SaleeColour™

ประกาศ

วันที่ 1 มกราคม 2555 (ฉบับแก้ไข 30 พฤศจิกายน 2560)

เลขที่ IT-01-55-001

เรื่อง นโยบายด้านความปลอดภัยระบบงาน IT

วัตถุประสงค์

เพื่อให้สอดคล้องและเป็นไปตามข้อกำหนดของกฎหมายที่เกี่ยวข้องกับระบบงาน IT เช่น พรบ. 60 และกฎหมายลิขสิทธิ์ ตลอดจนกฎหมายเกี่ยวกับทรัพย์สินนิติบุคคลหรือแนวนโยบายของบริษัทฯ รวมทั้งประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย โดยมีสาระดังต่อไปนี้

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. จัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษรและผู้บริหาร เจ้าหน้าที่แผนกคอมพิวเตอร์ และผู้ใช้งานของแต่ละแผนกงานต้องมีส่วนร่วมในการจัดทำนโยบาย และอย่างน้อยต้องได้รับอนุมัติจากคณะกรรมการบริหารหรือคณะกรรมการบริษัท [M]
2. กำหนดให้มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ โดยต้องมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง ซึ่งต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง [M]
3. ต้องจัดเก็บนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้อง สามารถเข้าถึงได้โดยง่าย [M]

การแบ่ง/แยกอำนาจหน้าที่ (Segregation of Duties)

1. กำหนดให้มีการจัดทำ Organize structure (Department)

Salee Colour PLC
858 Moo 2, Soi 1C/1 Bangpu Industrial Estate, Bangpumai, Muang Samutprakarn, Samutprakarn 10280, Thailand
Tel: (662) 323-2601-8 Fax: (662) 323-2227-8 www.saleecolour.com
Compound Values

2. กำหนดให้มีการจัดทำ Job description (JD) ของแต่ละตำแหน่งตาม Organize structure รวมทั้งการกำหนดหน้าที่รับผิดชอบลงใน JD อย่างชัดเจน

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

1. กำหนดให้ติดตั้งเครื่อง face / finger scan ที่ประตูเข้าห้องทำงานของแผนกไอที พร้อมทั้งลงทะเบียนใบหน้า เฉพาะพนักงานห้องไอที ตาม Organize Structure (department) เท่านั้น
2. กำหนดให้ติดตั้งเครื่อง face / finger scan ที่ประตูเข้าห้อง server พร้อมทั้งลงทะเบียนลายนิ้วมือเฉพาะ ผู้จัดการแผนกไอที, แอดมิน และ ผู้ช่วยแอดมิน เท่านั้น
3. กำหนดให้มีการตรวจสอบ transaction log ทุกวันจันทร์แรกของเดือน

การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

แบ่งออกเป็นกลุ่มดังนี้

1. <u>หมวดซอร์ฟแวร์ (Software)</u>
   a. ห้ามนำโปรแกรมผิดกฎหมาย (ไม่มีลิขสิทธิ์ที่ถูกต้อง) ใด ๆ ทุกประเภท มาติดตั้งลงในคอมพิวเตอร์ของบริษัทฯ ห้ามนำไฟล์ภาพ, ไฟล์วีดิโอหรือไฟล์ข้อมูลที่ผิดกฎหมายตลอดจนสื่อลามกอนาจารหรือข้อมูลที่ขัดต่อกฎหมายและขนบธรรมเนียมประเพณีอื่น ๆ มาบันทึกเก็บไว้ในระบบคอมพิวเตอร์ของบริษัทฯ
   b. ห้ามทำสำเนาข้อมูลของบริษัทฯ ออกไปนอกบริษัทฯก่อนได้รับอนุญาตจากผู้จัดการแผนก ไม่ว่าจะด้วยช่องทางใด ๆ
   c. ห้ามนำข้อมูลบริษัทฯอื่น ๆ ที่ล่อแหลมต่อการละเมิดสิทธิ์หรืออันอาจจะทำให้บริษัทฯ หรือบุคคลที่เป็นเจ้าของข้อมูลได้รับความเสียหาย มาเก็บไว้ในระบบคอมฯของบริษัทฯ
   d. ในกรณีที่ต้องการเพิ่มหรือแก้ไขโปรแกรมให้ปฏิบัติตามหมวดคำร้อง ที่ได้กำหนดไว้ในประกาศฉบับนี้
2. <u>หมวดฮาร์ดแวร์ (Hardware)</u>
   a. ห้ามนำอุปกรณ์ต่อพ่วงหรือสื่อบันทึกข้อมูลทุกชนิดที่ไม่ใช่ทรัพย์สินของบริษัทและที่ไม่ได้รับการจัดหาจากแผนกไอที มาต่อพ่วงกับระบบคอมพิวเตอร์ก่อนได้รับอนุญาตจากผู้จัดการแผนกไอที เช่น โทรศัพท์มือถือ คอมพิวเตอร์พกพา ต่าง ๆ ตลอดจนกล้องถ่ายภาพต่าง ๆ , Floppy disk, Handy drive, External Hard disk เป็นต้น

