Southland Rubber
Think Good, Better Will Follow

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy)

กลุ่มบริษัทเซาท์แลนด์รับเบอร์ได้จัดให้มีระบบสารสนเทศ เพื่อสนับสนุนประสิทธิภาพการดำเนินงาน เพื่อให้มีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัยถูกต้อง เชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง และสามารถป้องกันรักษาสารสนเทศที่เป็นความลับของกลุ่มบริษัทเซาท์แลนด์รับเบอร์ ทั้งที่เป็นข้อมูลของกลุ่มบริษัทเซาท์แลนด์รับเบอร์และข้อมูลส่วนบุคคลอื่นๆ ดังนั้นกลุ่มบริษัทเซาท์แลนด์รับเบอร์ จึงได้ประกาศนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และได้มีการปรับปรุงเนื้อหานโยบายอย่างต่อเนื่อง เพื่อเป็นแนวทางในการใช้งานที่เหมาะสมและสอดคล้องกับการกำกับดูแลของกลุ่มบริษัทเซาท์แลนด์รับเบอร์

วัตถุประสงค์ (Objective)

1. เพื่อกำหนดมาตรการความปลอดภัย การใช้งานด้านสารสนเทศ ผ่านระบบเครือข่ายของบริษัท ซึ่งผู้ใช้งานจะต้องให้ความสำคัญ และตระหนักถึงปัญหาที่เกิดขึ้น จากการใช้บริการระบบสารสนเทศ ผู้ใช้งานจะต้องรับทราบถึงข้อห้าม, ข้อปฏิบติ, ระเบียบและกฎเกณฑ์ต่าง ๆ ที่ทางบริษัทวางไว้ ไม่ละเมิดสิทธิ กระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด ซึ่งจะทำให้การใช้งานด้านสารสนเทศเป็นไปอย่างถูกต้องปลอดภัย มีประสิทธิภาพ ตรงตามวัตถุประสงค์ของบริษัท ที่ไม่เป็นการละเมิดซึ่งระเบียบ ข้อบังคับ กฎหมาย หรือทำให้เกิดความเสียหายได้ในภายหลัง
2. เพื่อป้องกันไม่ให้ระบบสารสนเทศของบริษัท ถูกบุกรุก เปลี่ยนแปลง ขโมย ทำลาย หรือการกระทำ อื่น ๆ ที่อาจสร้างความเสียหายต่อบริษัท
3. เพื่อสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียต่าง ๆ ว่าข้อมูลส่วนบุคคล จะได้รับการปกป้องตามมาตรฐาน ความปลอดภัยของบริษัท

ขอบเขต (Scope)

นโยบายนี้ให้มีผลบังคับใช้กับพนักงานทุกระดับและบุคคลภายนอก ที่ได้รับอนุญาตและต้องใช้งานระบบสารสนเทศของบริษัท

คำจำกัดความ (Definitions)

กลุ่มบริษัทเซาท์แลนด์รับเบอร์	หมายถึง บริษัทเซาท์แลนด์รับเบอร์จำกัด และบริษัทในเครือ
ข้อมูล	หมายถึง ข้อความ ข่าวสาร คำสั่ง ชุดคำสั่ง ภาพ เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ โดยสภาพของสิ่งนั้นเองหรือโดยผ่านกระบวนการใดๆ ทั้งที่อยู่ในรูป อิเล็กทรอนิกส์ หรือสื่อสิ่งพิมพ์
ทรัพย์สิน	หมายถึง วัตถุ สิ่งของ อันมีค่าของบริษัททั้งที่สามารถจับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ในระบบเครือข่าย ซอฟต์แวร์ หรือสื่อบันทึกข้อมูล เป็นต้น และรวมถึงสิ่งที่ไม่สามารถจับต้อง ได้ เช่น ข้อมูล หรือแฟ้มข้อมูล เป็นต้น

