นโยบายระบบงานเทคโนโลยีสารสนเทศ

บริษัท เชฎฐ์ เอเชีย จำกัด (มหาชน) และบริษัทย่อย

นโยบายระบบงานเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

นโยบายระบบสารสนเทศจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแนวทางการใช้งานเพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท เชฎฐ์ เอเชีย จำกัด (มหาชน) และบริษัทย่อย (“**กลุ่มบริษัทฯ**”) อีกทั้ง ต้องการลดความเสี่ยงในการใช้งานที่ไม่ถูกต้องหรือเหตุที่ทำให้ต้องหยุดการทำงาน ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากต้องหยุดการใช้งาน

2. คำนิยาม

“กลุ่มบริษัทฯ”	หมายถึง	บริษัท เชฎฐ์ เอเชีย จำกัด (มหาชน) และบริษัทย่อย ได้แก่ (1) บริษัท รีโซลูชั่น เวย์ จำกัด (2) บริษัท บริหารสินทรัพย์ ซีเอฟ เอเชีย จำกัด และ (3) บริษัท คอร์ทส์ เม็กก้าสโตร์ (ประเทศไทย) จำกัด
“ผู้บังคับบัญชา”	หมายถึง	พนักงานระดับตั้งแต่หัวหน้างานขึ้นไปตามโครงสร้างการบริหารงานของแต่ละบริษัท
“เจ้าหน้าที่เทคโนโลยีสารสนเทศ”	หมายถึง	เจ้าหน้าที่ปฏิบัติหน้าที่ในฝ่ายเทคโนโลยีสารสนเทศของกลุ่มบริษัทฯ
“ผู้ใช้งาน”	หมายถึง	บุคคลที่ได้รับอนุญาตในการใช้งานเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊กและระบบเน็ตเวิร์คของกลุ่มบริษัทฯ
“ระบบเน็ตเวิร์ค”	หมายถึง	ระบบที่สามารถใช้ในการเชื่อมต่อสื่อสารหรือการรับส่งข้อมูลต่าง ๆ ของบริษัท เช่น ระบบแลน (Lan) ระบบไวร์เลสแลน (WirelessLan) ระบบอินเตอร์เน็ต (Internet)

3. การกำหนดความรับผิดชอบและสิทธิในการใช้งานระบบของผู้ใช้งาน (Role & Permission)

กลุ่มบริษัทฯ กำหนดสิทธิในการใช้งานโดยผู้ใช้งานสามารถใช้งานฟังก์ชัน เพิ่ม (Add) ลบ (Delete) แก้ไขข้อมูล (Edit) หรือเข้าดูได้อย่างเดียว (View) ขึ้นอยู่กับหน้าที่ความรับผิดชอบของแต่ละบุคคลและแต่ละแผนก เช่น ผู้ใช้งานบางรายมีสิทธิเข้าดูข้อมูลแต่ไม่สามารถแก้ไขข้อมูลได้ ผู้ใช้งานบางคนมีสิทธิเพิ่มข้อมูลแต่ไม่มีสิทธิลบข้อมูล เป็นต้น โดยจะมีผู้ควบคุมดูแลระบบ (Administrator) ซึ่งเป็นเจ้าหน้าที่เทคโนโลยีสารสนเทศ เป็นผู้ควบคุมในจัดการการให้สิทธิต่าง ๆ แก่ผู้ใช้งาน

กลุ่มบริษัทฯ ได้กำหนดให้ผู้ควบคุมดูแลระบบต้องมีการเรียกดูข้อมูลของการบันทึกการใช้งาน (Logging) ของผู้ใช้งาน เพื่อจัดทำเป็นในรูปแบบของรายงานที่มีรายละเอียดของการระบุวัน เวลาที่เข้าใช้งาน และฟังก์ชันของการเข้าใช้งาน เพื่อตรวจสอบความถูกต้องของสิทธิผู้ใช้งาน แล้วจัดทำข้อมูลส่งให้ผู้บริหารระดับสูงรับทราบทุกเดือน

4. การกำหนดความสำคัญของข้อมูล

คำจำกัดความของ “**ข้อมูล**” ตามที่กลุ่มบริษัทฯ กำหนด หมายถึง ข้อเท็จจริงที่เกิดขึ้นจากการเก็บบันทึกเหตุการณ์ ซึ่งอยู่ในรูปของตัวเลข ตัวอักษร ภาพ สัญลักษณ์ต่าง ๆ ที่มีความหมายเฉพาะตัว เช่น ข้อความ วันที่ ชื่อ ที่อยู่ เบอร์โทรศัพท์ เป็นต้น โดยลักษณะข้อมูลและประเภทของข้อมูล จัดแบ่งดังนี้

