นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนสำคัญในการสนับสนุนการดำเนินธุรกิจของบริษัทให้เกิดประสิทธิภาพและเป็นที่น่าเชื่อถือ บริษัทจึงมุ่งมั่นที่จะพัฒนาระบบการรักษาความปลอดภัยด้านสารสนเทศ ตามหลักการสำคัญ คือ การธำรงไว้ซึ่งการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) เพื่อนำไปปฏิบัติ และให้มั่นใจได้ว่า

1. ผู้ที่ได้รับอนุญาตเท่านั้น ที่สามารถจะเข้าถึงระบบ ข้อมูล หรือสถานที่จัดเก็บข้อมูลระบบสารสนเทศได้
2. มีการควบคุมการเข้ารหัสรักษาความลับของข้อมูลที่สำคัญอย่างเหมาะสม
3. มีการป้องกันด้านความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม ให้ระบบสารสนเทศมีความปลอดภัยและพร้อมใช้งานอยู่เสมอ
4. ระบบสารสนเทศ มีความถูกต้อง เชื่อถือได้
5. มีการตรวจสอบ ติดตามและประเมินผลความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ
6. มีกระบวนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ จัดทำแผน ดำเนินการฝึกซ้อม และปรับปรุงอย่างต่อเนื่อง เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน
7. มีการส่งเสริมให้พนักงานมีความรู้ ความสามารถที่เหมาะสม และมีจิตสำนึกเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง

อนึ่ง ความมั่นคงปลอดภัยด้านสารสนเทศ ถือเป็นความรับผิดชอบของทุกคน ดังนั้น จึงเป็นหน้าที่ของพนักงานและบุคคลภายนอกที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของบริษัทต้องดำเนินการในทุกวิถีทางเพื่อทำให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท