ORNSIRIN

นโยบายสารสนเทศ

1. หลักการและเหตุผล

เนื่องด้วยบริษัท อรสิริน โฮลดิ้ง จำกัด (มหาชน) และบริษัทในเครือ ตระหนักถึงความสำคัญของการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการธุรกิจ จึงกำหนดนโยบายฉบับนี้เพื่อให้บริษัทมีกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร เพื่อให้สอดคล้องกับหลักการกำกับ ดูแลกิจการที่ดีตลอดจนกฎหมายอื่นที่เกี่ยวข้องเพื่อให้เหมาะสมกับบริบทการดำเนินธุรกิจ

2. คำอธิบายคำศัพท์

ระบบเครือข่าย = ระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ

คอมพิวเตอร์แม่ข่าย = เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟแวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่นๆ หรือควบคุมการทำงานในระบบเครือข่าย

เครื่องคอมพิวเตอร์ = อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่ทำงานด้วยระบบอิเล็กทรอนิกส์โดยทำงานตามคำสั่งผ่านทางซอฟแวร์ให้ได้ผลตามที่ต้องการ อาทิ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพาได้ (Notebook Computer)

อุปกรณ์คอมพิวเตอร์ = อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์

ระบบสารสนเทศ = ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและการควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ อาทิ อุปกรณ์คอมพิวเตอร์ รบบเครือข่าย โปรแกรม ระบบงาน และสารสนเทศ

สารสนเทศ = ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปแบบของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผน การตัดสินใจ และอื่น ๆ ได้

ระบบงาน = การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบจัดเก็บเอกสาร ระบบจองยานพาหนะ

ระบบปฏิบัติการ (Operating System) = ซอฟแวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุม การทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) อุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

ข้อมูล = ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบเครื่องคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง ส่ง รับ เก็บรักษา หรือประมวลได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

ไฟล์ (File) = ข้อมูลที่ถูกรวบรวมลงสื่อบันทึกและระบุเป็นหนึ่งหน่วยมีโดย ชื่อเฉพาะ เช่น ซอฟแวร์การทำงาน และไฟล์เอกสารต่างๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลง สื่อบันทึก

ผู้ใช้งาน (User) = เจ้าหน้าที่หรือบุคคลภายนอกที่มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ

ผู้บริหารเครือข่าย (Network Administrator) = บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลบำรุงรักษาเครือข่าย

ผู้บริหารคอมพิวเตอร์แม่ข่าย (Host/Server Administrator) = บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์แม่ข่าย

บัญชีผู้ใช้งาน (User Account) = บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ

บัญชีผู้บริหารคอมพิวเตอร์แม่ข่าย (Administrator Account) = บัญชีผู้บริหารคอมพิวเตอร์แม่ข่ายใช้ในการบริหารระบบคอมพิวเตอร์แม่ข่าย

IT Help Desk = บริการให้ความช่วยเหลือและแก้ไขปัญหาด้านระบบคอมพิวเตอร์และเครือข่าย

ผู้รับบริการ= ผู้บริหารและพนักงานผู้ปฏิบัติงานของบริษัทกลุ่มอรสิริน

พนักงานสารสนเทศ= เจ้าหน้าที่ผู้บริการงานด้านการให้ความช่วยเหลือและแก้ไขปัญหาด้าน ระบบคอมพิวเตอร์และเครือข่ายของแผนกเทคโนโลยีสารสนเทศ

เจ้าหน้าที่ผู้ปฏิบัติงาน= พนักงานสารสนเทศผู้รับมอบหมายให้ดำเนินการให้ความช่วยเหลือและแก้ไขปัญหา ด้านระบบคอมพิวเตอร์และเครือข่ายของแผนกเทคโนโลยีสารสนเทศ

SLA (Service Level Agreement) = ข้อตกลงเพื่อรับประกันการบริการระหว่างผู้ให้บริการกับ ผู้รับบริการ เพื่อเพิ่มความมั่นใจแก่ผู้รับบริการว่าเจ้าหน้าที่จะสามารถให้บริการได้ตาม ระยะเวลาแต่ละกระบวนงานที่กำหนดไว้ไม่ถือเป็นข้อผูกพันอาจมีการเปลี่ยนแปลงได้

3. การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

ระเบียบปฏิบัติ

1. จัดให้มีการทำและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ
2. แสดง เจตนารมณ์หรือสื่อสารให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการ ปฏิบัติตาม นโยบายด้านความมั่นคงปลอดภัยขององค์กรโดยเคร่งครัดอย่างสม่ำเสมอ
3. จัดให้มีการประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอโดยกำหนดให้มีวาระการประชุมที่ต้องหารือกันอย่างน้อยดังนี้
    - การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงและผลการตรวจสอบ
    - แผนการดำเนินการเชิงป้องกัน/แก้ไขจากผลการตรวจสอบดังกล่าว
    - การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป
    - การประเมินความเสี่ยงและแผนลดความเสี่ยงจัดให้มี ทรัพยากรด้านบุคลากร งบประมาณการบริหารจัดการและวัตถุดิบที่เพียงพอต่อการจัดการดังกล่าว
4. จัดให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยเพื่อให้เจ้าหน้าที่ขององค์กรมีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ในเบื้องต้น
5. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อลดความเสี่ยงหรือปัญหาที่พบ
6. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจสอบภายในด้าน และจัดให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ
7. จัดให้มีการแจ้งเวียนให้เจ้าหน้าที่ทั้งหมดได้ระมัดระวังและดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน เพื่อป้องกันการสูญหาย
8. กำหนดนโยบายการใช้งานระบบเครือข่ายอย่างชัดเจนว่าบริการใดที่อนุญาตให้ใช้งานและบริการใดไม่อนุญาตให้ใช้งาน รวมทั้งปรับปรุงนโยบายตามความจำเป็นนโยบายการใช้งานระบบเครือข่าย
9. ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติศาสนาและพระมหากษัตริย์การพนันลามกอนาจารอื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมายผิดศีลธรรมหรือผิดจริยธรรมในเวลาทำงาน

