แถลงการณ์การกำกับดูแลและแนวปฏิบัติด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

(Information Technology Security Statement)

เพื่อให้ระบบสารสนเทศของ บริษัท พีทีที โกลบอล เคมิคอล จำกัด (มหาชน) และบริษัทในเครือ มีความมั่นคงปลอดภัย ดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ สอดคล้องตามหลักมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) หรือกรอบการดำเนินงานที่เป็นมาตรฐานสากลและกำหนดแนวปฏิบัติเพื่อสร้างความตระหนัก รวมถึงกำหนดวิธีการป้องกันภัยคุกคาม การใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการปฏิบัติให้เกิดความสอดคล้องกับกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายที่เกี่ยวข้องกับประธานเจ้าหน้าที่บริหาร โดยมีสาระสำคัญ ดังนี้

1. กำหนดให้หน่วยงาน Cybersecurity ทำหน้าที่ทบทวน หรือปรับปรุงนโนบาย กรอบการดำเนินงาน และ/หรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้สอดคล้องกับมาตรฐานสากล กฎหมาย และข้อกำหนดต่าง ๆ ที่เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง พร้อมทั้งมีหน้าที่รับผิดชอบบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกันภัยคุกคามทางไซเบอร์จากกระบวนการทางธุรกิจ และจากกระบวนการทางผลิตในแต่ละพื้นที่โรงงาน
2. กำหนดข้อปฏิบัติการใช้บริการด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับหลักมาตรฐานสากล เพื่อป้องกันการโจมตีทางไซเบอร์ ตลอดจนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องกับการบริหารความเสี่ยงในระดับองค์กร โดยขอบเขตของการปฏิบัติและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงสินทรัพย์และบุคลากรทั้งหมดขององค์กร อีกทั้งหน่วยงานภายนอกที่เกี่ยวข้อง
3. ติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุกด้านไซเบอร์ ให้ครอบคลุมระบบสารสนเทศของบริษัทฯ ควบคุมการจัดการเข้าถึงข้อมูล การแลกเปลี่ยนข้อมูล การสำรองและทำลายข้อมูล พร้อมทั้งจัดให้มีการเฝ้าระวังโดยหน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ และรายงานข้อมูลภัยคุกคามด้านไซเบอร์ให้แก่ผู้บริหารรับทราบ อย่างน้อยไตรมาสละ 1 ครั้ง
4. จัดทำแผนการตอบสนองเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการจัดการเหตุการณ์ผิดปกติได้อย่างรวดเร็วและมีประสิทธิภาพ ตลอดจนมีการติดตามเหตุการณ์ที่เกิดขึ้นและจัดทำแผนฟื้นฟูหลังจากเกิดเหตุการณ์ผิดปกติ เพื่อลดผลกระทบต่อกระบวนการธุรกิจ รวมถึงจัดให้มีการซ้อมแผนเพื่อประเมินความถูกต้องและมีประสิทธิผลของแผน
5. สร้างความตระหนักรู้และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้กับพนักงานทุกคน ผ่านการสื่อความและจัดอบรมให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) เพื่อให้พนักงานมีความเข้าใจและสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ พร้อมทั้งมีความรับผิดชอบต่อความปลอดภัยของข้อมูลในงานของตนเอง และเฝ้าระวังพฤติกรรมหรือกิจกรรมที่อาจเป็นภัยด้านด้านความมั่นคงปลอดภัยทางไซเบอร์

นอกจากนี้บริษัทฯ มีการประกาศใช้นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ซึ่งได้รับอนุมัติโดยประธานเจ้าหน้าที่บริหารบริษัทฯ โดยบังคับใช้ในธุรกิจและการดำเนินงานทั้งหมดตลอดห่วงโซ่อุปทานของบริษัทฯ ทั้งนี้ บริษัทฯ สนับสนุนให้คู่ค้า ผู้รับเหมา และหุ้นส่วนทางธุรกิจอื่นๆ (เช่น ธุรกิจที่บริษัทฯ ไม่ได้เข้าไปมีส่วนร่วมในการบริหาร พันธมิตรร่วมทุน ผู้รับใบอนุญาต ผู้ให้บริการภายนอก) ปฏิบัติตามนโนบายดังกล่าว ในการนี้ ผู้บริหารทั้งหมดเป็นแบบอย่างที่ดีและแสดงความรับผิดชอบในการปฏิบัติตามนโยบายดังกล่าว ในขณะเดียวกัน พนักงานทุกคนต้องทำความเข้าใจและสามารถปฏิบัติตามนโยบายอย่างต่อเนื่องในการปฏิบัติหน้าที่ของตนตามนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