราบและทดสอบ เพื่อให้มั่นใจว่าไม่มีผลกระทบต่อการดำเนินงานทางธุรกิจและความปลอดภัยของระบบสารสนเทศ

2.4) การเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

2.4.1) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ ต้องทบทวนและทดสอบการทำงานของระบบงานซอฟต์แวร์สำเร็จรูป ที่มีความสำคัญภายหลังการเปลี่ยนแปลงระบบปฏิบัติการทุกครั้ง และแจ้งการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องทราบและทดสอบ เพื่อให้มั่นใจว่าไม่มีผลกระทบต่อการดำเนินงานทางธุรกิจและความปลอดภัยของระบบสารสนเทศ

2.4.2) หน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ ต้องหมั่นตรวจสอบเช็ครุ่นซอฟต์แวร์สำเร็จรูปให้มีความปลอดภัยอยู่เสมอ หากมีการยกเลิกสายการผลิตให้รวบรวมและรายงานต่อคณะกรรมการบริหารความเสี่ยง

2.5) หลักปฏิบัติวิศวกรรมระบบด้านความปลอดภัยสารสนเทศ (Secure system engineering principles)

2.5.1) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ ต้องได้รับการศึกษาอบรมทางด้านความปลอดภัยสารสนเทศอย่างสม่ำเสมอให้เท่าทันเทคโนโลยีที่ก้าวหน้า เพื่อมาประยุกต์ใช้เพื่อรักษาความปลอดภัยสารสนเทศขององค์กร และต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้

- การให้สิทธิต่ำที่สุด (least privilege) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
- การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (need to know) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
- การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (defense in-depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การออกแบบในลักษณะเปิด (open design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (algorithm) ที่เป็นมาตรฐานและสามารถตรวจสอบการทำงานได้

2.6) ความปลอดภัยของสภาพแวดล้อมในการพัฒนาระบบ (Secure development environment)

2.6.1) หน่วยงานที่รับผิดชอบด้านวิศวกรรมระบบสารสนเทศ ต้องออกแบบ และควบคุมระบบงานทดสอบ (UAT environment) ให้มีความปลอดภัยเทียบเท่าระบบงานจริง (Production environment) ตามความเหมาะสม

2.7) การพัฒนาซอฟต์แวร์ที่ดำเนินการโดยหน่วยงานภายนอก (Outsourced software development)

2.7.1) หน่วยงานที่รับผิดชอบว่าจ้างหน่วยงานภายนอกด้านสารสนเทศ ต้องกำหนดความต้องการด้านความปลอดภัยให้หน่วยงานภายนอกปฏิบัติตาม โดยมีแนวทางดังนี้

- กำหนดเรื่องสิทธิบัตรหรือลิขสิทธิ์ความเป็นเจ้าของซอฟต์แวร์ และสิทธิความเป็นเจ้าของในซอร์สโค้ดของโปรแกรม ลงในข้อตกลงหรือสัญญาให้ชัดเจน
- กำหนดสัญญาหรือข้อตกลงด้านความปลอดภัยในการพัฒนาโปรแกรม อาทิ การไม่เขียนโปรแกรมแอบแฝง
- กำหนดความรับผิดชอบหากเกิดปัญหาที่เกี่ยวข้องกับซอฟต์แวร์
- ควรมีข้อตกลงการส่งมอบซอร์สโค้ดที่สำรองเก็บไว้กับบริษัทผู้ผลิตซอฟต์แวร์ กำหนดไว้ในกรณีบริษัทผู้ผลิตไม่สามารถให้บริการต่อได้ (Escrow Arrangement)

2.7.2) ในกรณีที่พัฒนาโครงการ (Project) ซึ่งดำเนินการโดยหน่วยงานภายนอก โดยใช้พื้นที่การปฏิบัติงานอยู่ภายนอกองค์กร หน่วยงานที่รับผิดชอบว่าจ้างหน่วยงานภายนอกด้านสารสนเทศ ต้องประสานงานกับหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อจัดส่งเอกสารเกี่ยวกับความต้องการด้านความปลอดภัยสำหรับหน่วยงานภายนอกหรือจัดให้มีการสอบทานความปลอดภัยของระบบงานในสถานที่ปฏิบัติงานของหน่วยงานภายนอกด้วย

2.8) การทดสอบความปลอดภัยของระบบ (System security testing)

2.8.1) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการทดสอบสารสนเทศ ตามความต้องการด้านความปลอดภัยสารสนเทศ ก่อนนำระบบงานไปใช้งานจริง (Production environment)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2.9) การทดสอบความปลอดภัยของระบบ (System acceptance testing)

2.9.1) คณะกรรมการตรวจรับหรือผู้ตรวจรับ ต้องตรวจรับระบบตามหลักเกณฑ์การตรวจรับและการปฏิบัติตามข้อกำหนด ทั้งนี้ต้องสอบทานผลการทดสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ก่อนลงนามพิจารณาอนุมัติการตรวจรับ โดยมีประธานคณะกรรมการตรวจรับควบคุมและตรวจสอบ

2.9.2) หน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องสอบทานความเหมาะสมของหลักเกณฑ์และขั้นตอนการตรวจรับระบบสารสนเทศในเรื่องที่เกี่ยวกับความปลอดภัยสารสนเทศ

3. ข้อมูลสำหรับการทดสอบ (Test data)

3.1) การป้องกันข้อมูลสำหรับการทดสอบระบบ (Protection of system test data)

3.1.1) เจ้าของข้อมูลสารสนเทศ ต้องกำหนดความต้องการในการขอใช้ข้อมูลสารสนเทศที่สำคัญจากระบบงานจริงมาใช้ในการทดสอบ และจัดทำใบคำขอใช้ข้อมูลสารสนเทศ

3.1.2) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ ต้องจัดให้มีการพิสูจน์ตัวตน และกำหนดลำดับขั้นการเข้าถึงข้อมูลสารสนเทศที่สำคัญก่อนนำมาใช้ทดสอบ

3.1.3) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ ต้องต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง โดยการควบคุมต่างๆ ต้องประกอบด้วย

- ต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อนการนำสำเนาข้อมูลจริงไปยังระบบงานทดสอบในแต่ละครั้ง

- มีการควบคุมการเข้าถึงข้อมูลที่ใช้ในการทดสอบระบบ
- มีการดัดแปลงข้อมูลจริงที่สำคัญบางส่วนก่อนนำมาใช้ในการทดสอบ
- ทำการลบข้อมูลทดสอบออกจากระบบทันทีเมื่อเสร็จสิ้นการทดสอบ
- มีการจัดเก็บบันทึกการนำสำเนาข้อมูลจริงที่ใช้ในการทดสอบ เพื่อตรวจสอบ

กิจกรรมการทดสอบ (Audit Trail)

3.1.4) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ ต้องแปลงข้อมูลสารสนเทศที่สำคัญก่อนนำมาใช้ทดสอบ รวมทั้งสอบทานผลการแปลงข้อมูลสารสนเทศที่สำคัญ

3.1.5) หน่วยงานที่รับผิดชอบด้านการพัฒนาระบบ ต้องทำลายข้อมูลสารสนเทศที่ใช้ในการทดสอบภายหลังสิ้นสุดการพัฒนาและทดสอบระบบ โดยมีผู้จัดการโครงการขึ้นไปหรือเทียบเท่าควบคุมและตรวจสอบ

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 20 การใช้บริการ Cloud Computing

วัตถุประสงค์

- 1) เพื่อเป็นการนำเทคโนโลยีสารสนเทศ Cloud Computing มาใช้ หรือใช้บริการจากผู้ให้บริการภายนอก โดยประยุกต์ใช้งานเพื่อรองรับการดำเนินธุรกิจของ ธพส.
- 2) เพื่อให้การกำกับดูแลสอดคล้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูล และระบบสารสนเทศ (Integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (Availability)
- 3) เพื่อให้เกิดประโยชน์สูงสุดในการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพมากที่สุด

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ใช้งาน

ข้อปฏิบัติ

เพื่อให้เกิดการควบคุมการใช้บริการ Cloud Computing จากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ในงานด้านโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ หรือระบบงานในการจัดเก็บข้อมูล หรือดำเนินการใดๆ เกี่ยวกับข้อมูล หรือระบบสารสนเทศ ซึ่งครอบคลุมการใช้บริการประเภท Cloud Infrastructure as a Service (IaaS) Platform as a Service (PaaS) และ Software as a Service (SaaS) ให้มีข้อปฏิบัติ ดังนี้

1) ต้องมีการบริหารความเสี่ยงให้เหมาะสมกับรูปแบบ และลักษณะของการใช้บริการ Cloud Computing ดังต่อไปนี้

1.1) การประเมินความเสี่ยงการใช้บริการ Cloud Computing ควรครอบคลุมถึงความเสี่ยงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย และการพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอก จนอาจทำให้การเปลี่ยนแปลง หรือการยกเลิกการใช้บริการทำได้ยาก (Vendor lock-in) และส่งผลกระทบต่อระบบงานที่สำคัญของ ธพส. นอกจากนี้ ในกรณีที่จำเป็นต้องมีการใช้บริการในต่างประเทศ ต้องประเมินความเสี่ยงที่อาจเกิดขึ้นจากการขัดข้อง หรือปิดกั้นเครือข่าย หรือระบบสื่อสารระหว่างประเทศ (Information Access Risk) และความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (Cross-Border Compliance)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

1.2) การบริหารความเสี่ยงการให้บริการ Cloud Computing ควรสอดคล้องกับความเสี่ยงจากการให้บริการ โดยต้องได้รับความเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงขององค์กร

1.3) ต้องมีการจัดทำสัญญาการให้บริการจากผู้ให้บริการ Cloud Computing เป็นลายลักษณ์อักษร หรือจัดทำข้อตกลงการให้บริการ (Service Level Agreement) โดยระบุบทบาท หน้าที่ ความรับผิดชอบ ขอบเขตงานที่ใช้บริการครอบคลุมสาระสำคัญ หรืออย่างน้อยดังนี้

- 1.3.1) ขอบเขตการให้บริการ ประเภท และเงื่อนไขการให้บริการ
- 1.3.2) เงื่อนไขความเป็นเจ้าของข้อมูล สิทธิการใช้ และลิขสิทธิ์ที่เกี่ยวข้อง
- 1.3.3) ข้อกำหนดด้านการเข้าถึงข้อมูลของผู้ให้บริการ สิทธิการเข้าถึง และเงื่อนไขการเปิดเผยข้อมูล
- 1.3.4) มาตรฐานของการปฏิบัติงานขั้นต่ำที่ต้องการจากผู้ให้บริการ Cloud Computing
- 1.3.5) ระบบการควบคุมภายในของผู้ให้บริการ Cloud Computing
- 1.3.6) การจัดทำแผนฉุกเฉินสำหรับการให้บริการของผู้ให้บริการ Cloud Computing ควรสอดคล้องกับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ของ ทรส.
- 1.3.7) การรายงานผลการปฏิบัติงานของผู้ให้บริการ Cloud Computing
- 1.3.8) ความรับผิดชอบของ ทรส. และผู้ให้บริการ Cloud Computing ภาระผูกพันในกรณีที่เกิดปัญหาในการให้บริการ เงื่อนไข หรือแนวทางในการเปลี่ยนแปลง หรือยกเลิกสัญญา
- 1.3.9) ข้อกำหนดและเงื่อนไขการส่งมอบข้อมูลเมื่อมีการยกเลิก หรือสิ้นสุดการให้บริการ
- 1.3.10) ข้อกำหนดด้านเงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง
- 1.3.11) ข้อกำหนดและมาตรการป้องกันการรั่วไหลของข้อมูลที่เกิดขึ้นจากผู้ให้บริการ
- 1.3.12) ข้อกำหนดด้านสิทธิในการตรวจสอบ หรือการเปิดเผยรายงานผลการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- 1.3.13) บทบาทหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยของผู้ให้บริการ Cloud Computing และ ทรส. (โมเดลความรับผิดชอบด้านความมั่นคงปลอดภัยร่วมกัน)
- 1.3.14) ประเมินความเสี่ยงที่เกี่ยวข้องกับความต่อเนื่องในการให้บริการจากการยกเลิกสัญญาการใช้ระบบ Cloud Computing และแนวทางการยกเลิก หรือสิ้นสุดการให้บริการ โดยพิจารณาเงื่อนไขและข้อกำหนดที่ระบุในสัญญาการให้บริการ

1.4) ต้องกำหนดกระบวนการ และหลักเกณฑ์ในการคัดเลือกผู้ให้บริการ Cloud Computing ที่ชัดเจน เพื่อให้มั่นใจว่าผู้ให้บริการจะสามารถให้บริการได้อย่างต่อเนื่อง และสามารถตอบสนองความต้องการของ ทรส. โดยครอบคลุมเนื้อหาดังต่อไปนี้

- 1.4.1) ผู้ให้บริการ Cloud Computing มีมาตรฐานสากล หรือผลการตรวจสอบด้านความมั่นคงปลอดภัยในขอบเขตที่ให้บริการ เช่น มาตรฐาน ISO/IEC 27001 ISO/IEC 27017 ISO/IEC 27018 มาตรฐาน CSA STAR มาตรฐาน PCI DSS และ SOC 2 Report (Type I หรือ Type II)
- 1.4.2) ความพร้อมด้านเทคโนโลยีของผู้ให้บริการ Cloud Computing ในการให้บริการ
- 1.4.3) ชัดความสามารถของการให้บริการ (Capacity) ทั้งในกรณีการใช้งานที่กำหนด ทรัพยากรที่ตายตัว และกรณีที่เป็นการใช้จ่ายตามจริง
- 1.4.4) ข้อตกลงการให้บริการ (Service Level Agreement) ของผู้ให้บริการ Cloud Computing สอดคล้องกับความต้องการทางธุรกิจของ ทรส.

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

1.4.5) ความพร้อมในการดำเนินงานให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และนโยบายของ ธพส.

1.4.6) บริการ Cloud Computing ที่ใช้งานสามารถโอนย้ายข้อมูลได้หากมีการยกเลิกการใช้งาน

1.4.7) ประสิทธิภาพการให้บริการ และความมั่นคงทางการเงินของผู้ให้บริการ Cloud Computing

1.5) แม้ว่าการใช้บริการ Cloud Computing จะดำเนินงานโดยผู้ให้บริการ Cloud Computing อย่างไรก็ตาม ธพส. ต้องตรวจสอบโมเดลความรับผิดชอบด้านความมั่นคงปลอดภัยร่วมกัน (Shared Responsibility Model) เพื่อพิจารณาความรับผิดชอบในการรักษาความมั่นคงปลอดภัยระหว่าง ธพส. และผู้ให้บริการ Cloud Computing

1.6) ต้องจัดให้มีการทบทวนและประเมินประสิทธิภาพการให้บริการ Cloud Computing และมีแนวทางในการรับทราบการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ให้บริการ รวมถึงแนวทางในการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการ (Day-to-day incident)

2) จัดให้มีการกำหนดหน้าที่ผู้ให้บริการ Cloud Computing ให้เหมาะสมกับรูปแบบ และประเภทการให้บริการ Cloud Computing ตามลักษณะการให้บริการดังต่อไปนี้

2.1) เลือกใช้และกำหนดรายละเอียดรูปแบบการใช้ประเภทการบริการของ Cloud Computing ที่รองรับการดำเนินธุรกิจของ ธพส.