4. การจัดการกับเอกสารที่เกี่ยวข้องกับระบบ

ระเบียบปฏิบัติ

1. จัดทำและปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัยอย่างน้อย ให้ครอบคลุมระบบงานเครื่องเซิร์ฟเวอร์และอุปกรณ์ที่มีความสำคัญ ดังนี้
   - คู่มือระบบงานต่างๆทั้งในส่วนของผู้ใช้งานและผู้ดูแล ระบบ
   - คู่มือการตรวจสอบสถานะของเซิร์ฟเวอร์และระบบเครือข่าย
   - คู่มือการตรวจสอบระบบและอุปกรณ์ต่าง ๆ ในห้องเครื่อง
   - คู่มือการสำรองข้อมูล
   - คู่มือการตรวจสอบทรัพยากรของระบบ
2. ให้จำกัดการเข้าถึงคู่มือการปฏิบัติงานเฉพาะทีมงานที่มีความเกี่ยวข้องเท่านั้น
3. หากมีการจัดเก็บคู่มือการปฏิบัติงานไว้บนระบบเครือข่ายจัดให้มีการป้องกันการเข้าถึงเพื่อให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น

5. การจัดการระบบเครือข่าย

ระเบียบปฏิบัติ

1. ปรับปรุงผังเครือข่ายให้มีความทันสมัยอย่างสม่ำเสมอ
2. จัดแบ่งและปรับปรุงระบบเครือข่ายออกเป็นกลุ่ม ๆ ตามลักษณะการใช้งาน เช่น แบ่งตามกลุ่มเครื่องเซิร์ฟเวอร์ เครื่องลูกข่าย และระบบงานที่มีความสำคัญ
3. จำกัดการเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์ระบบงานหรืออุปกรณ์ที่มีความสำคัญ โดยจะต้องกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อได้จะต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบเท่านั้น
4. ปิดบริการบนเครื่องเซิร์ฟเวอร์ที่ไม่มีความจำเป็นในการใช้งาน
5. กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจากภายในเครือข่ายเพื่อเข้าสู่เครื่องเซิร์ฟเวอร์หรืออุปกรณ์เครือข่าย
6. กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจากระยะไกลภายนอกองค์กรเข้ามาสู่เครือข่ายภายในองค์กร
7. ติดตั้ง Patch แบบอัตโนมัติบนเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้งานทั้งหมดขององค์กร
8. ปรับแต่งไฟร์วอลล์เพื่อให้เป็นไปตามนโยบายการใช้งานระบบเครือข่ายที่ตามที่ผู้บริหารได้กำหนดไว้

6. การจัดการ พ้นสภาพ หรือย้ายหน่วยงานของพนักงาน

ระเบียบปฏิบัติ

1. ถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายออกจากระบบต่าง ๆ ทั้งหมดตามระเบียบของแผนกบุคคลภาย โดยที่ได้รับแจ้งจากทางแผนกบุคคลภายใน 15 วัน
2. ถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายออกจากระบบต่าง ๆ ทั้งหมดฉุกเฉินภายใน 1 วัน โดยทันทีที่ได้รับแจ้งจากทางแผนกบุคคล
3. จัดให้มีตรวจสอบความถูกต้องของข้อมูลผู้ใช้สิทธิในระบบต่าง ๆ

7. การใช้งานห้องเครื่อง Server

ระเบียบปฏิบัติ

1. ผู้ที่สามารถเข้าถึงห้องเครื่องคอมพิวเตอร์ Data Center ต้องมีหน้าที่ในการปฏิบัติงานภายในห้องเท่านั้น
2. การนำบุคคลภายนอกเข้าห้องเครื่อง Data Center ต้องผ่านการอนุมัติจากประธานเจ้าหน้าที่สายการเงิน (CFO)
3. ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น
4. ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง
5. ตรวจสอบประตูทางเข้า-ออกและหน้าต่างของห้องเครื่องให้ปิดล็อกอยู่เสมอ
6. ตรวจสอบสภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ ได้แก่ ระบบกระแสไฟฟ้า ระบบการระบายอากาศ ระบบการปรับอุณหภูมิ ระบบUPS ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมออย่างน้อยวันละ1 ครั้ง
7. จัดวางเครื่องคอมพิวเตอร์อุปกรณ์สื่อสารหรือทรัพย์สินอื่นๆไว้ในบริเวณที่มี ความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียง ได้โดยง่าย
8. ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ1 ครั้งว่ายังใช้งานได้เป็นปกติหรือไม่
9. ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องเครื่องอย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษ หรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้องเครื่อง
10. ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย
11. ตรวจสอบห้องสายสัญญาณสื่อสารให้มีการปิดล็อกอยู่เสมอ
12. จัดทำหรือต่อสัญญาการบำรุงรักษาระบบงานสำคัญไฟร์วอลล์เราท์เตอร์ อุปกรณ์ UPS สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องเครื่องให้ครบถ้วน
13. จัดให้ระบบงานสำคัญเครื่องเซิร์ฟเวอร์และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์ UPS และระบบกระแสไฟฟ้าสำรอง (electricity power generator) เพื่อสนับสนุนการทำงานอย่างครบถ้วน
14. การเข้าห้องเครื่องคอมพิวเตอร์ Data Center สำหรับการตรวจสอบภายในของบริษัทหรือการเข้าตรวจเยี่ยมของผู้บริหาร ผู้มีหน้าที่ปฏิบัติงาน เป็นผู้นำพาเข้าห้องเครื่อง Data Center และลงบันทึกในการเข้าทุกครั้ง

