ประกาศบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

ที่ 038/2561

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561

- -

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549 มาตรา 5 และมาตรา 7 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

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

ข้อ 1 ประกาศนี้ เรียกว่า “ประกาศ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561 ”

ข้อ 2 วัตถุประสงค์

2.1 เพื่อให้เกิดความเชื่อมั่น และความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ให้ดำเนินงานได้อย่างมี ประสิทธิภาพและประสิทธิผล

2.2 เพื่อกำหนดมาตรฐาน นโยบาย และแนวทางปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ตระหนักถึงความสำคัญของการ รักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงาน

2.3 เพื่อเผยแพร่นโยบายและแนวทางปฏิบัติให้เจ้าหน้าที่ทุกระดับและบุคคลภายนอกที่ปฏิบัติงานให้กับ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ได้รับทราบ และถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

เลขที่ 120 อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210 www.dad.co.th
โทร 0-2142-2222 โทรสาร 0-2143-888-9

2.4 เพื่อให้เกิดการบริหารจัดการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและมีการปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยอย่างต่อเนื่อง

ข้อ 3 ขอบเขตการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด มีขอบเขตครอบคลุมเนื้อหา ดังนี้

3.1 การเข้าถึงและการใช้งานสารสนเทศ

3.1.1 การเข้าถึงข้อมูลและการควบคุมการใช้งานสารสนเทศ

3.1.2 การกำหนดประเภทข้อมูล ระดับข้อมูล และระดับชั้นความลับของข้อมูล

3.1.3 ข้อกำหนดการใช้งานตามภารกิจ

3.1.4 การบริหารจัดการการเข้าถึงของผู้ใช้งานระบบสารสนเทศ

3.1.5 การบริหารจัดการ และการใช้งานรหัสผ่าน

3.1.6การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ที่อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ที่ไม่มีสิทธิ์

3.1.7 การเข้ารหัสสำหรับข้อมูลที่เป็นความลับ

3.1.8 การควบคุมการเข้าถึงระบบเครือข่าย

3.1.8.1 การยืนยันตัวบุคคลในการใช้งานเครือข่าย

3.1.8.2 การป้องกันพอร์ตที่ใช้สำหรับการปรับแต่งระบบ

3.1.8.3 การควบคุมการเชื่อมต่อเครือข่าย

3.1.8.4 การควบคุมการจัดเส้นทางบนเครือข่าย

3.1.9 การเข้าถึงระบบปฏิบัติการ

3.1.10 การควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

3.1.11 การปฏิบัติงานจากภายนอกสำนักงาน

3.1.12 การใช้งานอินเตอร์เน็ต โซเชี่ยลเน็ตเวิร์ก และจดหมายอิเล็กทรอนิกส์

3.1.13 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

3.1.14 การควบคุมการใช้บริการผู้ให้บริการภายนอก

3.1.15 การจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control)

3.1.16 การจัดการและรักษาความปลอดภัยของดาต้าเซ็นเตอร์

3.1.17 การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศที่สำคัญ

3.2 การสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน

3.2.1 การสำรองข้อมูล

3.2.2 การเตรียมความพร้อมกรณีฉุกเฉิน

3.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ 4 การกำหนดขอบเขตความรับผิดชอบ

แบ่งขอบเขตความรับผิดชอบเป็น 2 ระดับ คือ ระดับนโยบาย และระดับปฏิบัติ ดังต่อไปนี้

4.1 ระดับนโยบาย

กำหนดให้ผู้บริหารสูงสุด (Managing Director) ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบเทคโนโลยีสารสนเทศ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรือผลกระทบแก่องค์กร อันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด เป็นผู้รับผิดชอบในการสั่งการ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ และคำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

4.2 ระดับปฏิบัติ

4.2.1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ ผู้รับผิดชอบ ได้แก่

4.2.1.1 ฝ่ายเทคโนโลยีสารสนเทศ

4.2.1.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.2.1.3 เจ้าหน้าที่ที่ได้รับมอบหมาย

4.2.1.4 ผู้ใช้งาน

4.2.2 นโยบายการสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน

4.2.2.1 ฝ่ายเทคโนโลยีสารสนเทศ

4.2.2.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.2.2.3 เจ้าหน้าที่ที่ได้รับมอบหมาย

4.2.3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

4.2.2.1 ฝ่ายเทคโนโลยีสารสนเทศ

4.2.2.2 ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบจากภายนอก

4.2.2.3 ผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ 5 ต้องมีการตรวจสอบ ประเมิน ทบทวน และปรับปรุงนโยบายและแนวปฏิบัติอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

ข้อ 6 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561 ของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ถือเป็นมาตรฐาน โดยอ้างอิงรายละเอียดแนบท้ายประกาศ

นี้ เพื่อใช้เป็นแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศที่มีความมั่นคง ปลอดภัย และเชื่อถือได้ และเป็นไปตามกฎระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด และผู้ที่เกี่ยวข้องต้องถือปฏิบัติตามอย่างเคร่งครัด

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ 18 ธันวาคม พ.ศ. 2561

(นายทรงพล ชีวะปัญญาโรจน์)

กรรมการบริษัท รักษาการแทน กรรมการผู้จัดการ

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ว่าด้วย คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ประกอบด้วย

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

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

ฝ่ายเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบเทคโนโลยีสารสนเทศ คอมพิวเตอร์ และเครือข่ายภายใน ธพส.

ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของ ธพส. เป็นผู้ที่มีอำนาจตัดสินใจเกี่ยวกับระบบเทคโนโลยีสารสนเทศ มีบทบาทหน้าที่ และความรับผิดชอบ ในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ คอมพิวเตอร์ และเครือข่าย ของ ธพส.

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือ เป้าหมาย

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

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลอื่นเพื่อการจัดการระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (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.อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

/สารสนเทศ...

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก มาผ่านการประมวลผลให้ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการปฏิบัติงาน บริหาร การวางแผน และการตัดสินใจ

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

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

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหาร 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 (E-Doc Flow) ที่ใช้งานใน ธพส.

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

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยี สารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารที่มีคุณค่าสำหรับองค์กร

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non- Repudiation) และความน่าเชื่อถือ (Reliability)

/เหตุการณ์ด้านความ...

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการ รับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษร หรืออักขระพิเศษ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัว บุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่ง/โปรแกรมไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ล็อก (Logs) หมายถึง รายการลงบันทึก ที่ถูกสร้างโดยอัตโนมัติเมื่อมีการเข้าถึง หรือใช้งาน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 1 ว่าด้วย การควบคุมการเข้าถึงและใช้งานสารสนเทศ

วัตถุประสงค์

1) เพื่อป้องกันการบุกรุกที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงัก
2) เพื่อกำหนดมาตรการ การอนุญาต การกำหนดสิทธิ์ และการมอำนาจ ในการเข้าถึงและใช้งานสารสนเทศ
3) เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมายตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมายตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

1) จัดทำทะเบียนสินทรัพย์ โดยจำแนกเป็นกลุ่มทรัพยากรระบบ การทำงาน และสถานที่เก็บหรือประมวลผล และระบุสิทธิ์ในการเข้าถึงสินทรัพย์นั้น

2) กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ดังนี้

2.1) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตาม ความจำเป็นต่อการใช้งานระบบสารสนเทศ

2.2) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะ ในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

2.3) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้งาน โดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ

/3) ให้มีการกำหนด...