PolyMerit CompositeASIA POLY POLYMER

b. ห้ามนำอุปกรณ์ต่อพ่วงหรือสื่อบันทึกข้อมูลต่าง ๆ เช่น Floppy disk, Handy drive, External Hard disk ที่เป็นทรัพย์สินของบริษัทฯ ออกนอกบริษัทฯ ก่อนได้รับอนุญาตจากผู้จัดการแผนกที่สังกัด หรือแผนกไอที

c. ห้ามรื้อหรือแกะตลอดจนโยกย้ายคอมพิวเตอร์และอุปกรณ์ต่อพ่วงทุกชนิด

3. **หมวดการสื่อสาร** เช่น อินเตอร์เน็ต, โทรศัพท์, อีเมล์ ฯลฯ

a. ห้ามพนักงานที่ได้รับอนุญาตให้ใช้ช่องทางสื่อสารต่างๆ ของบริษัทฯ เช่น อินเตอร์เน็ต, อีเมล์ นำไปวิพากษ์วิจารณ์บุคคลที่ไม่เกี่ยวข้องหรือไม่ได้เป็นพนักงานของบริษัท เพื่อหวังผลอย่างใดอย่างหนึ่งให้เกิดขึ้นกับผู้ถูกวิจารณ์ เช่น การเมือง ศาสนา และสถานบันต่าง ๆ

b. ห้ามใช้สื่อที่ได้รับอนุญาตทำการหรือสื่อสารกับสื่อและเว็บไซต์ที่ผิดกฎหมาย หรือล่อแหลมสุ่มเสี่ยงที่จะทำให้เกิดความเสียหายกับบุคคลใดบุคคลหนึ่งตลอดจนความเสียหายที่อาจจะสะท้อนกลับมาถึงบริษัทฯ เช่น เว็บไซต์วิพากษ์วิจารณ์การเมือง ศาสนา หรือโจมตีกลุ่มบุคคล หรือเว็บไซต์ที่สุ่มเสี่ยงต่อการแพร่กระจายของไวรัสคอมพิวเตอร์

c. ห้ามนำอีเมล์ที่ได้รับอนุญาตให้ใช้งาน ที่มีแอดเดรส @saleecolour.com ทำการ forward เมล์ที่มีเนื้อหาเกี่ยวข้องกับการเมือง หรือเนื้อหาที่จะส่งผลในทางลบกับบุคคลที่ไม่ใช่พนักงานของบริษัทฯ

d. ห้ามนำโปรแกรม skype รับส่งไฟล์ทุกชนิดกับบุคคลภายนอกที่ไม่ใช่พนักงานของบริษัทฯ

e. ห้ามทำการ download หรือรับส่งไฟล์ที่มีส่วนขยายไฟล์ดังนี้ .exe, .com, .zip, .rar, .bat

4. **หมวดผู้ใช้งาน (People ware)**

a. ห้ามบุคคลที่ไม่ใช่พนักงานของบริษัทฯ เข้าใช้งานคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของบริษัทฯในทุกกรณี

b. ห้ามพนักงานที่ได้รับ username, password ที่ทางแผนกไอทีจัดสรรให้เพื่อนำไปใช้งานในระบบ ไปให้หรือบอกกับบุคคลอื่น ไม่ว่าจะเป็นพนักงานของบริษัทด้วยกันเองหรือกับบุคคลภายนอก

c. หากพนักงานลาออกให้แผนกบุคคลทำรายงานพนักงานลาออกส่งให้แผนกไอทีในทุก ๆ วันศุกร์สุดท้ายของเดือน

d. หากพนักงานต้องการมีสิทธิ์ในการเข้าใช้งานระบบ ให้ดำเนินการในหมวดคำร้องที่ได้กำหนดไว้ในประกาศฉบับนี้

e. กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านสำหรับการเข้าใช้งานระบบคอมพิวเตอร์ (Active directory) โดยปฏิบัติประกาศ IT-01-58-001_password

f. กรณีผู้ใช้งานไม่ได้ใช้งานคอมฯ สักระยะ และจำเป็นผละจากคอมพิวเตอร์ ให้ผู้ใช้งานทำการ sign out หรือล็อคออกจากชื่อตนเอง