2.2) กำหนดมาตรฐานการรักษาความลับ ความปลอดภัยของข้อมูล

2.2.1) ผู้ให้บริการต้องมีแนวทาง หรือมาตรฐานในการรักษาความปลอดภัย ความลับของระบบงานตามมาตรฐานสากล

2.2.2) ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการติดตาม ประเมินผล ตรวจสอบผู้ให้บริการ เพื่อให้มั่นใจว่าผู้ให้บริการสามารถดำเนินการได้ตามแนวทางที่ได้ตกลงไว้

2.3) ผู้ให้บริการต้องจัดให้มีการสำรองข้อมูล และระบบงานสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

2.4) ผู้ให้บริการต้องจัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ที่ครอบคลุมถึงการให้บริการ Cloud Computing เพื่อให้สามารถปฏิบัติงานได้จริง รวมทั้งต้องจัดให้มีกระบวนการในการบริหารจัดการปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการให้บริการ และมีการรายงานปัญหาหรือเหตุการณ์ผิดปกติ และการจัดการปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว ให้ ธพส. รับทราบในระยะเวลาที่เหมาะสม

2.5) ผู้ให้บริการต้องกำหนดให้มีวิธีการพิสูจน์ตัวตนแบบ multi-factor หรือนำเสนอแนวทางการพิสูจน์ตัวตนที่มีความปลอดภัย มีประสิทธิภาพ และเป็นที่ยอมรับตามมาตรฐานสากล

3) มาตรการรักษาความปลอดภัย

3.1) ผู้ให้บริการต้องมีการรักษาความปลอดภัยข้อมูลสารสนเทศ เช่น เข้ารหัสข้อมูล (Data Encryption) การควบคุมกุญแจที่ใช้เข้าถึง และเข้ารหัสข้อมูลบนระบบ Cloud Computing (Key Management) เป็นต้น

3.2) ผู้ให้บริการต้องมีแนวทางการป้องกันภัยคุกคาม อย่างน้อย ดังต่อไปนี้

3.2.1) การโจมตีในลักษณะ DDoS (Distributed Denial of Service)

3.2.2) การป้องกันภัยคุกคามในรูปแบบใหม่ (Advanced Persistent Threat)

3.2.3) การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี (Malware)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

- 3.3) ผู้ให้บริการต้องมีการแบ่งแยกเครือข่าย (Network Segregation)
- 3.4) ผู้ให้บริการต้องออกแบบระบบงานสารสนเทศให้มีการป้องกันการบุกรุกแบบลำดับชั้น (Defense-in-Depth)
- 3.5) ผู้ให้บริการต้องสร้างความมั่นคงปลอดภัยให้กับระบบงานสารสนเทศ (Hardening) เช่น การหาช่องโหว่ และป้องกันปัญหาที่เกิดขึ้นจากการทดสอบ เพื่อให้มั่นใจว่าระบบงานสารสนเทศมีความมั่นคงปลอดภัย
- 3.5.1) แกะไขการตั้งค่าที่เป็น Default ของระบบงานสารสนเทศ เช่น User Password ของ Router เป็นต้น
- 3.5.2) ติดตั้ง Patch หรือ Hotfix ให้เป็น Version ล่าสุด
- 3.5.3) ปิดการใช้งาน user account ไม่จำเป็นและจัดการสิทธิให้เหมาะสม
- 3.5.4) ปิด Port หรือบริการต่างๆ ที่ไม่จำเป็น เช่น Telnet หรือ FTP เป็นต้น
- 3.6) กรณีผู้ให้บริการใช้บริการ Cloud Sub เงื่อนไขการบริการของ Cloud Sub ถือเป็นส่วนหนึ่งของผู้ให้บริการ และผู้ให้บริการต้องรับผิดชอบต่อการบริการของ Cloud Sub เสมือนกับที่ผู้ให้บริการเป็นผู้ให้บริการด้วยตนเอง
- 4) ผู้ให้บริการต้องยินยอมให้มีการตรวจสอบ โดยผู้ตรวจสอบภายในของ ธพส. หรือ ผู้ตรวจสอบภายนอกของ ธพส. ในการเรียกดูข้อมูลที่เกี่ยวข้อง และเข้าตรวจสอบการดำเนินงาน และการควบคุมภายในของผู้ให้บริการ Cloud Computing ทั้งในกรณีที่ผู้ให้บริการประกอบธุรกิจในประเทศและต่างประเทศ
- ทั้งนี้ ในกรณีที่ไม่สามารถจัดให้มีการตรวจสอบผู้ให้บริการได้ ธพส. มีสิทธิขอเรียกดูผลการตรวจสอบของผู้ให้บริการที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระที่มีหัวข้อและขอบเขตการตรวจสอบสอดคล้องกับขอบเขตการดำเนินงาน และภาระหน้าที่ความรับผิดชอบของผู้ให้บริการ หรือได้มาตรฐานสากลในการตรวจสอบด้านเทคโนโลยีสารสนเทศ เช่น มาตรฐาน ISO/IEC 27001 ISO/IEC 27017 ISO/IEC 27018 มาตรฐาน CSA STAR มาตรฐาน PCI DSS และ SOC 2 Report (Type I หรือ Type II)

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)
ส่วนที่ 2 นโยบายการสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน
เรื่องที่ 1 การสำรองข้อมูล

วัตถุประสงค์

- 1) เพื่อให้ข้อมูลและระบบสารสนเทศขององค์กร มีความพร้อมในการใช้งานในกรณีฉุกเฉิน โดยเกิดความเสียหายต่อองค์กรน้อยที่สุด
- 2) เพื่อให้ข้อมูลที่ได้มีการสำรองไว้ ถูกจัดเก็บอยู่ในสถานที่ปลอดภัย และพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อปฏิบัติ

- 1) มีกระบวนการจัดเตรียมระบบสำรองให้อยู่ในสภาพพร้อมใช้
- 2) มีคู่มือสำหรับวิธีการสำรองข้อมูลที่ชัดเจน
- 3) มีบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดขององค์กร และกำหนดระบบสารสนเทศที่ต้องจัดทำระบบสำรอง
- 4) กำหนดรายละเอียดของระบบสารสนเทศที่ต้องสำรองข้อมูล อย่างน้อย ดังนี้
 - 4.1) ข้อมูลของระบบสารสนเทศ (Database)
 - 4.2) ข้อมูลการตั้งค่าต่างๆของระบบ (Configuration)
 - 4.3) ระบบปฏิบัติการ
 - 4.4) ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ
- 5) กำหนดความถี่ในการสำรองข้อมูล ที่ชัดเจนและสอดคล้องกับระดับความสำคัญของชนิดและชั้นข้อมูล
- 6) กำหนดรูปแบบการสำรองข้อมูลตามความเหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น Full Backup หรือ Incremental Backup
- 7) บันทึกรายละเอียดการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วันเวลา ชื่อข้อมูลที่สำรอง และผลการดำเนินการ
- 8) จัดเก็บข้อมูลที่ได้สำรองไว้ในสถานที่ปลอดภัย มีการระบุรายละเอียดของข้อมูลที่สำรอง บนสื่อเก็บข้อมูลอย่างชัดเจน
- 9) มีการเข้ารหัสข้อมูลสำหรับข้อมูลลับที่ได้สำรองเก็บไว้ เพื่อป้องกันมิให้ข้อมูลสำรองถูกเปิดเผย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 2 นโยบายการสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน

เรื่องที่ 2 การเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

- 1) เพื่อให้มีแนวทางในการป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเสียหาย ถูกทำลาย หรือถูกเปลี่ยนแปลง จากไวรัสคอมพิวเตอร์ โปรแกรมชุดคำสั่งไม่พึงประสงค์ ผู้บุกรุก ภัยพิบัติ โดยสามารถกู้ข้อมูลที่มีปัญหากลับมาใช้งานได้
- 2) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องได้รับรู้เข้าใจ ตระหนักถึงความสำคัญของการสำรองข้อมูล เพื่อความมั่นคงปลอดภัยด้านสารสนเทศ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อปฏิบัติ

- 1) มีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์
- 2) มีการบริหารจัดการความเสี่ยงสำหรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และทำให้เกิดการหยุดชะงัก ตามเอกสาร “การบริหารจัดการความเสี่ยงด้านสารสนเทศ”
- 3) จัดทำแผนกู้คืนระบบเมื่อเกิดสถานการณ์ฉุกเฉินตามเอกสาร “แผนบริหารความต่อเนื่อง” โดยมีรายละเอียด ดังนี้
 - 3.1) มีการกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
 - 3.2) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบ
 - 3.3) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการผลิตภัณฑ์ (Vendor) หรือผู้ให้บริการภายนอก (Outsource) เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
- 4) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบกระแสไฟฟ้า ระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ที่มีประสิทธิภาพและเพียงพอ
- 5) มีการตรวจสอบหรือทดสอบระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
- 6) มีการใช้ระบบสำรองเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า
- 7) มีการจัดทำแผนฉุกเฉินสำหรับระบบกระแสไฟฟ้า เช่น ในกรณีที่ระบบกระแสไฟฟ้าเกิดการล้มเหลวหรือดับ
- 8) มีการจัดหาเครื่องกำเนิดกระแสไฟฟ้าสำรองเพื่อจ่ายไฟสำรองให้ในกรณีที่กระแสไฟฟ้าหลักเกิดการหยุดชะงักหรือดับเป็นระยะเวลายาวนาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

9) มีการจัดเตรียมเชื้อเพลิงสำรองเพียงพอสำหรับเครื่องกำเนิดกระแสไฟฟ้าสำรองในช่วงเกิดเหตุฉุกเฉิน

10) มีแหล่งจ่ายกระแสไฟฟ้ามากกว่าหนึ่งแหล่ง เพื่อสนับสนุนกระบวนการทำงานของระบบสารสนเทศที่สำคัญ

11) มีการจัดทำระบบไฟส่องสว่างฉุกเฉินเพื่อรองรับในกรณีที่กระแสไฟฟ้าหลักเกิดขัดข้อง และต้องการแสงสว่างในพื้นที่หรือบริเวณต่างๆ

12) มีระบบจ่ายน้ำที่เพียงพอสำหรับระบบปรับอากาศที่ต้องใช้น้ำในการทำงาน

13) มีระบบจ่ายน้ำที่เพียงพอเพื่อสนับสนุนระบบดับเพลิงของอาคาร

14) มีการติดตั้งระบบแจ้งเตือนในกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

15) มีระบบสายสื่อสารสำรอง ซึ่งเชื่อมต่อไปยังผู้ให้บริการเครือข่าย และหรือผู้ให้บริการโทรคมนาคม เพื่อใช้เป็นเส้นทางสำรอง

16) มีการทดสอบการกู้คืนข้อมูลที่สำรองไว้ ว่าสามารถกู้คืนได้อย่างครบถ้วนและสามารถใช้งานได้ตามปกติ อย่างน้อยปีละ 1 ครั้ง

17) ต้องกำหนดความถี่ในการสำรองข้อมูลของระบบสารสนเทศ ให้ขึ้นอยู่กับความสำคัญของระบบสารสนเทศ และสภาพการเปลี่ยนแปลงข้อมูล โดยระบบที่มีความสำคัญมาก หรือมีการเปลี่ยนแปลงข้อมูลบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

18) มีการทบทวนและปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน การบริหารจัดการความเสี่ยงด้านสารสนเทศ และแผนบริหารความต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 3 นโยบายการประเมินความเสี่ยง และการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ

เรื่องที่ 1 การตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้เข้าใจ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด

ผู้รับผิดชอบ

- 1) ฝ่ายดิจิทัล
- 2) ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3) เจ้าหน้าที่ที่ได้รับมอบหมาย
- 4) ผู้ตรวจสอบภายใน (Internal Auditor) หรือภายนอก (External Auditor)

ข้อปฏิบัติ

- 1) มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ
- 2) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
- 3) มีการตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบภายนอก (External Auditor)
- 4) มีข้อตกลงร่วมกันเพื่อกำหนดขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับการตรวจ
- 5) มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่เป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว
- 6) มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา ในกรณีทดสอบที่มีผลกระทบกับข้อมูลจริงในระบบสำคัญ
- 7) มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ ในกรณีทดสอบที่มีผลกระทบกับข้อมูลจริงในระบบสำคัญ
- 8) มีการจัดเก็บหลักฐานและข้อมูลในการตรวจสอบอย่างมั่นคงปลอดภัย
- 9) มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ
- 10) มีการกำหนดตัวบุคคลากรผู้ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนเองดูแลหรือรับผิดชอบ)
- 11) ต้องประเมินความเสี่ยงด้านสารสนเทศตามเอกสาร “การบริหารจัดการความเสี่ยงด้านสารสนเทศ” โดยครอบคลุมเนื้อหาตามมาตรฐาน COSO (Committee of Sponsoring Organizations)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

12) เครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยที่จำเป็นต้องใช้ ต้องได้รับการปกป้องจากการลักลอบใช้งานโดยไม่ได้รับอนุญาตหรือใช้ในทางที่ผิดวัตถุประสงค์รวมถึงมีการควบคุมจำกัดการเข้าถึงข้อมูลเฉพาะผู้ที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

13) เมื่อดำเนินการตรวจสอบและประเมินการรักษาความความมั่นคงปลอดภัยแล้ว ต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงขององค์กรทราบ พร้อมทั้งเสนอแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าการรักษาความมั่นคงปลอดภัยด้านสารสนเทศยังมีจุดบกพร่อง

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 3 นโยบายการประเมินความเสี่ยง และการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ

เรื่องที่ 2 การดำเนินโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศภายในองค์กร

วัตถุประสงค์

เพื่อให้การดำเนินโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศภายในบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ครอบคลุมถึงทุกหน่วยงานและทุกโครงการที่มีการพัฒนา จัดทำ ใช้งาน หรือเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์ ฮาร์ดแวร์ โครงสร้างพื้นฐาน และการใช้บริการ Third-party เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และกำกับดูแลได้อย่างเหมาะสม

ผู้รับผิดชอบ

- ฝ่ายงานที่รับผิดชอบโครงการ
- เจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลโครงการ
- ฝ่ายนิติกิจ

ข้อปฏิบัติ

- ฝ่ายงานที่รับผิดชอบโครงการ ที่มีความประสงค์จะดำเนินโครงการใหม่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ต้องแจ้งให้ฝ่ายนิติกิจรับทราบก่อนเริ่มดำเนินโครงการทุกครั้ง
- ฝ่ายงานที่รับผิดชอบโครงการ ต้องเข้าใจและรับทราบถึงนโยบายความมั่นคงปลอดภัยสารสนเทศของ ธพส. กฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง
- ฝ่ายนิติกิจ มีหน้าที่พิจารณาและให้คำปรึกษาในประเด็นที่เกี่ยวข้อง เช่น
 - มาตรฐานเทคนิคและสถาปัตยกรรม (Architecture)
 - ความมั่นคงปลอดภัยสารสนเทศ (Information Security)
 - การจัดการข้อมูลและการเชื่อมต่อระบบ (Data & Integration)
 - การปฏิบัติตามข้อกำหนดและข้อกำหนดทางคอมพิวเตอร์ (Compliance & Regulation)
- ฝ่ายงานที่รับผิดชอบโครงการ ต้องกำกับให้ผู้รับจ้าง หรือผู้รับจ้างพัฒนาระบบปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของ ธพส. รวมถึงคำสั่งวิธีปฏิบัติและเงื่อนไขที่เกี่ยวข้อง
- ฝ่ายงานที่รับผิดชอบโครงการ ควรพิจารณาดำเนินการประเมินและทดสอบความมั่นคงปลอดภัยผ่าน การทดสอบเจาะระบบ (Penetration Testing: Pen Test) หรือการตรวจสอบช่องโหว่ด้วยเครื่องมือ (Vulnerability Assessment: VA Scan) สำหรับบริการที่สำคัญของโครงสร้างพื้นฐานทางสารสนเทศ โดยเฉพาะระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับเครือข่าย อินเทอร์เน็ต (Internet Facing) ทั้งนี้ การดำเนินการควรสอดคล้องกับระดับความเสี่ยงของระบบ และคำนึงถึงผลกระทบหรือความเสี่ยงที่อาจเกิดขึ้นจากการทดสอบเจาะระบบ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

6) ฝ่ายงานที่รับผิดชอบโครงการ ต้องคำนึงถึงเงื่อนไขความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ สำหรับโครงการด้านโครงสร้างพื้นฐาน

- 2.5.1) มีความตระหนักถึงการรักษาความมั่นคงปลอดภัยในข้อมูลและทรัพย์สินของ ธพส. และ รับผิดชอบต่อการบริหารจัดการด้านความมั่นคงปลอดภัยข้อมูล
 - 2.5.2) เมื่อพบเจอเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นกับ ธพส. ต้องแจ้งหน่วยงานที่ควบคุมดูแลการดำเนินงานโครงการให้ทราบทันที
 - 2.5.3) ห้ามนำอุปกรณ์ที่ไม่ใช่ของ ธพส. เข้ามาเชื่อมต่อกับคอมพิวเตอร์ และระบบเครือข่าย ภายในของ ธพส. เว้นแต่ได้รับอนุญาตจากหน่วยงาน ธพส. ที่ควบคุมดูแลการดำเนินงาน
 - 2.5.4) ห้ามนำข้อมูลและสื่อบันทึกข้อมูลจัดอยู่ในระดับชั้นความลับขึ้นไปออกจาก ธพส. โดยไม่ได้รับอนุญาตและไม่มีการควบคุมที่เหมาะสม หากมีความจำเป็นต้องใช้ข้อมูลที่จัดอยู่ในระดับชั้นความลับขึ้นไป ผู้รับจ้างต้องขออนุญาตจากเจ้าของข้อมูล และปฏิบัติตามเงื่อนไขของขอบเขตการดำเนินงาน และต้องเก็บรักษาข้อมูลไว้เป็นความลับของ ธพส.
 - 2.5.5) กำหนดให้ระบบหรืออุปกรณ์ที่จัดหา สามารถบริหารจัดการสิทธิการเข้าถึงได้
 - 2.5.6) ซอฟต์แวร์ทุกประเภทที่นำมาใช้กับงาน ธพส. ต้องเป็นซอฟต์แวร์ที่ถูกลิขสิทธิ์ และไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมัลแวร์ใด ๆ ที่สามารถก่อให้เกิดความเสียหายต่อระบบสารสนเทศของ ธพส. ทั้งนี้ หาก ธพส. ตรวจพบผู้รับจ้างต้องรับผิดชอบในความเสียหายที่เกิดขึ้นทั้งหมด
- ให้มีการป้องกันเชิงลึก (Hardening) หลังการติดตั้งระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงแอปพลิเคชัน และระบบฐานข้อมูลที่อยู่ในขอบเขตงานของผู้รับจ้าง เช่น อัปเดตแพทช์ (OS และ Software) และการตั้งค่าอุปกรณ์/ระบบผ่านอุปกรณ์ความปลอดภัย (Firewall) เป็นต้น