3) ให้มีการกำหนดสิทธิของผู้ใช้งาน ดังนี้

3.1) กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งานแต่ละกลุ่ม ได้แก่

3.1.1) สิทธิอ่านอย่างเดียว

3.1.2) สิทธิการเพิ่มข้อมูล

3.1.3) สิทธิการแก้ไขข้อมูล

3.1.4) สิทธิการลบข้อมูล

3.1.5) สิทธิการอนุมัติ/อนุญาต

3.1.6) ไม่มีสิทธิ

3.2) กำหนดการระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการ เข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

3.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์ อักษรและได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย ตามแบบลงทะเบียนผู้ใช้งาน

4) กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ดังนี้

4.1) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตาม ความจำเป็นต่อการใช้งานระบบสารสนเทศ

4.2) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะ ในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

4.3) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้งาน โดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและ กำหนดให้มีการลงนามอนุมัติ

เอกสารแนบท้ายประกาศ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 2 ว่าด้วย การกำหนดประเภทข้อมูล ระดับข้อมูล และระดับชั้นความลับของข้อมูล

วัตถุประสงค์

1) เพื่อให้มีความตระหนักถึงความสำคัญของข้อมูล และมีวิธีปฏิบัติที่เหมาะสมในการรักษาความมั่นคงปลอดภัยของข้อมูลแต่ละประเภท ระดับ และชั้นความลับ

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

4) ผู้ใช้งาน

ข้อปฏิบัติ

1) จัดแบ่งประเภทข้อมูล เป็นข้อมูลด้านการบริหาร ข้อมูลด้านการดำเนินงาน และข้อมูลด้านการให้บริการ

1.1) ข้อมูลด้านการบริหาร ได้แก่

1.1.1) นโยบาย

1.1.2) ข้อมูลยุทธศาสตร์ แผน และภารกิจของบริษัท

1.1.3) ผลการปฏิบัติงาน

1.1.4) กฎหมาย ระเบียบ แนวปฏิบัติ

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) ข้อมูลด้านการ...

1.3) ข้อมูลด้านการให้บริการ ได้แก่

1.3.1) ข้อมูลวิชาการและองค์ความรู้

1.3.2) ข้อมูลพื้นที่อาคาร

1.3.3) ข้อมูลการให้บริการ อื่นๆ

2) จัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภท ตามระเบียบว่าด้วยการรักษา ความลับทางราชการ พ.ศ. 2544 เป็น 3 ชั้น คือ

2.1) ลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

2.2) ลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง

2.3) ลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะ ก่อให้เกิดความเสียหาย

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 จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูล ของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 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 การเข้ารหัสสำหรับข้อมูลที่เป็นความลับ

9) มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท หรือกรณีส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองข้อมูลไว้ในสื่อบันทึกข้อมูล และลบข้อมูลสำคัญที่เก็บอยู่ในเครื่องคอมพิวเตอร์ออกก่อน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 3 ว่าด้วย ข้อกำหนดการใช้งานตามภารกิจ

วัตถุประสงค์

1) เพื่อควบคุมและป้องกันไม่ให้เกิดการเข้าถึงสารสนเทศโดยผู้ที่ไม่เกี่ยวข้องตามภารกิจ
2) เพื่อกำหนดข้อปฏิบัติเพื่อควบคุมการเข้าถึงที่สอดคล้องและเหมาะสมตามภารกิจของผู้ใช้งาน

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

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

1) การควบคุมการเข้าถึงสารสนเทศตามภารกิจ
    1.1) ติดตั้งโปรแกรมเฉพาะที่เกี่ยวข้องตามภารกิจบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน
    1.2) กำหนดสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ ในฟังก์ชันงานที่เกี่ยวข้องตามภารกิจ
    1.3) กำหนดสิทธิการเข้าถึงระดับชั้นข้อมูลตามภารกิจ
    1.4) มีการจำกัดระยะเวลาใช้งานระบบเทคโนโลยีสารสนเทศ ตามประเภทภารกิจ
2) การปรับปรุงให้สอดคล้องกับข้อกำหนดในการปฏิบัติงานและข้อกำหนดด้านความปลอดภัย
    2.1) มีการกำหนดพื้นที่การเข้าดำเนินงานที่สอดคล้องตามภารกิจ
    2.2) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงาน
    2.3) ทบทวนสิทธิ์ของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิ์เมื่อไม่มีความเกี่ยวข้อง
    2.4) การเปลี่ยนรหัสผ่านของผู้ใช้โปรแกรม ให้มีความถี่ที่เหมาะสมตามภารกิจที่เกี่ยวข้องกับโปรแกรมนั้น
    2.5) การเปลี่ยนรหัสผ่านในการเข้าถึงพื้นที่ทางกายภาพ ให้มีความถี่ที่เหมาะสมกับความสำคัญของพื้นที่ และตามความสำคัญของข้อมูล

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 4 ว่าด้วย การบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

1) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว
2) เพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
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 หรือกำหนดโดยใช้ ID พนักงาน ที่เป็นเลข หรือ email ที่ไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

/2.4) จัดทำเอกสาร...

2.4) จัดทำเอกสารที่แสดงถึงสิทธิ และหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบตาม ลำดับขั้นการบริหารงานของ ธพส.

2.5) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวย การฝ่ายหรือผู้ดูแลระบบที่ได้รับมอบหมาย

2.6) ทบทวนสิทธิ์ของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิ์เมื่อไม่มีความเกี่ยวข้อง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

3) มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ 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 ว่าด้วย การบริหารจัดการ และการใช้งานรหัสผ่าน

วัตถุประสงค์

1) เพื่อให้เกิดความรัดกุมในการกำหนดรหัสผ่านในการเข้าถึง และใช้งานสารสนเทศ

2) เพื่อให้ผู้ใช้ระมัดระวัง และตระหนักถึงความสำคัญของการบริหารจัดการ และใช้งานรหัสผ่านของตนเอง ที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูล

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
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 เพื่อให้สามารกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ ดังนี้

/2.1) เปลี่ยนรหัสผ่าน...

2.1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

2.2) ตั้งรหัสผ่านที่ยากต่อการคาดเดา

2.3) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิพม์ปกติ ตัวเลข เข้าด้วยกัน

2.4) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

2.5) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

2.6) เก็บรักษาชื่อผู้ใช้-รหัสผ่านของตนเองไว้เป็นความลับ ไม่แจกจ่ายให้แก่ผู้อื่น และไม่ใช้ชื่อผู้ใช้-รหัสผ่านของผู้อื่น

2.7) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

2.8) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

2.9) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากความจำเป็นในการปฏิบัติงาน หลังจากดำเนินการเรียบร้อย ให้เปลี่ยนรหัสผ่านโดยทันที

2.10) มีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

2.11) ในกรณีที่ไม่ใช้ระบบ Single Sign On ให้หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

2.12) หลีกเลี่ยงการใช้รหัสผ่านเดิม

2.13) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 6 ว่าด้วย การควบคุมสินทรัพย์สารสนเทศ และการใช้งานระบบคอมพิวเตอร์ที่อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ที่ไม่มีสิทธิ์

วัตถุประสงค์

1) เพื่อควบคุม และป้องกันไม่ให้สินทรัพย์สารสนเทศหรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการ เข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

1) กำหนดให้มีข้อปฏิบัติในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ เพื่อป้องกันไม่ให้มีผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ดูแล ดังนี้

1.1) ต้องล็อกเอาต์ออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

1.2) กำหนดให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 30 นาทีและต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

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) มีระบบรักษาความ...

2.3) มีระบบรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัยดูแลอาคาร และมีการติดตั้งกล้องวงจรปิดเพื่อบันทึกเหตุการณ์ไว้ใช้ในการตรวจสอบภายหลัง

2.4) บุคลากรที่ปฏิบัติงานในพื้นที่ต้องปิดล็อกประตู และหน้าต่างทุกครั้งหลังเลิกงาน

2.5) ดำเนินการทดสอบระบบป้องกันการบุกรุกทาง กายภาพว่าใช้งานได้ตามปกติอย่างสม่ำเสมอ

3) กำหนดให้มีการควบคุมการเข้าออกพื้นที่ใช้งาน ดังนี้

3.1) จัดทำบันทึกการเข้า-ออกพื้นที่ใช้งานสำหรับ บุคคลภายนอกหรือผู้มาติดต่อ

3.2) มีเจ้าหน้าที่ดูแลบุคคลภายนอกหรือผู้มาติดต่อในพื้นที่ที่มีความสำคัญทุกครั้งจนเสร็จสิ้นภารกิ

3.3) กรณีบุคคลภายนอกหรือผู้มาติดต่อต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเข้ามาในบริเวณพื้นที่ใช้งาน ต้องบันทึกแบบฟอร์มการเข้า-ออก ในรายการอุปกรณ์ด้วยทุกครั้ง

3.4) มีการควบคุมการเข้าออกสถานที่ตั้งของระบบเทคโนโลยีสารสนเทศอย่างรัดกุม และอนุญาตให้เฉพาะผู้มีสิทธิและความจำเป็นผ่านเข้าถึงพื้นที่ได้ เท่านั้น

3.5) กรณีที่ต้องการนำทรัพย์สินสารสนเทศ ออกจากพื้นที่ใช้งาน ต้องขออนุมัติจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศก่อนทุกครั้ง

3.6) จัดให้มีการทบทวนสิทธิการเข้าถึงพื้นที่ หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

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

4.1) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.2) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

4.3) จัดพื้นที่หรือบริเวณส่งมอบไว้ต่างหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในองค์กร

4.4) ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตราย ก่อนจะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

4.5) ต้องลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขาย หรือผู้ให้บริการภายนอก ให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

5) กำหนดให้มีการจัดวางและป้องกันอุปกรณ์ ดังนี้

5.1) ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของระบบเทคโนโลยี สารสนเทศน้อยที่สุด

5.2) ต้องแยกอุปกรณ์ที่มีความสำคัญเก็บไว้ในที่ที่มีความปลอดภัย

5.3) ไม่นำอาหารและเครื่องดื่ม เข้ามาในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ

5.4) ดำเนินการตรวจสอบ ดูแลสภาพแวดล้อม อุณหภูมิ ความชื้น ภายในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายต่ออุปกรณ์ ภายในบริเวณดังกล่าว

5.5) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรอย่างเพียงพอ ได้แก่ ระบบ กระแสไฟฟ้าสำรองและป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการเกิดกระแสไฟฟ้าผิดปกติ ระบบปรับอากาศ ระบบระบายอากาศ และระบบควบคุมความชื้น

5.6) ต้องตรวจสอบหรือทดสอบการทำงานของระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบต่างๆ สามารถทำงานได้ตามปกติ และลดความเสี่ยงจากการทำงานของระบบล้มเหลว

6) กำหนดให้มีการรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่นๆ ดังนี้

/6.1) ผู้ใช้งานต้องระมัดระวัง...

6.1) ผู้ใช้งานต้องระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน หรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหาย หรือเสียหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

6.2) ผู้ใช้งานต้องเก็บเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลสำคัญไว้ในที่ปลอดภัย เช่น ในตู้ หรือโต๊ะที่สามารถล็อกได้ และแยกเอกสารสำคัญสำหรับทำลายไว้ต่างหาก เพื่อความปลอดภัยของทรัพย์สิน

6.3) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

6.4) ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ และสื่อสารต่างๆ โดยไม่ได้รับอนุญาต

7) กำหนดมาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์ ดังนี้

7.1) ต้องล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนการส่งซ่อมหรือเปลี่ยนอุปกรณ์

7.2) ต้องลบข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำลายหรือจำหน่าย

7.3) ต้องฟอร์แมตฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์โดย

7.3.1) ใช้วิธีแบบเขียนทับซ้ำจำนวน 1 ครั้ง ตามมาตรฐาน NIST 800-88 สำหรับข้อมูลที่เป็นชั้นความลับที่ไม่ลับมาก

7.3.2) เขียนทับซ้ำจำนวน 3 ครั้ง ตามมาตรฐาน DoD 5220.22-M สำหรับข้อมูลที่มีชั้นความลับเป็นลับมาก

7.3.3) เขียนทับซ้ำจำนวน 7 ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลลับมากที่สุด

7.3.4) ลบข้อมูลการดำเนินงานที่มีอายุตั้งแต่ 5 ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

7.3.5) ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล และเจ้าของข้อมูลในการลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ
เรื่องที่ 7 ว่าด้วย การเข้ารหัสสำหรับข้อมูลที่เป็นความลับ

วัตถุประสงค์

1) เพื่อให้ข้อมูลและสารสนเทศของ บริษัท ธนารักษ์ พัฒนาสินทรัพย์ จำกัด (ธพส.) มีความมั่นคงปลอดภัย

2) เพื่อป้องกันความเสียหายอันเกิดจากการรั่วไหล เปลี่ยนแปลง ทำซ้ำข้อมูล และสารสนเทศที่มีความสำคัญ หรือเป็นความลับ

ผู้รับผิดชอบ

๑) ฝ่ายเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

๓) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

๔) ผู้ใช้งาน

ข้อปฏิบัติ

1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและผ่านระบบงานสารสนเทศ

2) ผู้ใช้งานกำหนดรหัสผ่านในการเข้าถึงไฟล์ข้อมูลลับ เพื่อป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในคอมพิวเตอร์ที่ใช้งาน

3) ต้องมีการเข้ารหัสข้อมูลที่เป็นความลับซึ่งจัดเก็บไว้ในรูปแฟ้มอิเล็กทรอนิกส์ หรือในฐานข้อมูล ด้วยวิธีที่เป็นมาตรฐานสากล

4) ผู้ใช้งานต้องนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544

5) การรับ-ส่งข้อมูลสำคัญ ข้อมูลที่เป็นความลับผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส ด้วยวิธีที่เป็นมาตรฐานสากลเพื่อความมั่นคงปลอดภัย

6) ผู้ใช้งานไม่แชร์ไฟล์ข้อมูลลับบนเครือข่ายเพื่ออนุญาตให้ผู้อื่น เข้าถึงได้

/7) กำหนดให้ใช้การเข้า...