8. การจัดการทรัพยากรของเครื่องเซิร์ฟเวอร์

ระเบียบปฏิบัติ

1. ดำเนินการตรวจสอบทรัพยากรของเซิร์ฟเวอร์สำหรับระบบงานสำคัญ ๆ สิ่งที่ควรตรวจสอบ ประกอบด้วย ปริมาณการใช้ CPU ปริมาณการใช้ฮาร์ดดิสก์ปริมาณการใช้ หน่วยความจำ และปริมาณการใช้เครือข่าย รวมทั้งควรมีการตรวจสอบการใช้งานเครือข่ายโดย ภาพรวม
2. บันทึกข้อมูลการใช้ทรัพยากรดังกล่าวไว้ด้วย (เพื่อใช้ในการตรวจสอบแนวโน้มการใช้ทรัพยากร รวมทั้งวางแผนจัดซื้อเพิ่มเติมตามความจำเป็นในอนาคต)
3. ตั้งและหมั่นตรวจสอบสัญญาณนาฬิกาของเครื่องเซิร์ฟเวอร์ตามที่พ.ร.บ.ว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ได้ระบุไว้และของระบบงานสำคัญให้มีความถูกต้องอยู่เสมอ (โดยสามารถอ้างอิง เวลาได้จาก“clock.thaicert.org”)

9. การจัดการไวรัสคอมพิวเตอร์

ระเบียบปฏิบัติ

1. ตรวจสอบว่าเครื่องเซิร์ฟเวอร์ป้องกันไวรัสยังทำงานตามปกติ และมีการปรับปรุงฐานข้อมูลไวรัส (Virus signature) อยู่ตลอดเวลา หากพบว่าทำงานผิดปกติให้รีบดำเนินการแก้ไขโดยทันที
2. ทำการติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งานเพื่อให้ทำงานในลักษณะทันทีทันใด (Real-time Scan) เมือมีการเปิดไฟล์ขึ้นมาใช้งาน

3. ทำการติดตั้งและปรับปรุงโปรแกรมป้องกัน ไวรัสให้ทันสมัย กับเครื่องลูกข่ายทั้งหมด เครื่อง เซิร์ฟเวอร์สำหรับระบบงานสำคัญ

10.การสำรองข้อมูล

ระเบียบปฏิบัติ

1. กำหนดรายชื่อของระบบงานสำคัญทั้งหมดและเมล์เซิร์ฟเวอร์
2. กำหนดรายชื่อของเซิร์ฟเวอร์ตามที่พ.ร.บ.ได้กำหนดไว้ เช่น เว็บเซิร์ฟเวอร์ เป็นต้น
3. กำหนดผู้รับผิดชอบในการสำรองข้อมูล
4. กำหนดชนิดของข้อมูลบนระบบงานหรือบนเซิร์ฟเวอร์ดังกล่าวที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อย ต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบเช่นซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้อง เป็นต้น
5. กำหนดความถี่ในการสำรองข้อมูลของระบบงานหรือเซิร์ฟเวอร์ดังกล่าว
6. ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

11.การจัดเก็บข้อมูลตามพรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ปี 2560

ระเบียบปฏิบัติ

1. จัดเก็บข้อมูลล็อกดังต่อไปนี้อย่างน้อยเป็นระยะเวลา 90 วัน เครื่องเซิร์ฟเวอร์FTP (FTP.log) Firewall/Proxy/Gateway (เช่นFW.log) Web (Access.log)
2. จำกัดการเข้าถึงข้อมูลล็อกดังกล่าวโดยกำหนดให้เฉพาะผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถเข้าถึงได้

12.การลงทะเบียนและควบคุมการเข้าถึงระบบ

ระเบียบปฏิบัติ

1. กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้งานใหม่ตาม “แบบฟอร์มสำหรับลงทะเบียนผู้ใช้งาน” และ กำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์ม แต่ควรให้สิทธิความจำเป็นในการใช้งานเท่านั้น
2. ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งานสำหรับพนักงานเจ้าหน้าที่ของกลุ่มบริษัทอรสิริน และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
3. ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งานสำหรับหน่วยงานภายนอก และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
4. ให้ทำการจัดส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และแนบเอกสาร “ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่าย” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

13.การพัฒนาระบบงาน

ระเบียบปฏิบัติ

1. จัดให้มีการตรวจรับและทดสอบระบบงานใหม่ โดยผู้ใช้งานที่เกี่ยวข้องให้ครอบคลุมตามข้อกำหนดที่ระบุจนกระทั่งการสามารถใช้งานได้ตรงตามความต้องการของหน่วยงาน จึงจะเปิดให้บริการระบบงานนั้นได้
2. สำหรับระบบงานสำคัญให้กำหนดมาตรฐานการเข้ารหัสข้อมูลที่มีการรับ-ส่งระหว่างเครื่องลูกข่ายกับเครื่องเซิร์ฟเวอร์และกำหนดให้พัฒนาระบบตามมาตรฐานนี้
3. พัฒนาระบบงานตามแนวทางในการตรวจสอบข้อมูลนำเข้า