PolyMerit CompositeASIA POLY POLYMER

5. **หมวดคำร้อง (Petition)** ในกรณีที่มีความจำเป็นใด ๆ อันเป็นการนอกเหนือหรือต้องการกระทำการยกเว้นซึ่งขัดต่อข้อห้ามในประกาศฉบับนี้ ให้ปฏิบัติดังนี้
   a. กรอกข้อความในระบบ Computer System Request Online (CSRO) เพื่อแจ้งรายละเอียดรวมทั้งความประสงค์ เหตุผล ให้ครบถ้วน
   b. หัวหน้าต้นสังกัดในระดับผู้จัดการทำการพิจารณาและอนุมัติ ในระบบเช่นเดียวกัน
   c. กรณีที่คำร้องได้รับการอนุมัติจากหัวหน้าต้นสังกัดแล้วจะต้องได้รับการพิจารณาและอนุมัติจากผู้จัดการแผนกไอทีก่อนจึงจะดำเนินการต่อได้ตามคำร้องที่ร้องขอมา
   d. การดำเนินการใด ๆ ตามคำร้องที่ได้รับการอนุมัติจากผู้จัดการแผนกไอที จะต้องเป็นการกระทำภายใต้การควบคุมดูแลโดยพนักงานแผนกไอทีที่ได้รับการมอบหมายงานจากผู้จัดการแผนกไอทีเท่านั้น
   e. หลังจากพนักงานแผนกไอทีดำเนินการตามคำร้องเสร็จสิ้น ให้แจ้งผลการดำเนินงานต่อพนักงานที่ยื่นคำร้อง
   f. พนักงานที่ยื่นคำร้องจะต้องตรวจสอบการดำเนินงานว่าเป็นไปตามคำร้องที่ยื่นหรือไม่ ถ้าใช่ให้ทำการบันทึกรับทราบในระบบ Computer System Request Online และทำการปิดคำร้อง
   g. ผู้จัดการแผนกไอที ทำการอนุมัติ ก่อนนำระบบที่ทำการแก้ไขเสร็จแล้ว ขึ้นสู่ server เพื่อใช้งานจริงต่อไป

   ** เพิ่มเติม ในกรณีที่ทางแผนกไอทีต้องการแก้ไขหรือพัฒนาระบบ ให้ปฏิบัติเช่นเดียวกับคำร้องทั่วไป (ปฏิบัติตาม ข้อ 5) แต่มีความแตกต่างคือ ผู้อนุมัติในข้อ g. ต้องเป็นระดับกรรมการบริษัทฯ

6. **หมวดบทลงโทษ** (Punishment) ในกรณีที่มีการฝ่าฝืนประกาศฉบับนี้
   a. หากตรวจพบการละเมิดหรือฝ่าฝืนในประกาศฉบับนี้ จะพิจารณาลงโทษขั้นสูงสุด และหากเป็นบุคคลภายนอกจะดำเนินการตามกฎหมาย
   b. หากพบว่าเป็นการฝ่าฝืนเพื่อดำเนินการหรือส่อเจตนาให้เห็นว่าหวังผลให้เกิดความเสียหายต่อบริษัทฯ จะทำการลงโทษตามขั้นตอนของกฎหมายให้ถึงที่สุด
   c. หากการฝ่าฝืนได้สร้างความเสียหายให้บุคคลอื่น จะถือว่าเป็นความผิดส่วนบุคคล ทางบริษัทฯจะไม่รับผิดชอบต่อความผิด หรือความเสียหายที่เกิดขึ้นแต่อย่างใด และบริษัทฯจะพิจารณาลงโทษเพิ่มเติมตามประกาศและระเบียบบริษัทฯ

PolyMerit CompositeASIA POLY POLYMER

7. **ทบทวน ตรวจสอบ** (Monitor)
    a. กำหนดให้มีแผนบำรุงรักษาอุปกรณ์ไอที พร้อมทั้งกำหนดผู้รับผิดชอบไว้ใน JD อย่างชัดเจน
    b. กำหนดให้มีการทบทวน หรือ review ตามภาคผนวก Appendix (Security Policies) ในทุกวันจันทร์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

1. ในกรณีที่ต้องการแก้ไขเปลี่ยนแปลงหรือพัฒนาระบบ ให้ปฏิบัติตามหมวดคำร้อง ที่บรรจุไว้ในประกาศฉบับนี้

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

1. ติดตั้งระบบ DR-Site ภายใต้เงื่อนไข
    a. RTO, RPO <= 4 ชั่วโมง
    b. Backup site อยู่ห่าง HQ อย่างน้อย 15 กิโลเมตร
    c. สถานที่ต้อง Backup site ได้มาตรฐานตามข้อกำหนด ซึ่งทางเราเลือกใช้ CS-Loginfo
    d. มี Datalink ระหว่าง Backup site & HQ เฉพาะโดยไม่นำไปใช้งานร่วมกับงานอื่น ความสามารถในการส่งถ่าย Data อยู่ที่ 10/10 MB.
2. กำหนดให้มีการจัดทำแผน สำรอง / กู้คืนข้อมูล และมีการตรวจสอบทบทวนการปฏิบัติตามแผน

ประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 30 พฤศจิกายน 2560

(นายรัช ทองวานิช)

ประธานกรรมการบริหาร

PolyMerit CompositeASIA POLY POLYMER