นโยบายการบริหารจัดการ ความมั่นคงปลอดภัยด้านสารสนเทศ

(Information Security Management System Policy)

ขอบเขต (Scope)

ครอบคลุมการดำเนินงานด้านเทคโนโลยีสารสนเทศ บริษัท โรงพยาบาลบำรุงราษฎร์ จำกัด (มหาชน) และบริษัทย่อย (บริษัทฯ) โดยครอบคลุมถึงทรัพย์สินของบริษัทฯ ทุกประเภท (ไม่ว่าทรัพย์สินนั้นจะตั้งอยู่ในบริษัทฯ หรือไม่ก็ตาม) ได้แก่

- **ข้อมูล (ฐานข้อมูล, เอกสาร, อีเมล์ เป็นต้น) รวบถึงข้อมูลส่วนบุคคล**
- **ซอฟต์แวร์ลิขสิทธิ์ หรือโปรแกรมที่พัฒนาขึ้น**
- **ทรัพย์สินทางกายภาพ (ห้องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ โน๊ตบุ๊ค แท็บเล็ต เครื่องพิมพ์ พื้นที่ทำงาน เป็นต้น)**
- **พนักงานและบุคลากรที่บริษัทฯ ว่าจ้าง**
- **งานบริการต่าง ๆ (ระบบสำรองไฟฟ้า การสื่อสาร ระบบเครือข่าย เป็นต้น)**

คำจำกัดความ (Definition)

- **การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** (Information Security) หมายถึง การรักษาไว้ซึ่งความลับของข้อมูล (Confidentiality) ความถูกต้อง ครบถ้วนของข้อมูล (Integrity) และข้อมูลมีสภาพพร้อมใช้งาน (Availability) เพื่อป้องกันข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือ ถูกแก้ไข เปลี่ยนแปลง หรือ ข้อมูลสูญหายจนไม่สามารถใช้งานได้
- **มาตรการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** (Information Security Control) หมายถึง กระบวนการระบุบริบทที่เกี่ยวข้องกับความเสี่ยงด้านสารสนเทศ (Identify) การปกป้องทรัพย์สินสารสนเทศ (Protect) การตรวจจับเหตุการณ์ผิดปกติ (Detect) การรับมือเหตุการณ์ผิดปกติ (Response) และการกู้คืนสินทรัพย์สารสนเทศจากความเสียหายเพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง (Recovery)

รายละเอียด (Details)

บริษัทฯ กำหนดนโยบายในภาพรวมเพื่อการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยจัดแบ่งสาระสำคัญออกเป็น 13 หมวด ดังต่อไปนี้

1. **การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ** (Information Security Policy) **บริษัทฯ จัดให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร และต้องสื่อสารนโยบายดังกล่าวแก่แก่พนักงานและหน่วยงานภายนอกที่เกี่ยวข้อง เพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง ตลอดจนทบทวนนโยบายตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อองค์กร**
2. **ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร** (Human Resources Security) **บริษัทฯ กำหนดให้มีมาตรการในการควบคุมความมั่นคงปลอดภัยเกี่ยวกับการบริหารจัดการบุคลากร และการให้ความรู้เกี่ยวกับความมั่นคงปลอดภัยให้แก่บุคลากรที่เหมาะสม เพื่อให้มั่นใจได้ว่าพนักงานของบริษัทฯ และบุคลากรอื่น ๆ ที่บริษัทฯ ได้ว่าจ้างมาทำงานมีความตระหนักและปฏิบัติตามนโยบายของบริษัทฯ รวมถึงการถอดถอนสิทธิในการเข้าถึงระบบและการคืนทรัพย์สินเมื่อสิ้นสุดการจ้างงาน**
3. **การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร** (Asset Management) **บริษัทฯ จัดให้มีการจัดทำบัญชีทรัพย์สิบที่ระบุผู้ถือครองหรือดูแลทรัพย์สิน โดยกำหนดหลักเกณฑ์ในการใช้งาน และการส่งคืนทรัพย์สินรวมถึงการทำลายสื่อบันทึกข้อมูลที่เหมาะสม**

