JWD InfoLogistics Public Company Limited
36 Krungthep Kreetha Rd.,
Huamark, Bangkapi, Bangkok
10240, Thailand.
T : +66 2710 4000
www.jwd-group.com

ความเสี่ยงที่อาจเกิดขึ้นใหม่ (Emerging Risk)

1. ความเสี่ยงความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

ประเด็นด้านการคุ้มครองข้อมูลส่วนบุคคล ตามกฎหมายที่กำหนดเกี่ยวกับหลักเกณฑ์หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลของลูกค้า ผู้ถือหุ้น พนักงาน คู่ค้า และผู้มีส่วนได้เสียกับบริษัทฯ ไม่ให้ถูกละเมิดสิทธิและเสรีภาพของบุคคล ซึ่งเป็นหน้าที่ของผู้ประกอบการที่ต้องจัดให้มีมาตรการที่ทำให้มั่นใจว่าข้อมูลส่วนบุคคลได้รับความคุ้มครอง และมีการบริหารจัดการข้อมูลอย่างเหมาะสม

เพื่อการบริหารและจัดการความเสี่ยงดังกล่าว บริษัทฯ ได้มีการดำเนินการในด้านต่างๆ อาทิ การจัดทำนโยบายความปลอดภัยและการจัดทำนโยบายความมั่นคงและความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยครอบคลุมมาตรการรักษาความปลอดภัยทั้งทางเทคนิคและการบริหารเพื่อปกป้องข้อมูลส่วนบุคคลจากการสูญหาย การเข้าถึงการใช้หรือการเปิดเผยโดยไม่ได้รับอนุญาต และจัดให้มีการทบทวนมาตรการความปลอดภัยและพัฒนาเทคโนโลยีอย่างต่อเนื่องเพื่อให้มีประสิทธิภาพมากขึ้น

2. ความเสี่ยงด้านภัยคุกคามทางไซเบอร์

ปัจจุบันภัยคุกคามของระบบเทคโนโลยีสารสนเทศจากการถูกโจมตีและอาชญากรรมทางไซเบอร์เป็นความเสี่ยงสำคัญที่ส่งผลกระทบต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นเครื่องมือหลักในการปฏิบัติงาน และเป็นความเสี่ยงที่อาจส่งผลให้เกิดผลกระทบต่อการดำเนินธุรกิจ อาทิเช่น การดำเนินธุรกิจหยุดชะงัก การสูญหายหรือการรั่วไหลของข้อมูลที่สำคัญ ข้อมูลทางการค้า ข้อมูลส่วนบุคคลของลูกค้า คู่ค้าและพนักงาน เป็นต้น และประกอบกับกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการบังคับใช้กฎหมาย ข้อบังคับ และมาตรฐานต่างๆ เพิ่มมากขึ้น ส่งผลให้ภาครัฐและเอกชนต้องตระหนักและให้ความสำคัญถึงการพัฒนากลยุทธ์ด้านความปลอดภัยของระบบบริหารจัดการเทคโนโลยีสารสนเทศ

บริษัทฯ จึงกำหนดนโยบายและมาตรการจัดการความเสี่ยงด้านความปลอดภัยของระบบสารสนเทศและการป้องกันข้อมูลส่วนบุคคล โดยมีคณะทำงานบริหารความต่อเนื่อง (BCP Committee) และคณะปฏิบัติการด้านระบบสารสนเทศ (IT Committee) กำกับดูแลกระบวนการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของข้อมูล และกำหนดแผนกลยุทธ์เพื่อยกระดับมาตรฐานการกำกับดูแลระบบการรักษาความมั่นคงปลอดภัยของบริษัทฯและบริษัทในกลุ่ม ให้อยู่ในระดับมาตรฐานสากลและดำเนินการตรวจประเมินความเสี่ยง บริหารจัดการระบบสารสนเทศและการควบคุมความมั่นคงปลอดภัยทางไซเบอร์ การป้องกันและรักษาข้อมูลส่วนบุคคลอย่างสม่ำเสมอ และกำหนดให้รายงานต่อคณะกรรมการบริษัทป พิจารณาทบทวนแผนกลยุทธ์อย่างต่อเนื่องและแผนการปรับปรุงเสถียรภาพของเทคโนโลยีสารสนเทศให้มีระบบมาตรฐานการป้องกันตรวจจับและตอบโต้การโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพตามกรอบการดำเนินงานตามมาตรฐานสากล รวมถึงส่งเสริมให้มีการอบรมเสริมสร้างความรู้การใช้เทคโนโลยีอย่างถูกต้องและมีความปลอดภัยจากการถูกคุกคามทางไซเบอร์ให้กับพนักงานอย่างต่อเนื่อง