ลักษณะของข้อมูล

(ก) ข้อมูลที่คำนวณไม่ได้ ได้แก่ ตัวอักษร รูปภาพ รหัสประจำตัว

(ข) ข้อมูลที่คำนวณได้ ได้แก่ ตัวเลขที่มีความหมายในการคำนวณ

ประเภทของข้อมูล

(1) ข้อมูลเพื่อการวางแผน หมายถึง ข้อมูลที่มีความสำคัญเกี่ยวกับการวางแผนงานการบริหาร ใช้ในการควบคุม การตัดสินใจ โดยได้มีการสรุปเป็นหมวดหมู่เป็นตาราง มีการคำนวณ จัดเรียงลำดับ ซึ่งเรียกกันทั่วไปว่า สารสนเทศ

(2) ข้อมูลการปฏิบัติงาน หมายถึง ข้อมูลที่เกิดขึ้นจากการปฏิบัติงานที่เกิดขึ้นเป็นประจำ

(3) ข้อมูลอ้างอิง หมายถึง ข้อมูลที่มีไว้สำหรับบ่งชี้แหล่งที่มาของข้อมูล

ทั้งนี้ กลุ่มบริษัทฯ กำหนดให้ข้อมูลนั้นแบ่งแยกต่างความสำคัญของข้อมูล ได้ 3 ประเภท ได้แก่

(1) ข้อมูลที่ถือเป็นความลับ หมายถึง ข้อมูลที่มีความสำคัญอย่างสูงต่อการแข่งขันทางธุรกิจ เช่น แผนกลยุทธ์ แผนการควบกิจการ ตัวเลขในการประมาณการทางการเงิน รวมถึงข้อมูลที่มีความสำคัญต่อการดำเนินธุรกิจ และข้อมูลที่ถูกกำหนดสิทธิให้สามารถเข้าถึงได้โดยบุคคลบางกลุ่มเท่านั้น หรือข้อมูลที่เป็นข้อมูลส่วนบุคคล เช่น ข้อมูลเงินเดือนของพนักงาน ข้อมูลทางการตลาด ข้อมูลทางบัญชี (ต้นทุนการผลิตต่าง ๆ) ทั้งนี้ ให้รวมถึงข้อมูลส่วนบุคคลตามกฎหมายข้อมูลส่วนบุคคลด้วย

(2) ข้อมูลที่ใช้เฉพาะภายในกลุ่มบริษัทฯ หมายถึง ข้อมูลที่ใช้เฉพาะในส่วนงานต่าง ๆ ภายในกลุ่มบริษัทฯ อาจจะเปิดเผยข้อมูลได้เฉพาะผู้มีส่วนเกี่ยวในหน้าที่นั้นๆ ในกลุ่มบริษัทฯ เท่านั้น ซึ่งส่วนมากจะไม่เปิดเผยหรือให้แผนกอื่น ๆ ที่ไม่เกี่ยวข้องรับทราบ เช่น ข้อมูลทางการเงิน เอกสารทางบัญชี หรือข้อมูลลูกค้า ซึ่งข้อมูลดังกล่าวถือเป็นข้อมูลที่ไม่ควรเปิดเผยให้แก่บุคคลภายนอกรับทราบ

(3) ข้อมูลที่สามารถเปิดเผยต่อบุคคลภายนอก คือข้อมูลที่บุคคลภายนอกสามารถรับรู้ได้ โดยไม่ส่งผลกระทบในทางที่ไม่ดีต่อกลุ่มบริษัทฯ เช่น ข้อมูลประชาสัมพันธ์จากทางกลุ่มบริษัทฯ เป็นต้น

ทั้งนี้ ในการเปลี่ยนแปลงหรือแก้ไขข้อมูลต่าง ๆ ที่มีความสำคัญและมีผลกระทบของกลุ่มบริษัทฯ จะต้องได้รับความเห็นชอบจากหัวหน้างาน หัวหน้าแผนก ผู้จัดการแผนก และต้องผ่านการอนุมัติจากผู้บริหารระดับสูงทุกครั้งที่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูลของกลุ่มบริษัทฯ