7) ฝ่ายงานที่รับผิดชอบโครงการ ต้องคำนึงถึงเงื่อนไขความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ สำหรับโครงการด้านการพัฒนาระบบสารสนเทศ

- 2.6.1) มีความตระหนักถึงการรักษาความมั่นคงปลอดภัยในข้อมูลและทรัพย์สินของ ธพส. และ รับผิดชอบต่อการบริหารจัดการด้านความมั่นคงปลอดภัยข้อมูล
- 2.6.2) เมื่อพบเจอเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นกับ ธพส. ต้องแจ้งหน่วยงานที่ควบคุมดูแลการดำเนินงานโครงการให้ทราบทันที
- 2.6.3) ห้ามนำอุปกรณ์ที่ไม่ใช่ของ ธพส. เข้ามาเชื่อมต่อกับคอมพิวเตอร์ และระบบเครือข่าย ภายในของ ธพส. เว้นแต่ได้รับอนุญาตจากหน่วยงาน ธพส. ที่ควบคุมดูแลการดำเนินงาน
- 2.6.4) ห้ามนำข้อมูลและสื่อบันทึกข้อมูลจัดอยู่ในระดับชั้นความลับขึ้นไปออกจาก ธพส. โดยไม่ได้รับอนุญาตและไม่มีการควบคุมที่เหมาะสม หากมีความจำเป็นต้องใช้ข้อมูลที่จัดอยู่ในระดับชั้นความลับขึ้นไป ผู้รับจ้างต้องขออนุญาตจากเจ้าของข้อมูล และปฏิบัติตามเงื่อนไขของขอบเขตการดำเนินงาน และต้องเก็บรักษาข้อมูลไว้เป็นความลับของ ธพส.

- 2.6.5) ซอฟต์แวร์ทุกประเภทที่นำมาใช้กับงาน ธพส. ต้องเป็นซอฟต์แวร์ที่ถูกลิขสิทธิ์ และไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมัลแวร์ใด ๆ ที่สามารถก่อให้เกิดความเสียหายต่อระบบสารสนเทศของ ธพส. ทั้งนี้ หาก ธพส. ตรวจพบผู้รับจ้างต้องรับผิดชอบในความเสียหายที่เกิดขึ้นทั้งหมด
- 2.6.6) กำกับให้ผู้รับจ้างใช้วิธีการแบบปลอดภัยในการพัฒนาโปรแกรมตามมาตรฐานสากลที่เป็นที่ยอมรับ เช่น OWASP เป็นต้น
- 2.6.7) การพัฒนาระบบงานที่เชื่อมต่อกับโครงข่ายของ ธพส. ต้องใช้พอร์ตสื่อสาร (Service Port) ของระบบงานตามที่ฝ่ายดิจิทัลกำหนดให้เท่านั้น
- 2.6.8) ต้องกำหนดให้ระบบที่พัฒนาสามารถจำกัดสิทธิ์ในการเข้าถึงระบบ และข้อมูลที่สำคัญของ ธพส.
- 2.6.9) ข้อมูลใด ๆ ที่นำมาทดสอบการพัฒนาระบบของ ธพส. ต้องได้รับการควบคุมตามที่ฝ่ายงานที่รับผิดชอบโครงการกำหนด เช่น การเลือกใช้ข้อมูลอย่างเหมาะสม ต้องดำเนินการลบข้อมูลที่นำมาทดสอบเมื่อพัฒนาระบบเสร็จสิ้น เป็นต้น
- 2.6.10) การดำเนินการเปลี่ยนแปลงที่เกี่ยวข้องกับการพัฒนาระบบของ ธพส. ต้องได้รับการอนุมัติจากผู้อำนวยการฝ่ายของหน่วยงานเจ้าของโครงการ และผู้อำนวยการฝ่ายดิจิทัล
- 2.6.11) ผู้รับจ้างต้องจัดการเหตุการณ์ที่มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ในระหว่างการพัฒนา ระบบ ตลอดจนระยะเวลาที่รับจ้างบำรุงรักษาระบบ
- 2.6.12) ข้อมูลหรือโปรแกรม (Source Code) ที่ผู้รับจ้างพัฒนาขึ้นตามสัญญาฉบับนี้ให้ถือเป็นกรรมสิทธิ์ หรือลิขสิทธิ์ หรือสิทธิของ ธพส.

เรื่อง นโยบายและแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้ ธพส. ใช้เป็นนโยบายและแนวปฏิบัติในการกำหนดกระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ ในการเตรียมรองรับเหตุการณ์และลดผลกระทบต่าง ๆ ที่อาจเกิดขึ้น รวมถึงการฟื้นฟูระบบเทคโนโลยีสารสนเทศของ ธพส. ให้กลับคืนสู่สภาพปกติได้ภายในระยะเวลาที่เหมาะสม เพื่อให้ ธพส. สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง หรือได้รับผลกระทบน้อยที่สุดจากเหตุการณ์หยุดชะงัก อันเป็นการสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้เสียในการให้บริการของ ธพส.

แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศถือเป็นส่วนหนึ่งของแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ซึ่งเป็นแผนงานในการทำให้ธุรกิจดำเนินไปได้อย่างต่อเนื่อง และกลับคืนสู่สภาพที่สามารถดำเนินต่อไปได้ในกรณีที่เกิดเหตุการณ์ฉุกเฉิน โดยมีรายละเอียดที่ครอบคลุมปัจจัยการดำเนินธุรกิจของ ธพส. เช่น สถานที่ อุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายสื่อสาร และบุคลากร เป็นต้น

การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

1. มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร ที่ได้รับการอนุมัติจากคณะกรรมการ ธพส. โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
2. จัดให้มีคณะกรรมการหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและพนักงานของฝ่ายงานต่างๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ฝ่ายดิจิทัล ฝ่ายแผนและบริหารความเสี่ยง ฝ่ายสื่อสารองค์กร ฝ่ายการตลาด ฝ่ายพัฒนาธุรกิจ ฝ่ายวิศวกรรม และบริหารโครงการ เป็นต้น
3. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการดำเนินธุรกิจปริมาณงาน ความซับซ้อนของเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่างๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของ ธพส.

4. กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการดังนี้

4.1 การประเมินความเสี่ยง (risk Analysis) เพื่อให้ ธพส. สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อเหตุการณ์หยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศโดยมีแนวทางดำเนินการอย่างเหมาะสมเพียงพอ

4.2 การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) เพื่อให้ทราบถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีผลต่อการดำเนินธุรกิจของ ธพส. รวมถึงผลกระทบจากการหยุดชะงักและความเชื่อมโยงของการดำเนินธุรกิจกับระบบเทคโนโลยีสารสนเทศ เช่น วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

หยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) และกำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO)

4.3 แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรมีการระบุกระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น ให้ครอบคลุม

4.3.1 ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่น ๆ ที่เกี่ยวข้อง

4.3.2 ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบ รวมถึงผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผน

4.3.3 รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบเครือข่ายสื่อสาร เป็นต้น

4.3.4 ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศการตอบสนองต่อเหตุการณ์ฉุกเฉินและแผนการสื่อสารให้ฝ่ายงานที่เกี่ยวข้องรับทราบ

4.3.5 ขั้นตอนในการดำเนินการกู้คืนระบบ ควรระบุรายละเอียดอย่างชัดเจนและเพียงพอเพื่อให้สามารถใช้เป็น Checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้

4.3.6 ขั้นตอนในการกลับคืนสู่ภาวะปกติ (Return to Normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

4.3.7 แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง

4.4 การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ หรือจัดให้มีการฝึกอบรมแก่ผู้มีส่วนเกี่ยวข้อง

4.4.1 ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางการสื่อสารที่ชัดเจนให้ผู้บริหารและพนักงานทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน

4.4.2 จัดให้มีการฝึกอบรมแก่ผู้ที่มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ 1 ครั้ง โดยครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงานและการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น

4.5 การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

4.5.1 จัดให้มีแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียดอย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ และบทบาทหน้าที่ของผู้ที่เกี่ยวข้อง

4.5.2 มีการรายงานผลการทดสอบต่อคณะกรรมการ โดยมีรายละเอียดอย่างน้อยครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมแนวทางปรับปรุงแก้ไข

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

4.5.3 ควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน

เป้าหมาย : เพื่อให้ ทรส. มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหายโดยที่ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่อง และสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. กำหนดนโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และกำหนดให้มีคณะทำงานที่รับผิดชอบในการดำเนินการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายและแนวทางที่ได้กำหนดไว้ เพื่อเสนอให้คณะกรรมการ ทรส. พิจารณานุมัติใช้เป็นแผนในการดำเนินการ

2. ติดตามดูแลให้พนักงานและผู้ที่เกี่ยวข้องปฏิบัติงานตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และจัดให้มีการประเมินประสิทธิภาพของนโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง รวมถึงเมื่อมีการเปลี่ยนแปลงนโยบายหรือระบบเทคโนโลยีสารสนเทศที่สำคัญ

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานเพื่อให้บรรลุเป้าหมายตามนโยบาย โดยจัดให้มีกลยุทธ์ แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนผู้บริหารในการดำเนินงานจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เช่น คณะกรรมการ คณะทำงาน หน่วยงานรับผิดชอบ เป็นต้น

2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง เพื่อสร้างการมีส่วนร่วมของผู้มีส่วนได้เสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง

3. ส่งเสริม สนับสนุนความรู้ ความเข้าใจแก่ผู้ปฏิบัติงาน

4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานตามนโยบาย ก่อนนำเสนอคณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบายและเป้าหมายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

2. รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติ เพื่อให้ ธพส. บรรลุตามเป้าหมายที่กำหนด และนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย

2. จัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยต้องมีการประเมินและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการดำเนินธุรกิจ เพื่อจัดลำดับความสำคัญของระบบเทคโนโลยีสารสนเทศ และกำหนดเป้าหมายการกู้ระบบและภารกิจหลักให้กลับคืนมาได้ภายในระยะเวลาที่ยอมรับได้ เพื่อให้เกิดความเชื่อมั่นกับผู้มีส่วนได้เสียต่อการดำเนินธุรกิจของ ธพส.

3. กำหนดให้มีการสื่อสาร อบรมแก่ผู้มีส่วนได้เสียที่เกี่ยวข้องอย่างครบถ้วน และให้มีการทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับสภาพแวดล้อมของการดำเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบเทคโนโลยีสารสนเทศ

4. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย ทวนสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงานด้านการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาวะวิกฤต ต่อคณะกรรมการ ธพส. เป็นประจำทุกปี

เรื่อง นโยบายการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกิจเป็นไปอย่างต่อเนื่อง รวมทั้งป้องกันปัญหา และภัยคุกคามต่างๆ ที่อาจเกิดขึ้น ธพส. จึงกำหนดนโยบายการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อสื่อสารและเผยแพร่ให้กรรมการ ผู้บริหาร และพนักงานของ ธพส. รับทราบและถือปฏิบัติ ดังนี้

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

1. กำหนดให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมสอดคล้องตามหลัก 3 Lines of Defense โครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. จัดให้มีหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

3. สำรองข้อมูลพร้อมทั้งทดสอบการรีสโตร์ฐานข้อมูลอย่างสม่ำเสมอ และการเตรียมความพร้อมในกรณีฉุกเฉิน โดยครอบคลุมปัจจัยเสี่ยงที่จะเกิดความเสียหายดังนี้

3.1 ปัจจัยภายใน ได้แก่ 1) ระบบฐานข้อมูลหลักเสียหายหรือข้อมูลถูกทำลาย 2) การโดนไวรัสโจมตี 3) การถูกเจาะหรือลักลอบเข้าระบบฐานข้อมูลโดยไม่ได้รับอนุญาต

3.2 ปัจจัยภายนอก ได้แก่ 1) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้ง ของเครื่องแม่ข่ายหลักของระบบฐานข้อมูล 2) การขโมยเครื่องแม่ข่ายของระบบฐานข้อมูล 3) การชำรุดเสียหายของเครื่องแม่ข่ายของระบบฐานข้อมูล 4) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

4. มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลระหว่างผู้ใช้งานและผู้ดูแลระบบเทคโนโลยีสารสนเทศ การกำหนดสิทธิ์เปลี่ยนแปลง เพิ่มเติม หรือแก้ไขสิทธิ์ในการเข้าถึงข้อมูลผู้ใช้งาน ระบบสารสนเทศ และผู้ดูแลระบบเทคโนโลยีสารสนเทศนั้น จะทำโดยผู้ดูแลระบบสารสนเทศ ดังนี้

4.1 เพิ่มข้อมูลการกำหนดสิทธิ์เมื่อเข้ามาทำงานใหม่

4.2 ปรับปรุงข้อมูลการกำหนดสิทธิ์เมื่อโยกย้ายตำแหน่ง หรือหน่วยงาน

4.3 ลบข้อมูลการกำหนดสิทธิ์เมื่อเกษียณอายุหรือลาออกจากงาน

5. ให้มีการบำรุงรักษาอุปกรณ์เครือข่ายและระบบคอมพิวเตอร์

6. จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล อย่างน้อยปีละ 1 ครั้ง

เป้าหมาย : เพื่อป้องกันความเสียหายและลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านนโยบาย
2. สนับสนุนให้การดำเนินธุรกิจของ ธพส. เป็นไปตามนโยบาย

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานตามนโยบาย เพื่อให้บรรลุตามเป้าหมาย โดยจัดให้มีกลยุทธ์ แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนผู้บริหารในการดำเนินงาน เช่น คณะกรรมการ คณะทำงาน หน่วยงานรับผิดชอบ เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง สร้างการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ เพื่อให้บุคลากรทุกระดับและทุกฝ่ายให้ความตระหนักและมีแนวทางการบริหารความเสี่ยงเพื่อให้มีการป้องกัน ติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น
4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานด้านนโยบาย ก่อนนำเสนอคณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติ ตามนโยบาย สนับสนุน ผลักดันการปฏิบัติตามนโยบาย ภายใต้ขอบเขตของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงาน

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย ทวนสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงาน ต่อผู้บริหาร คณะอนุกรรมการ และคณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบงานและเครื่องมือ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล

วัตถุประสงค์

เพื่อป้องกันไม่ให้ข้อมูลของบริษัท ธนาคารพัฒนาสินทรัพย์ จำกัด (ธพส.) โดนบุกรุก ทำลาย แทรกแซง หรือโจรกรรมในรูปแบบต่าง ๆ ที่จะส่งผลให้เกิดความเสียหายต่อการดำเนินธุรกิจของ ธพส. และเป็นไปตามแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูล จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อเป็นแนวทางให้ผู้บริหารและพนักงานถือปฏิบัติได้อย่างถูกต้องเหมาะสม ดังนี้

ขอบเขตของนโยบาย

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลทั้งที่อยู่ในระบบคอมพิวเตอร์และนอกระบบของ ธพส. ทั้งที่อยู่ภายในและภายนอกสถานที่ปฏิบัติงานของ ธพส. รวมทั้งคลาวด์ที่ ธพส. ใช้จัดเก็บข้อมูลด้วย ซึ่งครอบคลุมถึงบุคคลดังต่อไปนี้

1. พนักงานและหน่วยงานภายในทั้งหมดของ ธพส.
2. บุคคลภายนอกที่ได้รับสิทธิ์เข้าถึงทรัพย์สินและหรือที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของ ธพส.

