การบริหารงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์

คณะกรรมการบริษัท ได้มอบหมายให้ คณะกรรมการบริหารความเสี่ยง บรรษัทภิบาล และความยั่งยืน ทำหน้าที่กำกับดูแลและให้คำปรึกษาการดำเนินงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ ผ่านกรรมการผู้จัดการ เพื่อความคล่องตัวและประสิทธิภาพสูงสุดในการดำเนินงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

นโยบาย

บริษัทฯ ตระหนักถึงความสำคัญของการบริหารงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ จึงได้กำหนดนโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศของบริษัทฯ เป็นลายลักษณ์อักษร เพื่อเป็นแนวทางให้ยึดถือปฏิบัติในการบริหารจัดการบริหารงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

นโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ

โดยมีรายละเอียดตามที่เผยแพร่บนเว็บไซต์
https://www.ttwplc.com/th/about-ttw/company-policy#tab-governance-7

เป้าหมาย ปี 2568

เป้าหมาย	ดัชนีชี้วัด
1.พนักงานและผู้บริหารทุกคนได้รับการสื่อสารและรับทราบนโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ	ร้อยละ 100
2.พนักงานและผู้บริหารทุกคนได้รับการอบรมการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ	ร้อยละ 100
3.การละเมิด/รั่วไหลข้อมูลทางธุรกิจขององค์กร	0 กรณี
4.ข้อร้องเรียนเกี่ยวกับการละเมิด/รั่วไหลข้อมูลทางธุรกิจขององค์กร	0 กรณี

หมายเหตุ: ผู้มีส่วนได้ส่วนเสีย ได้แก่ พนักงาน ผู้ถือหุ้น/นักลงทุน ลูกค้า คู่ค้า/ผู้ส่งมอบ/ผู้รับเหมา ชุมชน และหน่วยงานรัฐ/สิ่งแวดล้อม

เป้าหมายระยะยาว

เป้าหมาย	ดัชนีชี้วัด
1.พนักงานและผู้บริหารทุกคนได้รับการสื่อสารและรับทราบนโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ	ร้อยละ 100
2.พนักงานและผู้บริหารทุกคนได้รับการอบรมการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ	ร้อยละ 100
3.การละเมิด/รั่วไหลข้อมูลทางธุรกิจขององค์กร	0 กรณี
4.ข้อร้องเรียนเกี่ยวกับการละเมิด/รั่วไหลข้อมูลทางธุรกิจขององค์กร	0 กรณี

หมายเหตุ: ผู้มีส่วนได้ส่วนเสีย ได้แก่ พนักงาน ผู้ถือหุ้น/นักลงทุน ลูกค้า คู่ค้า/ผู้ส่งมอบ/ผู้รับเหมา ชุมชน และหน่วยงานรัฐ/สิ่งแวดล้อม

ผลการดำเนินงาน

การดำเนินงาน	ผลลัพธ์		
	ปี 2566	ปี 2567	ปี 2568
1.พนักงานและผู้บริหารทุกคนได้รับการสื่อสารและรับทราบนโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ	ร้อยละ 100	ร้อยละ 100	ร้อยละ 100
2.พนักงานและผู้บริหารทุกคนได้รับการอบรมการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ	ร้อยละ 100	ร้อยละ 100	ร้อยละ 100
3.การละเมิด/รั่วไหลข้อมูลทางธุรกิจขององค์กร	0 กรณี	0 กรณี	0 กรณี
4.ข้อร้องเรียนเกี่ยวกับการละเมิด/รั่วไหลข้อมูลทางธุรกิจขององค์กร	0 กรณี	0 กรณี	0 กรณี

หมายเหตุ: ผู้มีส่วนได้ส่วนเสีย ได้แก่ พนักงาน ผู้ถือหุ้น/นักลงทุน ลูกค้า คู่ค้า/ผู้ส่งมอบ/ผู้รับเหมา ชุมชน และหน่วยงานรัฐ/สิ่งแวดล้อม

การเปลี่ยนแปลงและพัฒนาการที่สำคัญเกี่ยวกับการทบทวนนโยบาย แนวปฏิบัติการบริหารงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ ในรอบปีที่ผ่านมา

ในปี 2568 บริษัทฯ ได้ดำเนินการเปลี่ยนแปลงและพัฒนาการที่สำคัญเกี่ยวกับการบริหารงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้

1. ปรับปรุงนโยบายการใช้งาน Password และการใช้งาน Multi-Factor Authentication (MFA) ให้ครอบคลุมผู้ใช้งานทั้งบริษัท
2. ปรับปรุงคู่มือการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันและเสริมสร้างความมั่นคงปลอดภัยทางด้านไซเบอร์ให้รัดกุมมากขึ้น
3. สร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ให้กับผู้ใช้งานด้วยการประสานงานกับส่วนทรัพยากรบุคคลในการจัดอบรมเรื่อง Cybersecurity Awareness
4. เปิดใช้งาน Microsoft Defender EDR เพื่อตรวจจับและตอบสนองต่อภัยคุกคาม

แนวทางการดำเนินงาน

ความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรถือเป็นประเด็นสำคัญที่อาจก่อให้เกิดผลกระทบต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร เช่น โอกาสในการเกิดผลกระทบต่อความปลอดภัยในการดำเนินงาน ระบบการทำงานล่ม รวมถึงโอกาสในการละเมิดข้อมูลส่วนบุคคลทั้งของพนักงาน ลูกค้า และคู่ค้า/ผู้ส่งมอบ/ผู้รับเหมา