เพื่อให้การปฏิบัติตามนโยบายเป็นไปด้วยความเรียบร้อย กลุ่มบริษัทฯ มีมาตรการป้องกันในการจำกัดการเข้าถึงข้อมูลความลับที่ไม่เปิดเผยต่อสาธารณะ โดยให้รับรู้ได้เฉพาะผู้บริหารระดับสูงสุดเท่าที่จะทำได้และเปิดเผยบางส่วนต่อพนักงานของกลุ่มบริษัทฯ ตามความจำเป็นเท่าที่ต้องทราบเท่านั้น กำชับให้พนักงานรับทราบถึงสารสนเทศที่เป็นความลับ และมีข้อจำกัดในการนำไปใช้ ผู้ฝ่าฝืนจะถูกลงโทษตามกฎระเบียบของกลุ่มบริษัทฯ หรืออาจถูกลงโทษตามกฎหมายแล้วแต่กรณี

5. การแบ่งแยกหน้าที่ความรับผิดชอบของระบบงานและหน่วยงาน (Role)

กลุ่มบริษัทฯ กำหนดให้ผู้อำนวยการฝ่าย ผู้จัดการฝ่าย หรือผู้จัดการแผนก แล้วแต่ว่าผู้ใดจะอยู่ในระดับสูงสุดของแต่ละหน่วยงานเป็นผู้รับผิดชอบในการดูแลข้อมูลและการปฏิบัติงานของระบบงานนั้น ๆ รวมถึงมีหน้าที่รับผิดชอบในระบบงาน โดยการรับผิดชอบของเจ้าของระบบงาน มีดังต่อไปนี้

(1) เป็นผู้ตัดสินใจในการยินยอมหรือไม่ยินยอมในการขอใช้งานโปรแกรม และเข้าถึงข้อมูลในแต่ละระบบงาน ซึ่งหมายถึงการร้องขอข้อมูลในรูปแบบของเอกสารด้วย

(2) มีหน้าที่ในการอนุมัติการขอเปลี่ยนแปลงหรือการขอแก้ไขโปรแกรมและข้อมูล

(3) ในขั้นตอนการเปลี่ยนแปลงระบบงานในทุก ๆ ขั้นตอนนั้น ผู้ที่รับผิดชอบระบบงานและหน่วยงานจะเป็นผู้กำหนดขั้นตอนการปฏิบัติงาน กำหนดผู้ที่จะต้องรับผิดชอบในการตรวจสอบและสอบทาน โดยจะต้องจัดทำขึ้นเป็นลายลักษณ์อักษรและสามารถตรวจสอบได้

พนักงานของแต่ละแผนกจะเป็นเพียงผู้ใช้งาน (User) เท่านั้น โดยที่จะมีเจ้าหน้าที่เทคโนโลยีสารสนเทศเป็นผู้ดูแลความปลอดภัยของระบบสารสนเทศของกลุ่มบริษัทฯ

6. การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

กลุ่มบริษัทฯ ได้กำหนดให้ผู้ใช้งานมีการดำเนินการพิสูจน์ตัวตนเกี่ยวกับระบบสารสนเทศของกลุ่มบริษัทฯ ดังต่อไปนี้

(1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย หรือกระทำการอันใดทำให้ผู้อื่นล่วงรู้รหัสผ่าน

(2) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งานไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

(3) ผู้ใช้งานต้องตั้งรหัสผ่านให้คาดการณ์ยากและมีความปลอดภัย โดยการกำหนดรหัสผ่านให้ปฏิบัติตามระเบียบที่กำหนดของแต่ละโปรแกรม

(4) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๆ ตามกำหนดของแต่ละโปรแกรม หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

(5) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนโดยการลงบันทึกการเข้าใช้งานด้วยบัญชีผู้ใช้งานของตัวเอง (Login by User ID) ทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกลุ่มบริษัทฯ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านโดนล็อกก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้เจ้าหน้าที่เทคโนโลยีสารสนเทศผู้ดูแลระบบทราบทันที โดยที่

- คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
- เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานใหม่อีกรอบทุกครั้ง
- เครื่องคอมพิวเตอร์ทุกเครื่องมีการกำหนดการตั้งเวลาพักหน้าจอ (screen server) อัตโนมัติ โดยเวลาในการพักหน้าจอระบบ Collection ภายใน 15 วินาที และหน้าจอ Windows ภายใน 5 นาที

(6) หากผู้ใช้งานมีการใส่รหัสผ่านผิดเกินจำนวนครั้งตามกำหนดของแต่ละโปรแกรม ระบบจะระงับการใช้ของบัญชีผู้ใช้งานทันทีเพื่อป้องกันการเข้าใช้งานของบุคคลที่ไม่ใช่เจ้าของเครื่อง

7. การบริหารจัดการทรัพย์สิน (Assets Management)

กลุ่มบริษัทฯ มีนโยบายในการบริหารจัดการทรัพย์สินของกลุ่มบริษัทฯ ในส่วนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ดังนี้