7) กำหนดให้ใช้การเข้ารหัสข้อมูลบนระบบเครือข่ายไร้สาย ที่เป็นมาตรฐานสากล เช่น WPA WPA2 WPA-PSK หรือ WPA2-PSK เป็นต้น

8) กำหนดให้ใช้ระบบสารสนเทศสำคัญจากภายนอกสำนักงาน (Teleworking) ผ่านช่องทางที่มีการเข้ารหัสที่เป็นมาตรฐานสากล เช่น VPN เพื่อความมั่นคงปลอดภัย

9) กำหนดให้ผู้ที่สามารถใช้เครื่องมือวิเคราะห์ข้อมูลการจราจรบนเครือข่ายได้ ต้องได้รับการอนุมัติสิทธิจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเป็นลายลักอักษร และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 8 ว่าด้วย การเข้าถึงระบบเครือข่าย

วัตถุประสงค์

1) เพื่อให้สามารถ ตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรได้อย่างถูกต้อง
2) เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลและสารสนเทศขององค์กรผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

1) การยืนยันตัวบุคคลในการใช้งานเครือข่าย

1.1) มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนอนุญาตให้เข้าถึงระบบเครือข่าย ด้วยการใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

1.2) ผู้ใช้งานต้องเข้าสู่ระบบเครือข่ายด้วยชื่อผู้ใช้และรหัสผ่าน ที่ได้รับอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

1.3) ผู้ใช้งานต้องยืนยันตัวบุคคลเพื่อใช้งานเครือข่ายด้วยชื่อผู้ใช้และรหัสผ่านของตัวเองเท่านั้น หากมีปัญหาในเข้าถึงระบบเครือข่าย 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

/โดยกำหนดชั้นความลับ...

โดยกำหนดชั้นความลับในการเข้าถึงข้อมูลเป็นลับมาก และมีวิธีการป้องกันการแก้ไข เปลี่ยนแปลงโดยไม่ได้รับอนุญาต รวม ทั้งจำกัดสิทธิ์การเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

1.6) กำหนดให้มีการบันทึกการเข้า-ออกเครือข่าย และความพยายามเข้าสู่เครือข่ายของผู้ใช้งานไว้อย่างน้อย 90 วัน นับตั้งแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

2) การป้องกันพอร์ตที่ใช้สำหรับการปรับแต่งระบบ

2.1) มีการติดตั้งไฟร์วอลล์เพื่อควบคุมการรับส่งข้อมูลระหว่างเครือข่ายขององค์กรกับเครือข่ายภายนอก โดยการปิดพอร์ตที่เข้าสู่ระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน

2.2) การเปิดพอร์ตใดๆ บนเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น

2.3) มีการตรวจสอบและทำรายงานหมายเลขพอร์ตบนเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ที่เปิดให้บริการอย่างน้อยเดือนละครั้ง

2.4) ผู้ใช้งานที่ต้องการใช้พอร์ตของเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ บนเครือข่ายขององค์กรจากเครือข่ายภายนอกจะต้องได้รับการอนุมัติสิทธิจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ โดยมีการระบุระยะเวลาการใช้พอร์ตเป็นกรณีๆ

2.5) มีการกำหนดสิทธิบุคคลในการเข้าออก-ห้องคอมพิวเตอร์แม่ข่าย ห้อง Data Center และห้องระบบเครือข่าย

2.6) การเข้าถึงพอร์ตของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายของ Out Source จะต้องได้รับการอนุมัติสิทธิจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ โดยมีการระบุระยะเวลาการใช้พอร์ตเป็นกรณีๆ

3) การควบคุมการเชื่อมต่อเครือข่าย

3.1) มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจจับการโจมตี และตรวจจับการใช้งานในลักษณะที่ผิดปกติ จากเครือข่ายภายนอก

3.2) ต้องมีการป้องกัน IP Address ภายในระบบเครือข่ายมิให้มองเห็นจากการเชื่อมต่อจากภายนอก

3.3) การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ต้องได้รับอนุมัติสิทธิจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเป็นกรณีไป

3.4) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

3.5) กำหนดให้มีการจำกัดช่วงระยะเวลาการเชื่อมต่อเครือข่ายแต่ละครั้งไม่เกิน 8 ชั่วโมง และหากไม่มีการใช้งานนานเกิน 30 นาที ต้องยกเลิกการเชื่อมต่อระบบและมีการพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ 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) กำหนดการแบ่งพื้นที่...

4.2) กำหนดการแบ่งพื้นที่และเส้นทางบนเครือข่ายดังต่อไปนี้

4.2.1) Internal Zone เป็นส่วนที่ไม่อนุญาตให้มีการเริ่มการเชื่อมต่อจากเครือข่ายภายนอก โดยกำหนดให้เครื่องคอมพิวเตอร์ลูกข่ายทั้งหมดต้องอยู่ในส่วนนี้

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

4.4) ระบบทั้งหมดที่จะติดตั้งใหม่ใน Demilitarized Zone จะต้องได้รับการอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ 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 ที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดไว้

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

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 อย่างสม่ำเสมออย่างน้อยเดือนละหนึ่งครั้ง

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 9 ว่าด้วย การเข้าถึงระบบปฏิบัติการ

วัตถุประสงค์

1) เพื่อป้องกันความเสียหายของข้อมูลและสารสนเทศ ที่อยู่ในเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์คอมพิวเตอร์ของผู้ใช้งาน
2) เพื่อป้องกันการละเมิดข้อมูลและสารสนเทศขององค์ รวมถึงข้อมูลส่วนบุคคลของผู้อื่น ผ่านการใช้งานอุปกรณ์คอมพิวเตอร์ของผู้ใช้งาน
3) เพื่อให้ผู้ใช้ตระหนักถึงการรักษาความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ จากการเข้าถึงระบบปฏิบัติการ

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4) ผู้ใช้งาน

ข้อปฏิบัติ

1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) Laptop Tablet และ Smart Phone ที่ใช้ในการปฏิบัติงาน

2) ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ ตามนโยบายการเข้าถึงและการใช้งานสารสนเทศ ว่าด้วย การบริหารจัดการ และการใช้งานรหัสผ่าน ข้อที่ 2

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) ห้ามไม่ให้ผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากตรวจพบถือเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

/7) ผู้ดูแลระบบต้อง...

