นโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) บริษัท โรงพยาบาลจุฬารัตน์ จำกัด (มหาชน)

บริษัท โรงพยาบาลจุฬารัตน์ จำกัด (มหาชน) และบริษัทในเครือ “บริษัท” ได้จัดให้มีระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ขึ้นเพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้บริษัทฯ ดังนั้นเพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพสูงสุด รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานในลักษณะที่มีความเสี่ยงที่ทำให้เกิดความเสียหาย บริษัทฯ จึงจัดทำนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศขึ้นเพื่อให้เป็นแนวทางและกฎเกณฑ์มาตรฐานสำหรับพนักงานและบุคคลที่มีหน้าที่หรือมีความเกี่ยวข้องในการทำงานมีสาระสำคัญดังนี้

โครงสร้างของคณะกรรมการ : บริษัทฯ ได้กำหนดบทบาทและหน้าที่ความรับผิดชอบของการบริหารความปลอดภัยด้านสารสนเทศ ผ่านโครงสร้างองค์กรดังนี้

- **Information Security Management Committee : ประกอบด้วยผู้บริหารระดับสูงของบริษัท โรงพยาบาลจุฬารัตน์ จำกัด (มหาชน) หรือบริษัทในเครือ มีบทบาทและหน้าที่ดังนี้**
  - อนุมัติ ประกาศใช้นโยบายหรือระเบียบปฏิบัติอื่น ๆ ที่เกี่ยวข้องกับนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - กำหนดและอนุมัติเกณฑ์สำหรับความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้
  - พิจารณาผลการประเมินความเสี่ยงและแผนการแก้ไขความเสี่ยงที่สำคัญขององค์กร
  - พิจารณาลงโทษผู้ที่ละเมิดนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - ให้การสนับสนุนด้านทรัพยากรที่จำเป็นในการดำเนินงาน
- **Data Protection Officer : พนักงานในบริษัทฯ หรือผู้ที่ได้รับมอบหมาย มีบทบาทและหน้าที่หลัก ดังนี้**
  - กำกับดูแลและให้คำแนะนำเกี่ยวกับการจัดเก็บและการใช้งานข้อมูลส่วนบุคคลในระบบต่าง ๆ
  - ทำการตรวจสอบการจัดเก็บและการใช้งานข้อมูลส่วนบุคคลในระบบต่าง ๆ และรายงานความเสี่ยง เหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศรวมถึงแนวทางแก้ไขให้คณะกรรมการฯ และผู้เกี่ยวข้องรับทราบ
  - ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นในบริษัทฯ
  - จัดการอบรมและให้ความรู้กับพนักงานของบริษัทฯ ในเรื่องการใช้งานและปกป้องข้อมูลส่วนบุคคล
  - ติดตามและเผยแพร่ข่าวสารเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศให้กับผู้เกี่ยวข้องในบริษัท
  - ประสานกับหน่วยงานต่าง ๆ ในเรื่องการบริหารจัดการข้อมูลทั้งภายในและภายนอกบริษัทฯ

