นโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทในเครือได้จัดให้มีระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ขึ้นเพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้บริษัทฯ ดังนั้นเพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพสูงสุด รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานในลักษณะที่มีความเสี่ยงที่ทำให้เกิดความเสียหาย บริษัทฯ จึงจัดทำนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศขึ้นเพื่อให้เป็นแนวทางและกฎเกณฑ์มาตรฐานสำหรับพนักงานและบุคคลที่มีหน้าที่หรือมีความเกี่ยวข้องในการทำงาน

นโยบายฉบับนี้ให้มีผลบังคับใช้กับผู้ใช้งานสารสนเทศและระบบสารสนเทศของบริษัทฯ ทุกคน โดยไม่มีการยกเว้น

นโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ กำหนดให้มีสาระสำคัญดังนี้

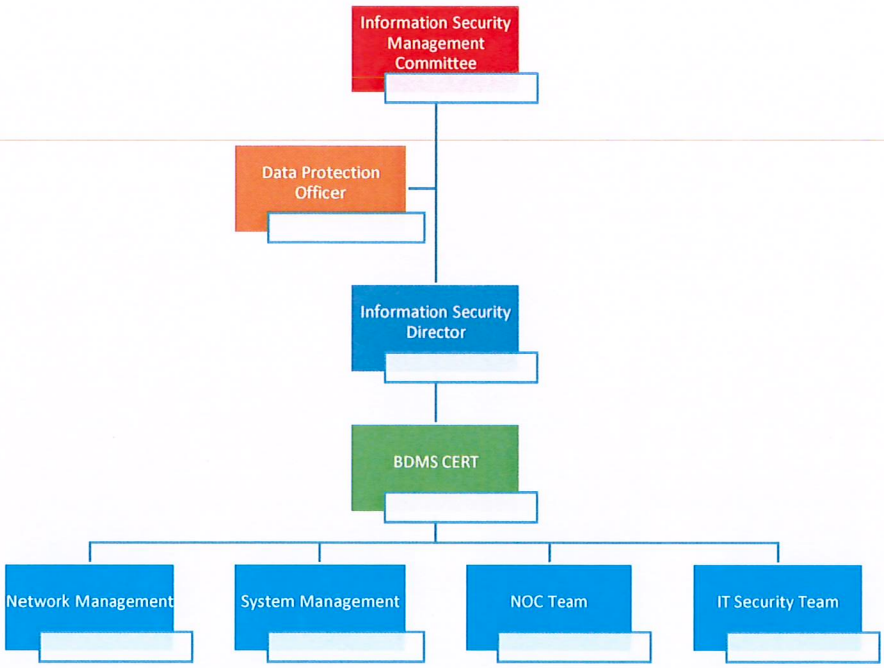
- นิยามทั่วไป
- โครงสร้างและบทบาทหน้าที่ของคณะกรรมการ
- แนวทางปฏิบัติ
- การปฏิบัติตาม การตรวจสอบ และมาตรการทางวินัย

นิยามทั่วไป : นิยามของนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศฉบับนี้

- “บริษัทฯ” หมายถึง บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทในเครือที่บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) ถือหุ้นเกิน 50%
- “ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของบริษัทฯ
- “Information Security Management Committee” หมายถึง คณะบุคคลที่ได้รับการแต่งตั้งจากบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) หรือได้รับการแต่งตั้งจากกรรมการผู้อำนวยการใหญ่
- “พนักงาน” หมายถึง พนักงานและลูกจ้างของบริษัทฯ รวมถึงบุคคลอื่นที่บริษัทฯ มอบหมายให้ปฏิบัติงานภายใต้ข้อกำหนดหรือสัญญา
- “ข้อมูล” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ ไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

- “เครือข่ายคอมพิวเตอร์” หมายถึง การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ที่อยู่ห่างไกลกันเข้าด้วยกัน เพื่อให้สามารถใช้ทรัพยากรร่วมกันได้ รวมถึงระบบ Internet และ Intranet ของบริษัทฯ
- “ผู้ดูแลเครือข่ายคอมพิวเตอร์” หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการควบคุม ดูแลระบบเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- “บัญชีผู้ใช้งาน” หมายถึง ชื่อผู้ใช้งานและรหัสผ่านที่บริษัทฯ ออกให้เฉพาะรายบุคคล เพื่อเข้าใช้งานทรัพยากรเทคโนโลยีสารสนเทศ
- “ทรัพยากรเทคโนโลยีสารสนเทศ” หมายถึง เครือข่ายคอมพิวเตอร์ของบริษัทฯ รวมทั้งเครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องคอมพิวเตอร์พกพา เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์อิเล็กทรอนิกส์พกพา โทรศัพท์มือถือ และอุปกรณ์ต่อพ่วงกับคอมพิวเตอร์ทั้งหมด ที่ได้รับการอนุมัติให้ใช้ภายในบริษัทฯ ทั้งที่เป็นและไม่เป็นของบริษัทฯ รวมถึงข้อมูลและซอฟต์แวร์ต่างๆ ที่ถูกจัดเก็บและใช้งาน

<u>โครงสร้างของคณะกรรมการ</u> : บริษัทฯ ได้กำหนดบทบาทและหน้าที่ความรับผิดชอบของการบริหารความปลอดภัยด้านสารสนเทศ ผ่านโครงสร้างองค์กรดังนี้



