SANKO PLASTICS (THAILAND) CO.,LTD.

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

(Information Technology Security Policy)

บริษัทตระหนักถึงความสำคัญของการนำเทคโนโลยีสารสนเทศ และการสื่อสารซึ่งเป็นปัจจัยสำคัญ ที่ช่วยส่งเสริมการดำเนินธุรกิจ และเพิ่มประสิทธิภาพการทำงานให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ บริษัทจึงกำหนดนโยบายฉบับนี้ขึ้น เพื่อให้ธุรกิจงานของบริษัทมีกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี โดยอ้างอิงจากหลักเกณฑ์และแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยี สารสนเทศ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายอื่นที่เกี่ยวข้อง มาปรับใช้ให้เหมาะสมกับบริบท การดำเนินธุรกิจของบริษัทโดยนโยบายการดำเนินการด้านเทคโนโลยีสารสนเทศของบริษัทดังนี้

1) นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2) นโยบายรักษาความมั่นคงปลอดภัยของระบบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์ เพื่อให้บริษัทมีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับ องค์กร ที่สอดคล้องและเหมาะสมกบการดำเนินธุรกิจ รวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการ สนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความเสี่ยง เพื่อให้บริษัทสามารถบรรลุวัตถุประสงค์ และเป้าหมายหลักของบริษัทได้ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการที่ดี

3. ขอบเขตการบังคับใช้ นโยบายฉบับนี้มีผลบังคับใช้กับบริษัทซันโค พลาสติกส์ (ประเทศไทย) จำกัด โดยนโยบายหลักเกณฑ์ ระเบียบปฏิบัติและคำสั่งที่ใช้ อยู่ก่อนนโยบายฉบับนี้ ให้ยังมีผลใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับนโยบายฉบับนี้

4.คำนิยาม

ซันโคหมายถึง บริษัท ซันโค พลาสติกส์ (ประเทศไทย) จำกัด

ผู้บริหาร หมายถึง ผู้บริหารธุรกิจซันโค ระดับผู้จัดการหน่วยงานขึ้นไป

บุคลากรของซันโค หมายถึง กรรมการ ผู้บริหาร และพนักงานทุกระดับของ ซันโค รวมถึงลูกจ้าง โครงการ ลูกจ้างชั่วคราว และลูกจ้างรายวันตามสัญญาจ้าง

นโยบาย หมายถึง นโยบายเทคโนโลยีสารสนเทศ

สายงานเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานตามโครงสร้างของซันโคที่มีหน้าที่รับผิดชอบงาน ด้านเทคโนโลยีสารสนเทศ และวิศวกรรมระบบเทคโนโลยีสารสนเทศ

ผู้ใช้งาน หรือ ผู้ปฏิบัติงาน หมายถึง พนักงานประจำ พนักงานตามสัญญาจ้าง ผู้รับจ้าง ผู้ให้บริการ ภายนอก คู่ค้าหรือลูกค้า

ผู้ให้บริการภายนอก หมายถึง บุคคลจากภายนอกบริษัท ซึ่งซันโค ว่าจ้างเพื่อให้บริการที่เกี่ยวข้องกับระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือ ระบบ IT หรือ ระบบสารสนเทศ หรือ เทคโนโลยีสารสนเทศ หมายถึง ระบบสารสนเทศ ระบบฐานข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบการรักษาความปลอดภัยทาง สารสนเทศ (Information Security) ระบบงาน (ซอฟต์แวร์สำเร็จรูป ซอฟต์แวร์ประยุกต์) และระบบสื่อสารของ ซันโคทั้งนี้ไม่ว่าระบบดังกล่าวจะเกี่ยวข้องกับข้อมูลส่วนบุคคลหรือไม่ก็ตาม และหมายรวมถึง “ระบบ เครือข่ายและคอมพิวเตอร์” ตามที่กำหนดใน “นโยบายการใช้งานระบบเครือข่ายและคอมพิวเตอร์” (Network and Computer Usage Policy) สารสนเทศ หรือข้อมูลสารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความหรือ

กราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆได้รวมถึงข้อมูลส่วนบุคคล

ข้อมูล หมายถึง ข้อมูล ข้อความ สารสนเทศ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบ คอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย

ข้อมูลส่วนบุคคล มีความหมายตามที่กาหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลและตามที่ระบุใน “นโยบายคุ้มครองข้อมูลส่วนบุคคล ของซันโค”

สินทรัพย์ หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของสายงานเทคโนโลยีสารสนเทศ รวมถึงทรัพย์สินสารสนเทศของซันโค

ทรัพย์สินสารสนเทศ หมายถึง

1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ

2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่อง บันทึกข้อมูล และอุปกรณ์อื่นใด

3) ทรัพย์สินสารสนเทศ ประเภท ข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ และหมายรวมถึงข้อมูลส่วนบุคคลที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์หรือ ข้อมูลคอมพิวเตอร์ด้วย

4) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดจากการพัฒนา หรือสิทธิ์ในการใช้จากเจ้าของผลิตภัณฑ์ สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล หมายถึง อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้

การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์ หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอน หรือสถานที่ประมวลผลข้อมูล

5. บทบาทหน้าที่และความรับผิดชอบ

สายงานเทคโนโลยีสารสนเทศ

5.1 กาหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบาย

5.2 กาหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติเฉพาะเรื่องที่เกี่ยวข้องกับการคุ้มครองข้อมูล ส่วนบุคคลที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์

