CENTRALRETAIL

นโยบายและพันธกิจด้านความปลอดภัยของเทคโนโลยีสารสนเทศ

บริษัท เซ็นทรัล รีเทล คอร์ปอเรชั่น จำกัด (มหาชน)

15 ธันวาคม 2564

นโยบายและพันธกิจด้านความปลอดภัยเทคโนโลยีสารสนเทศ

บริษัท เซ็นทรัล รีเทล คอร์ปอเรชั่น จำกัด (มหาชน) ("บริษัทฯ") ได้เล็งเห็นถึงความสำคัญของการบริหารจัดการองค์กร เพื่อขับเคลื่อนขยายธุรกิจ ฐานะการเงินให้มั่นคง และสร้างผลตอบแทนที่เหมาะสมต่อผู้ถือหุ้น ตลอดจนการปฏิบัติตามหลักบรรษัทภิบาลที่ดี และหลักการตรวจสอบและถ่วงดุลในสภาพแวดล้อมการแข่งขันทางธุรกิจที่บริษัทฯ เผชิญอยู่ในปัจจุบันซึ่งได้เปลี่ยนแปลงไปตามกาลเวลา ทั้งจากปัจจัยภายนอกหรือปัจจัยภายในที่ส่งผลต่อความสามารถของบริษัทฯ ในการบรรลุพันธกิจตามเป้าหมายที่วางไว้

เพื่อให้มั่นใจว่า บริษัทฯ สามารถบรรลุมาตรฐานการป้องกันตามที่ลูกค้า ผู้ถือหุ้น และผู้มีส่วนได้เสียที่ได้คาดหวัง บริษัทฯ จึงนำมาตรฐานสากล อาทิ ISO 27001, NIST, CSF และ CIS มาเป็นส่วนหนึ่งของโปรแกรมความปลอดภัยทางสารสนเทศแบบไฮบริดของเรา เพื่อจัดการกับความเสี่ยงและการปกป้องข้อมูล และระบบหลักๆ ของบริษัทฯ ดังนั้นจึงเห็นสมควรให้กำหนดนโยบายและพันธกิจด้านเทคโนโลยีสารสนเทศขึ้น

1. คำนิยาม

1.1. "บริษัทย่อย" หมายถึง บริษัทย่อยตามคำนิยามที่ระบุไว้ในประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ กจ. 17/2551 เรื่อง การกำหนดบทนิยามในประกาศเกี่ยวกับการออกและเสนอขายหลักทรัพย์ (รวมทั้งที่แก้ไขเพิ่มเติม) ที่ประกอบธุรกิจหลักตามประกาศคณะกรรมการกำกับตลาดทุนที่ กจ. 39/2559 เรื่อง การขออนุญาตและการอนุญาตให้เสนอขายหุ้นที่ออกใหม่ (รวมทั้งที่แก้ไขเพิ่มเติม) ที่มีอยู่ในขณะนี้ หรือในอนาคต

1.2. "บริษัทฯ" หมายถึง บริษัท เซ็นทรัล รีเทล คอร์ปอเรชั่น จำกัด (มหาชน)

1.3. "บุคคล" หมายถึง บุคคลธรรมดา

1.4. "บุคลากรของบริษัทฯ" หมายถึง กรรมการ ผู้บริหาร พนักงานประจำ พนักงานชั่วคราว และพนักงานสัญญาจ้างของบริษัทฯ หรือบริษัทย่อย

1.5. "หน่วยธุรกิจ" หมายถึง หน่วยธุรกิจ(Business Unit)ต่างๆ ของบริษัทฯ และ/หรือบริษัทย่อย ที่มีอยู่ในขณะนี้หรือในอนาคต

2. นโยบายและพันธกิจด้านเทคโนโลยีสารสนเทศ

2.1. บริษัทฯ ถือว่าพันธกิจด้านเทคโนโลยีสารสนเทศของบริษัทฯ เป็นปัจจัยเกื้อหนุนที่มีคุณค่าของบริษัทฯ ในการสร้างเสริมความมั่นคงของบริษัทและบริษัทย่อย ดังนั้นพันธกิจด้านเทคโนโลยีสารสนเทศของบริษัทฯ จึงถือเป็นพันธกิจที่สำคัญของบริษัทฯ

2.2. บริษัทฯ จะดำเนินการต่างๆ ดังนี้:

2.2.1. รักษาความลับ ความถูกต้อง และความพร้อมใช้งานตามวัตถุประสงค์

(ก). การรักษาความลับ หมายถึง การปกป้องทรัพยากรสารสนเทศ และข้อมูลต่างๆ จากการเข้าถึงโดยไม่ได้รับอนุญาต (เช่น การเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ)

(ข). ความสมบูรณ์ หมายถึง ความสมบูรณ์ของอุปกรณ์เกี่ยวข้องกับการรักษาฟังก์ชั่นของทรัพยากรสารสนเทศ (เช่น การถูกคัดลอกข้อมูลโดยทุจริต หรือไม่มีสิทธิ)

(ค). ความพร้อมใช้งาน หมายถึง การปกป้องทรัพยากรสารสนเทศจากการหยุดชะงักโดยไม่ได้ตั้งใจ (เช่น การปฏิเสธบริการ)

2.2.2. จัดให้มีความรับผิดชอบร่วมกัน

(ก). การรักษาระดับความปลอดภัยทางสารสนเทศที่ดีทั่วทั้งกลุ่ม เป็นผลประโยชน์ และสิ่งที่บริษัทฯ ต้องการจากบุคลากรของบริษัทฯ ทุกท่าน

(ข). บุคลากรของบริษัทฯ ทุกท่านต้องรับผิดชอบในการปกป้องทรัพยากรสารสนเทศที่อยู่ภายใต้การควบคุมของตน เช่น ความรับผิดชอบในการปกป้องข้อมูลส่วนบุคคล รหัสผ่าน และข้อมูลที่ละเอียดอ่อน ฯลฯ

(ค). ฝ่ายบริหารไซต์/แผนก/สำนักงาน/หน่วยงานมีหน้าที่รักษาระดับความปลอดภัยทางสารสนเทศให้บรรลุ “มาตรฐานความปลอดภัยขั้นต่ำ” เป็นอย่างน้อย

(ง). จัดให้มีรายละเอียดคู่มือ หรือแนวปฏิบัติ เกี่ยวกับมาตรฐานความปลอดภัยขั้นต่ำได้กำหนดไว้ในเอกสาร

2.2.3. แนวทางการป้องกันตามความเสี่ยง บริษัทฯ จะดำเนินการ

(ก). จัดการสภาพแวดล้อมทางสารสนเทศที่ทันสมัยทั่วทั้งกลุ่ม โดยให้ความสำคัญเท่าเทียมกันจากความเสี่ยงที่ไม่จำเป็น รวมถึงทรัพยากรสารสนเทศ และข้อมูลสำหรับการดำเนินงาน

(ข). สร้างความสมดุลระหว่างการเปิดกว้างและการควบคุม ตลอดจนต้นทุนและผลประโยชน์

(ค). นำแนวทางการรักษาความปลอดภัยทางสารสนเทศที่มีประสิทธิภาพมาใช้ เพื่อปกป้องความเสี่ยง รวมถึงมีการแบ่งชั้นข้อมูลออกเป็นระดับ หรือประเภทความเสี่ยงที่แตกต่างกัน ระดับที่ของการป้องกัน ที่จะกำหนดชั้นก็จะแตกต่างไปตามความเสี่ยงนั้นๆ

2.2.4. จัดให้มีการการป้องกันในเชิงลึก

จัดให้มีการลดความเสี่ยงให้มีประสิทธิภาพมากขึ้น ด้วยการใช้มาตรการหลายอย่างในระดับต่างๆ ดังต่อไปนี้ (แต่ไม่จำกัดเพียง):

(ก). เครือข่าย – แยกตามความเสี่ยง การตรวจจับการบุกรุก การต่อต้านการปฏิเสธบริการ ฯลฯ

(ข). เซิร์ฟเวอร์ – การจัดการช่องโหว่ การรักษาความปลอดภัยทางกายภาพ ฯลฯ

(ค). อุปกรณ์ปลายทาง – การตอบสนองการตรวจจับปลายทาง (EDR)/การป้องกันไวรัส (AV), การปิดช่องโหว่, การรักษาความปลอดภัยทางกายภาพ ฯลฯ