7) ผู้ดูแลระบบต้อง Update ระบบปฏิบัติการ เว็บเบราเซอร์ และโปรแกรมอรรถประโยชน์ต่างๆ ให้ทันสมัยเพื่อปิดช่องโหว่ในการโจมตี หรือจากภัยคุกคามอื่นๆ

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 ว่าด้วย การควบคุมอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

วัตถุประสงค์

1) เพื่อป้องกันความเสียหายต่อองค์กรที่อาจเกิดขึ้นจากการใช้งานอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดรายการโปรแกรมที่ต้องติดตั้ง และโปรแกรมที่ห้ามติดตั้งลงในคอมพิวเตอร์แบบพกพาที่จะนำมาใช้ปฏิบัติงานที่เชื่อมต่อกับระบบสารสนเทศและเครือข่ายของ ธพส.
2) ผู้ใช้งานต้องตรวจสอบคอมพิวเตอร์แบบพกพาที่นำมาใช้ปฏิบัติงานว่าได้ติดตั้งโปรแกรมตามที่ ฝ่ายเทคโนโลยีสารสนเทศกำหนดไว้หรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งผู้ดูแลระบบ หรือเจ้าหน้าที่ที่ได้รับมอบหมาย เพื่อขอรับการติดตั้งก่อนการใช้งาน
3) ผู้ใช้งานต้องตรวจสอบคอมพิวเตอร์แบบพกพาที่นำมาใช้ปฏิบัติงานว่าไม่ได้ติดตั้งโปรแกรมที่ห้ามติดตั้งตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด
4) ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากคอมพิวเตอร์แบบพกพา
5) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กร ต้องเป็นโปรแกรมที่ลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น
6) หากมีการนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินขององค์กรมาใช้งานกับระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศก่อนการใช้งาน

/7) กำหนดให้มีการ...

7) กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์แบบพกพาที่นำมาปฏิบัติงานภายในองค์กร ทั้งที่เป็นทรัพย์สินส่วนตัวและขององค์กร

8) ผู้ใช้ต้องมีการสำรองข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์แบบพกพาอย่างสม่ำเสมอ

9) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดเตรียมอุปกรณ์หรือพื้นที่ที่สามารถใช้สำรองข้อมูลออกมาจากเครื่องคอมพิวเตอร์แบบพกพา

10) ผู้ใช้ต้องมีการเข้ารหัสข้อมูลสำคัญ และข้อมูลที่เป็นความลับก่อนจะสำรองข้อมูลออกมาจากเครื่องคอมพิวเตอร์แบบพกพา

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 11 ว่าด้วย การปฏิบัติงานจากภายนอกสำนักงาน

วัตถุประสงค์

1) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต รวมทั้งการโจมตีระบบสารสนเทศขององค์กรจากภายนอก
2) เพื่อให้เกิดประสิทธิภาพในการตรวจติดตามเหตุการณ์ไม่พึงประสงค์

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

1) การเข้าสู่เครื่องคอมพิวเตอร์ขององค์กรจากระยะไกล (Remote Access) ซึ่งเป็นช่องทางที่มีความเสี่ยงสูงต่อความมั่นคงปลอดภัย ต้องได้รับอนุมัติสิทธิ์จากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทุกครั้ง และเมื่อเลิกใช้งานแล้วต้องยกเลิกสิทธิ ดังกล่าวทันที
2) การเข้าสู่เครื่องคอมพิวเตอร์ขององค์กรจากระยะไกล ต้องมีการจำกัดเวลาในการได้รับสิทธิ์ในการเข้าถึง ตามระดับสิทธิ์ หรือตามความจำเป็น
3) ต้องมีการพิสูจน์ตัวตนก่อนเข้าสู่เครื่องคอมพิวเตอร์ขององค์กรจากระยะไกล
4) ไม่อนุญาตให้ครอบครัว หรือผู้อื่น เข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลขององค์กรจากภายนอกสำนักงาน
5) มีการอัพเดทซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่ใช้งานจากระยะไกลให้เป็นเวอร์ชั่นปัจจุบัน
6) ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัส หรือป้องกันชุดคำสั่งไม่พึงประสงค์ ในเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้เชื่อมต่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกล
7) ซอร์สโค้ด และสารสนเทศของ ธพส. ถือเป็นทรัพย์สินทางปัญญา ห้ามไม่ให้ผู้ปฏิบัติงานจากระยะไกล คัดลอก แก้ไข เผยแพร่ โดยไม่ได้รับอนุญาต

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 12 ว่าด้วย การใช้งานอินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ และโซเชี่ยลเน็ตเวิร์ก

วัตถุประสงค์

1) เพื่อให้ใช้งานอินเตอร์เน็ต จดหมายอิเล็กทรอนิกส์ และโซเชี่ยลเน็ตเวิร์ก สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ
2) เพื่อให้เกิดความมั่นคงปลอดภัยในการใช้งานอินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ และโซเชี่ยลเน็ตเวิร์ก

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

1) ไม่ใช้อินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม หรือเว็บไซต์ที่ละเมิดลิขสิทธิ์
2) ห้ามเปิดเผยข้อมูลลับรวมทั้งข้อมูลที่ยังไม่ได้ประกาศอย่างเป็นทางการของหน่วยงานผ่านอินเทอร์เน็ตและโซเชี่ยลเน็ตเวิร์ก
3) การดาวน์โหลด และการอัพเดทโปรแกรมต่างๆ จากอินเทอร์เน็ตต้องกระทำโดยไม่ละเมิดลิขสิทธิ์
4) ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่อรับส่งข้อความ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
5) ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กรโดยไม่แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ ในเชิงธุรกิจจากการใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร
6) ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Mail Box) ของตนเองทุกวัน

/7) ต้องระบุชื่อเรื่อง...

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) ต้องไม่เผยแพร่ข้อความที่ให้ร้ายอันจะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน และบุคคลอื่น

11) ห้ามเผยแพร่ภาพ หรือข้อความใดๆ อันก่อให้เกิดความเสียหายต่อองค์กร รวมทั้งละเมิดสิทธิของบุคคลอื่น ผ่านช่องทางอินเทอร์เน็ต และโซเชี่ยลเน็ตเวิร์ค

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 13 ว่าด้วย การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

วัตถุประสงค์

1) เพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล ของผู้ใช้บริการ และบุคลากร ของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด
2) เพื่อสร้างความมั่นใจในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ให้แก่ผู้ใช้บริการและบุคลากรของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
4) ผู้ใช้งาน

ข้อปฏิบัติ

1) หน่วยงานต้องจัดเก็บข้อมูลส่วนบุคคลในรูปอิเล็กทรอนิกส์อย่างจำกัด เท่าที่จำเป็นต้องใช้งาน
2) หน่วยงานต้องระบุวัตถุประสงค์ในการรวบรวมและจัดเก็บข้อมูลส่วนบุคคลในรูปอิเล็กทรอนิกส์ โดยต้องแจ้งให้เจ้าของข้อมูลทราบทุกครั้งที่มีการให้ข้อมูล
3) ห้ามหน่วยงานนำข้อมูลส่วนบุคคลไปใช้งานนอกเหนือจากที่ระบุไว้ในวัตถุประสงค์
4) ต้องมีการเข้ารหัสข้อมูลส่วนบุคคลซึ่งจัดเก็บไว้ในรูปแฟ้มอิเล็กทรอนิกส์ หรือในฐานข้อมูล ด้วยวิธีที่เป็นมาตรฐานสากล และมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์การเข้าถึงข้อมูลเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
5) แต่งตั้งผู้รับผิดชอบในการเข้าถึง และแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล
6) หน่วยงานต้องไม่จัดเก็บข้อมูลเกี่ยวกับพฤติกรรมทางเพศ ประวัติอาชญากรรม หรือการกระทำความผิดหรือได้รับโทษใด ๆ ประวัติสุขภาพ แหล่งกำเนิดของเผ่าพันธุ์ ความคิดทางการเมือง ความเชื่อในทางศาสนา ยกเว้นเพื่อวัตถุประสงค์ในทางการแพทย์หรือการรักษาพยาบาล และความมั่นคง
7) หน่วยงานต้องไม่จัดเก็บข้อมูลที่อาจเป็นผลร้าย หรือทำให้เสียชื่อเสียง หรืออาจก่อให้เกิดการเลือกปฏิบัติโดยไม่เป็นธรรม หรือเกิดความไม่เท่าเทียมกันแก่บุคคลใดๆ
8) หน่วยงานต้องไม่เปิดเผยเลขบัตรประจำตัวประชาชนของบุคคลใดๆ ผ่านทางสื่อสาธารณะ