เครื่องคอมพิวเตอร์แม่ข่าย	หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่าย ที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลซอฟต์แวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่น ๆ หรือควบคุมการทำงานในเครือข่าย
พนักงาน	หมายถึง ลูกจ้างประจำของบริษัท ทั้งประเภทรายเดือน รายวัน หรือลูกจ้างชั่วคราว
บุคคลภายนอก	หมายถึง ลูกค้า คู่ค้า ผู้เข้าเยี่ยม ผู้มาติดต่อ
ผู้ใช้งาน	หมายถึง พนักงานและบุคคลภายนอกที่ได้รับอนุญาตให้ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท
ผู้ประสานงานด้านสารสนเทศ	หมายถึง พนักงานที่ได้รับการแต่งตั้ง มอบหมายให้ดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์เบื้องต้น
ผู้ดูแลระบบ	หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลอื่น ๆ เพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น
ผู้บังคับบัญชา	หมายถึง ผู้ดูแลและบังคับบัญชาของผู้ใช้งาน และผู้บริหารระดับสูง
ระบบสารสนเทศ	หมายถึง ระบบคอมพิวเตอร์ ระบบเก็บข้อมูล ระบบสื่อสารข้อมูลทุกประเภท อุปกรณ์สื่อสาร เครื่องสแกนหรืออุปกรณ์ใด ๆ ที่เกี่ยวข้อง
เครือข่ายคอมพิวเตอร์	หมายถึง ระบบการสื่อสารระหว่างเครื่องคอมพิวเตอร์จำนวนตั้งแต่ 2 เครื่องขึ้นไป
เครื่องคอมพิวเตอร์	หมายถึง อุปกรณ์ทางอิเล็กทรอนิกส์ที่ทำหน้าที่รับข้อมูล ประมวลผล แสดงผล และเก็บข้อมูล ซึ่งอุปกรณ์ดังกล่าวมีทั้งแบบตั้งโต๊ะและแบบพกพา
บัญชีชื่อผู้ใช้งาน	หมายถึง Username, User Account, Email ชื่อผู้ใช้งานอื่น ๆ ที่ได้รับจากบริษัทและหรือบริษัทภายนอก ในการเข้าใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ถือเป็นทรัพย์สินของทางบริษัท
จดหมายอิเล็กทรอนิกส์	หมายถึง ระบบที่ผู้ใช้งานใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ใช้งานสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAPเป็นต้น
รหัสผ่าน	หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ
การเข้าถึงและการใช้งานด้านสารสนเทศ	หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

หน้าที่ความรับผิดชอบ (Roles & Responsibilities)

1. หน้าที่ของ IT/IS Manager
    1.1 กำหนดเป้าหมาย นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของกลุ่มบริษัทเซาท์แลนดรับเบอร์ โดยกำหนดให้ไปใน ทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท
    1.2 ปรับปรุงและพัฒนานโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (Policy, Standard, Procedure และ Guideline) เพื่อให้กลุ่มบริษัทเซาท์แลนด์รับเบอร์ ได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)
    1.3 บริหาร และเฝ้าระวังการโจมตีระบบและภัยต่างๆที่อาจเกิดขึ้นกับระบบของกลุ่มบริษัทเซาท์แลนด์รับเบอร์
    1.4 มีการบริหารความเสี่ยงและการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจของกลุ่มบริษัทเซาท์แลนด์รับเบอร์
    1.5 เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ
2 หน้าที่ของ ผู้บังคับบัญชา
    2.1 ชี้แจง และส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและตักเตือนลงโทษทางวินัย ในกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม
3 หน้าที่ของผู้ใช้งาน (User)
    3.1 ต้องทำความเข้าใจ รับทราบ และปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของกลุ่มบริษัทเซาท์แลนด์รับเบอร์โดยเคร่งครัด
    3.2 ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกัน ดูแลข้อมูลและระบบสารสนเทศของกลุ่มบริษัทเซาท์แลนด์รับเบอร์ให้มีความปลอดภัย
    3.3 รายงานต่อผู้บังคับบัญชา ผู้ดูแลระบบของกลุ่มบริษัทเซาท์แลนด์รับเบอร์ทันที เมื่อพบว่าอุปกรณ์ ข้อมูลสารสนเทศสำคัญสูญหาย หรือพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อกลุ่มบริษัทเซาท์แลนด์รับเบอร์
4 หน้าที่ของ ผู้ดูแลระบบ (Administrator)
    4.1 ให้มีการจัดทำเอกสาร มาตรการ และขั้นตอนควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของกลุ่มบริษัทเซาท์แลนด์รับเบอร์
    4.2 ดูแล ปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของกลุ่มบริษัทเซาท์แลนด์รับเบอร์ รวมถึงการควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ
    4.3 รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศให้กับ Assistant Managing