4. **การควบคุมการเข้าถึง** (Access Control) บริษัทฯ จัดให้มีการควบคุมการเข้าถึงระบบสารสนเทศทั้งภายในและภายนอกบริษัทฯ อย่างปลอดภัย โดยต้องกำหนดรหัสผ่าน การกำหนดสิทธิในการใช้งาน การทบทวนสิทธิการใช้งาน และต้องได้รับอนุญาตตามระเบียบของบริษัทฯ

5. **การเข้ารหัสข้อมูลสำหรับข้อมูลที่เป็นความลับ** (Encryption) บริษัทฯ จัดให้มาตรการเข้ารหัสข้อมูลตามความเหมาะสมเพื่อรักษาข้อมูลสำคัญที่เป็นความลับโดยให้ข้อมูลนั้นเข้าถึงหรือใช้งานได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น

6. **ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม** (Physical and Environmental Security) บริษัทฯ กำหนดให้มีมาตรการในการควบคุมเกี่ยวกับความปลอดภัยด้านสถานที่และสภาพแวดล้อม การควบคุมการเข้าออกสถานที่ที่ติดตั้งระบบคอมพิวเตอร์ ระบบสำรองไฟ ระบบปรับอากาศ ระบบป้องกันอื่น ๆ (เช่น ระบบสแกนนิ้วมือ กล้องวงจรปิด ระบบดับเพลิงอัตโนมัติ) เพื่อป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องเข้าถึงและก่อให้เกิดความเสียหายกับทรัพย์สินสารสนเทศ รวมถึงการบำรุงรักษาอุปกรณ์ต่าง ๆ ให้อยู่ในสภาวะที่เหมาะสมและพร้อมใช้งาน

7. **ความมั่นคงปลอดภัยสำหรับการดำเนินงาน** (Operations Security) บริษัทฯ จัดให้มีวางแผนด้านทรัพยากรสารสนเทศให้สามารถพร้อมใช้งาน มีระบบป้องกันที่เหมาะสม ระบบบันทึกเหตุการณ์ผิดปกติ การตรวจสอบการใช้งานระบบ ระบบสำรองข้อมูล การรับส่งหรือการแลกเปลี่ยนข้อมูล (เช่น อีเมล์, อินเตอร์เน็ต) รวมถึงการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change Management) เพื่อให้มั่นใจว่าระบบสารสนเทศของบริษัทฯ มีความมั่นคงปลอดภัย

8. **ความมั่นคงปลอดภัยในการสื่อสารข้อมูล** (Network Communications Security) บริษัทฯ กำหนดให้มีมาตรการการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย การจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัทฯ

9. **การจัดหา การพัฒนา และการบำรุงรักษาระบบ** (Systems Acquisition, Development and Maintenance) บริษัทฯ กำหนดให้มีมาตรการด้านความมั่นคงปลอดภัยของระบบสารสนเทศในทุกขั้นตอนตลอดวงจรชีวิตการพัฒนาระบบซึ่งครอบคลุมถึงกระบวนในการพัฒนา การทดสอบ และข้อมูลสำหรับใช้ทดสอบ รวมถึงการตรวจสอบความมั่นคงปลอดภัยของข้อมูลที่ใช้นำเข้า หรือนำออกไปใช้ นอกจากนี้มาตรการการดังกล่าวให้ถือเป็นส่วนหนึ่งในการพิจารณาหรือจัดจ้างจากผู้ให้บริการภายนอกด้วย