4. ทำการทดสอบระบบงาน และบันทึกผลการทดสอบเก็บไว้เป็นลายลักษณ์อักษรตามแนวทางในการตรวจสอบข้อมูลนำเข้า

5. พัฒนาระบบงานเพื่อให้สามารถกำหนดรหัสผ่านที่มีความเข้มแข็งตามระเบียบปฏิบัติสำหรับการตั้ง รหัสผ่าน และมีการกำหนดให้รหัสผ่านมีอายุการใช้งาน 90 วัน เมื่อใช้งานครบกำหนดจะต้องทำการกำหนดรหัสผ่านใหม่เพื่อเข้าใช้งานระบบต่อไป

6. รวบรวมและจัดเก็บซอร์ซโค้ดของระบบงานทั้งหมดไว้ในสถานที่เดียวกันที่มีความปลอดภัย และควบคุมให้มีเวอร์ชันของซอร์ซโค้ดอย่างน้อย 2 เวอร์ชันล่าสุด และกำหนดให้ผู้ที่เกี่ยวข้องเท่านั้นจึงจะสามารถเข้าถึงได้

7. จัดให้มีการอบรมสำหรับระบบงานใหม่ให้แก่ผู้ใช้งานทั้งหมดที่เกี่ยวข้อง

8. จัดทำคู่มือการใช้งานสำหรับระบบงานใหม่อย่างน้อยสำหรับผู้ใช้งานและผู้ดูแลระบบ

14.การป้องกันไวรัส

ระเบียบปฏิบัติ

1. ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติให้ดำเนินการแก้ไขโดยทันที

2. หากเครื่องของผู้ใช้งานยังไม่มีโปรแกรม ตรวจสอบไวรัส หรือ พบ Virus กรณีพบ Virus แต่ โปรแกรม Anti Virus ไม่สามารถกำจัดได้ให้รีบแจ้งแผนกสารสนเทศทันที

3. การแจ้งซ่อมให้ใช้แบบแจ้งซ่อมคอมพิวเตอร์หรือบันทึกข้อมูลผ่านระบบซ่อมแผนกสารสนเทศ

15.การป้องกันการละเมิดลิขสิทธิ์และสิทธิทางปัญญา

ระเบียบปฏิบัติ

1. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

2. ระมัดระวังการใช้งานเอกสารหรือข้อมูลต่างๆ ซึ่งอยู่ในรูปแบบใดก็ตาม และได้มีการกำหนดเงื่อนไขการใช้งานเอาไว้ ต้องปฏิบัติตามเงื่อนไขดังกล่าวอย่างเคร่งครัด เพื่อไม่ให้เป็นการละเมิดทรัพย์สินทางปัญญาของบุคคลอื่น

16.การจัดเก็บข้อมูลเอกสารและข้อมูลสื่ออิเล็กทรอนิกส์

ระเบียบปฏิบัติ

1. การจัดเก็บข้อมูลเอกสารทั่วไปในส่วนของสารสนเทศ กำหนดให้มีการเก็บโดยมีระยะเวลาในการจัดเก็บ 2 ปี

2. การจัดเก็บข้อมูลเอกสารที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในส่วนของสารสนเทศ กำหนดให้มีการเก็บโดยมีระยะเวลาในการจัดเก็บ 2 ปี นับจากวันที่หมดสัญญา

3. การจัดเก็บข้อมูลสื่อข้อมูลอิเล็กทรอนิกส์ทั่วไปในส่วนของสารสนเทศ กำหนดให้มีการเก็บโดยมีระยะเวลาในการจัดเก็บ 5 ปี และในส่วนของแผนกอื่น ๆ อ้างอิงตาม ISO ตามแต่ละแผนกไป

4. การจัดเก็บข้อมูลสื่อข้อมูลอิเล็กทรอนิกส์ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในส่วนของสารสนเทศ กำหนดให้มีการเก็บโดยมีระยะเวลาในการจัดเก็บ 2 ปี นับจากวันที่หมดสัญญา

17.การทำลายสื่อบันทึกข้อมูลที่เสีย/ไม่ได้ใช้งานแล้ว

ระเบียบปฏิบัติ

1. การทำลายข้อมูลเอกสาร อ้างอิงระยะเวลาที่จัดเก็บ ตามข้อ 16.1 จะทำลายโดยใช้เครื่องบดกระดาษ หรือการเผาทำลายและการทำลายจะต้องได้รับการอนุมัติจาก ผู้มีอำนาจลงนามอนุมัติจากฝ่ายสารสนเทศ

2. การทำลายข้อมูลสื่อข้อมูลอิเล็กทรอนิกส์ทั่วไป กรณีที่ไม่ได้ใช้งานหรือครบระยะเวลาในการจัดเก็บ อ้างอิง ตามข้อ 16.2 จะทำการลบหรือล้างข้อมูล และการทำลายจะต้องได้รับการอนุมัติจาก ผู้มีอำนาจลงนามอนุมัติจากฝ่ายสารสนเทศ