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูล ดังนี้

1. ปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่มีกรรมสิทธิ์ของ ธพส.
2. สร้างความมั่นใจว่าข้อมูลของ ธพส. ต้องไม่มีการแก้ไข ดัดแปลง หรือ โดนทำลายโดย ผู้ที่ไม่ได้รับอนุญาต
3. สร้างความมั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูล และบริการได้อย่างรวดเร็วและเชื่อถือได้
4. ระบุหน้าที่และความรับผิดชอบของผู้บริหารและพนักงานต่อข้อมูลที่อยู่ในความดูแล
5. สร้างความมั่นใจว่าสิทธิ์การเข้าถึงข้อมูลทั้งที่อยู่ในระบบและนอกระบบคอมพิวเตอร์มีกระบวนการพิสูจน์ตัวตนที่น่าเชื่อถือ
6. สร้างความมั่นใจว่าการให้สิทธิ์เข้าใช้ข้อมูลทั้งที่อยู่ในระบบและนอกระบบคอมพิวเตอร์มีการกำหนดสิทธิ์และมีขั้นตอนอนุมัติให้เข้าถึงตามระดับชั้นความสำคัญข้อมูล
7. สร้างความมั่นใจว่าผู้มีส่วนร่วมที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

8. รักษาความมั่นคงปลอดภัยที่เป็นไปด้วยประสิทธิภาพ ประสิทธิผล จำเป็นต้องมีข้อตกลงร่วมกัน และได้รับความร่วมมือจากทั้งผู้บริหารและพนักงาน ประกอบไปด้วย

8.1 รักษาความปลอดภัยถือว่าเป็นหน้าที่ของผู้บริหารและพนักงานทุกคน รวมถึงบุคคลภายนอกผู้ได้รับสิทธิ์การเข้าถึงข้อมูลของ ธพส. ทั้งที่อยู่ในระบบและนอกระบบคอมพิวเตอร์

8.2 บริหารและการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องดำเนินการอย่างต่อเนื่อง

9. สร้างจิตสำนึก รู้จักหน้าที่ รับผิดชอบ และดำเนินการตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่าง ๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้ผู้บริหาร พนักงานและบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบ เป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิภาพ

คำจำกัดความ

1. ธพส. หมายถึง บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด
2. ผู้ปฏิบัติงาน หมายถึง พนักงาน พนักงานทดลองงาน ลูกจ้างประจำ ลูกจ้างชั่วคราว และผู้บริหารของ ธพส.
3. ผู้บริหาร หมายถึง กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ และพนักงานที่มีตำแหน่งตั้งแต่ผู้จัดการส่วน หรือผู้อำนวยการขึ้นไป
4. ผู้ใช้งาน หมายถึง ผู้ปฏิบัติงาน รวมไปถึงบุคคลภายนอกที่ได้รับอนุญาตจาก ธพส. ให้มีรหัสเข้าใช้งานบัญชีรายชื่อผู้สามารถเข้าใช้งาน และ/หรือ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ที่เชื่อมโยงระบบคอมพิวเตอร์ซึ่งสามารถเข้าถึงข้อมูลของ ธพส.
5. ระบบคอมพิวเตอร์ หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุ อุปกรณ์การเก็บรักษาและการถ่ายโอนข้อมูลชนิดต่าง ๆ ระบบ Internet และระบบ Intranet รวมถึง อุปกรณ์ไฟฟ้าและสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ที่เป็นทรัพย์สินของ ธพส. และหน่วยงานอื่นที่อยู่ระหว่างการติดตั้งและยังไม่ได้ส่งมอบ หรือของผู้ปฏิบัติงานที่นำเข้ามาติดตั้งหรือใช้งานในสถานประกอบการของ ธพส.
6. ข้อมูล หมายถึง โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรือ อุปกรณ์ใด ๆ
7. ข้อมูลสำคัญ หรือข้อมูลความลับ หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของ ธพส. หรือที่มีพันธะผูกพันตามข้อกำหนดของกฎหมายจรรยาบรรณในการประกอบธุรกิจ หรือที่ ธพส. ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของ ธพส. การรั่วไหลของข้อมูลสำคัญหรือข้อมูลที่เป็นความลับดังกล่าว อาจเป็นเหตุให้การดำเนินธุรกิจของ ธพส. ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือเสื่อมเสียชื่อเสียง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

8. ระบบที่มีความสำคัญ หมายถึง ระบบคอมพิวเตอร์ที่ ธพส. ใช้ประโยชน์ หรือใช้ในการบริการทางธุรกิจ ที่ก่อให้เกิดรายได้โดยตรง และให้หมายรวมถึงระบบที่สนับสนุนให้เกิดรายได้ ระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยให้การดำเนินธุรกิจของ ธพส. ทั้งนี้ หากระบบที่มีความสำคัญดังกล่าวหยุดการทำงาน หรือมีประสิทธิภาพ ในการทำงานลดลงจะทำให้การดำเนินธุรกิจของ ธพส. ต้องหยุดชะงัก หรือด้อยประสิทธิภาพ

9. ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่น เพื่อการจัดการระบบเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบ คอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

10. การรักษาความมั่นคงปลอดภัย หมายถึง มาตรการและหรือกระบวนการที่กำหนดขึ้น เพื่อป้องกันดูแลรักษาระบบคอมพิวเตอร์ ระบบที่มีความสำคัญ และข้อมูลสำคัญต่อการดำเนินธุรกิจของ ธพส.

11. บุคคลภายนอก หมายถึง บุคลากร องค์กรหรือหน่วยงานภายนอกที่ ธพส. อนุญาตให้มีสิทธิในการเข้าถึงและใช้ งานข้อมูลหรือทรัพย์สินต่าง ๆ ของ ธพส. โดยจะได้รับสิทธิในการใช้ ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล เช่น ผู้รับจ้าง (Outsource) ผู้พัฒนาระบบหรือจัดหาวัสดุ อุปกรณ์ต่าง ๆ (Supplier) ที่ปรึกษา (Consultant)

หน้าที่ความรับผิดชอบ

1. หน้าที่ของผู้บริหาร

1.1 ชี้แจงให้ผู้ปฏิบัติงานทราบถึงนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการ ปฏิบัติคำแนะนำและกระบวนการต่าง ๆ ของ ธพส. ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัย

1.2 ดูแล แนะนำ และตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม

1.3 พิจารณาลงโทษทางวินัยแก่ผู้กระทำความผิดอย่างเสมอภาคและเป็นธรรม

2. หน้าที่ของผู้ปฏิบัติงาน

2.1 ผู้ปฏิบัติงานทุกคน ต้องปฏิบัติดังต่อไปนี้

2.1.1 ต้องเรียนรู้ ทำความเข้าใจและปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติคำแนะนำและกระบวนการต่าง ๆ ของ ธพส. ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด

2.1.2 ให้ความร่วมมือในการป้องกันระบบคอมพิวเตอร์และข้อมูลของ ธพส.

2.1.3 แจ้งให้ผู้บังคับบัญชาทราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุก โจรกรรม ทำลาย แทรกแซงการทำงานหรือกิจกรรมที่อาจสร้างความเสียหายให้แก่ ธพส.

2.2 ผู้ปฏิบัติงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ต้องปฏิบัติดังต่อไปนี้

2.2.1 ต้องออกจากกระบวน (Log-out, Log-off) ทุกกระบวนเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน

2.2.2 ต้องล็อกหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้น ๆ เพื่อป้องกันให้บุคคลอื่นลักลอบเข้าไปใช้งาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2.2.3 ต้องตรวจสอบข้อมูลที่น่ามาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย

2.2.4 ต้องเก็บรักษารหัสผ่าน (Password) เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับ หรือข้อมูลส่วนบุคคลของคณะกรรมการ ธพส. และผู้ปฏิบัติงาน ธพส. ซึ่งจะต้องเก็บรักษาไว้ไม่ให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้ผู้ปฏิบัติงานต้องเปลี่ยนรหัสผ่าน เมื่อรหัสกำหนดอายุตามระยะเวลาที่กำหนด โดยอ้างอิงมาตรฐานการตั้งรหัสผ่านอย่างปลอดภัยตาม IT Security Standard

2.2.5 ผู้ปฏิบัติงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอก ต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติ ตามนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล

ทั้งนี้ เพื่อให้การป้องกันระบบคอมพิวเตอร์และข้อมูลของ ธพส. เป็นไปอย่างมีประสิทธิภาพ ธพส. ต้องจัดให้มีมาตรการและการบริหารจัดการที่ดี ดังนี้

การบริหารจัดการระบบ เพื่อให้มีมาตรการในการป้องกันทรัพย์สินของ ธพส. อย่างเหมาะสม

1. กำหนดให้มีบัญชีทรัพย์สิน
2. กำหนดให้มีชั้นความลับและการควบคุม
3. กำหนดให้มีการบริหารจัดการซอฟต์แวร์ลิขสิทธิ์

การบริหารจัดการหน่วยงานและบุคลากร เพื่อให้ผู้ปฏิบัติงานและบุคคลภายนอกที่ทำความสัญญากับ ธพส. เข้าใจในหน้าที่ความรับผิดชอบของตนเอง รวมถึงตระหนักถึงการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน

1. ก่อนการจ้าง
2. ระหว่างการจ้างงาน
3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

การรักษาความมั่นคงปลอดภัยสถานที่และอุปกรณ์ เพื่อป้องกันการเข้าถึงสถานที่และอุปกรณ์โดยไม่ได้รับอนุญาต ซึ่งอาจทำให้เกิดความเสียหายและการแทรกแซงการทำงานของระบบคอมพิวเตอร์และข้อมูลของ ธพส.

1. การรักษาความมั่นคงปลอดภัยสถานที่
2. การรักษาความมั่นคงปลอดภัยอุปกรณ์

การบริหารจัดการการสื่อสารและการดำเนินงาน เพื่อสร้างความมั่นใจว่าการดำเนินงานบนระบบคอมพิวเตอร์มีความมั่นคงปลอดภัยจากการล้มเหลวของระบบคอมพิวเตอร์

1. กำหนดขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ
2. กำหนดให้มีการบริหารจัดการการส่งมอบข้อมูลแก่บุคคลภายนอก
3. กำหนดให้มีการสำรองและการกู้คืนข้อมูล
4. กำหนดให้มีการจัดการความมั่นคงปลอดภัยของเครือข่าย
5. กำหนดให้มีการจัดการข้อมูลแบบคลาวด์ และบริหารจัดการแพทช์

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

การบริหารจัดการการควบคุมการเข้าถึง เพื่อควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

1. การบริหารจัดการในการเข้าถึงระบบของผู้ใช้งาน
2. การบริหารจัดการรหัสผ่าน
3. การควบคุมการเข้าถึงระบบ
4. การควบคุมอุปกรณ์คอมพิวเตอร์เครื่องมือสื่อสารและการปฏิบัติงานจากภายนอก ธพส.

การจัดหา การพัฒนา และการบำรุงรักษาระบบ เพื่อให้การจัดหา การพัฒนาและการบำรุงรักษาระบบคำนึงถึงความมั่นคงปลอดภัยเป็นสำคัญ

1. ข้อกำหนดรักษาความมั่นคงปลอดภัยสำหรับระบบ
2. การประมวลผลบนแอปพลิเคชัน
3. การควบคุมการเข้ารหัส
4. การรักษาความมั่นคงปลอดภัยของข้อมูล
5. การรักษาความมั่นคงปลอดภัยในการพัฒนา และกระบวนการสนับสนุน

การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย กำหนดให้มีประเมิน และบริหารจัดการเพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น และทำให้มั่นใจว่าเหตุการณ์ด้านความมั่นคงปลอดภัย รวมถึงจุดอ่อนที่เกี่ยวข้องกับระบบคอมพิวเตอร์ได้รับการสื่อสารและสามารถดำเนินการแก้ไขได้ทันเวลา

การจัดการความต่อเนื่องทางธุรกิจ กำหนดให้มีการป้องกันระบบคอมพิวเตอร์และข้อมูลที่สำคัญต่อกระบวนการในการดำเนินธุรกิจของ ธพส.

กฎหมายและข้อบังคับที่เกี่ยวข้อง กำหนดให้มีการกำกับปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้อง อาทิ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เป็นต้น รวมถึงกฎหมายระเบียบข้อบังคับอื่นที่เกี่ยวข้อง ซึ่งใช้บังคับอยู่แล้วในขณะนี้และที่จะได้ออกใช้บังคับต่อไปในภายหน้า

หน่วยงานรับผิดชอบ

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของข้อมูล
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย สอบทานความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงานตามนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลต่อผู้บริหาร และคณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบบริหารจัดการข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงานธุรกิจของ ธพส.

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เรื่อง นโยบายการบริหารความต่อเนื่องทางธุรกิจ

วัตถุประสงค์

เพื่อให้การดำเนินธุรกิจของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) เป็นไปอย่างต่อเนื่องไม่หยุดชะงัก สามารถสร้างความมั่นใจเพื่อตอบสนองและบรรเทาผลกระทบต่อผู้มีส่วนได้เสีย ธพส. จึงให้ความสำคัญแก่การตระหนักถึงความเสี่ยงและภาวะวิกฤตต่างๆ ที่คุกคามความต่อเนื่องในการดำเนินธุรกิจ โดยกำหนดให้มีระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) รวมถึงการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อบรรเทาผลกระทบและมีการตอบสนองต่อผู้มีส่วนได้เสียที่มีประสิทธิภาพ จึงเห็นควรกำหนดเป็นนโยบายการบริหารความต่อเนื่องทางธุรกิจ เพื่อเป็นแนวปฏิบัติของคณะกรรมการ ผู้บริหาร และพนักงาน ดังนี้

การบริหารความต่อเนื่องทางธุรกิจ

1. กำหนดให้มีคณะกรรมการหรือหน่วยงานที่มีหน้าที่รับผิดชอบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Committee : BCM Committee) เพื่อทำหน้าที่กำกับดูแลการบริหารความต่อเนื่องทางธุรกิจในภาพรวมของ ธพส. โดยมุ่งเน้นการพัฒนากระบวนการบริหารความต่อเนื่องทางธุรกิจตามกรอบมาตรฐานสากล รวมถึงจัดทำแผนการบริหารความต่อเนื่องทางธุรกิจ และส่งเสริมให้ผู้บริหารและพนักงาน ทุกหน่วยงานปฏิบัติตามระบบการบริหารความต่อเนื่องทางธุรกิจ ให้มีการฝึกซ้อมการปฏิบัติตามแผนและทบทวนปรับปรุงแผนอย่างต่อเนื่องจนเกิดเป็นวัฒนธรรมองค์กร
2. ให้มีการจัดการความเสี่ยงจากการหยุดชะงักทางธุรกิจที่กระทบต่อการให้บริการแก่ผู้มีส่วนได้ส่วนเสีย ที่บริษัทเผชิญอยู่ในปัจจุบันและอนาคต
3. ให้มีกระบวนการบริหารความเสี่ยงทางธุรกิจ และภาพรวมโครงสร้างการกำกับดูแลการบริหารความเสี่ยง รวมทั้งวัฒนธรรมความเสี่ยงของบริษัทฯ
4. ให้มีการพิจารณาความสัมพันธ์ระหว่างการให้บริการที่ต้องกอบกู้ตามกรอบการบริหารความต่อเนื่องทางธุรกิจสอดคล้องและรักษาคูณค่าของกิจการตามพันธกิจ และตามนโยบายของรัฐ
5. ให้มีระบบการรายงานความเสี่ยงที่กระทบต่อการทำธุรกิจ และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง
6. ให้มีการทดสอบภาวะวิกฤตที่ระบุถึงความถี่และความถี่และสาระสำคัญของการทดสอบ เพื่อประเมินประสิทธิผลของแผนการบริหารความต่อเนื่องทางธุรกิจ ทั้งกรณีที่เป็นประจำและตามสถานการณ์ที่นำไปสู่การทดสอบแบบเฉพาะกิจ
7. ให้กำหนดช่วงความเปราะบางที่ยอมรับได้ (Disruption risk tolerance) สำหรับความเสี่ยงของงานบริการหลักที่สำคัญให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Corporate Risk Appetite)
8. ให้ใช้ช่วงความเปราะบางที่ยอมรับได้ในกระบวนการติดตาม วัด ประเมินประสิทธิผลของแผนการบริหารความต่อเนื่องทางธุรกิจ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