10. **ความสัมพันธ์กับผู้ให้บริการภายนอก** (Supplier Relationships) บริษัทฯ ต้องกำหนดให้มีมาตรการป้องกันทรัพย์สินด้านสารสนเทศที่สามารถเข้าถึงโดยผู้ให้บริการภายนอก ต้องมีข้อตกลงเป็นลายลักษณ์อักษร สัญญาการใช้บริการ สัญญารักษาความลับ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล กับผู้ให้บริการภายนอกที่สามารถเข้าถึงระบบ การประมวลผล การจัดเก็บ หรือการสื่อสารสารสนเทศ ที่ผู้ให้บริการภายนอกต้องปฏิบัติ และการบริหารจัดการด้านการเปลี่ยนแปลงที่เกิดขึ้นในการให้บริการจากผู้ให้บริการภายนอก

11. **การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ** (Information Security Incident Management) บริษัทฯ จัดให้มีผู้รับผิดชอบและกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่กระทบกับความปลอดภัยระบบสารสนเทศ และการละเมิดมาตรการคุ้มครองป้องข้อมูลส่วนบุคคลของบริษัทฯ รวมถึงการรายงานเหตุการณ์ที่ผิดปกติและจุดอ่อนที่เกี่ยวกับความปลอดภัย รวมถึงข้อมูลส่วนบุคคลรั่วไหลต่อผู้บริหารฝ่ายเทคโนโลยีสารสนเทศและหน่วยงานกำกับที่เกี่ยวข้อง

12. **แผนกู้คืนระบบสารสนเทศกรณีเกิดภัยพิบัติ** (IT Disaster Recovery Plan) บริษัทฯ จัดให้มีแผนงานด้านความต่อเนื่องในการดำเนินธุรกิจในระบบสารสนเทศ เพื่อรองรับกรณีที่เกิดหตุการณ์วิกฤตหรือภัยพิบัติซึ่งทำให้ระบบสารสนเทศหรือระบบเครือข่ายไม่สามารถใช้งานได้ตามปกติ โดยจัดให้มีการทดสอบแผนความต่อเนื่องทางธุรกิจอย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสม เพื่อนำผลลัพธ์ไปปรับปรุงแผนงานให้เหมาะสมกับการดำเนินธุรกิจ

13. **การปฏิบัติตามข้อกำหนด** (Compliance) บริษัทฯ จัดให้มีการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับของหน่วยงานราชการและหน่วยงานกำกับที่กำหนดไว้ รวมถึงข้อกำหนดต่าง ๆ ในสัญญาที่ผูกพันกับบริษัทฯ

บทบาทและความรับผิดชอบ (Role and Responsibility)

Chief Information Security Officer มีหน้าที่กำกับดูแลให้การปฏิบัติงานเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศที่บริษัทฯ ได้ประกาศไว้

ผู้บริหารของแต่ละหน่วยงาน มีหน้าที่รับผิดชอบทรัพย์สินและข้อมูลต่าง ๆ ที่อยู่ภายใต้การดูแลของหน่วยงานตามนโยบายของบริษัทฯ ให้อยู่ในสภาพที่มีความมั่นคงปลอดภัย รวมถึงประสานงานกับหน่วยงาน IT ในการร่วมตรวจสอบ และประเมินผลของมาตรการด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ได้นำมาปฏิบัติ

พนักงาน ผู้จัดจำหน่าย คู่สัญญา และที่ปรึกษา มีหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัย มาตรฐาน วิธีปฏิบัติ และแนวทางในการดำเนินงานที่เกี่ยวข้อง เพื่อให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศในการปฏิบัติงาน

การบังคับใช้และบทลงโทษ (Enforcement and Penalties)

นโยบายฉบับนี้ถือเป็นส่วนหนึ่งของระเบียบบริษัทฯ หากพนักงานฝ่าฝืนหรือไม่ปฏิบัติตามอาจได้รับโทษทางวินัยตามที่ระบุในระเบียบข้อบังคับในการทำงาน ซึ่งบริษัทฯ จะพิจารณาลงโทษทางวินัยตามดุลยพินิจต่อไป