3. กรณีที่มีข้อมูลส่วนบุคคล ที่จัดเก็บอยู่ใน Harddisk, Thumb Drive / Flash Drive, External Harddisk หรือข้อมูลอิเล็กทรอนิกส์ หลังจากที่ได้รับการแจ้งจะทำการล้างข้อมูลภายในอุปกรณ์อิเล็กทรอนิกส์ ภายในระยะเวลา 30 วัน และจะทำลาย เมื่อได้รับการอนุมัติจากผู้มีอำนาจลงนามอนุมัติจากฝ่ายสารสนเทศลงนามอนุมัติและ DPO

4. การทำลายสื่อบันทึกข้อมูลที่ไม่ได้ใช้งานแล้ว เช่น Harddisk, Thumb Drive / Flash Drive, External Harddisk เมื่อครบระยะเวลา 3 เดือน จะทำการล้างข้อมูลภายในอุปกรณ์อิเล็กทรอนิกส์ เพื่อที่จะสามารถนำไปใช้งานต่อไป และการทำลายจะต้องได้รับการอนุมัติจากผู้มีอำนาจลงนามอนุมัติจากฝ่ายสารสนเทศ

5. การทำลายสื่อบันทึกข้อมูลที่ชำรุด เช่น Harddisk, Thumb Drive / Flash Drive, External Harddisk จะทำการทำลายภายในระยะเวลา 90-150 วัน โดยใช้วิธีการทำลายแบบทุบ แกะ หรือใช้คลื่นแม่เหล็กทำลาย ไม่ให้สามารถใช้งานได้ และการทำลายจะต้องได้รับการอนุมัติจากผู้มีอำนาจลงนามอนุมัติจากฝ่ายสารสนเทศ

18.การใช้งานคอมพิวเตอร์และระบบเครือข่าย

ระเบียบปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย และระเบียบการเชื่อมต่อคอมพิวเตอร์และเครือข่ายเอกสารฉบับนี้ มีจุดประสงค์เพื่อสร้างความเข้าใจเกี่ยวกับระเบียบการใช้ระบบ คอมพิวเตอร์และเครือข่าย ของบริษัทภายใต้การดูแลของแผนกเทคโนโลยีสารสนเทศ ซึ่งกล่าวถึงสิทธิหน้าที่ข้อปฏิบัติของผู้ใช้ระบบ

1. คำจำกัดความในระเบียบนี้

"บริษัท" หมายถึงบริษัท อรสิริน โฮลดิ้ง จำกัด (มหาชน)

"แผนกเทคโนโลยีสารสนเทศ" หมายถึง แผนกเทคโนโลยีสารสนเทศบริษัท อรสิริน โฮลดิ้ง จำกัด (มหาชน)

"เครื่องคอมพิวเตอร์และเครือข่าย" หมายถึง เครื่องคอมพิวเตอร์ที่เป็นสมบัติของบริษัททั้งที่อยู่ภายในและภายนอกส่วนกลาง รวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ อุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในบริษัท ตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ ที่มิได้จัดให้เป็นสื่อสาธารณะ

"แผนก" หมายถึง แผนกต่าง ๆ ของบริษัท อรสิริน โฮลดิ้ง จำกัด (มหาชน)

"ผู้ใช้งาน" หมายถึง พนักงานที่บริษัทอนุญาตให้ใช้เครื่องคอมพิวเตอร์และเครือข่ายได้

"บทลงโทษ" หมายถึง บทลงโทษที่บริษัทเป็นผู้กำหนดหรือบทลงโทษตามกฎหมาย

2. กฎระเบียบการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย

เครื่องคอมพิวเตอร์และเครือข่ายของบริษัทเป็นสมบัติของบริษัท ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต

1. ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไขใน การรับทราบกฎระเบียบหรือนโยบายต่าง ๆ ที่บริษัทกำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายของบริษัทมิได้
2. บริษัทให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้
3. บัญชีผู้ใช้งาน (User Account) ที่บริษัทให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
4. ห้าม ผู้ใช้งานปฏิบัติการใด ๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของบริษัท
5. ห้ามผู้ใช้งานทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่ายเช่นการประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูล ไปซื้อขายการรับบริการค้นหาข้อมูลโดยคิดค่าบริการการให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

6. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานจะต้องไม่อ่านเขียนลบ เปลี่ยนแปลง หรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาตการบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ของแผนกในบริษัท การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพ หรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว บริษัทไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว
7. บริษัทจะไม่ควบคุมเนื้อหาของข้อมูลข่าวสารที่เก็บและรับส่งผ่านเข้าออกเครื่องคอมพิวเตอร์ของหน่วยงานและจะไม่รับประกันในคุณภาพของการเก็บการรับส่งข้อมูลข่าวสารและการไม่สามารถใช้งานได้ของระบบบางส่วนหรือทั้งหมดและจะไม่รับผิดชอบในความเสียหายของการใช้งาน อันเนื่องมาจากวงจรสื่อสารชำรุดจานแม่เหล็กชำรุด ความล่าช้าแฟ้มข้อมูลหรือ จดหมายส่งไปไม่ถึงปลายทาง หรือส่งผิดสถานที่และความผิดพลาดในข้อมูลหรือความเสียหายอันเกิดจากการล่วงละเมิดโดยผู้ใช้งานอื่น ๆ
8. ห้ามใช้ระบบเครือข่ายเพื่อกระทำสิ่งผิดกฎหมายและผิดไปจากนโยบายด้านความมั่นคงปลอดภัย
9. ห้ามทำลาย ทำให้เสียหาย แก้ไข เปลี่ยนแปลง ทำซ้ำ หรือเพิ่มเติมข้อมูล และสารสนเทศผู้อื่นโดยมิชอบ
10. ห้ามเผยแพร่ข้อมูล หรือสารสนเทศที่เป็นเท็จ หรือดำเนินการใด ๆ ที่จะส่งผลให้เกิดความเสียหายแก่ผู้อื่นหรือบริษัท
11. ห้ามเผยแพร่ หรือจัดเก็บข้อมูลที่มีลักษณะลามก อนาจาร และขัดต่อศีลธรรมอันดี และห้ามเผยแพร่ข้อมูลภาพตัดต่อ เติม หรือดัดแปลง ของบุคคลอื่น ด้วยวิธีการใด ๆ ซึ่งจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ห้ามใช้ทรัพย์สินและบริการในระบบเครือข่ายเพื่อประกอบธุรกิจ
13. ห้ามกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่น
14. ห้ามใช้กรรมวิธีใด ๆ ก็ตามที่ทำให้การสื่อสารข้อมูลเกิดการชะลอตัว หรือรบกวนจนระบบเครือข่าย หรือทรัพย์สินหรือบริการอย่างหนึ่งอย่างใดไม่สามารถทำงานได้ตามปกติ
15. ห้ามทำลาย หรือพยายามทำลายระบบความมั่นคงปลอดภัยของระบบเครือข่าย
16. ห้ามเชื่อมต่อเข้าเว็บไซต์ที่เสี่ยงต่อการติดไวรัสคอมพิวเตอร์ เช่น เว็บไซต์เกมส์, สื่อลามกอนาจาร และการพนัน
17. ห้ามดาวน์โหลด บันทึกข้อมูล รูปภาพ หรือในรูปแบบต่าง ๆ ที่เสียงต่อการติดไวรัสคอมพิวเตอร์ และเป็นการละเมิดลิขสิทธิ์
18. ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์ส่วนตัว ตลอดจนอุปกรณ์พ่วงต่อทุกชนิด นำมาใช้ในการทำงานของบริษัท ตลอดจนการเชื่อมต่อกับเครื่องคอมพิวเตอร์ภายในบริษัท และเครือข่ายภายในบริษัทโดยไม่ได้รับอนุญาต กรณีผู้ใช้งานมีความจำเป็นต้องใช้ในการทำงานของบริษัท ให้ขออนุมัติจากทางต้นสังกัดและแจ้งขึ้นทะเบียนอุปกรณ์กับทางแผนกสารสนเทศ
19. ห้ามใช้สื่อโซเชียลมีเดีย กระทำอันมีลักษณะ ลามก อนาจาร และขัดต่อศีลธรรมอันดี และการแสวงหาผลประโยชน์เพื่อประกอบธุรกิจ และเข้าข่ายการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา
20. กรณีผู้ใช้งานฝ่าฝืนนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศ การยกเลิกผู้ใช้งานขึ้นอยู่กับดุลยพินิจของผู้บังคับบัญชาผู้ใช้งานและประธานเจ้าหน้าที่สายงานการเงิน (CFO)
21. ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/กฎ/ระเบียบ/คำแนะนำที่บริษัทกำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม ซึ่งจะมีผลบังคับใช้โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า
22. บริษัททรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งานและทรงไว้ซึ่งสิทธิที่จะยกเลิกหรือระงับการเชื่อมต่อและ/หรือการใช้งานใด ๆ ของผู้ใช้งานที่ล่วงละเมิดหรือพยายามจะล่วงละเมิดกฎระเบียบนี้
23. ห้ามผู้ใช้งานดาวน์โหลด เพลง ซึ่งเป็นลิขสิทธิ์ของค่ายเพลงมาเก็บไว้ในเครื่องคอมพิวเตอร์อันเป็นทรัพย์สินของบริษัท
24. การขอใช้สิทธิ Administrator นั้นต้องผ่านการอนุมัติขอใช้สิทธิ เป็นการพิจารณาจากผู้บริหารประธานเจ้าหน้าที่สายงานการเงิน (CFO) โดยจะต้องระบุความต้องการใช้สิทธิและระยะเวลาอย่างชัดเจน

3. การใช้งานอีเมล

ระเบียบปฏิบัติ

1. ห้ามมิให้เข้าถึงข้อมูลอีเมลของบุคคลอื่นโดยไม่ได้รับอนุญาต
2. ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
3. ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
4. ห้ามส่งอีเมลที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น
5. ห้ามส่งอีเมลที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
6. ห้ามปลอมแปลงอีเมลของบุคคลอื่น
7. ห้ามรับหรือส่งอีเมลแทนบุคคลอื่นโดยไม่ได้รับอนุญาต
8. ห้ามส่งอีเมลที่มีขนาดใหญ่เกินกว่าระบบกำหนดหรือตามที่องค์กรระบุไว้
9. ห้ามส่งอีเมลที่เป็นความลับขององค์กรเว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลอีเมลที่องค์กรกำหนดไว้
10. ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่อีเมลของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ
11. ให้ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับอีเมลเท่าที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลที่ส่งไป
12. ให้ใช้คำที่สุภาพในการส่งอีเมล
13. ให้ระบุชื่อของผู้ส่งในอีเมลทุกฉบับที่ส่งไป
14. ให้ทำการสำรองข้อมูลอีเมลตามความจำเป็นอย่าง
15. ในการส่งข้อมูลที่เกี่ยวข้องกับงาน และข้อมูลที่สำคัญ ต้องมีระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่บริษัทจัดไว้ให้ในการส่งข้อมูลเท่านั้นเพื่อป้องกันการรั่วไหลของข้อมูล
16. พนักงานที่ต้องการใช้อีเมลอื่นที่ไม่ใช่อีเมลบริษัทฯ ในการปฏิบัติหน้าที่ สามารถเขียนแบบฟอร์มขอใช้ได้ที่แผนกสารสนเทศ
17. หากพบว่าพนักงานมีการใช้อีเมลอื่นที่ไม่ใช่อีเมลบริษัทในการปฏิบัติหน้าที่ ทางแผนกสารสนเทศจะดำเนินการรายงานความผิดไปยังแผนกบุคคลดำเนินตามระเบียบข้อบังคับการทำงานของบริษัท

