นโยบายความมั่นคงปลอดภัยทางไซเบอร์

บริษัท อุบล ไบโอ เอทานอล จำกัด (มหาชน) หรือ UBE และบริษัทในเครือ (“บริษัทฯ”) มีการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ และความเสี่ยงด้านไซเบอร์อย่างมีประสิทธิภาพ สอดคล้องกับแนวปฏิบัติที่เป็นมาตรฐานสากล เพื่อระบุถึงการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ และความเสี่ยงด้านไซเบอร์อย่างมีประสิทธิภาพ สอดคล้องกับแนวปฏิบัติที่เป็นมาตรฐานสากล เพื่อป้องกันภัยคุกคาม การโจมตี การทำลายระบบสารสนเทศ และการจารกรรมข้อมูลทางไซเบอร์ว่าด้วย มาตรฐานการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Policy Standard Practice) พ.ศ. 2563 และกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ โดยมีสาระสำคัญ ดังนี้

1. ให้มีคณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีตัวแทนจากทางหน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ จากกระบวนการทางธุรกิจ และ จากกระบวนการทางผลิตในแต่ละพื้นที่โรงงานเป็นผู้รับผิดชอบความมั่นคงปลอดภัยทางไซเบอร์ และให้กำหนดหน้าที่ความรับผิดชอบพร้อมทั้งวิธีการบริหารจัดการ
2. พัฒนา และรักษากรอบการดำเนินงานหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้สอดคล้องกับมาตรฐานสากล และติดตามกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง และพิจารณาการปฏิบัติตามให้สอดคล้อง
3. ให้มีการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ โดยการประเมินจากภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) ความเป็นไปได้ (Likelihoods) และผลกระทบ (Impact) ต่อธุรกิจ รวมทั้งให้มีการจัดการความเสี่ยง ที่มีความสอดคล้องกับการบริหารความเสี่ยงในระดับองค์กร โดยขอบเขตของการบริหารความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงสินทรัพย์และบุคลากรทั้งหมดขององค์กร อีกทั้งหน่วยงานภายนอกที่เกี่ยวข้อง
4. สื่อความและจัดอบรมให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) เพื่อสร้างความตระหนักรู้ ความรับผิดชอบ และความเข้าใจการรับมือกับภัยคุกคามทางไซเบอร์ให้กับพนักงานอย่างน้อยปีละ 1 ครั้ง
5. ให้มีการติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุกด้านไซเบอร์ ให้ครอบคลุมระบบสารสนเทศของบริษัทฯ พร้อมทั้งจัดให้มีการเฝ้าระวัง และให้หน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ต้องรายงานข้อมูลภัยคุกคามด้านไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างน้อยไตรมาสละครั้ง
6. ให้จัดทำแผนการตอบสนองเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการจัดการเหตุการณ์ผิดปกติได้อย่างรวดเร็วและมีประสิทธิภาพ พร้อมทั้งลดผลกระทบต่อกระบวนการธุรกิจที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนการตอบสนองฯ อย่างน้อยปีละ 2 ครั้ง
7. ให้จัดทำแผนฟื้นฟูหลังจากเกิดเหตุการณ์ผิดปกติ เพื่อลดผลกระทบต่อกระบวนการธุรกิจที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนฟื้นฟูฯ เพื่อประเมินความถูกต้องและมีประสิทธิผลของแผน อย่างน้อยปีละ 1 ครั้ง
8. ให้มีการตรวจประเมินช่องโหว่ (Vulnerability Assessment) หรือ การทดสอบเจาะระบบ (Penetration Test) โดยครอบคลุมระบบโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) และโปรแกรมประยุกต์ (Application) สำหรับระบบสารสนเทศที่มีความเสี่ยงจากภัยคุกคามด้านไซเบอร์อย่างน้อยปีละ 1 ครั้ง