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 14 ว่าด้วย การควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก

วัตถุประสงค์

1) เพื่อให้เกิดความมั่นคงปลอดภัยแก่ข้อมูลและสารสนเทศจากการปฏิบัติงานโดยผู้ให้บริการภายนอก

2) เพื่อสร้างความมั่นใจว่าผู้ให้บริการภายนอกจะปฏิบัติตามข้อตกลงการให้บริการที่ทำไว้กับองค์กร

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อปฏิบัติ

1) ต้องกำหนดประเภทของการให้บริการที่ต้องการ ระดับการให้บริการที่พึงประสงค์ และมาตรการความมั่นคงปลอดภัย ไว้ในข้อตกลงการให้บริการ (Service Level Agreement) ให้เป็นส่วนหนึ่งของสัญญาจ้างระหว่าง ธพส. กับผู้ให้บริการภายนอก

2) ต้องกำหนดให้มีการวางแผนการถ่ายโอนงานก่อนที่จะมีการถ่ายโอนงานให้กับผู้ให้บริการภายนอก

3) ต้องกำหนดให้มีแผนการควบคุมเข้าถึงข้อมูลและระบบงานสำคัญ หรือเป็นความลับขององค์กร จากผู้ให้บริการภายนอก

4) กำหนดให้ผู้ให้บริการภายนอกต้องจัดส่งแผนการสร้างความต่อเนื่องในการปฏิบัติงาน เพื่อให้สามารถช่วยกู้คืนข้อมูลและสารสนเทศให้กลับมาใช้งานได้อย่างรวดเร็ว หลังจากเกิดเหตุหยุดชะงักจากการเรียกใช้บริการผู้ให้บริการภายนอก

5) กำหนดให้ผู้บริการภายนอกต้องรายงานเหตุการณ์ความมั่นคงปลอดภัย หรือจุดอ่อนในระบบสารสนเทศที่พบ

6) กำหนดให้ผู้บริการภายนอกต้องจัดการ และแก้ไขเหตุการณ์ความมั่นคงปลอดภัย หรือจุดอ่อนที่พบซึ่งเกี่ยวข้องกับบริการที่ว่าจ้าง

7) เมื่อพบว่าผู้ให้บริการภายนอกไม่สามารถให้บริการได้ตามระดับการให้บริการที่ตกลงไว้ ธพส. ต้องกำหนดให้ผู้บริการภายนอกต้องนำเสนอแผนการปรับปรุงตามความจำเป็น

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 15 ว่าด้วย การจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control)

วัตถุประสงค์

1) เพื่อให้เกิดความความต่อเนื่องในการให้บริการสารสนเทศ โดยไม่เกิดการติดขัดจากการพัฒนาหรือปรับปรุงระบบสารสนเทศขององค์กร
2) เพื่อป้องกันความเสียหายต่อข้อมูลและสารสนเทศจากการพัฒนาหรือปรับปรุงระบบสารสนเทศโดยผู้ให้บริการภายนอก หรือโดยบุคลากรของ ธพส. เอง

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
4) ผู้พัฒนาหรือปรับปรุงระบบ

ข้อปฏิบัติ

1) กำหนดให้มีแผนการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control) ในเอกสารข้อกำหนดของโครงการ (TOR) หรือในเอกสารโครงการพัฒนาหรือปรับปรุงระบบสารสนเทศ ทั้งจากการจัดจ้างผู้ให้บริการภายนอก หรือเจ้าหน้าที่ของ ธพส. เอง
2) แผนการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ อย่างน้อยต้องปฏิบัติตามข้อกำหนดต่อไปนี้

2.1) จะต้องจัดเก็บซอร์สโค้ด เอกสาร รูปภาพ และคลิปวีดีโอ ทั้งหมดที่เกี่ยวข้องกับโครงการพัฒนาหรือปรับปรุงระบบสารสนเทศ ไว้ในระบบการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control System) ที่เป็นที่รู้จักและยอมรับจากผู้พัฒนาซอฟต์แวร์ในภาคเอกชน

2.2) ระบบการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ประเภทซอร์สโค้ด ที่ใช้งานจะต้องสามารถแยก Branch และผสาน Branch ได้

2.3) ในแต่ละ Branch จะต้องสามารถกำหนดสิทธ์การเข้าใช้งานได้

2.4) ในแต่ละ Branch จะต้องสามารถ Commit และ Rollback ได้

/2.5) ระบบที่จัดเก็บไฟล์...

2.5) ระบบที่จัดเก็บไฟล์ประเภทซอร์สโค้ด ต้องเป็นระบบการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์แบบกระจาย (Distributed Version Control System) ซึ่งมีความคล่องตัวกับกาพัฒนาด้วยทีมงานขนาดใหญ่

2.6) ระบบที่ใช้เพื่อการจัดเก็บการเปลี่ยนแปลง ต้องสามารถค้นหา และแสดงประวัติการเปลี่ยนแปลงของไฟล์ได้

2.7) กำหนดให้มีการเข้าถึงคลังข้อมูล (Repository) ได้เฉพาะทีมพัฒนาที่เกี่ยวข้องเท่านั้น

2.8) ต้องกำหนดลำดับงาน (Work Flow) ของการจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ ที่ชัดเจน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 16 การจัดการและรักษาความปลอดภัยของดาต้าเซ็นเตอร์

วัตถุประสงค์

1) เพื่อให้เกิดความมั่นคงปลอดภัยต่ออุปกรณ์และระบบงานภายในห้องดาต้าเซ็นเตอร์

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4) ผู้ให้บริการภายนอกของ ธพส. (Outsourcing)

ข้อปฏิบัติ

1) ต้องจัดทำทะเบียนสินทรัพย์ในดาต้าเซ็นเตอร์ และระบุสิทธิ์ในการเข้าถึงสินทรัพย์นั้น

2) กำหนดให้ผู้เข้าใช้งานดาต้าเซ็นเตอร์ จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ตามความจำเป็นต่อการเข้าใช้งาน

3) ต้องมีการบันทึกเวลาเข้า-ออก ดาต้าเซ็นเตอร์ และระบุภารกิจ ทุกครั้ง

4) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงาน

5) ทบทวนสิทธิ์ของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิ์เมื่อไม่มีความเกี่ยวข้อง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

6) ต้องขออนุญาต และจดบันทึกรายละเอียดการนำอุปกรณ์เข้า-ออก จากดาต้าเซ็นเตอร์

7) ต้องไม่นำอุปกรณ์ที่อาจจะทำให้เครื่องแม่ข่ายติดโปรแกรมที่ไม่พึงประสงค์ เข้าไปในพื้นที่ดาต้าเซ็นเตอร์

8) ต้องล็อคเอาท์จากอุปกรณ์และเครื่องคอมพิวเตอร์ เมื่อไม่ได้ถูกใช้งานหรือเมื่อต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

/9) กำหนดให้มีการจัด...