19. การป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

ระเบียบปฏิบัติ

1. เพื่อการกระทำผิดกฎหมายหรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
2. เพื่อการกระทำที่ขัดต่อ พ.ร.บว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
3. เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
4. เพื่อการค้าขายหรือผลประโยชน์ส่วนตัวหรือผลประโยชน์ทางการเมือง
5. เพื่อ การเข้าถึง แสดง จัดเก็บ แจกจ่าย แก้ไข จัดทำ หรือบันทึกข้อมูลที่มีเนื้อหาไม่เหมาะสม เช่น ข้อมูลอันเป็นเท็จ ข้อมูลที่มีผลต่อความมั่นคงของสถาบันชาติศาสนาและพระมหากษัตริย์ภาพลามก อนาจาร ภาพตัดต่อของบุคคลอื่น หรือข้อมูลที่ก่อให้เกิดความเสื่อมเสียอับอายแก่องค์กรหรือบุคคล อื่น เป็นต้น
6. เพื่อทำการเผยแพร่ข้อมูล หรืออนุญาตให้ผู้อื่นเผยแพร่ข้อมูลเพื่อการกล่าวร้าย หมิ่นประมาทหรือ พาดพิงบุคคลอื่นจนทำให้องค์กรถูกฟ้องร้องหรือก่อให้เกิดความเสียหายแก่องค์กร
7. เพื่อการเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กรหรือบุคคลภายนอก
8. เพื่อขัดขวางหรือโจมตีการใช้งานระบบเครือข่ายขององค์กรหรือของหน่วยงานภายนอกอื่น
9. เพื่อแพร่กระจายไวรัส หนอนม้า โทรจัน สปายแวร์สแปมเมล์ หรือโปรแกรมไม่ประสงค์ดีอื่น ๆ
10. เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่อยู่
11. เว็บหรือห้องสนทนาใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
12. เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อองค์กร

20. การใช้งานเครื่องคอมพิวเตอร์โน๊ตบุ๊ค

ระเบียบปฏิบัติ

1. ในกรณีที่เป็นเครื่องโน้ตบุ๊คที่ใช้ร่วมกัน ให้ทำการกรอกแบบฟอร์มยืม-คืนสำหรับเครื่องคอมพิวเตอร์ โน้ตบุ๊คนั้นเพื่อขออนุมัติการนำไปใช้งานและป้องกันการสูญหาย
2. ตรวจสอบอย่างสม่ำเสมอว่าโปรแกรมป้องกันไวรัสที่ใช้งานอยู่ได้รับการปรับปรุงฐานข้อมูลรูปแบบไวรัสอย่างสม่ำสมอ
3. ให้ระมัดระวังและรักษาเครื่องคอมพิวเตอร์โน้ตบุ๊คเมื่อมีการนำไปใช้งานนอกสถาน ที่เพื่อป้องกัน การสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
4. เมื่ออยู่ในที่สาธารณะหรือในห้องประชุมห้ามปล่อยเครื่องทิ้งไว้โดยไม่มีผู้ดูแล
5. ตรวจสอบว่าได้มีการตั้งค่า Screen Server เพื่อให้ทำการล็อกหน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที

21. การกำหนดรหัสผ่านและป้องกันรหัสผ่าน

ระเบียบปฏิบัติสำหรับการกำหนดรหัสผ่าน

1. การตั้งรหัสต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร ทั้งในส่วนการเข้าใช้งานเครื่องคอมพิวเตอร์ และระบบ Real Estate Management System (RMS)
2. มีการผสมผสานกันระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็กตัวพิมพ์ใหญ่ตัวเลขและสัญลักษณ์เข้า ด้วยกัน
3. ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ปรากฏในพจนานุกรม
4. เปลี่ยนรหัสผ่านทุก ๆ 3 เดือน

22. ระเบียบปฏิบัติสำหรับการกำหนดและป้องกันรหัสผ่าน

1. เก็บรักษารหัสผ่านของตนเองไว้เป็นความลับห้ามเปิดเผยต่อผู้อื่น
2. กำหนดรหัสผ่านให้มีคุณสมบัติตามระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน
3. ห้ามบันทึกรหัสผ่านไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตน (เช่น โปรแกรมเว็บบราวเซอร์จะสามารถเลือกให้โปรแกรมช่วยจำรหัสผ่านไว้ให้)
4. ต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

23. การนำข้อมูลเผยแพร่สู่สาธารณะ

ระเบียบปฏิบัติ

1. ให้ผู้ที่เป็นเจ้าของข้อมูลที่ต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของบริษัทจะต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น