9. ให้มีการบริหารความต่อเนื่องทางธุรกิจแบบองค์รวม (Enterprise Continuity Management : ECM) และการประเมินความเสี่ยงและความมั่นคง เพื่อลดผลกระทบจากความผันผวนที่มีต่อความต่อเนื่องของการดำเนินธุรกิจให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงเชื่อมโยงระหว่างความเสี่ยง กลยุทธ์ และความคาดหวังของผู้มีส่วนได้ส่วนเสีย เพื่อให้มั่นใจว่าบริษัทฯ มีสถานะการบริหารความต่อเนื่องทางธุรกิจที่มั่นคง สามารถบรรลุดัชนีประสิทธิผลหรือเป้าหมายการบริหารความต่อเนื่องทางธุรกิจของบริษัท ทั้งในระยะสั้นและระยะยาว

10. ให้รายงานข้อมูลการบริหารภัยด้านการบริหารความต่อเนื่องทางธุรกิจและสถานะความเสี่ยงจากภัยตามประเภทของภัย โดยให้คำนึงถึงกรอบการบริหารความต่อเนื่องทางธุรกิจและนโยบายการบริหารความเสี่ยงในภาพรวมของบริษัท ซึ่งต้องจัดให้มีเอกสารที่เป็นลายลักษณ์อักษรที่พร้อมให้ตรวจสอบได้ตลอดเวลา

11. ให้แผนการบริหารความต่อเนื่องทางธุรกิจแต่ละแผนกำหนดโครงสร้างการกำกับดูแลการบริหารความเสี่ยงที่มีการแบ่งแยกบทบาทหน้าที่และการควบคุมดูแลความเสี่ยง เพื่อให้การบริหารความต่อเนื่องทางธุรกิจแบบองค์รวมของบริษัทฯ เป็นไปอย่างมีประสิทธิภาพ โดยมีคณะกรรมการบริหารความเสี่ยงกำกับให้บริษัทปฏิบัติตามหลักเกณฑ์ ตามนโยบายฉบับนี้

12. ให้มีวัฒนธรรมการบริหารความต่อเนื่องทางธุรกิจที่สอดคล้องกับกรอบการบริหารความเสี่ยงของบริษัทฯ โดยนำไปปฏิบัติใช้กับการดำเนินภารกิจของบริษัท และมีระบบการบริหารจัดการที่เหมาะสมเพื่อสนับสนุนการบริหารความต่อเนื่องทางธุรกิจ และเป็นส่วนหนึ่งของการทำงานของพนักงานทุกคนในองค์กร รวมทั้งจัดให้มีการอบรมพัฒนาบุคลากรของบริษัทฯ ให้มีความรู้ความเข้าใจ สร้างความระมัดระวัง และตระหนักถึงความเสี่ยงที่อาจจะเกิดขึ้นและมีผลกระทบต่อฝ่ายงาน ต่อองค์กร และต่อผู้เกี่ยวข้อง รวมทั้งส่งเสริมให้มีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่าง ๆ ภายในองค์กร ตลอดจนมีการบูรณาการการบริหารความต่อเนื่องทางธุรกิจเข้ากับการตัดสินใจทางธุรกิจ การกำกับดูแลกิจการ และการควบคุมภายในของบริษัทฯ

เป้าหมาย : เพื่อลดผลกระทบหรือป้องกันการหยุดชะงักของระบบและภารกิจหลักอันเป็นผลมาจากสภาวะฉุกเฉิน หรือภัยพิบัติต่าง ๆ ได้ภายในระยะเวลาที่ยอมรับได้

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน นโยบายด้านบริหารความต่อเนื่องของธุรกิจ
2. กำกับให้การดำเนินธุรกิจเป็นไปตามนโยบายบริหารความต่อเนื่องของธุรกิจ

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานเพื่อให้บรรลุเป้าหมายตามนโยบาย โดยจัดให้มีกลยุทธ์ แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เช่น คณะกรรมการ คณะทำงาน เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง เพื่อสร้างการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ ความเข้าใจแก่ผู้ปฏิบัติงานเพื่อให้การดำเนินธุรกิจเป็นไปด้วยความต่อเนื่อง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานตามนโยบาย ก่อนนำเสนอคณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติ เพื่อให้ ธพส. บรรลุตามเป้าหมายที่กำหนด

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. จัดทำแผนบริหารความต่อเนื่องของธุรกิจ โดยต้องมีการประเมินและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการดำเนินธุรกิจ เพื่อจัดลำดับความสำคัญของระบบ แล้วกำหนดเป้าหมายการกู้ระบบและภารกิจหลักให้กลับคืนมาได้ภายในระยะเวลาที่ยอมรับได้
3. กำหนดให้มีการสื่อสาร อบรมเพื่อสร้างรู้ความระมัดระวัง และตระหนักถึงความเสี่ยงที่อาจจะเกิดขึ้นและมีผลกระทบต่อฝ่ายงานและต่อองค์กร ให้แก่ผู้บริหาร พนักงานและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องอย่างครบถ้วน และให้มีการทดสอบซักซ้อม การปรับปรุงและการสอบทานแผนการบริหารความต่อเนื่องของธุรกิจเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับสภาพแวดล้อมของการดำเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบ IT
4. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย สอบทานความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงานด้านการบริหารความต่อเนื่องของธุรกิจต่อผู้ "บริหาร คณะอนุกรรมการ และคณะกรรมการ ธพส. เป็นประจำทุกปี
5. พัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจ และระบบเทคโนโลยีสารสนเทศ เพื่อสนับสนุนการดำเนินงาน

เรื่อง นโยบายข้อมูลและการตรวจสอบ

วัตถุประสงค์

เพื่อให้การดำเนินงานของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) มีกรอบแนวทางดำเนินการสำหรับการดูแลความมั่นคงปลอดภัยของสารสนเทศและการปกป้องข้อมูลสารสนเทศ อันสะท้อนให้เห็นถึงการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงที่ครอบคลุมในทุกประเด็น สอดคล้องตามจริยธรรมทางธุรกิจ และจรรยาบรรณที่กำหนดไว้ จึงเห็นสมควรกำหนด นโยบายด้านข้อมูลและการตรวจสอบ เพื่อเป็นแนวปฏิบัติสำหรับคณะกรรมการ ผู้บริหาร และพนักงานของ ธพส. ดังนี้

ข้อมูลและการตรวจสอบข้อมูล

1. ให้องค์กรที่รับผิดชอบงานในทุกด้านของบริษัท จัดทำทะเบียนและบันทึกข้อมูลที่เกี่ยวข้องกับงานของตน อาทิ ข้อมูลทางการเงิน ข้อมูลในการดำเนินธุรกิจ ข้อมูลรายชื่อบุคคล คู่ค้า ลูกค้า หน่วยงานสำคัญที่เกี่ยวข้องกับการดำเนินธุรกิจ ตลอดจนข้อมูลเกี่ยวกับพนักงาน และผู้มีส่วนได้เสียของบริษัทไว้อย่างถูกต้องครบถ้วน และทันเวลา โดยปฏิบัติตามหลักเกณฑ์ที่บริษัทหรือกฎหมายกำหนดไว้
2. ให้จัดทำรายงานข้อมูลอย่างถูกต้อง ตรงไปตรงมาตามข้อเท็จจริง โดยไม่บิดเบือนหรือบิดเบือนข้อมูลที่แท้จริง
3. จัดให้มีมาตรการในการเก็บรักษาข้อมูลที่สำคัญทางธุรกิจ ข้อมูลความลับเกี่ยวกับบริษัท ตลอดจนผู้มีส่วนได้ส่วนเสียของบริษัท และปฏิบัติตามอย่างเคร่งครัด โดยไม่เปิดเผยต่อผู้ไม่เกี่ยวข้องทั้งภายในและภายนอกบริษัท แม้จะเกษียณอายุ ลาออก หรือสิ้นสุดการทำงานกับบริษัทแล้วก็ตาม เว้นแต่เป็นไปตามข้อบังคับโดยกฎหมายหรือมติของคณะกรรมการบริษัท
4. บุคลากรของบริษัทต้องไม่นำข้อมูลภายในของบริษัทซึ่งยังมิได้เปิดเผยต่อสาธารณชนไปใช้แสวงหาผลประโยชน์แก่ตนเองและผู้อื่นในทางมิชอบ
5. บุคคลภายนอกซึ่งจำเป็นต้องเข้ามาเกี่ยวข้องหรือรับรู้ข้อมูลภายในที่สำคัญของบริษัท ต้องลงนามในข้อตกลงการรักษาความลับข้อมูล (Non-Disclosure Agreement: NDA) เพื่อให้มั่นใจว่าข้อมูลภายในของบริษัทจะถูกรักษาเป็นความลับอย่างรัดกุมและใช้ในกิจการของบริษัทเท่านั้น
6. การเปิดเผยข้อมูลที่สำคัญทางธุรกิจจะทำได้จนกว่าจะได้รับการอนุมัติให้เปิดเผย โดยผู้บริหารสูงสุด หรือผู้ได้รับมอบอำนาจเท่านั้น หากต้องตอบคำถามชี้แจงข้อมูลที่สำคัญทางธุรกิจ โดยที่ตนไม่มีหน้าที่ในการเปิดเผยข้อมูล ให้แจ้งเรื่องไปยังผู้มีหน้าที่ เพื่อดำเนินการเปิดเผยข้อมูลตามขั้นตอนต่อไป
7. ให้สำรองข้อมูลสำคัญของบริษัทไว้ในระบบฐานข้อมูลสารสนเทศที่บริษัทจัดไว้ โดยจัดให้มีการกำหนดสิทธิ์ผู้ใช้งานและการเข้าถึงข้อมูล
8. ให้มีคณะกรรมการหรือผู้รับผิดชอบตรวจสอบข้อมูลสำคัญของบริษัท อย่างสม่ำเสมอโดยให้กำหนดระยะเวลาทั้งการตรวจสอบข้อมูลและการทำลายข้อมูลแต่ละประเภทที่ชัดเจน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เป้าหมาย : มีการกำกับดูแลรักษาข้อมูลสารสนเทศที่สำคัญขององค์กรและข้อมูลสารสนเทศมีความพร้อมใช้งานถูกต้อง ทันกาล และเป็นปัจจุบัน

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านข้อมูลและการตรวจสอบ
2. สนับสนุนให้มีการดำเนินธุรกิจของ ธพส. เป็นไปตามนโยบายด้านข้อมูลและการตรวจสอบ

ผู้บริหาร :

1. สนับสนุน เพื่อขับเคลื่อนการดำเนินงาน โดยจัดให้มีกลยุทธ์ เป้าหมาย แผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนผู้บริหารในการดำเนินงานด้านข้อมูลและการตรวจสอบ เช่น คณะกรรมการ คณะทำงาน หน่วยงาน ผู้รับผิดชอบ เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง เพื่อสร้างการมีส่วนร่วมของผู้มีส่วนได้เสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ ปูจกจิตสำนึกและสร้างวัฒนธรรมด้านข้อมูลและการตรวจสอบ รวมถึงปฏิบัติตนเป็นให้แบบอย่างแก่พนักงาน
4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานด้านข้อมูล และการตรวจสอบก่อนนำเสนอคณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับเป้าหมายและนโยบายข้อมูลและการตรวจสอบ
2. รับทราบและถือปฏิบัติตามนโยบาย รวมทั้งช่วยสนับสนุน ผลักดันการปฏิบัติงานภายใต้ขอบเขตของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล

หน่วยงานบุคคลรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบายด้านข้อมูลและการตรวจสอบ
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย สอบทานความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูลพิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงานด้านข้อมูลและการตรวจสอบต่อผู้บริหารเป็นประจำทุกปี
3. พัฒนาระบบบริหารจัดการ และระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เรื่อง นโยบายและแนวปฏิบัติในการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ องค์กร (Information Security Management System (ISMS) Audit)

วัตถุประสงค์

1. เพื่อให้มั่นใจว่า บริษัทกำหนดนโยบายและข้อปฏิบัติเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำ
ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง
แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. เพื่อให้มั่นใจว่า บริษัทจัดให้มีการควบคุมด้านการรักษาความปลอดภัยระบบสารสนเทศ
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
3. เพื่อให้มั่นใจว่า บริษัทได้ดำเนินการควบคุมตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ
พ.ศ.2553
4. เพื่อให้ทราบปัญหา และอุปสรรคในการปฏิบัติงานตามพระราชบัญญัติว่าด้วยการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ และให้ข้อเสนอแนะ
เพื่อการพัฒนางาน

ขอบเขตการดำเนินงาน

1. ดำเนินการสอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการจัดให้มีการควบคุมและการปฏิบัติตาม
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และประกาศคณะกรรมการ
ธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของหน่วยงานของรัฐ พ.ศ. 2553 ที่บริษัทใช้อยู่ในปัจจุบัน
2. ดำเนินการสุ่มสอบทานการปฏิบัติตามนโยบายและข้อปฏิบัติของบริษัท
3. สังเกตการปฏิบัติงานจริงตามระบบควบคุมที่กำหนดตามนโยบายและข้อปฏิบัติ
4. สอบถามและสัมภาษณ์ ผู้บริหารและผู้ปฏิบัติงาน

ข้อมูลพื้นฐานเพื่อประกอบการตรวจสอบ

1. การตรวจสอบด้านสารสนเทศ ตามมาตรฐานการตรวจสอบภายในของกรมบัญชีกลางที่กำหนด
ในมาตรฐานการตรวจสอบภายในรหัส 1210.A3 กำหนดให้ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอ เกี่ยวกับ
ความเสี่ยงและการควบคุมพื้นฐานด้านสารสนเทศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2. โครงสร้างพื้นฐานด้านสารสนเทศ ประกอบด้วย

2.1 กระบวนการ (Process)

2.2 ข้อมูลสารสนเทศ (Information)

2.3 ฮาร์ดแวร์ (Hardware) เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ต่อพ่วง เป็นต้น

2.4 ซอฟต์แวร์ (Software)

2.5 เน็ตเวิร์ค (Network) เช่น อุปกรณ์เครือข่าย สายสัญญาณเครือข่าย เป็นต้น

2.6 บุคลากร (Personnel) บุคลากรที่เกี่ยวข้องในขอบเขต

2.7 สถานที่ (Site) เช่น อาคารสำนักงาน สถานที่ตั้ง เป็นต้น

2.8 บริษัทฯ (Organization) เช่น หน่วยงานภายนอกที่เกี่ยวข้องในขอบเขต เป็นต้น

2.9 เครื่องแม่ข่ายเสมือน (Virtual Machine)

3. การควบคุมความปลอดภัย แบ่งเป็น 3 ด้าน คือ

3.1 มุมมองทางด้านกายภาพ (Physical Control) ได้แก่ ระบบควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์ Hardware ระบบ Backup/Restore และ ระบบไฟสำรอง เช่น มี UPS เพียงพอหรือไม่ และอุปกรณ์เฝ้าระวังเช่น กล้องวงจรปิด (CCTV) เป็นต้น

3.2 มุมมองทางด้านเทคนิค (Technical Control) ได้แก่ การตรวจสอบระบบปฏิบัติการ (NOS Audit) การตรวจสอบอุปกรณ์เครือข่าย (Network Devices Audit) การตรวจสอบอุปกรณ์รักษาความปลอดภัย (Security Devices Audit) การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit) และการตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะ Server (Application Specific Audit)

3.3 มุมมองทางด้านการบริหารจัดการ (Administrative Control) ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่าครอบคลุม และ มีการปฏิบัติตามหรือไม่ ในขั้นตอนนี้รวมถึงการตรวจสอบว่าองค์กรมีการจัดฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) หรือไม่ ซึ่งตามปกติควรจะมีเป็นประจำทุกปี การตรวจสอบการบริหารจัดการนั้นต้องพิจารณาจากโครงสร้างบริษัท การแบ่งแยกหน้าที่ต่างๆ ในบริษัท การจัดทำแผนสำรองฉุกเฉิน และแผนรองรับเหตุการณ์ (Business Continuity Planning , Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management) สำหรับการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนดเป็นการตรวจสอบทางด้านกายภาพ และการตรวจสอบทางด้านการบริหารจัดการ

4. การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดในเรื่องต่อไปนี้

4.1 การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ดังนี้

4.1.1 การควบคุมระบบคอมพิวเตอร์ของหน่วยงานตาม มาตรา 15 เพื่อป้องกันผู้ให้บริการที่เข้าไปกระทำความผิดตามพระราชบัญญัติคอมพิวเตอร์ เช่น นำเข้าข้อมูลอันเป็นเท็จทำให้เกิดความเสียหายต่อความมั่นคง สร้างความตื่นตระหนกต่อประชาชน หรือเผยแพร่ภาพลามกอนาจาร เป็นต้น

4.1.2 การเก็บข้อมูลจราจร หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ และอื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ตามมาตรา 26 กำหนดให้บริษัทต้องจัดเก็บข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง

4.2 การควบคุมประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ดังนี้

4.2.1 ให้จัดทำนโยบายและข้อปฏิบัติให้ครอบคลุมเนื้อหาตามที่ประกาศกำหนด

4.2.2 ให้ทบทวนประกาศนโยบายและข้อปฏิบัติที่เผยแพร่ให้เป็นปัจจุบัน

4.2.3 ให้ปฏิบัติตามนโยบายและข้อปฏิบัติที่กำหนด

4.2.4 กรณีที่เกิดความเสียหาย อันตรายต่อองค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติผู้บริหารระดับสูงต้องรับผิดชอบต่อความเสียหายดังกล่าว

4.2.5 บริษัทสามารถเลือกใช้ข้อปฏิบัติที่ต่างจากประกาศได้หากมีความเหมาะสมกว่าหรือเทียบเท่า

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management System (ISMS) Audit)

2. สนับสนุนให้การดำเนินธุรกิจของ ธพส. ให้เป็นไปตามนโยบาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานตามนโยบาย ISMS Audit เพื่อให้บรรลุเป้าหมาย โดยจัดให้มีกลยุทธ์ แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนในการดำเนินงาน เช่น คณะกรรมการ คณะทำงาน บริษัทรับผิดชอบ เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง เพื่อสร้างการมีส่วนร่วมของผู้มีส่วนได้เสีย นำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ เพื่อให้บุคลากรทุกระดับและทุกฝ่ายให้ตระหนักถึงแนวทางการบริหารความเสี่ยงในมีการป้องกันและติดตาม เพื่อรับมือความเสี่ยงที่อาจเกิดขึ้น
4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณารายงานผลการดำเนินงาน ก่อนนำเสนอ คณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและถือปฏิบัติตามนโยบาย รวมทั้งช่วยสนับสนุน ผลักดันการปฏิบัติงานภายใต้ขอบเขตของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารคู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. ติดตามความก้าวหน้าในการดำเนินงาน ตรวจสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุง และจัดทำรายงานผลการดำเนินงานต่อผู้บริหาร คณะอนุกรรมการที่เกี่ยวข้อง และ คณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบการบูรณาการการดำเนินงานและระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยในการติดต่อสื่อสารและเครือข่าย ขององค์กร (Communication and Network Security Management)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจเกี่ยวข้องในการปฏิบัติงานเข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหาย ต่อข้อมูลและระบบสารสนเทศของบริษัท โดยมีการกำหนดนโยบายและแนวปฏิบัติควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่างๆ

ข้อปฏิบัติ

1. มาตรการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี (Malicious Software Prevention) ก่อนนำซอฟต์แวร์จากภายนอกมาใช้งานภายในบริษัท ผู้ใช้งานต้องทำการตรวจสอบซอฟต์แวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้นๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

1.1 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสมในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์

1.2 ผู้ดูแลระบบต้องมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยพร้อมใช้งานอยู่เสมอ

1.3 ผู้ดูแลระบบต้องทำการตรวจทานระบบข้อมูลเพื่อตรวจหาไวรัสและซอฟต์แวร์อันตรายอยู่เป็นประจำ

1.4 ผู้ใช้งานต้องตรวจหาไวรัสของไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตก่อนนำไปใช้งาน

1.5 ห้ามมิให้เจ้าหน้าที่ดำเนินการใดๆ ที่เกี่ยวกับการพัฒนาไวรัสหรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

1.6 ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกมาใช้ ผู้ใช้งานสื่อข้อมูลนั้นต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

2. มาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเทอร์เน็ต (Website and Internet Security)

2.1 ไม่ใช้อินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม หรือเว็บไซต์ที่ละเมิดลิขสิทธิ์

2.2 ห้ามเปิดเผยข้อมูลลับ รวมทั้งข้อมูลที่ยังไม่ได้ประกาศอย่างเป็นทางการของบริษัทผ่านอินเทอร์เน็ตและโซเชียลเน็ตเวิร์ก

2.3 การดาวน์โหลด และการอัปเดตโปรแกรมต่างๆ จากอินเทอร์เน็ตต้องกระทำโดยไม่ละเมิดลิขสิทธิ์

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐

ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐

โทร. ๐ ๒๑๔๖ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๔๔๔๔ www.dad.co.th

2.4 ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่อรับส่งข้อความ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.5 ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัท โดยไม่แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ ในเชิงธุรกิจจากการใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัท

2.6 ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Mail Box) ของตนเองทุกวัน

2.7 ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

2.8 ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้

2.8.1 จดหมายขยะ (Spam Mail)

2.8.2 จดหมายลูกโซ่ (Chain Letter)

2.8.3 จดหมายที่ละเมิดสิทธิของบุคคลอื่น

2.8.4 จดหมายที่มีเนื้อหาขัดต่อศีลธรรม

2.9 ต้องจำกัดผู้รับจดหมายอิเล็กทรอนิกส์ เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

2.10 ต้องไม่เผยแพร่ข้อความที่ให้ร้ายอันจะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัทและบุคคลอื่น

2.11 ห้ามเผยแพร่ภาพ หรือข้อความใดๆ อันก่อให้เกิดความเสียหายต่อบริษัท รวมทั้งละเมิดสิทธิของบุคคลอื่น ผ่านช่องทางอินเทอร์เน็ต และโซเชียลเน็ตเวิร์ก

3. มาตรการรักษาความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

3.1 กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย

3.2 ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้งานนอกที่ติดต่อกับบริษัท

3.3 ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

3.4 ต้องมีการลงนามในสัญญาระหว่างบริษัทและหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA)

4. มาตรการรักษาความมั่นคงปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

4.1 ฝ่ายดิจิทัลต้องกำหนดรายการโปรแกรมที่ต้องติดตั้ง และโปรแกรมที่ห้ามติดตั้งลงในคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone ที่จะนำมาใช้ปฏิบัติงานที่เชื่อมต่อกับระบบสารสนเทศและเครือข่ายของบริษัท

4.2 ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone ที่ใช้ในการปฏิบัติงาน

4.3 ผู้ใช้งานต้องล็อกหน้าจอหรือตั้ง Screen Server เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone ที่ใช้ปฏิบัติงาน เกินกว่า 30 นาที และเมื่อกลับมาใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

4.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นนำรหัสผู้ใช้งานและรหัสผ่านที่เข้าใช้เครื่องคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone ไปใช้งาน

4.5 ผู้ใช้งานต้องตรวจสอบคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone ที่นำมาใช้ปฏิบัติงานว่าได้ติดตั้งโปรแกรมตามที่ ฝ่ายดิจิทัลกำหนดไว้หรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งผู้ดูแลระบบ หรือเจ้าหน้าที่ที่ได้รับมอบหมาย เพื่อขอรับการติดตั้งก่อนการใช้งาน

4.6 ผู้ใช้งานต้องตรวจสอบคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone ที่นำมาใช้ปฏิบัติงานว่าไม่ได้ติดตั้งโปรแกรมที่ห้ามติดตั้งตามที่ฝ่ายดิจิทัลกำหนด

4.7 ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone

4.8 โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ส่วนบุคคล Laptop Tablet และ Smart Phone ของบริษัท ต้องเป็นโปรแกรมที่ลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

4.9 หากมีการนำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินของบริษัท มาใช้งานกับระบบเครือข่ายของบริษัท ต้องได้รับอนุญาตจากผู้อำนวยการอาวุโส ฝ่ายดิจิทัลก่อนการใช้งาน

4.10 กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์ที่นำมาปฏิบัติงานภายในบริษัท ทั้งที่เป็นทรัพย์สินส่วนตัวและของบริษัท

4.11 ผู้ใช้ต้องมีการสำรองข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

4.12 ฝ่ายดิจิทัล ต้องจัดเตรียมอุปกรณ์หรือพื้นที่ที่สามารถใช้สำรองข้อมูลออกมาจากเครื่องคอมพิวเตอร์

4.13 ผู้ใช้ต้องมีการเข้ารหัสข้อมูลสำคัญ และข้อมูลที่เป็นความลับก่อนจะสำรองข้อมูลออกมาจากเครื่องคอมพิวเตอร์

5. มาตรการควบคุมการเข้าถึง (Access Control)

5.1 การควบคุมการเข้าถึง

5.1.1 ต้องกำหนดประเภทของการให้บริการที่ต้องการ ระดับการให้บริการที่พึงประสงค์ และมาตรการความมั่นคงปลอดภัยไว้ในข้อตกลงการให้บริการ (Service Level Agreement) ให้เป็นส่วนหนึ่งของสัญญาจ้าง

5.1.2 ต้องกำหนดให้มีการวางแผนการถ่ายโอนงานก่อนที่จะมีการถ่ายโอนงานให้กับผู้ให้บริการภายนอก

5.1.3 ต้องกำหนดให้มีแผนการควบคุมเข้าถึงข้อมูลและระบบงานสำคัญ หรือเป็นความลับของบริษัท จากผู้ให้บริการภายนอก

5.1.4 กำหนดให้ผู้ให้บริการภายนอกต้องจัดส่งแผนการสร้างความปลอดภัยในการปฏิบัติงาน เพื่อให้สามารถช่วยกู้คืนข้อมูลและสารสนเทศให้กลับมาใช้งานได้อย่างรวดเร็ว หลังจากเกิดเหตุหยุดชะงักจากการเรียกใช้บริการผู้ให้บริการภายนอก

5.1.5 กำหนดให้ผู้ให้บริการภายนอกต้องรายงานเหตุการณ์ความมั่นคงปลอดภัย หรือจุดอ่อนในระบบสารสนเทศที่พบ

5.1.6 กำหนดให้ผู้บริการภายนอกต้องจัดการและแก้ไขเหตุการณ์ความมั่นคงปลอดภัย หรือจุดอ่อนที่พบซึ่งเกี่ยวข้องกับบริการที่ว่าจ้าง

5.1.7 เมื่อพบว่าผู้ให้บริการภายนอกไม่สามารถให้บริการได้ตามระดับการให้บริการที่ตกลงไว้ ธพส. ต้องกำหนดให้ผู้บริการภายนอกต้องนำเสนอแผนการปรับปรุงตามความจำเป็น

5.2 การควบคุมการเข้าถึงเครือข่ายและบริการคอมพิวเตอร์

5.2.1 มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนอนุญาตให้เข้าถึงระบบเครือข่าย ด้วยการใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

5.2.2 ผู้ใช้งานต้องเข้าสู่ระบบเครือข่ายด้วยชื่อผู้ใช้ และรหัสผ่านที่ได้รับอนุญาตจากผู้อำนวยการฝ่ายดิจิทัล

5.2.3 ผู้ใช้งานต้องยืนยันตัวบุคคลเพื่อใช้งานเครือข่ายด้วยชื่อผู้ใช้และรหัสผ่านของตนเองเท่านั้น หากมีปัญหาในเข้าถึงระบบเครือข่าย ต้องแจ้งให้ผู้ดูแลระบบ หรือเจ้าหน้าที่ที่ได้รับมอบหมายเพื่อแก้ไข

5.2.4 ผู้ใช้งานที่เป็นเจ้าของชื่อผู้ใช้ ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดจากความเสียหายจากการใช้งานเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น และผู้ใช้งานไม่ได้มอบชื่อผู้ใช้ และรหัสผ่านให้แก่ผู้กระทำความผิด

5.2.5 กำหนดให้เก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ไว้ในสื่อเก็บข้อมูลอย่างน้อย 90 วัน นับตั้งแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์โดย กำหนดขึ้นความลับในการเข้าถึงข้อมูลเป็นลับมาก และมีวิธีการป้องกันการแก้ไข เปลี่ยนแปลงโดยไม่ได้รับ อนุญาต รวมทั้งจำกัดสิทธิ์การเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

5.2.6 กำหนดให้มีการบันทึกการเข้า-ออกเครือข่าย และความพยายามเข้าสู่เครือข่ายของ ผู้ใช้งานไว้อย่างน้อย 90 วัน นับตั้งแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

เป้าหมาย : เพื่อป้องกันความเสียหายและลดความเสี่ยงด้านความมั่นคงปลอดภัยด้านการติดต่อสื่อสารและ เครือข่ายขององค์กร

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านความมั่นคงปลอดภัยด้านการติดต่อสื่อสารและเครือข่ายของ องค์กร
2. สนับสนุนให้การดำเนินธุรกิจของ ธพส. เป็นไปตามนโยบาย

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานตามนโยบาย เพื่อให้บรรลุตามเป้าหมาย โดยจัดให้มีกลยุทธ์ แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นตัวแทนผู้บริหารในการ ดำเนินงาน เช่น คณะกรรมการ คณะทำงาน หน่วยงานรับผิดชอบ เป็นต้น

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง สร้างการมีส่วนร่วมของผู้มีส่วนได้เสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง

3. ส่งเสริมสนับสนุนความรู้ เพื่อให้บุคลากรทุกระดับและทุกฝ่ายให้ตระหนักและมีแนวทางการบริหารความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศเพื่อให้มีการป้องกันไม่ให้บุคคลอื่นสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศ อุปกรณ์ที่ใช้งานด้านเทคโนโลยีสารสนเทศ และข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานด้านการบริหารจัดการความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศก่อนนำเสนอคณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและถือปฏิบัติตามนโยบาย รวมทั้งช่วยสนับสนุน ผลักดันการปฏิบัติงานภายใต้ขอบเขตของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย ตรวจสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงาน ต่อผู้บริหาร คณะอนุกรรมการ และคณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบการและเครื่องมือเพื่อสนับสนุนการดำเนินงาน

เรื่อง นโยบายและแนวปฏิบัติในการบริหารจัดการคอนฟิกูเรชัน (Configuration Management)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม จัดเก็บสถานะของ Software และ Hardware ค่าคอนฟิกูเรชันระบบสารสนเทศต่างๆ ที่ใช้งานภายใน บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ให้มีความปลอดภัย และลดความเสี่ยงที่จะเกิดขึ้น รวมถึงมีการสอบทานเพื่อป้องกันข้อผิดพลาดในการปฏิบัติงานให้เป็นไปตามมาตรฐาน โดยมีการกำหนดนโยบายและแนวปฏิบัติควบคุมให้สอดคล้องกับหน้าที่ของผู้รับผิดชอบ

การบริหารจัดการคอนฟิกูเรชัน (Configuration Management)

กระบวนการการบริหารจัดการคอนฟิกูเรชัน (Configuration Management)

1. เมื่อมีการปรับปรุง แก้ไข หรือเพิ่มเติมอุปกรณ์ ค่าคอนฟิกูเรชัน ต้องทำการร้องขอแก้ทางเจ้าหน้าที่ฝ่ายดิจิทัล โดยกรอกรายละเอียดลงแบบฟอร์มขอปรับปรุง/แก้ไข Configuration/Change Request ระบบสารสนเทศ
2. ระบุประเภทของอุปกรณ์ที่นำเข้ามาใช้งาน เช่น
 - 2.1 Network
 - 2.2 Server
 - 2.3 Hardware
 - 2.4 Operation System
 - 2.5 Application
 - 2.6 Computer
3. ตรวจสอบและพิจารณาถึงผลกระทบต่อค่าคอนฟิกูเรชัน (Configuration) โดยมีการจัดทำแผนการดำเนินงาน หากมีผลกระทบจะต้องปรับแก้ไขใหม่ หรือยุติการดำเนินงานจนกว่าจะไม่เกิดผลกระทบต่อองค์กร ให้ผู้จัดการส่วนในแต่ละส่วนงานของฝ่ายดิจิทัลพิจารณาเพื่อลดความเสี่ยงที่จะเกิดขึ้นกับองค์กร และรายงานต่อผู้อำนวยการอาวุโสฝ่ายดิจิทัลเพื่ออนุมัติการดำเนินงาน
4. จัดบันทึกค่าอุปกรณ์ตาม Baseline Standard ของอุปกรณ์ ดังนี้
 - 4.1 บันทึกข้อมูลจากอุปกรณ์ที่เกิดขึ้นใหม่
 - 4.2 บันทึกจากและการเปลี่ยนแปลงค่าจากอุปกรณ์เดิม
5. ปรับปรุง แก้ไขค่าคอนฟิกูเรชัน (Configuration) เดิมหรือ ติดตั้งค่าคอนฟิกูเรชัน (Configuration) ของอุปกรณ์ใหม่ จากนั้นทำการทดสอบก่อนใช้งานจริงแล้วดำเนินการ Update ข้อมูลของอุปกรณ์ที่ใช้งาน เพื่อให้เกิดข้อมูลที่เป็นปัจจุบันเสมอ
6. ตรวจสอบการกำหนดค่าคอนฟิกูเรชัน (Configuration) ที่ได้ปรับปรุงแก้ไข
7. จัดเก็บข้อมูลเกี่ยวกับการกำหนดค่าคอนฟิกูเรชัน (Configuration) กับอุปกรณ์ไว้ที่ฐานข้อมูล โดยมีการระบุหมายเลข Revision ที่มีการปรับแก้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