9) กำหนดให้มีการจัดการสภาพแวดล้อมทางกายภาพ ดังนี้

9.1) กำหนดพื้นที่การเข้าถึงอุปกรณ์ตามระดับความสำคัญของระบบงาน

9.2) มีระบบรักษาความปลอดภัยทางกายภาพป้องกันการบุกรุก ติดตั้งครอบคลุมพื้นที่ของดาต้าเซ็นเตอร์

9.3) บุคลากรที่เข้าปฏิบัติงานในพื้นที่ต้องปิดล็อกประตู ทุกครั้งหลังเลิกงาน

9.4) ดำเนินการทดสอบรักษาความปลอดภัยทางกายภาพอย่างสม่ำเสมอ เพื่อให้ใช้งานได้ตามปกติ

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

10.1) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

10.2) บุคคลภายนอกที่ได้รับอนุญาตให้เข้าปฏิบัติงานในดาต้าเซ็นเตอร์ ต้องแลกบัตรประจำตัวที่บริเวณทางเข้า-ออกอาคาร และลงบันทึกการเข้าปฏิบัติงานในดาต้าเซ็นเตอร์ทุกครั้ง

10.3) ต้องตรวจสอบวัสดุหรือส่วนประกอบในการผลิตที่เป็นอันตราย ก่อนจะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

10.4) ต้องลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขาย หรือผู้ให้บริการภายนอก ให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

11) กำหนดให้มีการจัดวางและป้องกันอุปกรณ์ไว้ในพื้นที่หรือบริเวณที่เหมาะสม

12) การนำสิ่งของ หรืออุปกรณ์เข้าภายในดาต้าเซ็นเตอร์ ต้องได้รับอนุญาตอย่างเป็นลายลักษณ์อักษรจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทุกครั้ง

13) ไม่นำอาหารและเครื่องดื่ม เข้ามาในบริเวณพื้นที่ดาต้าเซ็นเตอร์

14) ดำเนินการตรวจสอบ ดูแลสภาพแวดล้อม อุณหภูมิ ความชื้น อย่างสม่ำเสมอทุกๆ เดือน ภายในบริเวณพื้นที่ของดาต้าเซ็นเตอร์ เพื่อป้องกันความเสียหายต่ออุปกรณ์ต่างๆ

15) มีการระบุชนิดของงาน และภารกิจ ที่ไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล

16) การเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายภายในดาต้าเซ็นเตอร์จากระยะไกล (Remote Access) ต้องได้รับอนุมัติสิทธิจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทุกครั้งตามภารกิจ และระยะเวลาที่กำหนด

17) ไม่อนุญาตให้มีการลบ Logs การบันทึกเข้า-ออก Logs ของเครื่องแม่ข่าย และ Logs ของอุปกรณ์ในห้องดาต้าเซ็นเตอร์ ยกเว้นการลบตามระยะเวลาที่กำหนด หรือลบโดยผู้ที่รับผิดชอบ

18) หากมีการละเมิดข้อปฏิบัติในข้อ (2) (3) (6) (7) (9.3) (12) (16) หรือ (17) ให้มีการตั้งคณะกรรมการภายใน เพื่อสอบสวนความผิด

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ

เรื่องที่ 17 การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศที่สำคัญ

วัตถุประสงค์

1) เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศที่สำคัญของ บริษัท ธนารักษ์ พัฒนาสินทรัพย์ จำกัด และป้องกันการบุกรุกที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศที่สำคัญให้หยุดชะงัก

2) เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศที่สำคัญ ของบริษัท ธนารักษ์ พัฒนาสินทรัพย์ จำกัด ได้อย่างถูกต้อง

3) เพื่อกำหนดมาตรการ การอนุญาต การกำหนดสิทธิ์ และการมอบอำนาจ ในการเข้าถึงและใช้งานสารสนเทศที่สำคัญ

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

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 ให้แก่ผู้ใช้งาน โดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ ERP-SAP, ระบบสารสนเทศเพื่อสนับสนุนการตัดสินใจของผู้บริหาร (BI) และกำหนดให้มีการลงนามอนุมัติ

3) ให้มีการกำหนดสิทธิของผู้ใช้งาน ดังนี้

3.1) กำหนดสิทธิผู้ใช้งานแต่ละคนในการเข้าถึงข้อมูล ตามกลุ่มงานหรือภารหน้าที่ที่ผู้ใช้งานรับผิดชอบ

3.2) กำหนดการระงับสิทธิ การมอบอำนาจ เป็นลายลักษณ์อักษร

3.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับ การพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย ตามแบบลงทะเบียนผู้ใช้งาน

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

4.1) กำหนดสิทธิการเข้าถึงและใช้งานระบบสารสนเทศในฟังก์ชันงานที่เกี่ยวข้องตามภารกิจ

4.2) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงาน

4.3) ทบทวนสิทธิ์ของผู้ที่เกี่ยวข้องอยู่เสมอ และเพิกถอนสิทธิ์เมื่อไม่มีความเกี่ยวข้อง

4.4) ในกรณีมีความจำเป็นต้องให้สิทธิสูงสุดกับผู้ใช้งาน ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน

4.5) สิทธิสูงสุดสำหรับผู้ใช้งาน 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 ซึ่งต้องลงนามรับทราบตามลำดับขั้นการบริหารงานของ ธพส.

5.3) มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) ตาม 41 ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

6) กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่าน ดังนี้

6.1) มีขั้นตอนปฏิบัติสำหรับการตั้ง และเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

6.2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

6.3) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกัน ในการจัดส่งรหัสผ่าน

6.4) ผู้ใช้งานตอบกลับทันทีหลังจากได้รับรหัสผ่าน ต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และเปลี่ยนให้รหัสผ่านยากต่อการเดา

6.5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (password) ไม่เกิน 90 วันหรือทุกครั้งที่มีการ แจ้งเตือนให้เปลี่ยนรหัสผ่าน

7) กำหนดให้มีวิธีปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ ดังนี้

7.1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

7.2) ตั้งรหัสผ่านที่ยากต่อการคาดเดา

/7.3) กำหนดรหัสผ่าน...

