บริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน)
Don Muang Tollway Public Company Limited

40/40 ถนนวิภาวดีรังสิต แขวงสนามบิน
เขตดอนเมือง กรุงเทพฯ 10210
โทร : (66) (02) 792-6500
โทรสาร : (66) (02) 552-8065
เลขทะเบียน บมจ. 0107537001129

ISO 9001 & ISO 14001 CERTIFIED

40/40 ViphavadiRangsit Road,
Sanambin, DonMuang, Bangkok 10210
Tel. : (66) (02) 792-6500
Fax. : (66) (02) 552-8065
Plc Registration No. 0107537001129

ขั้นตอนปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber Security Policy)

ตามที่ บริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน) (**"บริษัทฯ"**) ได้ดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และได้อนุมัติใช้เอกสารนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ อย่างเป็นทางการตั้งแต่วันที่ 1 มิถุนายน 2564 ประกอบไปด้วยแนวปฏิบัติเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศซึ่งอ้างอิงมาตรฐานสากล ISO/IEC 27001:2013 จำนวน 15 ข้อ เพื่อให้พนักงานทุกท่านปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศอย่างมีประสิทธิภาพมากยิ่งขึ้น และสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงขอกำหนดขั้นตอนการปฏิบัติสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศเพิ่มเติมที่เกี่ยวข้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ดังนี้

1. การเข้ารหัสและการบริการกุญแจที่ใช้ในการเข้ารหัส (Cryptographic and Key Management)

   <u>ขั้นตอนปฏิบัติ</u>

   1.1 พนักงานจะต้องเข้ารหัสข้อมูลที่อยู่ในระดับชั้นความลับ Confidential (เช่นเอกสารสัญญาต่าง ๆ, เอกสารเทคนิคที่ส่งผลต่อความสามารถในการแข่งขันของบริษัทฯ),Secret (เช่น ข้อมูลที่เกี่ยวกับการประมูลงานเพื่อสรรหาธุรกิจใหม่ แผนการตลาดหรือแผนกลยุทธ์ในแต่ละปี) ไม่ว่าจะเป็นการเก็บรักษาภายในพื้นที่จัดเก็บของบริษัทฯ หรือการจัดส่งไปยังบุคคลอื่นภายนอกเพื่อการปฏิบัติงาน (รายละเอียดของการจัดระดับชั้นความลับอยู่ในนโยบายการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ ส่วนที่ 3 ข้อที่ 8 การบริหารจัดการทรัพย์สินเทคโนโลยีสารสนเทศ)

   1.2 การเข้ารหัสโดยใช้ซอฟต์แวร์มาตรฐาน (Software Standard) ที่ทางฝ่ายเทคโนโลยีสารสนเทศและจราจรอัจฉริยะได้ติดตั้งไว้ที่เครื่องคอมพิวเตอร์โดยมีซอฟต์แวร์ 7zip และ Microsoft Office

   1.3 พนักงานจะต้องจดจำรหัสและจัดเก็บรหัสไว้เป็นอย่างดี หากลืมรหัสการเข้าข้อมูล ฝ่ายเทคโนโลยีสารสนเทศและจราจรอัจฉริยะจะไม่สามารถปลดล็อคข้อมูลดังกล่าวได้

   1.4 พนักงานจะต้องระมัดระวังในการส่งข้อมูลออกไปยังบุคคลอื่นภายนอกบริษัทฯ เพื่อการปฏิบัติงาน ทุกช่องทางไม่ควรส่งรหัสออกภายนอกด้วยช่องทางเดียวกัน เช่น การส่งเมลให้กับบุคคลภายนอก พร้อมแนบไฟล์ที่เข้ารหัสข้อมูลควรจัดส่งรหัสข้อมูลทางช่องทาง Line หรืออีเมลคนละฉบับกัน

2. การใช้งานอุปกรณ์พกพาและการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Device and Teleworking)

ขั้นตอนปฏิบัติ

2.2 พนักงานจะต้องไม่นำอุปกรณ์ Removeable disk (Thumb drive , Flash Drive , External Disk , SSD, อื่นๆ) ที่ไม่ใช่ทรัพย์สินบริษัทฯ หรือนำอุปกรณ์ส่วนตัวมาปลั๊กเข้ากับอุปกรณ์สารสนเทศของบริษัทฯ กรณีได้รับการส่งข้อมูลโครงการฯด้วยอุปกรณ์ Removeable disk พนักงานสามารถร้องขอเพื่อเปิดสิทธิการโอนถ่ายข้อมูลชั่วคราวได้

2.3 พนักงานจะต้องไม่บันทึกหรือจัดเก็บข้อมูลบริษัทฯ ไว้บนอุปกรณ์จัดเก็บข้อมูลแบบพกพาส่วนตัว กรณีต้องการถ่ายโอนข้อมูลจากสื่อบันทึกข้อมูลแบบพกพาส่วนตัว สามารถร้องขอเพื่อเปิดสิทธิชั่วคราวได้

2.4 พนักงานจะต้องไม่นำคอมพิวเตอร์โน๊ตบุ๊คส่วนตัวมาปลั๊กเข้ากับระบบเครือข่ายสารสนเทศของบริษัทฯ

2.5 พนักงานจะต้องไม่นำอุปกรณ์โทรศัพท์มือถือหรือแท็บเล็ต รวมไปถึงอุปกรณ์เคลื่อนที่อื่น ๆ ส่วนตัวมาเชื่อมต่อระบบเครือข่ายสารสนเทศของบริษัทฯ ยกเว้นได้รับการอนุมัติจากผู้บังคับชาเพื่อใช้ในการปฏิบัติงานเท่านั้น

3. การใช้บริการอินเตอร์เน็ตและเครือข่ายไร้สาย Wi-Fi ของบริษัทฯ

3.1 พนักงานจะต้องใช้บริการเครือข่ายอินเตอร์เน็ตและเครือข่ายไร้สาย Wi-Fi เพื่อการปฏิบัติงานเท่านั้นและต้องได้รับการอนุมัติจากผู้บังคับบัญชา

3.2 พนักงานต้องลงทะเบียนผู้ใช้บริการเครือข่ายอินเตอร์และเครือข่ายไร้สาย Wi-Fi เพื่อระบุตัวตนในการเข้าใช้บริการเครือข่ายสารสนเทศของบริษัทฯ

3.3 พนักงานทุกท่านจะต้องกรอกแบบฟอร์มลงทะเบียนผู้ใช้บริการเครือข่ายอินเตอร์เน็ตและเครือข่ายไร้สาย Wi-Fi และขออนุมัติจากผู้บังคับบัญชาตามสายงานใหม่ทั้งหมดเพื่อปรับปรุงข้อมูลในระบบสารสนเทศให้ถูกต้องสมบูรณ์

ขั้นตอนปฏิบัติฉบับนี้มีผลบังคับใช้ในวันที่ 15 มีนาคม 2565 เป็นต้นไป

ประกาศ ณ วันที่ 2 มีนาคม 2565

(นายธานินทร์ พานิชชีวะ)

กรรมการผู้จัดการ