(1) ห้ามผู้ใช้งานกระทำการ ถอดชิ้นส่วน แก้ไขหรือกระทำการใด ๆ ที่ไม่ได้เป็นการใช้งานปกติของการใช้งานกับ คอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ระบบเน็ตเวิร์ค เครื่องคอมพิวเตอร์ เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงของกลุ่มบริษัทฯ โดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากเจ้าหน้าที่เทคโนโลยีสารสนเทศที่รับผิดชอบ

(2) ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด ที่เป็นของใช้งานส่วนตัวเชื่อมเข้าระบบเครือข่าย (Network) ของกลุ่มบริษัทฯ ยกเว้นได้รับอนุญาตจากผู้บังคับบัญชาและผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศแล้ว ให้นำอุปกรณ์ดังกล่าวมาลงทะเบียนประวัติเพื่อเชื่อมต่อระบบเน็ตเวิร์คกับเจ้าหน้าที่เทคโนโลยีสารสนเทศของกลุ่มบริษัทฯ ก่อนการใช้งาน

(3) เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ระบบเน็ตเวิร์ค เครื่องคอมพิวเตอร์ เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงของกลุ่มบริษัทฯ ได้ทำการขึ้นทะเบียนเป็นทรัพย์สินของกลุ่มบริษัทฯ จะอยู่ในการกำกับดูแลโดยแผนกสนับสนุนด้านระบบเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานของกลุ่มบริษัทฯ มิใช่เป็นทรัพย์สินของฝ่าย/ส่วนงานใด ๆ เจ้าหน้าที่เทคโนโลยีสารสนเทศจะส่งมอบให้ผู้ใช้งานรับผิดชอบดูแลตามความเหมาะสมในการใช้งาน และห้ามผู้ใช้งานทำการ เคลื่อนย้าย โยกย้าย หรือเปลี่ยนแปลงผู้ใช้งานโดยไม่ได้รับอนุญาตจากส่วนงานเทคโนโลยีสารสนเทศ

(4) ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่กลุ่มบริษัทฯ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

(5) กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของกลุ่มบริษัทฯ ที่ได้รับมอบหมายเป็นอย่างดี

(6) ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

(7) ห้ามมิให้ผู้ใช้งานให้ผู้อื่นยืมทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่มอบไว้ให้ใช้งาน ไม่ว่าในกรณีใด ๆ ก็ตามเว้นแต่การยืมนั้นได้รับการอนุมัติจากผู้บังคับบัญชา ถ้าหากความเสียหายใด ๆ ที่เกิดจากการละเมิดข้างต้นให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(8) ทรัพย์สินและระบบสารสนเทศต่างๆ ที่กลุ่มบริษัทฯ จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของกลุ่มบริษัทฯ เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินหรือระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่ไม่เกี่ยวของกับงานของกลุ่มบริษัทฯ หรือทำให้เกิดความเสียหายต่อกลุ่มบริษัทฯ

(9) เมื่อพนักงานพ้นสภาพการเป็นพนักงาน พนักงานต้องดำเนินการส่งคืนทรัพย์สินและอุปกรณ์เทคโนโลยีสารสนเทศทั้งหมดที่ได้รับมอบหมายคืนให้แก่ฝ่ายเทคโนโลยีสารสนเทศและ/หรือฝ่ายบุคคลโดยทันที ในสภาพที่พร้อมใช้งานตามปกติ และให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการระงับสิทธิการเข้าถึงระบบ

สารสนเทศ (Account Deactivation) ทั้งหมดของพนักงานรายนั้นโดยทันที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

8. การบริหารจัดการข้อมูลองค์กร (Corporate Management)

(1) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลและปฏิบัติตามข้อบังคับ กฎหมายและนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบริษัทฯ อย่างเคร่งครัด ไม่ว่าข้อมูลนั้นจะเป็นของกลุ่มบริษัทฯ ข้อมูลของลูกค้า หรือข้อมูลใด ๆ ที่อยู่ภายในครอบครองของกลุ่มบริษัทฯ

(2) ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของกลุ่มบริษัทฯ ถือเป็นทรัพย์สินของกลุ่มบริษัทฯ ห้ามมิให้ทำการเผยแพร่ ดัดแปลง ทำซ้ำ หรือทำลายซึ่งข้อมูลใด ๆ โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาและส่วนงานเทคโนโลยีสารสนเทศ

