บริษัท ไอ.ซี.ซี. อินเตอร์เนชั่นแนล จำกัด (มหาชน)
530 ซอยสาธุประดิษฐ์ 58 แขวงบางโพงพาง เขตยานนาวา กรุงเทพฯ 10120 โทรศัพท์: (02) 293-9000,293-9300
โทรสาร: (02) 294-3024 www.icc.co.th E-mail: webmaster@icc.co.th ทะเบียนเลขที่ 0107537001374

นโยบายความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศ

คณะกรรมการบริษัท ไอ.ซี.ซี.อินเตอร์เนชั่นแนล จำกัด (มหาชน) ให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศ ซึ่งเป็นปัจจัยสำคัญในการสนับสนุนการดำเนินธุรกิจของบริษัท จึงกำหนดให้มีการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศ อย่างมีประสิทธิภาพ สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายอื่นๆ ที่เกี่ยวข้อง และแนวปฏิบัติที่เป็นมาตรฐานสากล

ดังนั้น เพื่อให้บุคลากรของบริษัทรับทราบถึงหน้าที่ ข้อปฏิบัติเกี่ยวกับระบบเทคโนโลยีสารสนเทศอันเป็นความรับผิดชอบร่วมกันของคณะกรรมการบริษัท ผู้บริหาร พนักงาน และบุคคลที่เกี่ยวข้องทุกคน โดยกำหนดแนวทางปฏิบัติ เป็นลายลักษณ์อักษร ดังนี้

1. กำหนดให้ฝ่ายบริหารมีทิศทาง และการสนับสนุนเรื่องความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับต่างๆ รวมถึงเผยแพร่แก่บุคคลที่เกี่ยวข้องทั้งภายใน และภายนอกบริษัททราบ อีกทั้งยังต้องมีการทบทวนอย่างสม่ำเสมอ
2. ให้จัดทำโครงสร้างบริษัท สำหรับบริหารให้เกิดการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศ ในทุกกระบวนการดำเนินงาน และโครงการต่างๆของบริษัท โดยกำหนดหน้าที่ความรับผิดชอบ ช่องทางการติดต่อ ของบุคลากร รวมถึงหน่วยงาน ทั้งภายใน และภายนอกบริษัท ให้มีการควบคุมสิทธิ์การปฏิบัติงานจากระยะไกล และอุปกรณ์คอมพิวเตอร์พกพา
3. ก่อนการจ้างงาน ให้มีการตรวจสอบประวัติ และกำหนดหน้าที่ความรับผิดชอบไว้ในข้อสัญญาของผู้ปฏิบัติงาน และคู่สัญญา ในระหว่างการจ้างงานให้มีการสร้างความตระหนักถึงภัยไซเบอร์ที่ต้องระมัดระวัง รวมถึงโทษทางวินัย หากไม่ปฏิบัติ หรือละเมิด และเมื่อสิ้นสุดการจ้างงาน บริษัทต้องมีการยกเลิกการเข้าถึงสิทธิ์ต่างๆ ทั้งนี้ผู้ปฏิบัติงาน และคู่สัญญา ยังคงมีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศตามที่บริษัทกำหนด
4. ให้จัดหมวดหมู่ทรัพย์สิน และสถานที่สารสนเทศพร้อมทำป้ายบ่งชี้ โดยแบ่งตามข้อกำหนดกฎหมาย ประโยชน์คุณค่า มูลค่า หรือความสำคัญ พร้อมทั้งทำบัญชีทรัพย์สินที่ระบุหมวดหมู่ทรัพย์สิน ผู้รับผิดชอบ ผู้เบิกใช้ และทบทวนอยู่เสมอ เพื่อบริหาร และจัดการสื่อบันทึกข้อมูลที่เหมาะสมต่างๆ เช่น เรียกคืนทรัพย์สินเมื่อสิ้นสุดการจ้างงานหรือสัญญา วิธีการทำลายที่เหมาะสมกับระดับการป้องกันเมื่อยกเลิกใช้งาน