8. จัดทำ Report ในส่วนของการปรับปรุง แก้ไข หรือเพิ่มเติมอุปกรณ์ เพื่อส่งให้ผู้จัดการส่วนในแต่ละส่วนงานตรวจสอบความถูกต้อง และรายงานต่อผู้อำนวยการอาวุโสฝ่ายดิจิทัลรับทราบ

9. มีการตรวจสอบความปลอดภัยเชิงรุก (Compromise Assessment and Security Baseline) กรณีที่ไม่เป็นไปตามการตั้งค่าต้องประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอ และต้องได้รับการอนุมัติจากผู้อำนวยการฝ่ายดิจิทัล

การจัดทำเอกสาร Minimum Baseline Standard

เพื่อเป็นมาตรฐานในการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่างๆ อย่างเป็นลายลักษณ์อักษร และมีการทบทวนปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ โดยนำ Minimum Baseline Standard จากชนิดอุปกรณ์ ระบบปฏิบัติการ ซอฟต์แวร์เบื้องต้นที่มีการทดสอบแล้ว หรือเป็นค่าพื้นฐานมาตั้งต้น และจัดเก็บเป็น Version ที่ 1 พร้อมทั้งจัดทำเอกสาร Baseline Checklist เพื่อเป็นการตรวจสอบความถูกต้องและความเข้ากันได้ของการกำหนดค่า Configuration

การจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน (System Configuration Version Control)

จัดทำ Version Control ในการบริหารจัดการเปลี่ยนแปลง Configuration เพื่อเก็บประวัติการเปลี่ยนแปลงในแต่ละครั้งเมื่อมีการร้องขอ และมีการมอบหมายผู้ดูแลรับผิดชอบอย่างชัดเจน

แนวทางการวัดประสิทธิผลของการบริหารจัดการคอนฟิกูเรชัน (Configuration Management)

1. ค่าคอนฟิกูเรชันของอุปกรณ์ในระบบสารสนเทศ ไม่ต่ำกว่า 90% จะต้องถูกต้องตาม Baseline Standard โดยอุปกรณ์ใหม่หรือระบบที่มีการติดตั้งใหม่จะต้องยึดตาม Baseline Standard เป็นหลัก

2. ค่าคอนฟิกูเรชันของอุปกรณ์ในระบบสารสนเทศ ที่มีการปรับปรุง แก้ไข เปลี่ยนแปลงค่าต่างๆ ไม่ต่ำกว่า 90% ถูกต้องและเป็นปัจจุบัน โดยอ้างอิงจาก Baseline Standard และจากการรายงานผลการปรับปรุง แก้ไข เปลี่ยนแปลง ค่าคอนฟิกูเรชัน

เป้าหมาย : เพื่อลดความเสี่ยงและป้องกันข้อผิดพลาดในการปฏิบัติงานให้เป็นไปตามมาตรฐาน

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านการบริหารจัดการคอนฟิกูเรชัน (Configuration Management)

2. สนับสนุนให้การดำเนินธุรกิจของบริษัท ให้เป็นไปตามนโยบาย

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานตามนโยบาย เพื่อให้บรรลุตามเป้าหมาย โดยจัดให้มีกลยุทธ์ แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนผู้บริหารในการดำเนินงาน เช่น คณะกรรมการ คณะทำงาน หน่วยงานรับผิดชอบ เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง สร้างการมีส่วนร่วมของผู้มีส่วนได้เสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ เพื่อให้บุคลากรทุกระดับและทุกฝ่ายตระหนักรู้และมีแนวทางการบริหาร ความเสี่ยงเพื่อให้มีการป้องกัน ติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น
4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานก่อนนำเสนอ คณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติ ตามนโยบาย สนับสนุน ผลักดันการปฏิบัติตามนโยบาย ภายใต้ขอบเขตของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงาน

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสาร คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย ตรวจสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงาน ต่อผู้บริหาร คณะอนุกรรมการ และคณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบการและเครื่องมือ

เรื่อง นโยบายและแนวปฏิบัติในการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(IT Asset Management: ITAM)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการใช้งานทรัพย์สิน (Asset) ทั้งหมดที่เกี่ยวข้องกับข้อมูลในระบบสารสนเทศที่ใช้ภายในบริษัท ธนาคารพัฒนาสินทรัพย์ จำกัด (ธพส.) รวมถึงหน้าที่ความรับผิดชอบในการป้องกันทรัพยากรข้อมูลสารสนเทศให้มีความปลอดภัย และปรับปรุงทะเบียนทรัพย์สิน ให้มีความถูกต้องและเป็นปัจจุบัน มีความพร้อมใช้งาน และสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครอบคลุม การจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน

2. จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำ ปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ และบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศ สิ้นสุดตามอายุการใช้งาน (End of Life) หรือสิ้นสุดการให้บริการ (End of Support) จากผู้ผลิตได้อย่างเหมาะสม

3. มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Inventory List) ของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่รองรับระบบเทคโนโลยีสารสนเทศของบริษัทอย่างครบถ้วนและเป็นลายลักษณ์อักษรโดยครอบคลุมอย่างน้อย ดังนี้

3.1 ชื่อเครื่องแม่ข่าย

3.2 ชื่อระบบปฏิบัติการ (Operating System) และเวอร์ชัน (Version)

3.3 ชื่อระบบงาน (Application) และเวอร์ชัน (Version)

3.4 เจ้าของทรัพย์สิน (Owner)

3.5 ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (Specification)

3.6 หมายเลขอ้างอิงของฮาร์ดแวร์ (Serial Number) และหมายเลขอ้างอิงของซอฟต์แวร์ (Software license)

3.7 สถานที่ตั้ง

3.8 วันที่เริ่มติดตั้ง

3.9 ประเภทการครอบครอง (ซื้อหรือเช่า)

3.10 รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา

3.11 วันที่บำรุงรักษาล่าสุด

3.12 วันสิ้นสุดการใช้งานตามสัญญา (Warranty) และวันสิ้นสุดการรับประกันการใช้งาน (Support Contract)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

3.13 วันสิ้นสุดการให้บริการจากผู้ผลิต (End of Support)

4. มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

5. มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในบริษัทและกรณีให้ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของบริษัททันทีที่มีการยกเลิกสัญญาจ้างด้วย

6. รายงานการเปลี่ยนแปลงของทรัพย์สินในความรับผิดชอบของตนต่อผู้อำนวยการอาวุโสฝ่ายดิจิทัลเพื่อรับทราบ

7. กำหนดหน้าที่ความรับผิดชอบและควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control) ดังนี้

7.1 ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัทต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน

7.2 ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม

7.3 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัทเว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน

7.4 ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ รวมถึงอุปกรณ์ต่อพ่วงให้มีสภาพเดิม

7.5 ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ

7.6 ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็กไฟฟ้าแรงสูง ในที่มีการสัมผัสเตือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

7.7 ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับหรือโยน ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่

7.8 หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

7.9 ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน

7.10 การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท

7.11 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางอุปกรณ์ทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

8. มีการควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License) ให้ถูกต้องลิขสิทธิ์ และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมาย

เป้าหมาย: เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งาน และสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management : ITAM)
2. สนับสนุนให้การดำเนินธุรกิจของบริษัทให้เป็นไปตามนโยบาย

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานตามนโยบาย เพื่อให้บรรลุตามเป้าหมาย โดยจัดให้มีกลยุทธ์แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนผู้บริหารในการดำเนินงาน เช่น คณะกรรมการ คณะทำงาน หน่วยงานรับผิดชอบ เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง สร้างการมีส่วนร่วมของผู้มีส่วนได้เสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ เพื่อให้บุคลากรทุกระดับและทุกฝ่ายให้ความตระหนักและมีแนวทางการบริหารความเสี่ยงเพื่อให้มีการป้องกัน ติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น
4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงาน ก่อนนำเสนอคณะกรรมการ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติ ตามนโยบาย สนับสนุน ผลักดันการปฏิบัติตามนโยบาย ภายใต้ขอบเขตของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงาน

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย ทวนสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงาน ต่อผู้บริหาร คณะอนุกรรมการ และคณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบการและเครื่องมือ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศ และข้อมูลสารสนเทศ (IT Asset, Data and Information Security Management Policy)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการมิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้อง เข้าถึงและใช้อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย ระบบเทคโนโลยีสารสนเทศ และข้อมูลสารสนเทศที่ใช้ภายในบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด(ธพส.) โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์ในการเข้าถึง เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวตนได้

การกำหนดพื้นที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่ต้องการรักษาความปลอดภัย

เพื่อเป็นการควบคุม ป้องกัน และรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของระบบเทคโนโลยีสารสนเทศ อุปกรณ์ที่ใช้งานด้านเทคโนโลยีสารสนเทศ รวมไปถึงข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศ

1. การกำหนดพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่ต้องการรักษาความปลอดภัย

1.1 ภายในองค์กรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมโดยมีวัตถุประสงค์เพื่อการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

1.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

1.2.1 จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

1.2.2 บันทึกการเข้าออกพื้นที่ใช้งานและกำหนดเจ้าหน้าที่สำหรับรับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

1.2.3 จัดให้มีเจ้าหน้าที่สำหรับตรวจสอบประวัติการเข้าพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง

2. การควบคุมการเข้า-ออก พื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2.1 จัดทำเอกสารระบุสิทธิ์ของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงพื้นที่ โดยแบ่งแยกได้ดังนี้

2.1.1 มีการควบคุมการเข้าออกสถานที่ตั้งของระบบเทคโนโลยีสารสนเทศอย่างรัดกุม

2.1.2 การเข้า-ออกอาคารธนพิพัฒน์ ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการลงบันทึกข้อมูลในสมุดบันทึกการเข้า-ออก

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

2.1.3 กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำทรัพย์สินสารสนเทศเข้า-ออก บริเวณ อาคารธนพิพัฒน์ เช่น เครื่องแม่ข่าย หรืออุปกรณ์เครือข่าย ต้องขออนุญาตจากผู้อำนวยการฝ่ายดิจิทัลก่อน ทุกครั้ง โดยเจ้าหน้าที่รักษาความปลอดภัยจะต้องตรวจสอบแบบฟอร์มนำครุภัณฑ์เข้า-ออกอาคารให้ถูกต้อง

2.1.4 เจ้าหน้าที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่อขออนุญาตการเข้า-ออก ในแบบฟอร์ม การเข้า-ออกให้ถูกต้อง

2.1.5 ต้องมีเจ้าหน้าที่ ทรพ. ดูแลบุคคลภายนอกหรือผู้มาติดต่อในพื้นที่ที่มีความสำคัญ ทุกครั้งจนเสร็จสิ้นภารกิจ

การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security)

เพื่อเป็นการรักษาความปลอดภัยของข้อมูลสารสนเทศไม่ให้บุคคลที่ไม่เกี่ยวข้องเข้าถึง ล้วงรู้ หรือ แก้ไขเปลี่ยนแปลงข้อมูลสารสนเทศในส่วนที่มีอำนาจหน้าที่เกี่ยวข้อง และให้ตระหนักถึงความสำคัญของ ข้อมูลและมีวิธีปฏิบัติที่เหมาะสมในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศแต่ละประเภท ระดับ และชั้นความลับ

1. การกำหนดประเภทข้อมูลสารสนเทศ ระดับข้อมูลสารสนเทศ และระดับชั้นความลับข้อมูล สารสนเทศ (Information Classification)

1.1 การจัดแบ่งประเภทข้อมูลสารสนเทศ ประกอบด้วย

1.1.1 ข้อมูลการบริหาร ได้แก่

- นโยบาย
- ข้อมูลยุทธศาสตร์ แผน และภารกิจของบริษัท
- ผลการปฏิบัติงาน
- กฎหมาย ระเบียบ แนวปฏิบัติ ขั้นตอนปฏิบัติ
- ข้อมูลบุคลากร
- งบประมาณ

1.1.2 ข้อมูลสารสนเทศ ได้แก่

- ข้อมูลการเงินและบัญชี
- ข้อมูลทะเบียนสินทรัพย์
- ข้อมูลแจ้งซ่อม
- ข้อมูล Logs
- ข้อมูลการอนุมัติจัดซื้อจัดจ้าง

1.1.3 ข้อมูลด้านการให้บริการ ได้แก่

- ข้อมูลวิชาการและองค์ความรู้
- ข้อมูลพื้นที่อาคาร
- ข้อมูลการให้บริการอื่นๆ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

1.2 การจัดแบ่งระดับความสำคัญของข้อมูลสารสนเทศ สามารถแบ่งออกเป็น 4 ระดับ คือ

1.2.1 มากที่สุด

1.2.2 มาก

1.2.3 สำคัญ

1.2.4 ทั่วไป

1.3 การจัดแบ่งระดับชั้นความลับข้อมูลสารสนเทศ ได้แก่

1.3.1 ลับที่สุด หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากที่สุดต่อการดำเนินงานของบริษัท และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาตจะเกิดความเสียหายแก่บริษัทอย่างร้ายแรงที่สุด

1.3.2 ลับมาก หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากต่อการดำเนินงานของบริษัท และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาตจะเกิดความเสียหายแก่บริษัทอย่างร้ายแรง

1.3.3 ลับ หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่อการดำเนินงานของบริษัท และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่บริษัท

1.3.4 ใ้ภายใน หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่อการดำเนินงานของบริษัท และเปิดเผยได้เฉพาะภายในบริษัทฯ และบุคคลภายนอกที่มีความสัมพันธ์ทางการค้าเท่านั้น ซึ่งไม่เหมาะที่จะเปิดเผยต่อสาธารณชนเป็นการทั่วไป หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาต อาจเกิดความเสียหายแก่บริษัท อย่างไรก็ตาม ข้อมูลสารสนเทศในระดับชั้นนี้จะต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานรวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท

1.3.5 ทั่วไป หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญทั่วไปต่อการดำเนินงานของบริษัท และเป็นข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ อย่างไรก็ตาม ข้อมูลสารสนเทศในระดับชั้นนี้จะต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานรวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท

1.4 การจัดแบ่งระดับชั้นการเข้าถึงข้อมูล ได้แก่

1.4.1 ระดับชั้นสำหรับผู้บริหาร คือ พนักงาน ธพส. ระดับผู้จัดการขึ้นไป ที่มีหน้าที่เกี่ยวข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชา ระดับรองกรรมการผู้จัดการขึ้นไปหรือเทียบเท่า

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

1.4.2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป คือ พนักงาน ธพส. ที่มีหน้าที่เกี่ยวข้องและต้องได้รับอนุญาต จากผู้บังคับบัญชา ระดับผู้อำนวยการขึ้นไปหรือเทียบเท่า

1.4.3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย คือ พนักงาน ธพส. ที่มีหน้าที่เกี่ยวข้อง และต้องได้รับอนุญาตจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล

2. การกำหนดแนวปฏิบัติในการจัดเก็บข้อมูล การควบคุมการเข้าถึงข้อมูลสารสนเทศ รวมถึงการทำลายข้อมูลสารสนเทศ (Information Disposal)

2.1 การจัดเก็บข้อมูลสารสนเทศ

2.1.1 ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กำหนดระยะเวลาจัดเก็บข้อมูลสารสนเทศตามระดับความลับ

2.1.2 จัดเก็บข้อมูลสำรองในสื่อบันทึกข้อมูลและจัดทำรายการบันทึกให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

2.1.3 รักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศและอุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศของบริษัท เช่น โทรศัพท์มือถือ แล็ปท็อป แท็บเล็ต เป็นต้น และต้องระมัดระวังเป็นพิเศษในการใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการ

2.1.4 ตั้งรหัสผ่าน (password) ล็อกหน้าจอซึ่งบรรจุข้อมูลสารสนเทศเมื่อต้องการออกจากระบบสารสนเทศหรือเสร็จสิ้นงาน

2.1.5 รายงานฝ่ายดิจิทัลทันทีเมื่อข้อมูลสารสนเทศหรืออุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศสูญหายหรือถูกขโมย

2.2 การควบคุมการเข้าถึงข้อมูลสารสนเทศ

2.2.1 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบเทคโนโลยีสารสนเทศตามความจำเป็นต่อการใช้งาน