- Information Security Management Committee: ประกอบด้วยผู้บริหารระดับสูงของบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) หรือบริษัทในเครือ มีบทบาทและหน้าที่ดังนี้
  - อนุมัติ ประกาศใช้นโยบายหรือระเบียบปฏิบัติอื่นๆ ที่เกี่ยวข้องกับนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - กำหนดและอนุมัติเกณฑ์สำหรับความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้
  - พิจารณาผลการประเมินความเสี่ยงและแผนการแก้ไขความเสี่ยงที่สำคัญขององค์กร
  - พิจารณาลงโทษผู้ที่ละเมิดนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - ให้การสนับสนุนด้านทรัพยากรที่จำเป็นในการดำเนินงาน

- Data Protection Officer: พนักงานในบริษัทฯ หรือผู้ที่ได้รับมอบหมาย มีบทบาทและหน้าที่หลักดังนี้
  - กำกับดูแลและให้คำแนะนำเกี่ยวกับการจัดเก็บและการใช้งานข้อมูลส่วนบุคคลในระบบต่าง ๆ
  - ทำการตรวจสอบการจัดเก็บและการใช้งานข้อมูลส่วนบุคคลในระบบต่างๆ และรายงานความเสี่ยง เหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศรวมถึงแนวทางแก้ไขให้คณะกรรมการฯ และผู้เกี่ยวข้องรับทราบ
  - ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นในบริษัทฯ
  - จัดการอบรมและให้ความรู้กับพนักงานของบริษัทฯ ในเรื่องการใช้งานและปกป้องข้อมูลส่วนบุคคล
  - ติดตามและเผยแพร่ข่าวสารเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศให้กับผู้เกี่ยวข้องในบริษัทฯ
  - ประสานกับหน่วยงานต่างๆ ในเรื่องการบริหารจัดการข้อมูลทั้งภายในและภายนอกบริษัท

- Information Security Director: ตัวแทนผู้บริหารของบริษัทกรีนไลน์ฯ มีบทบาทและหน้าที่ดังนี้
  - ให้คำแนะนำและข้อเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการบริหารจัดการรักษาความปลอดภัยของข้อมูล
  - กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลระบบเทคโนโลยีสารสนเทศและผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ ในการปฏิบัติตามนโยบายฉบับนี้
  - สื่อสารให้พนักงานทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล
  - ให้การสนับสนุนและความรู้กับพนักงานและบุคคลภายนอกที่เกี่ยวข้องกับการปฏิบัติตามนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - ตรวจสอบการปฏิบัติตามนโยบายฯ ของพนักงานและบุคคลภายนอกเกี่ยวข้องอย่างเหมาะสม
  - พิจารณาการปรับปรุงนโยบายให้เหมาะสมกับสถานการณ์ในปัจจุบัน

- ประสานงานและหาแนวทางในการควบคุมและจัดการปัญหาในกรณีที่เกิดเหตุละเมิดนโยบายฯ หรือละเมิดความมั่นคงของข้อมูลขึ้นในองค์กร
- รายงานผลการดำเนินการแบบรายไตรมาสต่อ Information Security Management Committee
- รายงานความคืบหน้าเหตุการณ์หรือสถานการณ์ที่เกี่ยวข้องให้คณะกรรมการฯ รับทราบ
- ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในนโยบายฉบับนี้

- BDMS Computer Emergency Response Team (BDMS CERT): ประกอบด้วยทีมงานจากบริษัทกรีนไลน์ฯ หรือผู้ที่ได้รับมอบหมาย มีบทบาทและหน้าที่หลักดังนี้
  - ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ
  - ให้คำแนะนำและแก้ไขภัยคุกคามความมั่นคงด้านเทคโนโลยีสารสนเทศ
  - ติดตามและเผยแพร่ข่าวสารเหตุการณ์ต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้กับผู้เกี่ยวข้องในบริษัทฯ
  - ศึกษา ปรับปรุงเครื่องมือและแนวทางปฏิบัติให้ทันสมัยอยู่เสมอเพื่อเพิ่มความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของบริษัทฯ
  - ดำเนินการเรื่องอื่นๆ ที่เกี่ยวกับการบริหารจัดการความปลอดภัยสารสนเทศตามที่ผู้บังคับบัญชามอบหมาย

<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 พนักงานของบริษัทฯ คู่สัญญา ลูกจ้าง ผู้ให้บริการ ตลอดจนบุคคลภายนอกที่ใช้ข้อมูลของบริษัทฯ จำเป็นต้องทราบเนื้อหาและปฏิบัติตามเนื้อหาของนโยบายทั้งหมด
- การตรวจสอบ : บริษัทฯ สงวนสิทธิ์ในการกระทำการใดๆ ที่เห็นว่าจำเป็นเพื่อจัดการและป้องกันความมั่นคงปลอดภัยให้กับข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร
- มาตรการทางวินัย : หากมีการฝ่าฝืนข้อกำหนดของบริษัทฯ ที่ก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใดทั้งทางตรงและทางอ้อมถือเป็นความผิด ผู้กระทำการฝ่าฝืนจะต้องถูกพิจารณาลงโทษทั้งทางวินัยและทางกฎหมายตามความเหมาะสมต่อไป