5.3 ติดตามดูแลให้ผู้ใช้งานปฏิบัติตามนโยบาย หลักเกณฑ์ระเบียบปฏิบัติของบริษัทที่เกี่ยวข้อง อย่างถูกต้องเหมาะสม และหากมีการปฏิบัติที่ไม่ถูกต้องให้รายงานต่อคณะกรรมการบริหารทราบ

5.4 สื่อสารนโยบาย ให้แก่ผู้ใช้งาน ผู้ประกอบธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง

6. นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

บริษัทซันโคกำหนดให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่อง ดังต่อไปนี้

1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยี สารสนเทศ ผู้จัดการสายงานเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือ แนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่แล้ว นำเสนอ ให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)

• ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้อง มีการควบคุมการเข้า-ออกและการใช้งาน การตรวจสอบระบบต่าง ๆ เช่น ระบบเตือนอัคคีภัย ภายในห้อง เป็นต้น

• ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของซันโคเพื่อ ป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัย เช่น การดาวน์โหลดโปรแกรมจากภายนอก มาติดตั้ง ซึ่งอาจมีชุดคำสั่งไม่พึงประสงค์ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะ มัลแวร์ เช่น ไวรัส คอมพิวเตอร์ เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น

• ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของซันโคต้องมีการตรวจสอบ และเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต ตรวจสอบและเฝ้าระวังช่องโหว่ เชื่อมต่อเครือข่ายภายนอก โดยมีการจัดทำระบบป้องกัน

การเข้าถึงและการโจมตีจากภายนอก ให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงาน ใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกัน ชุดคำสั่งไม่พึงประสงค์ การกรองข้อมูลรับส่งอีเมล เป็นต้น

• ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานและการเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่าง ๆ ข้อมูลและข้อมูลส่วนบุคคล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการ เข้าถึง ใช้ แก้ไข เปลี่ยนแปลง ข้อมูลและข้อมูลส่วนบุคคลโดยมิชอบหรือโดยปราศจากอำนาจ

3. การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อ จัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

3.1. ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี

3.2. ความเสี่ยงจากผู้ปฏิบัติงานหรือความเสี่ยงด้านบุคคล ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลโดยมิชอบหรือปราศจากหรือนอกเหนืออำนาจหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้

3.3. ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้ง สถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น

3.4. ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่มีอยู่หรือการนำนโยบายไปปฏิบัติ หรือการปฏิบัติงานซึ่งอาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

4. การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่ซันโคยอมรับได้ จัดทำตาราง ลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมี หัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

5. กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหาร และจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

7. นโยบายการกำกับดู แลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของซันโค ที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ร่วมกันเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและ สามารถสนับสนุนการดำเนินงานของซันโคได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้อง สอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิด

เกี่ยวกับคอมพิวเตอร์และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัทซันโคจึงประกาศนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

1. บริษัทซันโค ต้องจัดให้มีหน้าที่ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความ เข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้าน เทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในซันโค เพื่อให้มีการประสานงาน และสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้

2. บริษัทซันโค ต้องจัดให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยี สารสนเทศ อย่างน้อยปี ละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความ ปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทซันโค

การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security)

1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(Information Security Policy)

• วัตถุประสงค์

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

• แนวทางปฏิบัติ

• ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรม อันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น

• ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้งานหรือรหัสผ่าน หรือข้อมูลยืนยันตัวตนของผู้อื่นทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชี ผู้ใช้

• ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีมาตรการป้องกนการเข้าถึงของผู้อื่น หรือมาตรการ ป้องกนการเข้าถึงที่บริษัทซันโคกำหนดไว้ เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอกหรือ กระทำการอื่นใดที่โดยปราศจากอำนาจหรือเกินขอบอำนาจ

• ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน หรือข้อมูลส่วนบุคคลใด ๆ โดยไม่ได้รับ อนุญาตจากบริษัทซันโค

• ห้ามรบกวน ขัดขวาง หรือกระทำด้วยประการใด ๆ ให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ ของบริษัทซันโคความเสียหายหรือถูกทำลายหรือไม่สามารถใช้การได้ตามปกติ เช่น การส่งชุดคำสั่งไม่พึงประสงค์ใด ๆ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรือ อุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น

• ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัทซันโคและของผู้อื่นที่อยู่ ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์

• ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือ ไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาชุดคำสั่งไม่พึงประสงค์ เช่น ไวรัส โปรแกรมป้องกนไวรัสก่อนทุกครั้ง

• ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่าน ของตนซึ่งซันโคกำหนดอนุญาตให้ ใช้สิทธิเป็นการเฉพาะตัว

วิธีการปฏิบัติให้เป็นไปตามนโยบาย

พน่วยงานเทคโนโลยีสารสนเทศ ได้จัดทำนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศโดยอ้างอิงมาตราบาน ISO/IEC 27011:2013 Information Security Management Systems เพื่อให้เกิดความมั่นคงปลอดภัยแก่สารสนเทศ

การลงโทษทางวินัย

•ตักเตือนด้วยวาจา

•ตักเตือนเป็นลายลักษณ์อักษร

•พักงานชั่วคราวโดยไม่ได้รับค่าจ้าง

•ปลดออก

•การดำเนินทางกฎหมายอาญาหรือแพ่ง

การลงโทษพนักงาน บริษัทไม่จำเป็นต้องปฏิบัติตามลำดับข้างต้น บริษัทอาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

ให้มีผลตั้งแต่วันที่ 1 พฤษภาคม 2568

SANKO Plastics (Thailand) Co., Ltd.
SPT
บริษัท ซันโค พลาสติกส์ (ประเทศไทย) จำกัด

Siwanon

(นายศิวานนท์ ศรีทุมมา)

กรรมการบริษัท