2.2.2 เจ้าของข้อมูล และผู้ดูแลระบบเทคโนโลยีสารสนเทศ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่เท่านั้น

2.2.3 ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการเข้าระบบให้แก่ผู้ใช้งานโดยต้องมีการจัดทำเอกสารขอสิทธิ์การเข้าระบบ และกำหนดให้มีการลงนามอนุมัติ

2.2.4 มีการกำหนดสิทธิ์ของผู้ใช้งาน ดังนี้

- สิทธิ์อ่านอย่างเดียว
- สิทธิ์การเพิ่มข้อมูล
- สิทธิ์การแก้ไขข้อมูล
- สิทธิ์การลบข้อมูล
- สิทธิ์การอนุมัติ/อนุญาต
- ไม่มีสิทธิ์

2.2.5 การระบุสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

2.2.6 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย ตามแบบทะเบียนผู้ใช้งาน

2.2.7 กำหนดให้มีการพิจารณามาตรการปิดบังข้อมูล (Data Masking) สำหรับข้อมูลสำคัญหรือข้อมูลส่วนบุคคล สอดคล้องกับส่วนที่ 1 นโยบายการเข้าถึงและการทำงานของสารสนเทศ เรื่องที่ 17 การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศที่สำคัญ ความต้องการทางธุรกิจ กฎหมาย และกฎระเบียบที่เกี่ยวข้อง ด้วยการทำเครื่องหมายหรือแทนที่ข้อมูล เพื่อไม่ให้อ้างถึงข้อมูลตัวตนของบุคคลได้

2.3 การทำลายข้อมูลสารสนเทศและสื่อบันทึกข้อมูล

2.3.1 ต้องล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนการส่งมอบหรือเปลี่ยนอุปกรณ์

2.3.2 ต้องล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำลายหรือจำหน่าย

2.3.3 กำหนดวิธีการทำลายข้อมูลสารสนเทศบนสื่อบันทึกข้อมูล ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการนำสื่อบันทึกกลับมาใช้ใหม่	วิธีการทำลาย
CD/DVD	-	ใช้การทุบ หรือทำลายให้เสียหาย
สื่อบันทึกข้อมูลแบบถอดแยกได้ เช่น Flash Drive	ใช้การ Format	หากไม่ต้องการนำกลับมาใช้งานซ้ำอีก ให้ใช้การทุบ หรือทำลายให้เสียหาย
ฮาร์ดดิสก์ และ SSD	ต้องฟอร์แมตฮาร์ดดิสก์และ SSD เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์และ SSD โดย 1) ใช้วิธีแบบเขียนทับซ้ำจำนวน 1 ครั้ง ตามมาตรฐาน NIST 800-88 สำหรับข้อมูลใช้ภายในและข้อมูลความลับ 2) เขียนทับซ้ำจำนวน 3 ครั้ง ตามมาตรฐาน DoD 5220.22- M สำหรับข้อมูลที่มีชั้นความลับเป็นลับมาก 3) เขียนทับซ้ำจำนวน 7 ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลลับมากที่สุด	สำหรับข้อมูลลับมากและข้อมูลลับมากที่สุด ใช้วิธีการทุบทำลายตามระเบียบที่ ๖พส. กำหนด

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

ประเภทสื่อ บันทึกข้อมูล	วิธีการนำสื่อบันทึกกลับมาใช้ใหม่	วิธีการทำลาย
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse สำหรับเอกสารที่เป็นชั้นความลับระดับทั่วไป	ใช้เครื่องทำลายเอกสารก่อนทิ้ง สำหรับเอกสารที่เป็นชั้นความลับทุกระดับ

2.3.4 ลบข้อมูลการดำเนินงานที่มีอายุตั้งแต่ 5 ปีขึ้นไป ออกจากฐานข้อมูล และสำรองข้อมูล จัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

2.3.5 ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล และเจ้าของข้อมูล ในการลบข้อมูลสารสนเทศออกจากฐานข้อมูล

3. เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าได้สิทธิ์ต่างๆที่ให้ไว้ยังคงมีความเหมาะสม

4. มีวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบเทคโนโลยีสารสนเทศ ผู้ดูแลระบบมีการกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

5. การรับส่งข้อมูลระดับชั้นความลับ ตั้งแต่ชั้น “ลับ” ขึ้นไปผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล มาตรการการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ

6. มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทหรือกรณีส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองข้อมูลไว้ในสื่อบันทึกข้อมูล และลบข้อมูลสำคัญที่เก็บอยู่ในเครื่องคอมพิวเตอร์ออกก่อน

7. กำหนดให้มีการติดตามและพิจารณาลบข้อมูลสำคัญ ข้อมูลส่วนบุคคล ที่มีการจัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือสื่อบันทึกข้อมูลใด ๆ ด้วยวิธีการที่มั่นคงปลอดภัยตามระยะเวลาการจัดเก็บข้อมูลที่กำหนด หรือเมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไป พร้อมทั้งจัดเก็บบันทึกการลบข้อมูลนั้นไว้เป็นหลักฐาน (Information Deletion)

8. กำหนดให้มีมาตรการควบคุมเพื่อป้องกันข้อมูลรั่วไหล สำหรับระบบเทคโนโลยีดิจิทัล ระบบเครือข่าย และอุปกรณ์ที่ใช้ในการประมวลผล จัดเก็บ และรับส่งข้อมูลสำคัญ (Data Leakage Prevention)

การบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ (Cryptography)

เพื่อป้องกันความเสียหายอันเกิดจากการรั่วไหล เปลี่ยนแปลง ทำซ้ำข้อมูลสารสนเทศที่มีความสำคัญ หรือเป็นความลับให้ข้อมูลสารสนเทศมีความมั่นคงปลอดภัย

1. การเข้ารหัสสำหรับข้อมูลที่เป็นความลับ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

1.1 ต้องมีการควบคุมการเข้าถึงข้อมูลสารสนเทศในแต่ละประเภทขึ้นความลับทั้งการเข้าถึงโดยตรงและผ่านระบบเทคโนโลยีสารสนเทศ

1.2 ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าถึงไฟล์ข้อมูลลับ เพื่อป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในคอมพิวเตอร์ที่ใช้งาน

1.3 ต้องมีการเข้ารหัสข้อมูลที่เป็นความลับซึ่งจัดเก็บไว้ในรูปแบบอิเล็กทรอนิกส์ หรือในฐานข้อมูล ด้วยวิธีที่เป็นมาตรฐานสากล

1.4 ผู้ใช้งานต้องนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544

1.5 ผู้ใช้งานไม่แชร์ไฟล์ข้อมูลลับบนเครือข่ายเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

1.6 ผู้ดูแลระบบต้องกำหนดรูปแบบการเข้ารหัสข้อมูลบนระบบเครือข่ายไร้สาย (Wireless Security) ที่เป็นมาตรฐานสากล เช่น WPA2 WPA-PSK หรือ WPA2-PSK (Wi-Fi Protected Access) เป็นต้น

1.7 การรับ-ส่งข้อมูลสำคัญ ข้อมูลที่เป็นความลับผ่านเครือข่ายสาธารณะ หรือการเข้าใช้งานระบบเทคโนโลยี จากภายนอกสำนักงาน ต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล เช่น VPN เป็นต้น

1.8 การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล ผู้ดูแลระบบต้องมีการกำหนดรหัสก่อนเข้าถึงข้อมูลที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

1.9 กำหนดให้ผู้ที่สามารถใช้เครื่องมือวิเคราะห์ข้อมูลการจราจรบนเครือข่ายได้ ต้องได้รับอนุมัติสิทธิจากผู้อำนวยการอาวุโสฝ่ายดิจิทัล เป็นลายลักษณ์อักษร และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2. การบริหารจัดการกุญแจ

ต้องมีการบริหารจัดการกุญแจ เพื่อการเข้ารหัสข้อมูลตลอดช่วงเวลาการใช้งาน โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัสการกำหนดความยาวของรหัสการใช้งาน และการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้การปฏิบัติให้เป็นไปตามนโยบาย และแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ เช่น มาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูลซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น โดยการบริหารจัดการกุญแจรวมถึงขั้นตอนการปฏิบัติงานต่าง ดังนี้

- การสร้างและการแจกจ่ายกุญแจรหัส
- ความลับของกุญแจส่วนบุคคล
- ความถูกต้องของกุญแจสาธารณะ
- การยกเลิกการใช้กุญแจรหัส
- การกู้คืนกุญแจรหัส
- การสำรองข้อมูลกุญแจรหัส
- การยกเลิกและทำลายกุญแจรหัสที่ไม่ใช้งานแล้ว
- การจัดการที่ไม่ขัดแย้งต่อกฎหมายใด ๆ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

- การจำกัดให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ในการเข้าใช้อุปกรณ์ที่ใช้ในการสร้าง เก็บ หรือสำรอง
กุญแจรหัส

เป้าหมาย : เพื่อป้องกันความเสียหายและลดความเสี่ยงด้านความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยี
สารสนเทศและข้อมูลสารสนเทศ

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและ
ข้อมูลสารสนเทศ
2. สนับสนุนให้การดำเนินธุรกิจของบริษัทเป็นไปตามนโยบาย

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานตามนโยบาย เพื่อให้บรรลุตามเป้าหมาย โดยจัดให้มีกลยุทธ์
แนวทางการบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนผู้บริหารในการ
ดำเนินงาน เช่น คณะกรรมการ คณะทำงาน หน่วยงานรับผิดชอบ เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง สร้างการมีส่วนร่วมของผู้มีส่วนได้เสีย
ในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ เพื่อให้บุคลากรทุกระดับและทุกฝ่ายตระหนักและมีแนวทางการบริหาร
ความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศเพื่อให้มีการป้องกันไม่ให้เกิด
ผู้อื่นสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศ อุปกรณ์ที่ใช้งานด้านเทคโนโลยีสารสนเทศ และข้อมูล
สารสนเทศโดยไม่ได้รับอนุญาต
4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานด้านการ
บริหารจัดการความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศก่อนนำเสนอ

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและถือปฏิบัติตามนโยบาย รวมทั้งช่วยสนับสนุน ผลักดันการปฏิบัติงานภายใต้ขอบเขต
ของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย ทวนสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงานต่อผู้บริหาร คณะอนุกรรมการ และคณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบการและเครื่องมือเพื่อสนับสนุนการดำเนินงาน

เรื่อง นโยบายและแนวปฏิบัติในการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหา ด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการบริหารจัดการเหตุการณ์ผิดปกติ มาการร้องขอการบริการ และ
ปัญหาด้าน เทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ภายใน
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ตลอดจนจัดทำกระบวนการและแนวทางการให้บริการรับแจ้ง
เหตุการณ์ วิเคราะห์ และแก้ไขปัญหาให้กลับสู่สภาวะปกติและมีประสิทธิภาพ เพื่อลดกระบวนการในการแก้ไข
ปัญหาเดียวกันที่เคยเกิดขึ้นแล้ว ให้กลับสู่สภาวะปกติได้โดยเร็ว

การบริหารจัดการเหตุการณ์ผิดปกติ และการร้องขอการบริการด้านเทคโนโลยีสารสนเทศ (IT Incident,
Service Requests and Problem Management)

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติและการร้องขอการ
บริการด้านเทคโนโลยีสารสนเทศ
2. บันทึกเหตุการณ์ผิดปกติและการร้องขอการบริการ และการกำหนดประเภท การจัดลำดับความ
รุนแรง การวิเคราะห์สาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ
3. กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติและรายงานความคืบหน้าเหตุการณ์ผิดปกติให้
ผู้เกี่ยวข้อง ผู้บริหารได้รับทราบ
4. จัดลำดับความรุนแรงของปัญหา และผลกระทบต่อการให้บริการ ผลกระทบต่อผู้ใช้งาน โดย
กำหนดกรอบระยะเวลาในการแก้ไขเหตุการณ์ผิดปกติและการร้องขอการบริการ คำนึงถึงเป้าหมายและระยะเวลา
ในการกู้คืน
5. มีศูนย์รับแจ้งเหตุการณ์ผิดปกติและการร้องขอการบริการ โดยทำหน้าที่ในการบันทึกและแก้ไขใน
เบื้องต้น
6. มีกระบวนการส่งต่อเหตุการณ์ผิดปกติของหน่วยงานผู้ร้องขอการบริการไปยังฝ่ายดิจิทัล
7. จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติและการร้องขอการบริการ
8. จัดลำดับความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองได้อย่างรวดเร็วและทัน
การณ์
9. วางกรอบแนวทางการประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก
10. วางกรอบแนวทางในการตรวจสอบ วิเคราะห์สาเหตุ และประเมินผลกระทบ
11. จัดทำรายงานเหตุการณ์ผิดปกติและการร้องขอการบริการเสนอต่อผู้บริหารหรือ คณะทำงานที่
ได้รับการแต่งตั้ง
12. จัดทำกระบวนการบริหารสภาวะวิกฤติ (Crisis management) เพื่อรองรับเหตุการณ์ผิดปกติและ
การร้องขอการบริการด้านเทคโนโลยีสารสนเทศที่เพิ่มระดับความรุนแรงหรือมีความยืดเยื้อ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

13. กำหนดให้มีการเก็บรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศที่มีอยู่ในปัจจุบันหรือมีแนวโน้มที่จะเกิดขึ้น เพื่อจัดทำข้อมูลข่าวกรองภัยคุกคามเชิงลึก (Threat intelligence) และกำหนดแนวทางการป้องกัน เพื่อลดผลกระทบจากภัยคุกคาม และหาแนวทางการปิดช่องโหว่ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

การสื่อสารแนวการบริหารจัดการเหตุการณ์ผิดปกติ

มีการสื่อสารแนวการบริหารจัดการเหตุการณ์ผิดปกติการร้องขอการบริการและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ของบริษัท

การกำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารจัดการเหตุการณ์ผิดปกติ

กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารจัดการเหตุการณ์ผิดปกติการร้องขอการบริการและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ของบริษัท

เป้าหมาย: เพื่อควบคุมการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ของบริษัท ให้เป็นไปอย่างมีประสิทธิภาพและมาตรฐาน

บทบาทหน้าที่และความรับผิดชอบ

คณะกรรมการ :

1. พิจารณาทบทวน ประเด็นสำคัญด้านบริหารจัดการเหตุการณ์ผิดปกติการร้องขอการบริการและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ของบริษัท
2. สนับสนุนให้การดำเนินธุรกิจของบริษัทให้เป็นไปตามนโยบาย

ผู้บริหาร :

1. สนับสนุน ผลักดันการดำเนินงานตามนโยบาย เพื่อให้บรรลุตามเป้าหมาย โดยจัดให้มีกลยุทธ์ แนวทางบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นตัวแทนผู้บริหารในการดำเนินงาน เช่น คณะกรรมการ คณะทำงาน หน่วยงานรับผิดชอบ เป็นต้น
2. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง สร้างการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง
3. ส่งเสริมสนับสนุนความรู้ เพื่อให้บุคลากรทุกระดับและทุกฝ่ายให้ความตระหนักและมีแนวทางการบริหารความเสี่ยงเพื่อให้มีการป้องกัน ติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น
4. ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานก่อนนำเสนอคณะกรรมการ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวนปี 2568)

พนักงาน :

1. ศึกษา ทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมาย
2. รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติ ตามนโยบาย สนับสนุน ผลักดันการปฏิบัติตามนโยบาย ภายใต้ขอบเขตของกฎหมาย กฎเกณฑ์ ข้อบังคับ ระเบียบ และแนวปฏิบัติที่บังคับใช้ในการปฏิบัติงาน

หน่วยงานรับผิดชอบ :

1. สื่อสาร ให้คำปรึกษา แนะนำ จัดทำเอกสารสนับสนุน คู่มือ แนวปฏิบัติ เพื่อสนับสนุนการดำเนินงานตามนโยบาย
2. ติดตามความก้าวหน้าในการดำเนินงานเทียบกับเป้าหมาย ทวนสอบความถูกต้อง ประมวลผลและวิเคราะห์ข้อมูล พิจารณาวางแผนปรับปรุงการดำเนินงาน และจัดทำรายงานผลการดำเนินงานต่อผู้บริหาร คณะอนุกรรมการ และคณะกรรมการ ธพส. เป็นประจำทุกปี
3. พัฒนาระบบการและเครื่องมือ

ประกาศ ณ วันที่ 24 พฤศจิกายน 2568



(นายนาฬิกาติศักดิ์ แสงสนิท)

กรรมการผู้จัดการ