7.3) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิพม์ปกติ ตัวเลข เข้าด้วยกัน

7.4) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

7.5) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

7.6) เก็บรักษาชื่อผู้ใช้-รหัสผ่านของตนเองไว้เป็นความลับ ไม่แจกจ่ายให้แก่ผู้อื่น และไม่ใช้ชื่อผู้ใช้-รหัสผ่านของผู้อื่น

7.7) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

7.8) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

7.9) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากความจำเป็นในการปฏิบัติงาน หลังจากดำเนินการเรียบร้อย ให้เปลี่ยนรหัสผ่านโดยทันที

7.10) มีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

7.11) ในกรณีที่ไม่ใช้ระบบ Single Sign On ให้หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

7.12) หลีกเลี่ยงการใช้รหัสผ่านเดิม

7.13) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป

8) กำหนดให้ระบบงานต้องมีการล็อกเอาท์อัตโนมัติ (Session Time-out) เมื่อผู้ใช้งานไม่ได้ใช้งาน

9) ไม่อนุญาตให้มีการลบ Logs การเข้า-ออกระบบ และการใช้งาน ระบบสารสนเทศที่สำคัญ ยกเว้นการลบตามระยะเวลาที่กำหนด หรือลบโดยผู้ที่รับผิดชอบ

10) หากมีการละเมิดข้อปฏิบัติในข้อ (2) (3.3) (6.6) (6.7) (6.8) (7.6) (7.10) หรือ (9) ให้มีการตั้งคณะกรรมการภายใน เพื่อสอบสวนความผิด

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 2 นโยบายการสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน

เรื่องที่ 1 ว่าด้วย การสำรองข้อมูล

วัตถุประสงค์

1) เพื่อให้ข้อมูลและระบบสารสนเทศขององค์กร มีความพร้อมในการใช้งานในกรณีฉุกเฉิน โดยเกิดความเสียหายต่อองค์กรน้อยที่สุด

2) เพื่อให้ข้อมูลที่ได้มีการสำรองไว้ ถูกจัดเก็บอยู่ในสถานที่ปลอดภัย และพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

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) บันทึกรายละเอียด...

7) บันทึกรายละเอียดการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วันเวลา ชื่อข้อมูลที่สำรอง และผลการดำเนินการ

8) จัดเก็บข้อมูลที่ได้สำรองไว้ในสถานที่ปลอดภัย มีการระบุรายละเอียดของข้อมูลที่สำรอง บนสื่อเก็บข้อมูลอย่างชัดเจน

9) มีการเข้ารหัสข้อมูลสำหรับข้อมูลลับที่ได้สำรองเก็บไว้ เพื่อป้องกันมิให้ข้อมูลสำรองถูกเปิดเผย

เอกสารแนบท้ายประกาศเรื่อง
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 2 นโยบายการสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน

เรื่องที่ 2 ว่าด้วย การเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

1) เพื่อให้มีแนวทางในการป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเสียหาย ถูกทำลาย หรือถูกเปลี่ยนแปลง จากไวรัสคอมพิวเตอร์ โปรแกรมชุดคำสั่งไม่พึงประสงค์ ผู้บุกรุก ภัยพิบัติ โดยสามารถกู้ข้อมูลที่มีปัญหากลับมาใช้งานได้

2) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องได้รับรู้เข้าใจ ตระหนักถึงความสำคัญของการสำรองข้อมูลเพื่อความมั่นคงปลอดภัยด้านสารสนเทศ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมายตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

3) เจ้าหน้าที่ที่ได้รับมอบหมายตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ

ข้อปฏิบัติ

1) มีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

2) มีการบริหารจัดการความเสี่ยงสำหรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและทำให้เกิดการหยุดชะงัก ตามเอกสาร “การบริหารจัดการความเสี่ยงด้านสารสนเทศ”

3) จัดทำแผนกู้คืนระบบเมื่อเกิดสถานการณ์ฉุกเฉินตามเอกสาร “แผนบริหารความต่อเนื่อง” โดยมีรายละเอียด ดังนี้

3.1) มีการกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

3.2) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบ

3.3) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการผลิตภัณฑ์ (Vendor) หรือผู้ให้บริการภายนอก (Outsourcing) เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

4) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบกระแสไฟฟ้า ระบบเครือข่าย คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ที่มีประสิทธิภาพและเพียงพอ

5) มีการตรวจสอบหรือทดสอบระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

6) มีการใช้ระบบสำรองเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า

/7) มีการจัดทำแผนฉุกเฉิน...

7) มีการจัดทำแผนฉุกเฉินสำหรับระบบกระแสไฟฟ้า เช่น ในกรณีที่ระบบกระแสไฟฟ้าเกิดการล้มเหลวหรือดับ

8) มีการจัดหาเครื่องกำเนิดกระแสไฟฟ้าสำรองเพื่อจ่ายไฟสำรองให้ในกรณีที่กระแสไฟฟ้าหลักเกิดการหยุดชะงักหรือดับเป็นระยะเวลายาวนาน

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 หรือมีการเปลี่ยนแปลงข้อมูลบ่อยต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

18) มีการทบทวนและปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน การบริหารจัดการความเสี่ยงด้านสารสนเทศ และแผนบริหารความต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.)

ส่วนที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้เข้าใจ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด

ผู้รับผิดชอบ

1) ฝ่ายเทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
3) เจ้าหน้าที่ที่ได้รับมอบหมาย ตามประกาศแต่งตั้งคณะกรรมการนโยบายการเข้าถึงและการใช้งานสารสนเทศ
4) ผู้ตรวจสอบภายใน (Internal Auditor) หรือภายนอก (External Auditor)

ข้อปฏิบัติ

1) มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ
2) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง
3) มีการตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบภายนอก (external auditor)
4) มีข้อตกลงร่วมกันเพื่อกำหนดขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับการตรวจ
5) มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว
6) มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา ในกรณีทดสอบที่มีผลกระทบกับข้อมูลจริงในระบบสำคัญ
7) มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ ในกรณีทดสอบที่มีผลกระทบกับข้อมูลจริงในระบบสำคัญ
8) มีการจัดเก็บหลักฐานและข้อมูลในการตรวจสอบอย่างมั่นคงปลอดภัย
9) มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ
10) มีการกำหนดตัวบุคลากรผู้ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนเองดูแลหรือรับผิดชอบ)

/11)ต้องประเมินความเสี่ยง...

11) ต้องประเมินความเสี่ยงด้านสารสนเทศตามเอกสาร “การบริหารจัดการความเสี่ยงด้าน สารสนเทศ” โดยครอบคลุมเนื้อหาตามมาตรฐาน COSO (Committee of Sponsoring Organizations)

12) เครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยที่จำเป็นต้องใช้ ต้องได้รับการปกป้องจากการลักลอบใช้งานโดยไม่ได้รับอนุญาตหรือใช้ในทางที่ผิดวัตถุประสงค์ รวมถึงมีการควบคุมจำกัดการเข้าถึงข้อมูลเฉพาะผู้ที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

13) เมื่อดำเนินการตรวจสอบและประเมินการรักษาความความมั่นคงปลอดภัยแล้ว ต้องรายงานให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงขององค์กรทราบ พร้อมทั้งเสนอแนวทางปรับปรุงแก้ไขในกรณีที่พบว่า การรักษาความมั่นคงปลอดภัยด้านสารสนเทศยังมีจุดบกพร่อง