คุณธรรม คุณภาพ คุณประโยชน์
กลุ่มสหยูเนี่ยน

บริษัท ยูเนี่ยนพลาสติก จำกัด (มหาชน)

11/1 ซอยเสรีไทย 62 แขวงมีนบุรี เขตมีนบุรี กรุงเทพฯ 10510
บมจ. 346 โทร. 66-2-517-0109-14 แฟกซ์ 66-2-5170529

ที่ MD/02/65

ประกาศ
เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำรายละเอียดและการปฏิบัติตามนโยบาย ดังนี้

รายละเอียดของนโยบาย มี 5 ข้อดังนี้

1) การแบ่งแยกอำนาจหน้าที่
2) การควบคุมการเข้าออก Server Room และการป้องกันความเสียหาย
3) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย
4) การความคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์
5) การสำรองข้อมูลระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

1) การแบ่งแยกอำนาจหน้าที่

วัตถุประสงค์

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้านโครงสร้างพื้นฐาน

แนวทางการปฏิบัติ

1) ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง
2) ต้องจัดให้มี Job description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนในฝ่ายคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร
3) ควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ ในกรณีจำเป็น เช่น ผู้บริหารระบบ เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ เป็นต้น

2) การควบคุมการเข้าออก Server Room และการป้องกันความเสียหาย

วัตถุประสงค์

1) การควบคุมการเข้าออกห้อง Server Room มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์
2) การป้องกันความเสียหาย มีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูล และระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออก Server Room และระบบป้องกันความเสียหายต่าง ๆ

แนวทางการปฏิบัติ

1) **การควบคุม** Server Room
   1.1) ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในห้อง Server Room หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกห้อง Server Room ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ เจ้าหน้าที่ดูแลระบบ เป็นต้น
   1.2) ต้องมีระบบเก็บบันทึกการเข้าออกห้อง Server Room โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างน้อยเดือนละ 1 ครั้ง
2) **การป้องกันความเสียหาย**
   2.1) ระบบป้องกันไฟไหม้
   ต้องมีอุปกรณ์ป้องกันไฟไหม้ เช่น ถังดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์ (ถังเขียว)
   2.2) ระบบป้องกันไฟฟ้าขัดข้อง
   ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า และเพื่อให้การดำเนินงานมีความต่อเนื่อง โดยกำหนดให้มีเครื่องสำรองไฟ (UPS)และมีการทดสอบอย่างน้อยปีละ 1 ครั้ง.
   2.3) ระบบควบคุมอุณหภูมิและความชื้น
   ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะของระบบคอมพิวเตอร์ โดยกำหนดให้ตั้งอุณหภูมิประมาณ 23 องศาเซลเซียส

3) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึงล่วงรู้หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

แนวทางปฏิบัติ

1) **การบริหารจัดการข้อมูล**

ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

2) **การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน**

2.1) ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานอินเตอร์เน็ต ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งให้มีการทบทวนสิทธิดังกล่าวตามความเหมาะสม

2.2) ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงานในช่วงที่ไม่ได้อยู่ปฏิบัติงานที่เครื่องคอมพิวเตอร์

3) **การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน**

3.1) ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งานก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User account เป็นของตนเอง

3.2) ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ความยาวขั้นต่ำ 8 ตัวอักษร

3.3) สำหรับผู้ใช้งานทั่วไป เปลี่ยนรหัสผ่านทุก ๆ 90 วัน

3.4) ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ เปลี่ยนรหัสผ่านทุก ๆ 60 วัน

3.5) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้น

3.6) ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

3.7) ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของพนักงานที่ลาออกแล้ว

3.8) กำหนดให้ผู้ใช้งานสามารถใช้คอมพิวเตอร์ตามที่ได้กำหนดไว้แล้วเท่านั้น

3.9) กำหนดให้มีการระงับสิทธิ์รหัสผู้ใช้ในระบบเครือข่ายทันทีเมื่อผู้ใช้งานมีการใส่รหัสผ่านผิดเกินกว่า 4 ครั้ง

บันทึกการตรวจสอบ

ต้องมีกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานและเก็บประวัติฯอย่างน้อย 90 วัน และบันทึกการเข้าใช้งานในอินเตอร์เน็ต,การรับส่งอีเมล์และเก็บประวัติฯอย่างน้อย 180 วัน

4) การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้น ซึ่งได้แก่ การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

แนวทางปฏิบัติ

1) **การกำหนดขั้นตอนการปฏิบัติงาน**

ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

2) **การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงาน**

2.1) การร้องขอ

2.1.1) การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ต้องจัดทำให้เป็นลายลักษณ์อักษร และได้รับการอนุมัติจากผู้มีอำนาจหน้าที่

2.1.2) ควรสอบทานระบบงานที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามระบบงาน

2.2) การปฏิบัติงานพัฒนาระบบงาน

2.2.1) ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงานออกจากส่วนที่ใช้งานจริงและควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น

2.2.2) ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

2.3) การทดสอบ

ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

2.4) การโอนย้ายระบบงานเพื่อใช้งานจริง

ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

2.5) ต้องจัดเก็บปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

2.6) การสื่อสารการเปลี่ยนแปลง

ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

5) การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา

แนวทางปฏิบัติ

1) **การสำรองข้อมูลและระบบคอมพิวเตอร์**

1.1) การสำรอง

1.1.1) ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ โปรแกรมระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

1.1.2) ขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยมีรายละเอียด ดังนี้

1.1.2.1) ข้อมูลที่ต้องสำรองที่สำคัญทางธุรกิจจะต้องสำรองทุกวันทำการ จำนวนที่สำรอง 3 ชุด

1.1.2.2) สถานที่จัดเก็บอยู่ที่ห้อง Server 2 ชุด และที่ Office บางปะกง (\\least\BackupShare) 1 ชุด

1.1.2.3) ส่วนข้อมูลและOS ที่อยู่ใน ErpServerและNorth จะต้องสำรองทุกวัน

1.1.2.4) สถานที่จัดเก็บสำรองข้อมูลของสำนักงานใหญ่เก็บไว้ที่สาขา ส่วนที่สาขาเก็บไว้ที่สำนักงานใหญ่

1.2) การทดสอบ

1.2.1) ต้องทดสอบข้อมูลสำรองทางธุรกิจอย่างน้อยเดือนละ 1 ครั้งและข้อมูลสำรองสำหรับ Server และ OS ปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

1.2.2) ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

1.3) การเก็บรักษา

ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

2) การเตรียมพร้อมกรณีฉุกเฉิน

ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว เพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้

1) ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

2) ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

3) ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

4) ต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

ทั้งนี้มีผลบังคับใช้ตั้งแต่วันที่ 15 มกราคม พ.ศ 2565

ประกาศ ณ. วันที่ 5 มกราคม 2565

ลงชื่อ.....

(นายสุทิน เผด็จภัย)

กรรมการผู้จัดการ