Director (Group) ทราบโดยทันที

4.4 ดูแล บริหารบัญชีผู้ใช้งาน และสิทธิ์ในการใช้ระบบสารสนเทศ เพื่อแก้ไข /เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงาน / อำนาจหน้าที่ / โอนย้าย

5 หน้าที่ของ หน่วยงานตรวจสอบภายใน (Internal Audit)

5.1 ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศตามความจำเป็น

ผู้ใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท จะต้องปฏิบัติตามแนวทาง ดังนี้

หมวด 1 ทั่วไป (General)

1.1 ผู้ใช้งานต้องทำความเข้าใจ รับทราบ และปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ซึ่งหมายรวมถึง

- นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Security Policy)
- นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (Email Policy)
- นโยบายและระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
- พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
- พ.ร.บ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562
- พ.ร.บ.ลิขสิทธิ์ (ฉบับที่ 4) พ.ศ. 2561
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562

หมวด 2 การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

2.1 ผู้ใช้งานมีหน้าที่ในการดูแล ป้องกัน และรักษาข้อมูลบัญชีชื่อของผู้ใช้งาน (User) ห้ามมิให้ใช้ร่วมกับผู้อื่น อีกทั้งห้ามมิให้ทำการเผยแพร่ แจกจ่าย คัดลอก หรือทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password) ของตนเอง หรือของผู้อื่น ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดขึ้นจากบัญชีผู้ใช้งานของตนเอง ไม่ว่าการกระทำดังกล่าวนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ยกเว้นกรณีที่พิสูจน์แล้วว่ามีสาเหตุมาจากข้อผิดพลาดของระบบ หรือข้อมูลในระบบถูกขโมย

2.2 ผู้ใช้งานมีหน้าที่ในการกำหนดรหัสผ่านเพื่อให้เกิดความปลอดภัย เมื่อได้รับการจัดสรรรหัสผ่านแล้ว ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านเป็นของตนเอง โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 4 ตัวอักษร และยากต่อการคาดเดาได้และผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ 6 เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน หรือตามความเหมาะสม

2.3 ในกรณีที่มีการเปลี่ยนแปลง, โยกย้าย, พนักงานเข้าใหม่ หรือลาออก เจ้าหน้าที่บุคคลจะต้องดำเนินแจ้งให้ผู้ดูแลระบบทำการสร้าง, ยกเลิก หรือเปลี่ยนแปลงบัญชี ผู้ใช้งานโดยทันที

2.4 ผู้ใช้งานจะต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท และหากพบว่าการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานจะต้องแจ้งให้ผู้ประสานงานด้านสารสนเทศหรือผู้ดูแลระบบทราบโดยทันที

2.5 ผู้ใช้งานต้องตระหนักถึงการประหยัดทรัพยากรพลังงาน หรือปิดเมื่อไม่ใช้งาน

หมวด 3 การบริหารจัดการทรัพย์สินสารสนเทศ (Information Assets Management)

3.1 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

3.2 ผู้ใช้งานต้องไม่เข้าไปในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบและผู้บริหารระดับสูง

3.3 ในกรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลรับผิดชอบทรัพย์สินของบริษัท หากเกิดความเสียหายผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายของทรัพย์สินที่ชำรุด เสียหาย หรือสูญหายตามมูลค่า ในการจัดการทรัพย์สินนั้นมาทดแทนทรัพย์สินเดิม หากความเสียหายนั้นเกิดขึ้นจากความประมาทของผู้ใช้งาน

3.4 ทรัพย์สิน สารสนเทศต่างๆ ที่บริษัทจัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์สำหรับการใช้งานทางธุรกิจของบริษัทเท่านั้น ดังนั้นจึงห้ามมิให้ผู้ใช้งานนำทรัพย์สิน สารสนเทศต่างๆไปใช้งานนอกเหนือจากวัตถุประสงค์ที่บริษัทกำหนด หรือก่อให้เกิดความเสียหายต่อบริษัท

3.5 ผู้ใช้งานต้องส่งมอบทรัพย์สินทั้งหมดของบริษัท ที่ได้มอบไว้ให้ใช้งานคืนแก่บริษัททันทีที่พ้นสภาพการเป็นพนักงานหรือคู่สัญญา