(ง). ระบบการใช้งาน – มาตรฐานการพัฒนา การประเมินช่องโหว่ การทดสอบการเจาะ ฯลฯ

(จ). ข้อมูล - การเข้ารหัส การป้องกันข้อมูลสูญหาย ฯลฯ

(ฉ). บุคคล – ความตระหนัก ความคิดไปในทางเดียวกัน และทักษะ ฯลฯ ตัวอย่างของการป้องกันที่มีประสิทธิภาพในเชิงลึก คือสถานการณ์ที่ผู้ใช้งานมีความคำนึงที่จะไม่เปิด

(ช). ไฟล์แนบอีเมลที่น่าสงสัยแม้ว่าการป้องกัน EDR/AV จะมีอยู่แล้วที่ End-Point, Network

(ซ). กำหนดระดับการเข้าถึงเซิร์ฟเวอร์

2.2.5. จัดให้มีแบบองค์รวมสำหรับขั้นตอนต่างๆ ในวัฏจักรของข้อมูล

ความก้าวหน้าอย่างรวดเร็วในด้านสารสนเทศทำให้วงจรชีวิตของทรัพยากรสารสนเทศค่อนข้างสั้นลง ตั้งแต่การสร้าง การปรับใช้ ไปจนถึงการหมดอายุของข้อมูล การปกป้องทรัพยากรข้อมูลสารสนเทศควรเชื่อมโยงกับขั้นตอนต่างๆ ในวงจรชีวิตด้วย ตัวอย่างเช่น การป้องกันความปลอดภัยทางสารสนเทศสำหรับระบบแอพพลิเคชั่นหรือทรัพยากรสารสนเทศอื่นๆ ควรถูกฝังอยู่ในวงจรที่เกี่ยวข้องตั้งแต่การเริ่มต้นโครงการไปจนถึงการกำจัด

2.2.6. จัดเตรียมแผน หรือแนวทางการรับมือกับเหตุการณ์ให้มีประสิทธิภาพ

บริษัทฯ ถือว่ามีความสำคัญอย่างยิ่งในบริษัทฯ ที่จะมีการจัดการเหตุการณ์ด้านความปลอดภัยที่มีประสิทธิภาพ เพื่อ

(ก). ตรวจสอบให้แน่ใจว่าบริษัทฯ สามารถลดการฉ้อโกงได้อย่างมีประสิทธิภาพในขณะที่ยังคงปฏิบัติตามกฎหมายและ

(ข). ภาระผูกพันด้านกฎระเบียบ รายละเอียดของ SOC (Security Operations Center) มีรายละเอียดโครงสร้างและนำไปใช้ได้ในนโยบายการรักษาความปลอดภัยของข้อมูลภายในฉบับเต็ม

3. การบังคับใช้ และการจัดการ

3.1. สร้างเสริมความสำนึกในการรับผิดชอบด้านเทคโนโลยีสารสนเทศ ให้แก่ คู่ค้า บุคลากรของบริษัทฯ ของแต่ละหน่วยธุรกิจด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรของบริษัทฯ เป็นประจำ

3.2. กำหนดสิทธิ และข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนของบุคลากรของบริษัทฯ ของหน่วยธุรกิจของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึก รวมทั้งการทำสำรองข้อมูลของการเข้าถึง หรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสม หรือตามระยะเวลาที่กฎหมายบัญญัติไว้

3.3. ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของแต่ละหน่วยธุรกิจอย่างน้อยปีละ หนึ่ง (1) ครั้ง

3.4. เพื่อให้บรรลุผลตามนโยบายและพันธกิจด้านเทคโนโลยีสารสนเทศนี้ กรรมการบริหาร หรือประธานเจ้าหน้าที่บริหารอาจแต่งตั้งบุคคลใดบุคคลหนึ่ง หรือให้คณะกรรมการและพันธกิจด้านเทคโนโลยีสารสนเทศ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศของแต่ละหน่วยธุรกิจ หรือให้ผู้ควบคุมความปลอดภัยข้อมูล เป็นผู้รับผิดชอบ ประเมินผลจัดการ และกำกับการปฏิบัติตามนโยบายนี้ก็ได้

นโยบายและพันธกิจด้านเทคโนโลยีสารสนเทศนี้ให้มีผลใช้บังคับตั้งแต่ วันที่ 15 ธันวาคม 2564 เป็นต้นไป

- ลงนาม -

(ดร.ประสาร ไตรรัตน์วรกุล)

ประธานกรรมการบริษัท

บริษัท เซ็นทรัล รีเทล คอร์ปอเรชั่น จำกัด (มหาชน)