(3) ผู้ใช้งานต้องปกป้อง ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

(4) ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กลุ่มบริษัทฯ ให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กลุ่มบริษัทฯ ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับกลุ่มบริษัทฯ ซึ่งอาจแต่งตั้งให้มีผู้รับผิดชอบทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาภายใต้กรอบของกฎหมายโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

9. การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

(1) ผู้ใช้งานทั่วไปมีสิทธิเข้าถึงการใช้งาน เครื่องคอมพิวเตอร์ ระบบเน็ตเวิร์คที่เป็นระดับผู้ใช้ (User) เท่านั้น

(2) ห้ามมิให้ผู้ใช้งานทำการแก้ไขการตั้งค่าของเครื่องคอมพิวเตอร์ เช่น ชื่อเครื่อง หมายเลขไอพี หมายเลขของการ์ดแลน โดยไม่ได้รับอนุญาตจากส่วนงานเทคโนโลยีสารสนเทศ

(3) ผู้ใช้งานมีสิทธิ์ที่จะเสนอหรือร้องขอให้มีการเพิ่ม หรือ ปรับปรุงรุ่นของโปรแกรมหรือฮาร์ดแวร์ ในเครื่องหรือในระบบของกลุ่มบริษัทฯ โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศจะต้องตรวจสอบและไม่ดำเนินการใด ๆ ก็ตามที่มีลักษณะดังนี้

(3.1) โปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(3.2) โปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบสารสนเทศมากกว่าผู้ใช้อื่น

(3.3) โปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับไวรัสคอมพิวเตอร์

(3.4) โปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(3.5) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(4) ห้ามเปิดหรือใช้งาน (Run) โปรแกรมที่กลุ่มบริษัทฯ ได้มีการประกาศห้ามใช้งาน

(5) ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมทั้งอุปกรณ์อื่นใดของกลุ่มบริษัทฯ ที่จัดเตรียมให้ เช่น เครื่องคอมพิวเตอร์ อีเมล เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อกลุ่มบริษัทฯ

(6) ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกลุ่มบริษัทฯ เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อกิจการของกลุ่มบริษัทฯ

(7) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกลุ่มบริษัทฯ เพื่อประโยชน์ทางการค้าที่มิใช่เป็นของกลุ่มบริษัทฯ

(8) ห้ามกระทำการใดๆ เพื่อการดาวน์โหลดหรือคัดลอกข้อมูลที่ไม่เกี่ยวข้องกับงานของกลุ่มบริษัทฯ ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่าย ระบบสารสนเทศของกลุ่มบริษัทฯ โดยเด็ดขาด

(9) ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของกลุ่มบริษัทฯ ต้องหยุดชะงัก

(10) ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นเพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

(11) ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของกลุ่มบริษัทฯ โดยไม่ได้รับอนุญาต

(12) กลุ่มบริษัทฯ มีสิทธิ์ที่จะทำการตรวจสอบการใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นที่กลุ่มบริษัทฯ จัดเตรียมให้แก่พนักงานเพื่อใช้ในการปฏิบัติงานของกลุ่มบริษัทฯ

(13) กลุ่มบริษัทฯ จะต้องมีการตรวจสอบการใช้ระบบโปรแกรมซอฟต์แวร์และฮาร์ดแวร์ที่ใช้เครื่องมือ/อุปกรณ์สำหรับการทำงาน เพื่อป้องกันการละเมิดลิขสิทธิ์หรือไม่เกี่ยวข้องกับการทำงาน อย่างสม่ำเสมอ

10. การจัดการเกี่ยวกับโปรแกรมคอมพิวเตอร์และลิขสิทธิ์ (Software and License Agreement)

(1) เจ้าหน้าที่เทคโนโลยีสารสนเทศจะต้องทำการติดตั้งซอฟต์แวร์ที่จำเป็นต่อหน้าที่ความรับผิดชอบของแต่ละบุคคลและแต่ละแผนก ให้พร้อมใช้ในเครื่องคอมพิวเตอร์ทุกเครื่องก่อนส่งมอบให้ผู้ใช้งาน

(2) กลุ่มบริษัทฯ ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญาสูงสุด ดังนั้น ซอฟต์แวร์ที่ได้รับการติดตั้งในอุปกรณ์สารสนเทศของกลุ่มบริษัทฯ จะต้องมีลิขสิทธิ์ถูกต้องจากเจ้าของผู้ผลิต (Software License) ห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ลงในอุปกรณ์ของกลุ่มบริษัทฯ โดยเด็ดขาด ยกเว้น ซอฟต์แวร์ที่กลุ่มบริษัทฯ พัฒนาเอง (In House Software) และซอฟต์แวร์ที่สามารถนำไปใช้งานโดยไม่ต้องเสียค่าใช้จ่ายค่าลิขสิทธิ์ (Freeware) ซึ่งจะต้องผ่านการอนุมัติจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศและติดตั้งโดยเจ้าหน้าที่เทคโนโลยีสารสนเทศเท่านั้น หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ กลุ่มบริษัทฯ ถือว่าเป็นความผิดส่วนบุคคลและจะดำเนินการตามกฎระเบียบของกลุ่มบริษัทฯ ต่อไป