หมวด4 การบริหารจัดการข้อมูลองค์กรและการควบคุมการเข้ารหัสข้อมูล (Corporate Data Management and Cryptographic Control)

4.1 บริษัทมีการกำหนดการเข้าถึงและการใช้ข้อมูลแต่ละประเภทเป็นไปตามระดับชั้นความลับของบริษัทดังต่อไปนี้

4.1.1 ลับที่สุด (Confidential) มีความสำคัญต่อบริษัทในระดับสูง หากสูญหายหรือถูก เปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อบริษัทอย่างมีนัยยะสำคัญ

4.1.2 ใช้ภายในบริษัท (Internal Use) เป็นข้อมูลที่อนุญาตให้ใช้ภายในบริษัท หากสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อบริษัท

4.1.3 สาธารณะ (Public) เป็นข้อมูลที่ใช้เผยแพร่สู่สาธารณะ การเปิดเผยข้อมูลประเภทนี้ ไม่ส่งผลกระทบใดกับบริษัท

4.2 ข้อมูลและสารสนเทศถือเป็นทรัพย์สินของบริษัท ห้ามมิให้ผู้ใช้งานทำการเผยแพร่ เปลี่ยนแปลง คัดลอก ทำซ้ำ หรือทำลาย อันอาจก่อให้เกิดความเสียหายต่อบริษัท เว้นแต่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา

4.3 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล มีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลบริษัทและข้อมูลของลูกค้า ดังนั้นหากเกิดการสูญหาย การนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้น

4.4 ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลลับที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ

4.5 ผู้ใช้งานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้น ครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

4.6 ข้อมูลใดที่ผู้ใช้งานพิจารณาว่าเป็นข้อมูลลับหรือมีจุดอ่อนด้านความมั่นคงปลอดภัยต้องได้รับการเข้ารหัส

4.7 ผู้ใช้งานจะต้องทำการสำรองข้อมูลเก็บไว้ในระบบ หรือสื่อบันทึกข้อมูลที่บริษัทจัดเตรียมให้โดยสม่ำเสมอ

4.8 ผู้ดูแลระบบต้องกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูลโดยรูปแบบการสำรองข้อมูล เช่น การสำรองข้อมูลแบบเต็ม (Full Back up) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Back up)

4.9 ผู้ดูแลระบบต้องใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

4.10 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ผู้ดูแลระบบต้องทำการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL(Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น

4.11 ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.12 ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application Program) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

หมวด 5 การบริหารจัดการระบบสารสนเทศ (Information Technology Infrastructure Management)

5.1 บริษัทได้จัดเตรียมระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่จำเป็นสำหรับการใช้งาน เพื่อวัตถุประสงค์ทางธุรกิจของบริษัท ผู้ใช้งานมีหน้าที่จะต้องใช้งานระบบสารสนเทศ เครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพาอย่างระมัดระวัง คุ้มค่า และเท่าที่จำเป็น โดยทุกครั้งที่ผู้ใช้งานเข้าใช้งานทรัพยากรระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ผู้ใช้งานจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

5.2 ห้ามผู้ใช้งานติดตั้งและหรือใช้โปรแกรมผิดประเภท และหรือโปรแกรมลงในเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา นอกเหนือที่ทางผู้ดูแลระบบเป็นผู้กำหนด, และหรือติดตั้งอุปกรณ์ที่ขยายสัญญาณหรือสามารถแจกจ่าย IP ได้ (DHCP) ที่มีการทำงานให้มี ผลกระทบกับการใช้งานระบบสารสนเทศและเครือข่ายหลัก

5.3 ห้ามผู้ใช้งานเผยแพร่, ดักจับ, ลักลอบสำเนา, เปลี่ยนแปลงและลบทิ้ง (ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด) ซึ่งมีลักษณะขัดต่อความสงบ และศีลธรรมอันดี กฎหมาย ความมั่นคงของประเทศ หรือส่งผลกระทบต่อการดำเนินกิจการของบริษัท

5.4 ห้ามใช้ทรัพยากรของบริษัททุกประเภทเพื่อประโยชน์ทางการค้าใดๆ ซึ่งไม่เกี่ยวข้องกับบริษัท หรือไม่ได้รับอนุญาตจากผู้บังคับบัญชา

