

ประกาศที่ 06/2569 นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อเป็นแนวทางและสนับสนุนการตัดสินใจทางด้านไอทีภายในกลุ่ม โดยอธิบายมาตรฐานและขั้นตอน รวมถึงวิธีปฏิบัติที่ปลอดภัย โดยยึดตามความรู้ และแนวปฏิบัติทั่วไปที่เป็นที่ยอมรับในปัจจุบัน นโยบายนี้มีผลบังคับใช้สำหรับ TIPCO ASPHALT GROUP (“กลุ่มบริษัทฯ”) บริษัทในเครือ และการดำเนินกิจการร่วมค้า และมีผลบังคับใช้กับพนักงานทุกคน ตลอดจนที่ปรึกษาและเจ้าหน้าที่หน่วยงานที่ทำงานในสถานที่ของกลุ่มหรือภายใต้การกำกับดูแล

หลักการ

1. ความมุ่งมั่นและความคาดหวัง (Commitment and Expectations)

โครงสร้างของเทคโนโลยีสารสนเทศของกลุ่มบริษัทได้ทำการเพิ่มมูลค่า โดยการให้บริการที่ดีที่สุดแก่บริษัท ปรับสมดุลความเสี่ยง และให้ผลตอบแทนจากการลงทุนในด้านเทคโนโลยีสารสนเทศ กลุ่มบริษัทฯ มุ่งมั่นที่จะปกป้องบุคคลและข้อมูลจากภัยคุกคามทางไซเบอร์ ในขณะเดียวกันสามารถลดความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยรวม เรากำกับและควบคุมการทำงานด้านเทคโนโลยีสารสนเทศผ่านการจัดการอย่างมีโครงสร้าง กระบวนการที่สอดคล้องกัน และสร้างความสัมพันธ์ที่แน่นแฟ้นกับธุรกิจ ดังนี้

- ปกป้องบุคคลและข้อมูลจากภัยคุกคามทางไซเบอร์
- เฝ้าระวังและตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ
- กำหนดหลักเกณฑ์สำหรับ ผู้ใช้ ผู้ดูแลระบบ ฝ่ายจัดการ และเจ้าหน้าที่รักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ
- จัดทำข้อกำหนดด้านความปลอดภัยทางสารสนเทศสำหรับผู้ให้บริการและผู้รับจ้างภายนอก
- กำหนดมาตรฐานของระบบและแอปพลิเคชัน (System and Applications)
- ลดความเสี่ยงโดยรวมด้านเทคโนโลยีสารสนเทศ (Mitigate overall IT risk)

ดังนั้น พนักงานทุกคนรวมถึงผู้รับเหมาที่มีการเข้าถึงระบบเทคโนโลยีสารสนเทศหรือฮาร์ดแวร์ของกลุ่ม จะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัดตลอดจนมีการใช้มาตรฐานระดับสูงในการทำงานอย่างสม่ำเสมอ คำแนะนำเพิ่มเติมสามารถอ้างอิงตามคู่มือการปฏิบัติงาน นโยบายฉบับนี้อ้างอิงตามหลักการ แนวทาง และหน้าที่ความรับผิดชอบที่กำหนดไว้ตามระบบมาตรฐานการจัดการความปลอดภัยของสารสนเทศ ISO 27001

2. ข้อปฏิบัติในด้านความปลอดภัยของข้อมูล (Information Security Instruction)

การรักษาความปลอดภัยของข้อมูลเป็นวิธีปฏิบัติในการปกป้องข้อมูลจากการเข้าถึง การใช้ การเปิดเผย การจัดวาง การแก้ไข การพิจารณา การตรวจสอบ การบันทึก หรือการทำลายโดยไม่ได้รับอนุญาต

คำแนะนำในการรักษาความปลอดภัยข้อมูลของกลุ่มบริษัทฯ จะกำหนดวิธีที่เราใช้ในการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล และควบคุมความปลอดภัยที่จำเป็นเพื่อปกป้องสินทรัพย์สารสนเทศ (Information Assets) โดยไม่คำนึงถึงรูปแบบของการนำข้อมูลไปใช้ เช่น การสำรองข้อมูลทางอิเล็กทรอนิกส์ (Electronic Backup) หรือการสำรองข้อมูลทางกายภาพ (Physical Backup)

จุดมุ่งหมายของการกำหนดแนวทางปฏิบัติการรักษาความปลอดภัยของข้อมูล เพื่อให้เกิดความมั่นใจในด้าน

- การรักษาความลับของข้อมูล (Confidentiality)
- การเข้าถึงและความพร้อมในใช้งานของระบบ (Access and Availability)
- ความสมบูรณ์ถูกต้องของข้อมูล (Data Integrity)

ข้อปฏิบัติในการรักษาความปลอดภัยของข้อมูลที่ใช้ระบบคอมพิวเตอร์ทั้งหมดของกลุ่มบริษัทฯ สามารถหาคำแนะนำเพิ่มเติมได้ตามคู่มือการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Work Instruction) ดังนี้

- การกำหนดความเป็นเจ้าของข้อมูลและการจำแนกประเภท (Information Ownership & Classification)
- ชื่อผู้ใช้ และ รหัสผ่าน (User ID & Password)
- การใช้งานที่ยอมรับได้และความรับผิดชอบ (Acceptable Use & Responsibility)
- การสำรองข้อมูลและการกู้คืน (Backup & Recovery)
- การวางแผนฉุกเฉินความต่อเนื่องทางธุรกิจ (Business Continuous Planning)

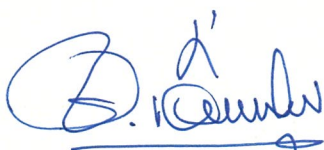
หน้าที่และความรับผิดชอบ

- พนักงานทุกคนมีหน้าที่ศึกษา ทำความเข้าใจ และปฏิบัติตามนโยบายและคู่มือการปฏิบัติที่เกี่ยวข้องชื่อผู้ใช้ และรหัสผ่าน (User ID & Password)
- หัวหน้างานและผู้จัดการมีหน้าที่ให้คำแนะนำและทำให้มั่นใจว่าพนักงานภายในการกำกับดูแลสามารถเข้าถึงนโยบายและคู่มือการปฏิบัติที่เกี่ยวข้องได้

สรุป

กลุ่มบริษัทฯ มุ่งมั่นปกป้องภัยคุกคามทางไซเบอร์ พร้อมทั้งลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยกำหนดมาตรฐานความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและแอปพลิเคชัน ซึ่งมีผลบังคับใช้กับพนักงาน ผู้รับเหมา และตัวแทนทางธุรกิจที่กระทำการในนามกลุ่มบริษัทฯ

ทั้งนี้ ตั้งแต่วันที่ 13 พฤษภาคม 2569 เป็นต้นไป



นายชายน้อย ฝื่อนโกสม
ประธานกรรมการ