(3) ซอฟต์แวร์ที่กลุ่มบริษัทฯ ได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้กับอุปกรณ์ส่วนตัวโดยเด็ดขาด

11. การจัดการเกี่ยวกับการป้องกันโปรแกรมไม่ประสงค์ดี (Malware)

(1) คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่กลุ่มบริษัทฯ โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศติดตั้งให้ใช้เท่านั้น

(2) ข้อมูลใด ๆ ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากอีเมล์หรือผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

(3) ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่เจ้าหน้าที่เทคโนโลยีสารสนเทศโดยไม่ชักช้า

(4) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งแก่เจ้าหน้าที่เทคโนโลยีสารสนเทศโดยทันที

(5) ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาต่อทรัพย์สินหรือข้อมูลของกลุ่มบริษัทฯ

12. การปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

(1) บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกลุ่มบริษัทฯ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

(2) ผู้ใช้งานหรือพนักงานของกลุ่มบริษัทฯ ที่ละเมิด ละเว้น ทำผิดข้อห้ามตามที่นโยบายระบุไว้ถือว่ามีความผิดทางวินัยตามกฎระเบียบของกลุ่มบริษัทฯ โดยระดับความผิดขึ้นอยู่กับผู้บริหารเป็นผู้ตัดสินใจ

13. การจัดทำแผนรองรับเหตุสุดวิสัย (Disaster Recovery Plan)

(1) กลุ่มบริษัทฯ ได้มีการกำหนดแผนงานรองรับเหตุสุดวิสัย ที่เกิดขึ้นกับระบบสารสนเทศ ที่ส่งผลให้เกิดการหยุดชะงักในการทำงาน พร้อมกำหนดระเบียบวิธีการปฏิบัติ เพื่อลดความเสี่ยงในการใช้งาน และทำให้เกิดประสิทธิภาพในการทำงานคงที่ โดยแผนรองรับเหตุสุดวิสัย และคู่มือปฏิบัติจัดทำขึ้นเพื่อรองรับหากเกิดขึ้นกับระบบเน็ตเวิร์ค อุปกรณ์การสำรองข้อมูล อุปกรณ์ชุดเครื่องคอมพิวเตอร์ชุดต่อพ่วงต่าง ๆ และอื่น ๆ ที่จำเป็นและส่งผลกระทบต่อการทำงาน

(2) กลุ่มบริษัทฯ ได้มีการจัดระบบการทดสอบแผนรองรับเหตุสุดวิสัยอย่างต่อเนื่อง สม่ำเสมอตามแผนงานและระเบียบปฏิบัติทุกปี พร้อมทำรายงานสรุปผลการทดสอบและผลกระทบที่เกิดขึ้นเพื่อหาจุดปรับปรุงและพัฒนาแผนงานการรองรับ และปรับเปลี่ยนระเบียบข้อปฏิบัติให้ทัน และตรงต่อปัญหาที่เกิดขึ้น

14. นโยบายเกี่ยวกับการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการจากภายนอก

(1) <u>การจัดหา การคัดสรร ผู้ให้บริการจากภายนอก</u>

ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการจัดหาผู้ให้บริการด้านเทคโนโลยีสารสนเทศที่มี ความ ชำนาญเฉพาะด้านของระบบต่าง ๆ ความต้องการของกลุ่มบริษัทฯ โดยสามารถตรวจสอบได้จากเอกสารรับรองมาตรฐานต่างๆ เช่น เอกสารรับรองมาตรฐานการทำงาน เอกสารตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์ เป็นต้น

ฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้สรุปผลการคัดสรรผู้ให้บริการ โดยอยู่บนพื้นฐานของการเปรียบเทียบราคา หรือหลักการตามนโยบายของแผนกจัดซื้อ โดยผู้บริหารระดับสูงจะเป็นผู้ตัดสินใจในการเลือกผู้ให้บริการ

(2) <u>การบำรุงรักษาระบบ</u>

ผู้ให้บริการต้องมีทีมงานช่วยเหลือบริการลูกค้า Customer Service Support โดยเฉพาะ เพื่อสามารถรองรับการร้องขอความช่วยเหลือจากกลุ่มบริษัทฯ ตลอดช่วงเวลาทำงานปกติของกลุ่มบริษัทฯ กล่าวคือ วันจันทร์ถึงวันศุกร์ เวลา 8.30 น. ถึง 17.30 น.