5.5 ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา โดยไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

5.6 ผู้ใช้งานควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ 10 นาทีเพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

5.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ผู้ใช้งานควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

5.8 ห้ามนำอุปกรณ์ส่วนตัวเกี่ยวกับคอมพิวเตอร์มาใช้งานในบริษัท เช่น Notebook, Flash drive, External Hard Drive และอื่นๆ ถ้านำมาใช้งานต้องได้รับอนุญาตจากผู้บังคับบัญชา และต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ หากอุปกรณ์ที่นำมาใช้งานนั้น เกิดความเสียหายผู้นำมาใช้จะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

หมวด 6 การปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

6.1 บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานจะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังว่า บริษัทถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดนั้นเอง

หมวด 7 ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

7.1 บริษัทได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น บริษัทอนุญาตซอฟต์แวร์ที่บริษัทมี คือ ซอฟต์แวร์ที่พัฒนาขึ้นเอง หรือที่บริษัทมีลิขสิทธิ์ ซึ่งผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น

7.2 ห้ามมิให้ผู้ใช้งานทำการติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่เป็นการละเมิดลิขสิทธิ์ และหากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทจะพิจารณาว่าเป็นการกระทำความผิดส่วนบุคคลซึ่งผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

7.3 ซอฟต์แวร์ซึ่งบริษัทได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการปฏิบติงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 8 การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

8.1 เครื่องคอมพิวเตอร์ของผู้ใช้งานจะได้รับติดตั้งโปรแกรมป้องกันต่างๆ ตามที่ผู้ดูแลระบบจัดเตรียมไว้ ห้ามผู้ใช้งานทำการเปลี่ยนแปลง ปรับแต่งหรือยกเลิก

8.2 ผู้ใช้งานควรจะ Scan Virus ก่อนทุกครั้ง เมื่อใช้งานไฟล์หรือข้อมูลที่ได้รับจากผู้ใช้งานอื่น หรือจากสื่อบันทึกข้อมูลต่างๆ

8.3 ผู้ใช้งานควรจะ Update Anti-Virus อย่างสม่ำเสมอและหรือตามผู้ดูแลระบบกำหนด เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้นได้

8.4 ผู้ใช้งานต้องพึงระวังไวรัส (Virus) และหรือสิ่งผิดปกติ ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งให้แก่ผู้ดูแลระบบทราบโดยทันทีหากพบเจอ

หมวด 9 การใช้งานระบบจดหมายอิเลกทรอนิกส์ (Electronic Mail)

ตามนโยบายการใช้งานจดหมายอิเล็คทรอนิกส์ของบริษัท

หมวด 10 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment security)

10.1 บริษัทมีการกำหนดผู้รับผิดชอบและพื้นที่ของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ต่างๆ โดยจัดทำเป็นเอกสารขึ้นเพื่อเป็นจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

10.2 ผู้บริหารระดับสูงมีการกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

10.3 ผู้บริหารระดับสูงได้กำหนดสิทธิ์ให้กับผู้ประสานและผู้ดูแลระบบให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์และการสื่อสารเพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

10.3.1 จัดทำทะเบียนผู้มีสิทธิ์และกำหนดผู้รับผิดชอบหน้าที่รับผิดชอบเข้าออกพื้นที่ใช้งานเพื่อใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ และการสื่อสาร

10.3.2 จัดให้มีการตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานเป็นประจำทุกเดือน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งาน อย่างน้อยปีละ 1 ครั้ง

นโยบายนี้จะมีการสื่อสารทั่วทั้งบริษัทรวมไปถึงผู้มีส่วนได้ส่วนเสีย กลุ่มบริษัทเซาท์แลนด์รับเบอร์จะทำการทบทวนนโยบายอย่างสม่ำเสมอ และทำให้พนักงานตระหนักถึงนโยบายนี้ เพื่อการปรับปรุงพัฒนาความมั่นคงปลอดภัยด้านสารสนเทศอย่างมีประสิทธิภาพและต่อเนื่อง

นายเพิ่ม ธีรศานต์วงศ์
กรรมการผู้จัดการ
1 มกราคม 2022