5. จัดให้มีการทำทะเบียน และควบคุมผู้ใช้งาน ครอบคลุมถึงผู้มีสิทธิพิเศษ ที่เข้าถึงสารสนเทศ และบริการเครือข่ายได้เฉพาะส่วนที่ได้รับอนุญาตเท่านั้น ต้องทบทวนอยู่เสมอ โดยผู้ดูแลระบบ รวมถึงผู้พัฒนาระบบ มีหน้าที่รักษาความลับ และควบคุมการเข้าถึงระบบสารสนเทศ และผู้ใช้งานมีหน้าที่รักษาข้อมูลความลับสำหรับการพิสูจน์ตัวตน
6. ให้มีการเข้ารหัสข้อมูล โดยพิจารณาระดับการป้องกันตามนโยบาย และระยะเวลาที่กำหนด พร้อมทั้งทำบัญชีระบบ ที่มีการใช้งาน และการเข้ารหัสข้อมูล
7. ให้มีการจัดทำกระบวนการปฏิบัติ ควบคุมพื้นที่เข้า-ออก สำหรับพื้นที่ควบคุม สำนักงาน และอื่นๆ เพื่อป้องกันความเสียหาย การจารกรรม อันตราย อันเป็นการรบกวนการดำเนินงานของบริษัทรวมถึงจัดวาง ติดตั้ง ป้องกัน และบำรุงรักษาอุปกรณ์สารสนเทศ ให้พร้อมใช้งานอยู่เสมอ
8. ให้จัดทำขั้นตอนปฏิบัติสำหรับการคาดการณ์ทรัพยากรที่ระบบต้องการใช้ การแยกระบบระหว่างการพัฒนากับระบบที่ให้บริการออกจากกัน การจัดการป้องกันโปรแกรมไม่พึงประสงค์ การสำรองข้อมูล การลงบันทึกเหตุการณ์ การบริหารจัดการช่องโหว่ทางเทคนิค การตรวจสอบระบบ และการเฝ้าระวังการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ รวมถึงทบทวนเมื่อมีการเปลี่ยนแปลงกระบวนทำงานที่สำคัญหรือตามรอบเวลาที่นโยบายกำหนด
9. ให้แยกเครือข่ายตามกลุ่มผู้ใช้งาน และระบบสารสนเทศ โดยระบุเครื่องมือความมั่นคงปลอดภัยของแต่ละกลุ่มเครือข่าย การแลกเปลี่ยนสารสนเทศกำหนดให้มีข้อตกลงการแลกเปลี่ยนสารสนเทศ ด้วยวิธีการที่ปลอดภัย และการรักษาความลับ หรือการไม่เปิดเผยข้อมูล ที่เหมาะสมกับระดับความจำเป็นในการป้องกัน
10. ให้กำหนดความปลอดภัยไซเบอร์ เป็นส่วนหนึ่งของความต้องการระบบ พร้อมทั้งจัดทำขั้นตอนปฏิบัติที่ปลอดภัยสำหรับ การพัฒนาระบบขึ้นเอง การจัดซื้อ การจัดจ้าง หรือการใช้เครือข่ายสาธารณะ ให้ครอบคลุมกระบวนการ การจัดหา การพัฒนา การตรวจรับ และการบำรุงรักษา
11. ให้มีข้อตกลงกำหนดความมั่นคงปลอดภัยทางไซเบอร์ และสารสนเทศกับคู่ค้า ที่เกี่ยวข้องกับห่วงโซ่อุปทานของบริการ และผลิตภัณฑ์ โดยพิจารณาข้อกำหนดจากการเข้าถึง การดำเนินงาน การจัดเก็บ และติดต่อสื่อสาร หรือจัดหาส่วนประกอบโครงสร้างพื้นฐานด้านสารสนเทศ รวมถึงให้มีการเฝ้าระวัง ตรวจสอบ ทบทวน และประเมินความเสี่ยงการให้บริการของคู่ค้าอย่างสม่ำเสมอ

12. กำหนดหน้าที่ และขั้นตอนปฏิบัติของผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศ ผู้ปฏิบัติงาน อันประกอบด้วย ผู้บริหารที่เกี่ยวข้อง ผู้ใช้งาน ผู้ดูแลระบบสารสนเทศ ผู้พัฒนาระบบ คู่สัญญา และบุคคลอื่น ๆ ที่เกี่ยวข้องต้องจดบันทึก และรายงานจุดอ่อนความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศ ที่มีในระบบ หรือบริการที่ตนเองใช้งาน รวมถึงรายงานโดยทันทีที่พบเหตุการณ์ หลังเกิดเหตุการณ์ให้ศึกษา และวิเคราะห์แล้วนำความรู้ที่ได้มาป้องกันเหตุที่จะเกิดในอนาคต รวมถึงการบ่งชี้ การเก็บรวบรวม การได้มา และการเก็บรักษาทรัพย์สินสารสนเทศ ซึ่งสามารถใช้เป็นหลักฐานได้
13. จัดให้มีข้อกำหนดการตอบสนองต่อความมั่นคงปลอดภัยไซเบอร์ และการวางแผนการจัดการเพื่อสร้างความต่อเนื่องของการดำเนินธุรกิจ ในสถานการณ์วิกฤต หรือภัยพิบัติ ต้องเตรียมเอกสาร กระบวนการทำงาน ระบบงาน อาทิ ระบบสำรองฉุกเฉิน เพื่อควบคุมความเสียหายให้อยู่ในระดับที่กำหนด ทั้งนี้ให้มีการปรับปรุง และทดสอบดำเนินการอย่างสม่ำเสมอ
14. ระบุข้อกำหนด ระเบียบ ข้อบังคับ มาตรฐาน กฎหมาย และข้อกำหนดทางเทคนิคสำหรับป้องกันข้อมูล โดยเฉพาะข้อมูลส่วนบุคคล จากการสูญหาย ถูกทำลาย ปลอมแปลง เข้าถึง และเปิดเผยที่ไม่ได้รับอนุญาต ลงในขั้นตอนปฏิบัติสำหรับระบบสารสนเทศ ต่างๆที่เกี่ยวข้อง เป็นลายลักษณ์อักษรอย่างชัดเจน ทั้งนี้จำเป็นต้องปรับปรุงให้สอดคล้องกับกฎหมายอยู่เสมอ

นโยบายความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศฉบับนี้ ได้รับอนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 10 เมื่อวันที่ 13 มกราคม พ.ศ. 2566 และมีผลใช้บังคับตั้งแต่วันที่ 15 กุมภาพันธ์ พ.ศ. 2566 เป็นต้นไป

.....

(นายธรรมรัตน์ โชควัฒนา)
กรรมการผู้อำนวยการ และประธานกรรมการบริหาร