แนวปฏิบัติมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

บริษัทกำหนดให้มีมาตรการรักษาความปลอดภัยของข้อมูลในการรักษาความลับ การรักษาความน่าเชื่อถือ และความพร้อมใช้ข้อมูล รวมทั้งป้องกันมิให้มีการนำข้อมูลส่วนบุคคลไปใช้ในทางมิชอบหรือมีการแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคล โดยกำหนดแนวปฏิบัติไว้ดังนี้

1. บริษัท กำหนดให้บุคลากรทุกคนของบริษัท ต้องปฏิบัติตามพรบ.คุ้มครองข้อมูลส่วนบุคคล และมีหน้าที่รักษาความปลอดภัยของข้อมูลส่วนบุคคล โดยไม่นำข้อมูลที่ได้รับมาจากการปฏิบัติงานไปใช้เพื่อวัตถุประสงค์อื่น หรือทำให้เกิดความเสียหายต่อบริษัท
2. บริษัท กำหนดบุคคลที่ได้รับอนุญาตการเข้าถึงข้อมูล มีสิทธิเข้าถึงข้อมูลส่วนบุคคล ให้เป็นไปตามคำสั่งหรือตามที่บริษัทมอบหมาย
   2.1 การเข้าถึงข้อมูลส่วนบุคคล ต้องเป็นบุคคลที่ได้รับมอบหมายเป็นลายลักษณ์อักษร และต้องกำหนดให้มีรหัสผ่าน การเปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยทุก 60 วัน
   2.2 กำหนดให้มีระบบการตรวจสอบอุปกรณ์ และ ระบบซอร์ฟแวร์ ที่มีประสิทธิภาพ เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล
   2.3 กำหนดให้มีการดูแล อุปกรณ์ และสถานที่ เพื่อการรักษาความปลอดภัยจากบุคคลที่ไม่เกี่ยวข้อง พร้อมทั้งมีระบบการบันทึกข้อมูลเข้า-ออก จากกล้องวงจรปิดตลอดเวลา
3. กำหนดให้มีระบบการรายงานต่อผู้บริหารระดับสูง อย่างสม่ำเสมอ หากพบอุปกรณ์ ระบบซอร์ฟแวร์ หรือ ข้อมูลที่อาจนำไปสู่การรั่วไหลของข้อมูลส่วนบุคคล โดยรายงานต่อคณะกรรมการบริหารอย่างน้อย ไตรมาสละครั้ง
4. กรณีข้อมูลส่วนบุคคล ที่บริษัทได้จัดเก็บ รวบรวม เกิดการรั่วไหลจากความไม่เสถียรของระบบซอร์ฟแวร์ และ/หรือ เกิดจากอาชญากรทางไซเบอร์(แฮกเกอร์) ที่เข้ามาทำความเสียหายให้กับตัวระบบข้อมูล บริษัทจะดำเนินการปิดระบบ เพื่อแก้ไขทันที และแจ้งให้เจ้าของข้อมูลทราบ พร้อมทั้งรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่บริษัททราบการรั่วไหลของข้อมูลส่วนบุคคล

มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

บริษัทจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลโดยครอบคุลมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลสอดคล้องตามมาตรการรักษาความปลอดภัยทางด้านสารสนเทศ ดังนี้

มาตรการ	การควบคุม
มาตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	1. ติดตั้งระบบป้องกันการบุกรุก (Firewall) 2. ติดตั้งซอฟต์แวร์ป้องกันไวรัส 3. กำหนดสิทธิ์การเข้าถึง หรือการเข้าใช้ข้อมูล 3.1 สิทธิ์การเข้าถึงไฟล์ข้อมูลระบบต้องได้รับการพิจารณาอนุมัติเท่าที่จำเป็น 3.2 สำหรับเครื่องคอมพิวเตอร์แม่ข่าย ด้วยการพิสูจน์ตัวตนของผู้เข้าใช้งาน 3.3 อุปกรณ์สื่อบันทึกข้อมูล เช่น Thumb-Drive สำหรับข้อมูลระดับชั้นความลับ (ต้องได้รับอนุมัติจากผู้บริหาร ก่อนการใช้งาน) 3.4 กำหนดให้เปลี่ยนรหัสผ่านทุก 60 วัน 4. ผู้ดูแลระบบต้องสำรองข้อมูลอย่างสม่ำเสมอ 4.1 สำรองข้อมูลทุกวัน 4.2 สำรองทั้งระบบทุกสัปดาห์ 4.3 กำหนดการทดสอบระบบข้อมูลที่สำรอง ปีละ 2 ครั้ง 5. เครื่องคอมพิวเตอร์ และ เครื่องคอมพิวเตอร์พกพา ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้ง และควร Log off ทุกครั้งเมื่อไม่ใช้งาน 6. ซอฟแวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับ หรือข้อมูลสำคัญ ทั้งที่ได้มาจากการพัฒนาขึ้น หรือจากการซื้อมา ต้องได้รับการตรวจสอบ ควบคุมและอนุมัติ ตามอำนาจดำเนินการอย่างเหมาะสม 7. ทบทวน และปรับปรุงมาตรการอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับสถานการณ์ปัจจุบัน
การใช้งาน E - Mail	1. บัญชี E – Mail ต้องได้รับการปกป้องด้วยรหัสผ่าน 2. พื้นที่จัดเก็บ E – Mail บนเครื่องเครือแม่ข่ายส่วนกลางของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้ผู้ใช้งานต้องเก็บรักษา E – Mail ที่เกี่ยวข้องกับการทำงาน เท่านั้น 3. ห้ามใช้บัญชี E – Mail ของบริษัท เพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย พรบ.ข้อกำหนด และ พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือนโยบาย ต่างๆ ที่บริษัทกำหนด 4. ผู้ใช้งานต้องใช้ความระมัดระวังเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส หรือโปรแกรมแฝง 5. ห้ามส่งข้อมูลเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อบริษัท หรือบุคคลอื่นๆ

มาตรการ	การควบคุม
การรักษาความปลอดภัย	1. จัดให้มีการควบคุมการเข้า – ออกในบริเวณ ห้องควบคุมเครือข่าย เฉพาะผู้ดูแลระบบ 2. ไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องควบคุมเครือข่าย และไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่าย ไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลใดๆ เว้นแต่ได้รับอนุญาต 3. การควบคุม เปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ ต้องมีการกำหนดผู้รับผิดชอบและผู้มีอำนาจในการดำเนินการ 4. ให้มีการแยกบัญชีผู้ใช้งานออกจากกันสำหรับระบบงานที่ใช้ในการพัฒนาทดสอบและระบบงานจริง
การป้องกันความเสียหาย	1. ระบบป้องกันไฟฟ้าขัดข้อง โดยมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์เครือข่าย 2. ระบบควบคุมอุณหภูมิและความชื้น เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม 3. ติดตั้งกล้องวงจรปิดบริเวณพื้นที่ห้องควบคุมเครือข่าย