(3) <u>ความปลอดภัยของข้อมูลในระบบสารสนเทศของกลุ่มบริษัทฯ</u>

ข้อมูลที่อยู่ภายในระบบสารสนเทศของกลุ่มบริษัทฯ นั้น ถือว่าเป็นทรัพย์สินของกลุ่มบริษัทฯ และเป็นความลับที่จะรู้ได้เพียงแค่ภายในกลุ่มบริษัทฯ เท่านั้น ทั้งนี้ผู้ให้บริการภายนอกจะต้องปฏิบัติตามเงื่อนไขในสัญญาอย่างเคร่งครัด

15. นโยบายเกี่ยวกับการเปลี่ยนแปลงและการแก้ไขระบบสารสนเทศ (Change Management)

กลุ่มบริษัทฯ กำหนดให้มีนโยบายเกี่ยวกับการเปลี่ยนแปลงและการแก้ไขระบบสารสนเทศ เพื่อเป็นระเบียบและแนวทางปฏิบัติกรณีที่ผู้รับผิดชอบของระบบงานหรือผู้ใช้งาน มีความต้องการที่จะทำการแก้ไข เปลี่ยนแปลงระบบสารสนเทศใด ๆ ของกลุ่มบริษัทฯ โดยจะต้องดำเนินการแจ้งให้แก่แผนกสนับสนุนด้านระบบเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานของกลุ่มบริษัทฯ รับทราบ โดยแผนกสนับสนุนด้านระบบเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานจะต้องจัดทำแผนงานที่ต้องระบุ วัตถุประสงค์ของการเปลี่ยนแปลง/แก้ไข รายละเอียดของการเปลี่ยนแปลง/แก้ไขและกระบวนการทดสอบ ผลของการเปลี่ยนแปลง/แก้ไข ผลกระทบที่เกิดขึ้นจากการเปลี่ยนแปลง/แก้ไข ระยะเวลาที่ใช้ในการดำเนินการเปลี่ยนแปลง/แก้ไข งบประมาณในการดำเนินการ ทั้งนี้ เมื่อมีการเปลี่ยนแปลง/แก้ไข ผู้รับผิดชอบระบบงานและผู้ที่เกี่ยวข้องกับระบบงานจะต้องเข้าร่วมในการทดสอบการใช้งาน จนมั่นใจว่าสามารถใช้งานได้จริงและมีประสิทธิภาพ ก่อนที่จะนำไปใช้งานระบบสารสนเทศของกลุ่มบริษัทฯ และจะต้องทำการบันทึกรายการแก้ไขข้อมูลที่จำเป็นไว้เป็นลายลักษณ์อักษร

ภายหลังจากการเปลี่ยนแปลง/แก้ไข จะต้องกำหนดให้มีติดตามผลการดำเนินการเปลี่ยนแปลง/แก้ไข หลังจากการใช้งานจริงสักระยะ เพื่อตรวจสอบความถูกต้องครบถ้วนตามความต้องการของผู้ใช้งาน และหาปัญหาที่อาจจะเกิดขึ้น ภายหลังจากการใช้งาน

16. นโยบายเกี่ยวกับการควบคุมการ เข้า - ออก และการปฏิบัติงานในห้องคอมพิวเตอร์แม่ข่ายของกลุ่มบริษัทฯ (Data Center)

กลุ่มบริษัทฯ ได้กำหนดให้ผู้ที่สามารถเข้าออกบริเวณห้องศูนย์ข้อมูล (Data Center) ได้ ต้องเป็นผู้ที่มีหน้าที่โดยตรง ได้แก่ เจ้าหน้าที่เทคโนโลยีสารสนเทศเป็นผู้มีสิทธิ์ในการเข้าถึงข้อมูลในการในการจัดการที่เกี่ยวข้องกับเครื่อง Server โดยที่กลุ่มบริษัทฯ ได้กำหนดให้มีการควบคุมการ เข้า - ออก ด้วยกุญแจ บัตรผ่านเฉพาะบุคคล (Access Card) รหัสผ่านเฉพาะบุคคล (Access PIN) หรือการยืนยันตัวตนด้วยข้อมูลทางชีวภาพ (Biometric Authentication) สำหรับบุคคลภายนอกที่มีความจำเป็นจะต้องเข้า – ออก บริเวณห้อง Data Center จะต้องได้รับการอนุญาตจากประธานเจ้าหน้าที่ฝ่ายปฏิบัติการก่อนและอยู่ภายใต้การดูแลของเจ้าหน้าที่ที่ได้รับสิทธิ์ในการเข้าออกห้อง Data Center เสมอ และจะต้องลงบันทึกการเข้า – ออก ห้อง Data Center ตามแบบฟอร์มที่กลุ่มบริษัทฯ กำหนดไว้ทุกครั้ง

