ประกาศ บริษัท ไออาร์พีซี จำกัด (มหาชน)

ที่ 028 /2562

เรื่อง นโยบายความมั่นคงปลอดภัยไซเบอร์

บริษัทฯ ให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เพื่อลดความเสี่ยงที่เกิดจากอาชญากรรมทางคอมพิวเตอร์ การโจมตี การจารกรรมข้อมูล ภัยคุกคามต่าง ๆ ที่ส่งผลกระทบต่อการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต การสื่อสาร ข้อมูลคอมพิวเตอร์ และระบบงานคอมพิวเตอร์ โดยสามารถป้องกัน รับมือ และแก้ไขสถานการณ์ด้านภัยคุกคามได้อย่างทันท่วงทีและมีประสิทธิภาพ อันจะช่วยสร้างความเชื่อมั่นให้กับบริษัทฯ ทั้งนี้ การรักษาความมั่นคงปลอดภัยไซเบอร์หมายรวมถึง เครื่องมือ (Tools) นโยบาย (Policies) แนวคิดการรักษาความปลอดภัย (Security Concepts) การรักษาความปลอดภัย (Security Safeguards และเทคโนโลยี (Technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

บริษัทฯ จึงกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ โดยให้มีผลบังคับใช้กับผู้บริหารและพนักงานทุกคน และให้ผู้บริหารของทุกหน่วยงานมีหน้าที่รับผิดชอบในการส่งเสริมให้พนักงานมีความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สนับสนุน ผลักดัน และติดตามการดำเนินการตามนโยบาย และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด ดังต่อไปนี้

1. หน่วยงานที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ต้องกำหนดแผนกลยุทธ์ พันธกิจ นโยบายและเป้าหมายการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ พร้อมทั้งจัดทำแบบประเมินความเสี่ยงและรายงานข้อมูลเกี่ยวกับภัยคุกคามทางด้านไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างสม่ำเสมอ
2. พัฒนาและรักษากรอบการดำเนินงานหรือแนวปฏิบัติที่เป็นมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
3. บริหารจัดการความเสี่ยงครอบคลุมระบบสารสนเทศที่อาจมีความเสี่ยงจากภัยคุกคามทางด้านไซเบอร์ พร้อมมาตรการป้องกันความเสี่ยงที่เหมาะสม
4. จัดให้มีการตรวจสอบช่องโหว่ ทดสอบสแกนช่องโหว่ และดำเนินการปิดช่องโหว่ เพื่อสร้างความปลอดภัยให้ระบบ และเฝ้าระวังภัยคุกคามทางด้านไซเบอร์อย่างสม่ำเสมอ
5. กำหนดให้มีมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางด้านไซเบอร์ และมีมาตรการฟื้นฟูความเสียหาย เพื่อให้ระบบและข้อมูลสำคัญของบริษัทฯ สามารถใช้งานในการดำเนินธุรกิจได้อย่างต่อเนื่อง
6. ผู้บริหาร และหน่วยงานที่เกี่ยวข้องต้องให้ความร่วมมือในการดำเนินการป้องกัน รับมือ และลดความเสี่ยงร่วมกับหน่วยงานที่รับผิดชอบทางด้านความมั่นคงปลอดภัยไซเบอร์
7. ส่งเสริมการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ และสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับผู้บริหารและพนักงานอย่างทั่วถึง

8. ผู้บริหาร พนักงาน ผู้รับจ้าง และพนักงานจ้างเหมา (Outsource) ต้องปฏิบัติตามข้อกำหนด ระเบียบ พระราชบัญญัติ และกฎหมายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่เกี่ยวข้องอย่างเคร่งครัด

จึงประกาศมาเพื่อทราบ และถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ 20 ธันวาคม 2562

(นายนพดล ปิ่นสุภา)

กรรมการผู้จัดการใหญ่