# นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

ของ

# บริษัท ไดนาสตี้ เซรามิค จำกัด (มหาชน) และบริษัทในเครือ

## หลักการและเหตุผล

เพื่อให้การดำเนินการใดๆ ด้านเทคโนโลยีสารสนเทศ ของ บริษัท ไดนาสตี้ เซรามิค จำกัด (มหาชน) ("บริษัทฯ") และบริษัทในเครือ มีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนข้อมูลและสินทรัพย์สารสนเทศของบริษัทฯ ได้รับการดูแลรักษาอย่างเหมาะสม บริษัทฯ ได้ตระหนักถึงความสำคัญของ การนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการธุรกิจจึงกำหนดนโยบายฉบับนี้เพื่อให้บริษัทฯ มีกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร เพื่อให้สอดคล้องกับหลักการกำกับดูแลกิจการที่ดีตลอดจนกฎหมายอื่นที่เกี่ยวข้องเพื่อให้เหมาะสมกับการดำเนินธุรกิจของบริษัทฯ

## นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

1) ด้านการตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

2) ด้านการบริหารและจัดการความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

3) ด้านรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

## 1.ด้านการตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

เพื่อให้มีความสอดคล้องกับ แผนกลยุทธ์องค์กรและเพื่อให้บรรลุเป้าหมายตามที่กำหนดไว้ ดังนี้

1) กำหนดหลักเกณฑ์และปัจจัยในการจัดลำดับความสำคัญของแผนงานด้านเทคโนโลยีสารสนเทศเพื่อให้เหมาะสมสอดคล้องกับแผนกลยุทธ์และเป้าหมายในการดำเนินธุรกิจ

2) จัดทำและอนุมัติงบประมาณด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับแผนงบประมาณและแผนกลยุทธ์องค์กร

3) จัดให้มีทรัพยากรบุคคลอย่างเพียงพอต่องานด้านเทคโนโลยีสารสนเทศ โดยให้มีการพัฒนา ทักษะของบุคลากรอย่างต่อเนื่อง รวมทั้งจัดจ้างบุคลากรด้านเทคโนโลยีสารสนเทศจากภายนอกเมื่อมีความจำเป็ น

4) จัดการความเสี่ยงในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้าน เทคโนโลยีสารสนเทศไม่ว่าจะเป็นบุคลากร หรือ งบประมาณ เกินกว่าที่กำหนดไว้

5) กำหนดหน้าที่และความรับผิดชอบของบุคลากรหน่วยงานเทคโนโลยีสารสนเทศ ในการ จัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

## 2. ด้านการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1) กำหนดให้มีการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและการบริหารความเสี่ยงองค์กร

2) กำหนดให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

3) กำหนดให้มีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยกำหนดขั้นตอน กระบวนการบริหาร และผู้มีหน้าที่รับผิดชอบ รวมถึงจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ผ่านบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

4) กำหนดให้มีการบริหารจัดการทรัพย์สินของบริษัท โดยระบุและกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศเพื่อให้ทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม

## 3. ด้านรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

กำหนดให้มีความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยคำนึงถึงลักษณะ ขนาด และความซับซ้อนของการประกอบธุรกิจ รวมทั้งกฎเกณฑ์ต่างๆ ที่เกี่ยวข้อง เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่างๆ ซึ่งกำหนดแนวทางการดำเนินการของบริษัท ไว้ดังนี้

### 3.1 การจำแนกประเภททรัพย์สินสารสนเทศ

ควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทฯ ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือ ลำดับขั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และ ช่องทางการเข้าถึง และ จัดให้มีการป้องกันบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

### 3.2 การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

จัดทำระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับ กรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง และ ให้มีการทดสอบสภาพพร้อมใช้งานของระบบสำรองและแผนรองรับกรณีเกิดเหตุการณ์ฉุกเฉินอย่างสม่ำเสมอ

### 3.3 การควบคุมการเข้ารหัสข้อมูล

กำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล ให้เหมาะสมกับความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายอย่างสม่ำเสมอ

**3.4 การควบคุมดูแลบุคลากรและผู้ใช้งาน**

**3.4.1 การใช้งานของผู้ใช้งาน**

*1.กำหนดมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน*

กำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโยลีสารสนเทศโดยการใส่รหัสผ่าน และให้ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งานและเครื่องคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งานหรือเมื่อเสร็จสิ้นการปฏิบัติงาน

*2.กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท*

กำหนดให้มีมาตรการที่เหมาะสมควบคุมความปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัทฯรวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัทฯ

*3.กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน*

จัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริงเพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์บนระบบที่ไม่ได้รับอนุญาตให้ใช้งานและกำหนดรายการซอฟต์แวร์มาตรฐานที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

**3.4.2 การควบคุมผู้ให้บริการภายนอก (IT Outsourcing)**

จัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอก เพื่อป้องกันทรัพย์สินสารสนเทศจากการเข้าถึงอย่างไม่เหมาะสม และ ควบคุมการส่งมอบงานให้เป็นไปตามข้อตกลงที่ได้จัดทำไว้ ทั้งนี้ให้ครอบคลุมถึงผู้รับดำเนินการมีการให้ผู้บริหารภายนอกรายอื่นๆ รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศอีกด้วย

**3.5 การจัดระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ**

**3.5.1 ด้านการสื่อสารข้อมูลสารเสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์**

ต้องควบคุมกำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งจากภายในกลุ่มบริษัทฯเอง หรือ จากภายนอก รวมถึงแบ่งแยกระบบตามความเหมาะสม โดยพิจารณาถึงความต้องการเข้าถึงระบบ ผลกระทบ และระดับความสำคัญของข้อมูลนั้นๆ

**3.5.2 การควบคุมการรับส่งข้อมูลสารสนเทศ**

-ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ทั้งในกลุ่มบริษัทฯ หรือ หน่วยงานภายนอก เป็นลายลักษณ์อักษร

-กำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นต้น จะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

-ต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทฯ มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทฯ อย่างเป็นลายลักษณ์อักษร

**3.6 การป้องกันภัยคุกคามต่อระบบสารสนเทศ**

-จากโปรแกรมไม่ประสงค์ดี บริษัทฯต้องกำหนดมาตรการสำหรับการตรวจจับ ป้องกัน และ การกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี

-จากช่องโหว่ทางเทคนิค บริษัทฯต้องควบคุมให้ระบบสารสนเทศของบริษัทฯได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดย จัดให้มีการทดสอบการเจาะระบบ จัดให้มีการประเมินช่องโหว่ของระบบ จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

**3.7 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ**

บริษัทฯ จัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม

**การทบทวนนโยบาย**

กำหนดให้มีการทบทวนนโยบายให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง

**การรายงาน**

กำหนดให้มีการรายงานการปฏิบัติตามนโยบายฯ รวมถึงระเบียบและข้อกำหนดต่างๆ ต่อคณะกรรมการบริษัทฯ อย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีเหตุการณ์เร่งด่วนใดๆ ที่ส่งผลกระทบต่อการปฏิบัติตามนโยบายฯ

อนุมัติโดยมติที่ประชุมคณะกรรมการบริษัทฯ ครั้งที่ 4/2567 เมื่อวันที่ 6 สิงหาคม 2567

(นายรุ่งโรจน์ แสงศาสตรา)
ประธานกรรมการ