BDMS
Bangkok Dusit Medical Services
ทะเบียนเลขที่ 0107537000025

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)
2 ซอยศูนย์วิจัย 7 ถนนเพชรบุรีตัดใหม่
กรุงเทพฯ 10310

Bangkok Dusit Medical Services PLC.
2 Soi Soonvijai 7, New Petchburi Rd.,
Bangkok 10310 Thailand

Tel +66 (0) 2310-3000 Fax +66 (0) 2310-3115
Contact Center Tel 1719
www.bdms.co.th

เลขประจำตัวผู้เสียภาษี 0107537000025

Tax ID: 0107537000025

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)

กรอบนโยบาย

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทในเครือได้จัดให้มีระบบเทคโนโลยีสารสนเทศขึ้นเพื่ออำนวยความสะดวกแก่บุคลากรในการปฏิบัติงานให้กับองค์กร ดังนั้นเพื่อให้การดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศของ บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทในเครือมีความสอดคล้องกับนโยบายขององค์กรและกฎหมายต่างๆที่เกี่ยวข้อง บริษัทฯ ได้กำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขึ้นเพื่อให้เป็นแนวทางและกฎเกณฑ์มาตรฐานสำหรับพนักงานและบุคคลที่มีหน้าที่หรือมีความเกี่ยวข้องในการทำงานให้สามารถปฏิบัติงานได้อย่างถูกต้อง

วัตถุประสงค์

เพื่อให้มั่นใจว่าการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของ บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทในเครือมีความเป็นมาตรฐานที่ชัดเจนและธำรงไว้ ซึ่งหลักการสำคัญ 3 ประการ คือ

1) การรักษาความลับของข้อมูล (Confidentiality) เพื่อให้ปลอดภัยจากการล่วงรู้หรือเปิดเผยโดยมิชอบ
2) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) เพื่อไม่ให้ข้อมูลถูกลบ เพิ่ม หรือแก้ไขโดยมิชอบ
3) การรักษาความคงอยู่ของระบบสารสนเทศและข้อมูลสารสนเทศ (Availability) เพื่อให้สามารถใช้งานและเข้าถึง ได้เมื่อมีความจำเป็น

ขอบเขต

นโยบายฉบับนี้ใช้บังคับกับผู้ใช้งานสารสนเทศขององค์กรทุกคนและระบบสารสนเทศทุกระบบโดยไม่มีการยกเว้น

นิยาม

ลำดับที่	คำศัพท์	คำนิยาม
1.	องค์กร	บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทในเครือที่บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) ถือหุ้นเกิน 50%

ลำดับที่	คำศัพท์	คำนิยาม
2.	คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ (Information Security Management Committee : ISMC)	คณะบุคคลที่ได้รับการแต่งตั้งกรรมการผู้อำนวยการใหญ่
3.	คณะทำงานด้านข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยสารสนเทศ (Privacy & Information Security Working Group : PSWG)	คณะทำงานที่ได้รับการแต่งตั้งจากประธานเจ้าหน้าที่ปฏิบัติการ ซึ่งประกอบไปด้วยตัวแทนด้าน Privacy และ Information Security จากแต่ละกลุ่มหรือบริษัทในเครือ
4.	บุคลากร	พนักงาน ลูกจ้าง รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานภายใต้ข้อกำหนดหรือสัญญา

<u>หน้าที่ความรับผิดชอบ</u>

องค์กรได้กำหนดบทบาทหน้าที่และความรับผิดชอบของการบริหารความปลอดภัยสารสนเทศ ผ่านโครงสร้างองค์กร ดังนี้

- คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ : ประกอบด้วยผู้บริหารระดับสูงขององค์กร มีบทบาทหน้าที่ดังนี้
  - อนุมัติ ประกาศใช้นโยบายหรือระเบียบปฏิบัติอื่นๆ ที่เกี่ยวข้องกับนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - กำหนดและอนุมัติเกณฑ์สำหรับความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้
  - พิจารณาผลการประเมินความเสี่ยงและแผนการแก้ไขความเสี่ยงที่สำคัญขององค์กร
  - พิจารณาลงโทษผู้ที่ละเมิดนโยบายการบริหารจัดการความปลอดภัยด้านสารสนเทศ
  - ให้การสนับสนุนด้านทรัพยากรที่จำเป็นในการดำเนินงาน

- อนุมัติ ประกาศใช้นโยบายหรือระเบียบปฏิบัติอื่นๆ ที่เกี่ยวข้องกับการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคลเพื่อสอดคล้องกับพระราชบัญญัติเกี่ยวข้องกับความปลอดภัยและความเป็นส่วนตัวของข้อมูล
- อนุมัติหลักเกณฑ์และข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ
- แต่งตั้งคณะทำงานในการดำเนินงานเพื่อกำหนดแนวทางการบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติ
- ตรวจสอบการดำเนินการตามนโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้การดำเนินการด้านข้อมูลส่วนบุคคลเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้อง

<u>แนวทางปฏิบัติ</u>

กำหนดให้ทุกบริษัทที่อยู่ภายใต้นโยบายฉบับนี้จะต้องจัดทำระเบียบปฏิบัติและแผนต่างๆ ตามรายละเอียดด้านล่าง และเสนอขออนุมัติเพื่อประกาศใช้งานจากคณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ สำหรับการทบทวนกำหนดให้ทุกบริษัทจะต้องทำการทบทวนระเบียบปฏิบัติต่างๆ ทุก 2 ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

- การบริหารจัดการทรัพย์สินด้านสารสนเทศ (Information Asset Management)
- การประเมินความเสี่ยงและการจัดการความเสี่ยงด้านสารสนเทศ (Risk Assessment & Risk Treatment)
- การจำแนกชั้นความลับและการจัดการข้อมูล (Information Classification & Handling)
- การใช้งานทรัพยากรสารสนเทศ (Acceptable Use)
- การบริหารจัดการบัญชีผู้ใช้งานข้อมูลและระบบสารสนเทศ (User Access Control)
- การรักษาความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Protection)
- การรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security)
- การบริหารจัดการผู้ให้บริการภายนอกด้านสารสนเทศ (3rd Party Management)
- การสำรองข้อมูลและการกู้คืนระบบสารสนเทศที่สำคัญ (Backup & Restore)
- แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ร้ายแรง (Cyber Security Incident Management)
- แผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Management)

<u>Workflow</u>

- ไม่มี

ช่องทางการสื่อสาร และการอบรม (Communication Channel & Training)

1. ประกาศแจ้งผ่านทางจดหมายอิเล็กทรอนิกส์ (อีเมล) หรือ
2. ติดประกาศที่บอร์ดของบริษัท หรือ
3. ศึกษาด้วยตนเองในระบบ e-document

การเฝ้าติดตามและการวัดกระบวนการ/การบริการ

คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ สามารถมอบหมายให้คณะทำงานด้านข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยสารสนเทศ (Privacy & Information Security Working Group : PSWG) เป็นตัวแทนติดตามและนำเสนอรายงานการวัดผลการดำเนินงานตามนโยบายและระเบียบปฏิบัติที่ประกาศใช้งานของกลุ่มต่างๆ อย่างน้อยปีละหนึ่งครั้ง

เอกสารคุณภาพที่เกี่ยวข้อง

- ไม่มี

เอกสารอ้างอิง

1. พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
2. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
3. Information Security Management System - ISO/IEC 27001: 2013
4. Information Security Management in Health - ISO/IEC 27799: 2016