17. นโยบายเกี่ยวกับการสำรองข้อมูล (Data Backup)

กลุ่มบริษัทฯ ได้กำหนดให้แผนกสนับสนุนด้านระบบเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานนี่มีหน้าที่ในการสำรองข้อมูล (Backup) ต่าง ๆ ของระบบ ได้แก่ ข้อมูล (Data) แอพพลิเคชั่น (Application) รวมถึงข้อมูลต่าง ๆ ที่จำเป็น โดยการสำรองข้อมูลจากเครื่องแม่ข่ายที่อยู่ภายในบริเวณของกลุ่มบริษัทฯ ไปจัดเก็บไว้ยังสถานที่จัดเก็บข้อมูลสำรองภายนอกกลุ่มบริษัทฯ แผนกสนับสนุนด้านระบบเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานจะต้องทำการสำรองข้อมูลในทุก ๆ วัน และบันทึกผลของการสำรองข้อมูล เพื่อตรวจสอบความครบถ้วนของการสำรองข้อมูลเพื่อป้องกันเหตุสุดวิสัยที่อาจเกิดขึ้น

18. นโยบายการทดสอบการกู้คืนระบบ (Recovery)

กลุ่มบริษัทฯ กำหนดให้มีการทดสอบการกู้คืนระบบโดยการเรียกคืนข้อมูลจากการสำรองข้อมูล เป็นประจำทุกเดือน และจะต้องบันทึกรายงานผลของการทดสอบการกู้คืนระบบไว้ทุกครั้ง

19. การทบทวนนโยบาย

นโยบายระบบงานเทคโนโลยีสารสนเทศจะได้รับการทบทวนและประเมินความเหมาะสมของนโยบายเป็นประจำทุกปี

20. การมีผลบังคับใช้

นโยบายระบบงานเทคโนโลยีสารสนเทศนี้ให้มีผลบังคับใช้ตั้งแต่วันที่ 12 พฤศจิกายน 2564 เป็นต้นไป โดยมีการแก้ไขปรับปรุงล่าสุด เมื่อวันที่ 26 กุมภาพันธ์ 2569

_____

(นายประดิษฐ์ เลี่ยวศิริกุล)
ประธานกรรมการบริษัท

รายการควบคุมเอกสาร

ครั้งที่	เลขที่เอกสาร	สรุปรายการ	อนุมัติโดย	วันที่มีผลบังคับใช้
00	-	ประกาศใช้	BOD 9/2564	12/11/2564
01	-	แก้ไขชื่อบริษัท เพื่อให้สอดคล้องกับการแปรสภาพเป็นบริษัทมหาชนจำกัด	BOD 1/2565 (ภายหลังการแปรสภาพ)	11/08/2565
02	Policy/IT/2567	ทบทวนประจำปี และแก้ไขเพิ่มเติมรายละเอียดให้สอดคล้องกับการปฏิบัติงานในปัจจุบัน	BOD 1/2567	28/02/2567
03	Policy/IT/2568	ทบทวนประจำปี และแก้ไขปรับปรุงความถี่ในการทดสอบการกู้คืนระบบ (Recovery) เป็นรายเดือน ทบทวนนโยบายการคืนทรัพย์สิน การเพิกถอนสิทธิ์การเข้าถึง และแก้ไขเพิ่มเติมมาตรการควบคุมให้สอดคล้องกับแนวทางการปฏิบัติงานในปัจจุบัน	BOD 1/2568	27/02/2568
04	Policy/IT/2569	ทบทวนประจำปี และแก้ไขเพิ่มเติมข้อการบริหารจัดการทรัพย์สิน (Assets Management) การคืนทรัพย์สิน การเพิกถอนสิทธิ์การเข้าถึง นโยบายเกี่ยวกับการควบคุมการเข้า - ออก ให้สอดคล้องกับแนวทางการปฏิบัติงานในปัจจุบัน และนโยบายการทดสอบการกู้คืนระบบ (Recovery) ให้เป็นรายเดือน	BOD 1/2569	26/02/2569