- **Information Security Director : ตัวแทนผู้บริหารของบริษัทฯ มีบทบาทและหน้าที่ดังนี้**
  - ให้คำแนะนำและข้อเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการบริหารจัดการรักษาความปลอดภัยของข้อมูล
  - กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลระบบเทคโนโลยีสารสนเทศและผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ ในการปฏิบัติตามนโยบายฉบับนี้
  - สื่อสารให้พนักงานทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล
  - ให้การสนับสนุนและความรู้กับพนักงานและบุคคลภายนอกที่เกี่ยวข้องกับการปฏิบัติตามนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - ตรวจสอบการปฏิบัติตามนโยบายของพนักงานและบุคคลภายนอกเกี่ยวข้องอย่างเหมาะสม
  - พิจารณาการปรับปรุงนโยบายให้เหมาะสมกับสถานการณ์ในปัจจุบัน
  - ประสานงานและหาแนวทางในการควบคุมและจัดการปัญหาในกรณีที่เกิดเหตุละเมิดนโยบายหรือละเมิดความมั่นคงของข้อมูลขึ้นในองค์กร
  - รายงานผลการดำเนินการแบบรายไตรมาสต่อ Information security Management Committee
  - รายงานความคืบหน้าเหตุการณ์หรือสถานการณ์ที่เกี่ยวข้องให้คณะกรรมการฯ รับทราบ
  - ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในนโยบายฉบับนี้
- CHG Computer Emergency Response Team (CHG CERT) : ประกอบด้วยทีมงานจากบริษัท หรือผู้ที่ได้รับมอบหมาย มีบทบาทและหน้าที่หลักดังนี้
  - ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ
  - ให้คำแนะนำและแก้ไขภัยคุกคามความมั่นคงด้านเทคโนโลยีสารสนเทศ
  - ติดตามและเผยแพร่ข่าวสารเหตุการณ์ต่างๆที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้กับผู้เกี่ยวข้องในบริษัทฯ
  - ศึกษา ปรับปรุงเครื่องมือและแนวทางปฏิบัติให้ทันสมัยอยู่เสมอเพื่อเพิ่มความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของบริษัทฯ
  - ดำเนินการเรื่องอื่นๆที่เกี่ยวกับการบริหารจัดการความปลอดภัยสารสนเทศตามที่ผู้บังคับบัญชามอบหมาย

<u>แนวทางปฏิบัติ</u> : กำหนดให้ทุกบริษัทที่อยู่ภายใต้นโยบายฉบับนี้จะต้องจัดทำระเบียบปฏิบัติและแผนต่างๆ ตามรายละเอียดด้านล่างและเสนอขออนุมัติเพื่อประกาศใช้งานจาก Information Security Management Committee ภายใน 180 วัน หลังจากที่นโยบายฉบับนี้มีผลบังคับใช้

- ระเบียบปฏิบัติเกี่ยวกับการใช้งานทรัพยากรสารสนเทศ
- ระเบียบปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและเชื่อถือได้
- ระเบียบปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สามารถรับมือได้อย่างเหมาะสม
- ระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการบัญชีผู้ใช้งานข้อมูลและระบบสารสนเทศ

- ระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการผู้ให้บริการภายนอกด้านสารสนเทศ
- ระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการทรัพย์สินด้านสารสนเทศ
- ระเบียบปฏิบัติเกี่ยวกับการสำรองข้อมูลและการกู้คืนระบบสารสนเทศที่สำคัญ
- ระเบียบปฏิบัติเมื่อเกิดเหตุการณ์ร้ายแรง
- กำหนดแผนการฟื้นฟูหลังภัยร้ายแรง

<u>การปฏิบัติตาม การตรวจสอบ และมาตรการทางวินัย :</u>

- การปฏิบัติตาม : บุคคลที่มีหน้าที่หรือมีความเกี่ยวข้องกับบริษัทฯ เช่น พนักงานของบริษัทฯคู่สัญญา ลูกจ้าง ผู้ให้บริการ ตลอดจนบุคคลภายนอกที่ใช้ข้อมูลของบริษัทฯ จำเป็นต้องทราบเนื้อหาและปฏิบัติตามเนื้อหาของนโยบายทั้งหมด
- การตรวจสอบ : บริษัทฯ สงวนสิทธิ์ในการกระทำการใด ๆ ที่เห็นว่าจำเป็นเพื่อจัดการและป้องกันความมั่นคงปลอดภัยให้กับข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร
- มาตรการทางวินัย : หากมีการฝ่าฝืนข้อกำหนดของบริษัทฯ ที่ก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใดทั้งทางตรงและทางอ้อมถือเป็นความผิด ผู้กระทำการฝ่าฝืนจะต้องถูกพิจารณาลงโทษทั้งทางวินัยและทางกฎหมายตามความเหมาะสมต่อไป

บริษัทจะทบทวนนโยบายนี้อย่างสม่ำเสมอ และพัฒนาแนวปฏิบัติที่เกี่ยวข้อง เพื่อให้แน่ใจว่าการดำเนินธุรกิจของเราสอดคล้องกับหลักนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) อย่างแท้จริง