24. การรักษาความปลอดภัย/ป้องกันการสูญหายของแฟ้มจัดเก็บรูปแบบ Electronic file

ระเบียบปฏิบัติ

บริษัท อรสิริน โฮลดิ้ง จำกัด (มหาชน) ใช้โปรแกรม Real Estate Management System (RMS) ในการจัดเก็บข้อมูลทางบัญชีและข้อมูลลูกค้าของบริษัท ทั้งหมดในคอมพิวเตอร์โดยมีระเบียบปฏิบัติดังนี้

1. กำหนดให้พนักงานที่ทำหน้าที่บันทึกข้อมูลต่างๆในคอมพิวเตอร์มีรหัส username และ password เพื่อการเข้าถึงงานในแต่ละประเภท โดยรหัสที่กำหนดให้จะเข้าถึง (Access_menu) และ ใช้งานได้เฉพาะงานในหน้าที่ของตนเองเท่านั้นไม่สามารถใช้งานในด้านอื่นที่ไม่เกี่ยวข้องได้
2. พนักงานของบริษัททุกคนได้รับการอบรมในเรื่องการรักษาข้อมูลลูกค้า ไม่เปิดเผยข้อมูลซึ่งจะต้องปฏิบัติตามระเบียบ

3. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งาน โปรแกรม Real Estate Management System (RMS) ต้อง Log out ออกจากโปรแกรมทุกครั้ง หากไม่ได้ปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ทุกครั้ง

4. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งาน โปรแกรม Real Estate Management System (RMS) ต้องเปลี่ยนรหัสผ่านใหม่ทุก 3 เดือน

5. กำหนดให้โปรแกรมสามารถตรวจสอบเหตุผิดพลาดของงานและสืบสวนย้อนกลับได้ว่ามีการเข้าถึง การบันทึกหรือแก้ไข มีการดำเนินการเมื่อใด

6. กำหนดให้โปรแกรมสามารถป้องกันการเข้าถึงข้อมูลและการนำข้อมูลในคอมพิวเตอร์ไปใช้งานโดยไม่ได้รับอนุญาต เช่น จำกัดสิทธิการ print รายงานต่าง ๆ เป็นต้น

7. กำหนดให้มีการติดตั้งโปรแกรมเพื่อป้องกันและปกป้องข้อมูลจากไวรัส มัลแวร์โทรจัน หนอน คอมพิวเตอร์และตรวจสอบให้มีการ update อัตโนมัติ

8. กำหนดให้มีการปิดระบบเพื่อป้องกันการใช้อุปกรณ์พกพา เช่น Hard disk External, USB Flash drive

9. สำรวจสายไฟในหน่วยงานไม่ให้ชำรุดสามารถใช้งานได้อย่างปลอดภัยเพื่อป้องกันอัคคีภัย

10. มีการจำลองเหตุการณ์ร่วมซ้อมแผนภาวะฉุกเฉินของบริษัทและเตรียมความพร้อม เมื่อเกิดเหตุการณ์ฉุกเฉินและมีเหตุจำเป็นต้องขนย้ายเครื่องServer

11. จัดให้มีอุปกรณ์ดับเพลิงและมีการตรวจสอบให้ใช้งานได้อย่างมีประสิทธิภาพเพื่อป้องกันหรือบรรเทาความเสียหายทางกายภาพที่อาจเกิดขึ้น

12. ห้องจัดเก็บ Server ปรับปรุงมาตรฐานเทคโนโลยีสารสนเทศของบริษัท โดยจัดเก็บ Server ไว้ในตู้ Rack สำหรับขนย้าย ภายในห้องติดตั้งเครื่องปรับอากาศและล็อคห้อง server เพื่อป้องกันบุคคลภายนอกเข้าไปโดยไม่ได้รับอนุญาต

13. กำหนดสิทธิรหัสผู้ใช้ username และ password สำหรับการใช้งาน server และการเข้าถึง database

25. การควบคุมการเข้าถึงระบบสารสนเทศ

ระเบียบปฏิบัติ

1. การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ(AccessControl)

1.1 กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

1.2 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้สารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ

(1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไขข้อมูล
- อนุมัติ
- ไม่มีสิทธิ

(2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

(3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อนุมัติต้นสังกัดและผู้ดูแลระบบที่ได้รับมอบหมาย

1.3 มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements foraccess control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

(1) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กาหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(2) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่งคงปลอดภัย

2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ครอบคลุมในเรื่องต่อไปนี้

- จัดทำแบบฟอร์มขอใช้ระบบสารสนเทศและให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
- มีการระบุชื่อ นามสกุลของผู้ใช้งาน
- มีการระบุรหัสบัญชีผู้ใช้เครือข่ายของผู้ใช้งาน
- มีการระบุ ตำแหน่ง หน่วยงานที่สังกัด
- มีการลงนามของผู้บังคับบัญชาของผู้ใช้งาน
- มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
- จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย
- มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ
- มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น
- การทบทวนสิทธิการเข้าใช้งาน ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้ระบบสารสนเทศและ ปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ 1 ครั้ง

3. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

3.1 ผู้ดูแลระบบต้องกำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการ ควบคุมการเข้าถึงข้อมูลการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภท

3.2 เจ้าของข้อมูลจะต้องทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

3.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกาหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูล

3.4 การรับส่งข้อมูลสาคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ EML Encryption เป็นต้น

3.5 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่บารุงรักษาเครื่องคอมพิวเตอร์ หรือนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

ประกาศใช้ ณ วันที่ 15 มีนาคม 2568 เป็นต้นไป