

10th-11th Floor, Lake Rajada Office Complex 2
195/11-12 Rajadapisek Road, Klongtoey
Bangkok 10110 THAILAND

Tel : (662) 661-9734-8
Fax : (662) 260-9176
<http://www.chemaman.com>

**นโยบายความมั่นคงปลอดภัยสารสนเทศ
บริษัท เคมีแมน จำกัด (มหาชน)**

บริษัท เคมีแมน จำกัด (มหาชน) ("บริษัท") ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นปัจจัยสำคัญในการสนับสนุนการดำเนินธุรกิจ และเพื่อให้การใช้ระบบเทคโนโลยีสารสนเทศของบริษัท เป็นไปอย่างมีประสิทธิภาพและปลอดภัย บริษัทจึงประกาศนโยบายความมั่นคงปลอดภัยสารสนเทศฉบับนี้ โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้งาน และบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีรายละเอียดดังต่อไปนี้

1. การดำเนินงานตามข้อกำหนดทางกฎหมาย

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท จะต้องดำเนินการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างเหมาะสม โดยปฏิบัติตามข้อกำหนดของกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้องอย่างเคร่งครัด

2. การสร้างให้มีความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องมีการส่งเสริมให้บุคลากรทุกคนในองค์กรมีความตระหนักรู้และให้ความสำคัญต่อภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของสารสนเทศขององค์กร โดยจะต้องปฏิบัติตามนโยบาย มาตรการ และแนวทางที่กำหนดไว้อย่างเคร่งครัด พร้อมทั้งเสริมสร้างความรู้ ความเข้าใจ และความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์อยู่เสมอ เพื่อร่วมกันป้องกันและลดความเสี่ยงจากเหตุการณ์ที่อาจเกิดขึ้นทั้งโดยเจตนาและไม่เจตนา

3. การกำหนดมาตรการการรักษาความปลอดภัยระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เหมาะสมกับประเภทของข้อมูล กำกับดูแลการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ตลอดจนดำเนินการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้ไม่ประสงค์ดี รวมถึงการป้องกันภัยคุกคามจากซอฟต์แวร์ที่อาจก่อให้เกิดความเสียหายต่อข้อมูลของบริษัท

10th-11th Floor, Lake Rajada Office Complex 2
195/11-12 Rajadapisek Road, Klongtoey
Bangkok 10110 THAILAND

Tel : (662) 661-9734-8
Fax : (662) 260-9176
<http://www.chemaman.com>

4. การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงอุปกรณ์ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และข้อมูล (Information) ให้มีความปลอดภัยสูงสุด รวมถึงกำกับดูแลกระบวนการเปลี่ยนแปลง การขนย้าย การทำลาย หรือการลบข้อมูล ให้เป็นไปตามหลักเกณฑ์ที่เหมาะสม และถูกต้องตามลิขสิทธิ์ เพื่อให้มั่นใจว่าระบบปราศจากซอฟต์แวร์ที่ไม่ได้รับอนุญาต ไวรัส หรือโปรแกรมมัลแวร์อื่น ๆ ทั้งนี้ ต้องมีการปรับปรุงโปรแกรมป้องกันไวรัส และโปรแกรมความปลอดภัย (Security Patch) ให้ทันสมัยอยู่เสมอ

5. การควบคุมการเข้าถึง พัฒนา หรือเปลี่ยนแปลงระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำกับดูแลควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ รวมถึงการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น โดยมีการกำหนดรหัสผ่าน การเข้าถึงระบบ และการพิสูจน์ตัวตนในทุกกระบวนการ ทั้งนี้ การเข้าถึงระบบเครือข่ายจากระยะไกลต้องดำเนินการผ่านกระบวนการพิสูจน์ตัวตนที่เหมาะสมและปลอดภัย

6. การตรวจสอบและติดตามความปลอดภัยของระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดเก็บบันทึกข้อมูลเหตุการณ์ (Log) และเฝ้าระวัง (Monitoring) อย่างเป็นระบบ เพื่อให้สามารถตรวจสอบการเข้าถึงที่อาจมีความผิดปกติ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

7. การวางแผนความต่อเนื่องทางธุรกิจและการกู้คืนระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ด้านเทคโนโลยีสารสนเทศ รวมถึงดำเนินการซักซ้อมแผนฟื้นฟูระบบสารสนเทศ (Disaster Recovery: DR) เป็นประจำทุกปี มีการสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมเพื่อให้มั่นใจว่าระบบสามารถดำเนินการได้อย่างต่อเนื่องในกรณีเกิดเหตุฉุกเฉิน

8. การกำหนดมาตรฐานการรักษาความปลอดภัยระดับสากล

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องดำเนินการด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศต้องเป็นไปตามมาตรฐานสากล เพื่อให้มั่นใจว่าระบบสารสนเทศของบริษัทมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถรองรับการดำเนินธุรกิจได้อย่างยั่งยืน

10th-11th Floor, Lake Rajada Office Complex 2
195/11-12 Rajadapisek Road, Klongtoey
Bangkok 10110 THAILAND

Tel : (662) 661-9734-8
Fax : (662) 260-9176
<http://www.chemaman.com>

9. การทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบัน

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องมีการทบทวนนโยบายให้ทันสมัยและสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลง และมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง ซึ่งต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูล และระบบคอมพิวเตอร์ กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง

10. ติดตามผลการดำเนินงานตามนโยบาย อย่างสม่ำเสมอ

หน่วยงานที่ได้รับมอบหมายให้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ จะต้องดำเนินการติดตามตรวจสอบ และประเมินผลการดำเนินงานตามนโยบายความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งกำกับดูแลให้หน่วยงานภายในปฏิบัติตามนโยบาย แนวปฏิบัติ และมาตรการต่าง ๆ ที่กำหนดไว้อย่างเคร่งครัด เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรเป็นไปอย่างมีประสิทธิภาพ และสอดคล้องกับกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง.

นโยบายความมั่นคงปลอดภัยสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ตั้งแต่ 3 มิถุนายน พ.ศ.2568 เป็นต้นไป

ประกาศ ณ วันที่ 3 มิถุนายน 2568

- ลายเซ็น -

หม่อมหลวงจันทรจุฑา จันทรทัต
ประธานกรรมการบริษัท