บริษัทฯ จึงนำระบบเทคโนโลยีสารสนเทศมาเป็นเครื่องมือสำคัญในการตอบสนองต่อความคาดหวังและความต้องการของผู้มีส่วนได้ส่วนเสีย โดยการมีแนวปฏิบัติ เครื่องมือ และกรอบการดำเนินงานและมาตรฐานที่ทันสมัย มีประสิทธิภาพ มีการบริหารความเสี่ยงและให้ความสำคัญกับระบบความปลอดภัยสอดคล้องตามมาตรฐานสากลและเป็นไปตามข้อกำหนดของรัฐ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 การบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพื่อให้สามารถรองรับการขยายธุรกิจตามกลยุทธ์องค์กรและป้องกันการละเมิดสิทธิของผู้มีส่วนได้ส่วนเสียจากการใช้ข้อมูลส่วนบุคคลในทางที่ไม่ถูกต้อง

การบริหารระบบการจัดการความปลอดภัยของข้อมูลตามมาตรฐานสากล

1. บริษัทฯ มีการประเมินประสิทธิภาพของนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง ในระบบการตรวจสอบของ ISO 9001 จากหน่วยงานตรวจสอบภายในและผู้ตรวจสอบภายนอก เพื่อปรับปรุงแก้ไขข้อบกพร่องของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ
2. บริษัทฯ มีผู้เชี่ยวชาญทางด้านระบบจากภายนอกเข้ามาตรวจสอบระบบและปรับปรุงแก้ไขอย่างน้อย ปีละ 2 ครั้ง ตามสัญญาการบำรุงรักษาระบบ

การควบคุมและการปฏิบัติด้านความปลอดภัยของข้อมูล

1. แผนความต่อเนื่องทางธุรกิจกรณีภัยคุกคามทางไซเบอร์

บริษัทฯ ให้ความสำคัญกับการบริหารความเสี่ยงด้านไซเบอร์เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่องแม้ในสถานการณ์ที่เกิดภัยคุกคามหรือการโจมตีทางไซเบอร์ โดยบริษัทฯ มีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ที่ครอบคลุม และเชื่อมโยงกับแผนฟื้นฟูระบบไอที (Disaster Recovery Plan: DRP) และ แผนตอบสนองเหตุการณ์ด้านไซเบอร์ (Incident Response Plan: IRP)

แผนทั้งหมดถูกออกแบบให้สามารถทำงานร่วมกันภายใต้กระบวนการบริหารเหตุการณ์ (Incident Management Process) เพื่อรับมือและลดผลกระทบจากการโจมตีระบบหรือเหตุขัดข้องทางไอที พร้อมทั้งมีการซ้อมตามแผน DRP อย่างน้อยปีละ 1 ครั้ง และทบทวนปรับปรุง BCP & IRP อย่างต่อเนื่อง

นอกจากนี้ บริษัทฯ ยังมีมาตรการด้านความมั่นคงปลอดภัยและการควบคุมความเสี่ยงที่เข้มงวด เพื่อให้การดำเนินธุรกิจมีความต่อเนื่อง และสอดคล้องกับข้อกำหนดของกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และแนวทางตามมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ (NIST CSF)

บริษัทฯ ให้ความสำคัญอย่างยิ่งต่อความสามารถในการดำเนินธุรกิจอย่างต่อเนื่อง แม้ในสถานการณ์ที่ไม่คาดคิด โดยได้จัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) ที่ครอบคลุมถึงเหตุการณ์สำคัญต่าง ๆ ที่อาจกระทบต่อการดำเนินงานและความมั่นคงปลอดภัยของข้อมูล ทั้งในด้านกายภาพและทางไซเบอร์ ดังนี้

กรณี/เหตุการณ์	มาตรการ
1.1 กรณีเกิดเหตุไฟดับหรือไฟไหม้ (Blackout หรือ Fire Incident) บริษัทมีแนวทางและกระบวนการปฏิบัติที่ชัดเจน เพื่อรองรับเหตุการณ์ฉุกเฉิน เช่น ไฟฟ้าดับหรือไฟไหม้ ซึ่งอาจส่งผลต่อการให้บริการหรือระบบที่สำคัญขององค์กร	▪ การสลับระบบไปยังแหล่งพลังงานสำรอง หรือระบบไฟฟ้าฉุกเฉินในศูนย์ข้อมูล ▪ การใช้งาน ศูนย์ข้อมูลสำรอง (Disaster Recovery Site) โดยอัตโนมัติเมื่อระบบหลักไม่สามารถให้บริการได้ ▪ แนวทางการอพยพบุคลากรออกจากพื้นที่ที่เกิดเหตุอย่างปลอดภัย ▪ การประสานงานกับผู้ดูแลอาคารและหน่วยงานฉุกเฉินภายนอก ▪ การจัดฝึกซ้อมแผนอพยพ และตรวจสอบความพร้อมด้านความปลอดภัยอย่างสม่ำเสมอ
1.2 กรณีเกิดภัยคุกคามด้านความมั่นคงปลอดภัยของข้อมูล (Information Security Threats) บริษัทมีการจัดทำแผนตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Response Plan: IRP) ซึ่งบูรณาการเข้ากับแผน BCP และ DRP อย่างเป็นระบบ เพื่อรับมือกับภัยคุกคามที่เกี่ยวข้องกับระบบสารสนเทศ เช่น การโจมตีด้วย Ransomware, การรั่วไหลของข้อมูล, การเข้าถึงโดยไม่ได้รับอนุญาต หรือการหยุดชะงักของบริการ	▪ การบริหารเหตุการณ์ผ่านศูนย์ SOC (Security Operations Center) ร่วมกับทีมไอทีและหน่วยงานที่เกี่ยวข้อง ▪ การตรวจจับ ควบคุมความเสียหาย และฟื้นฟูระบบที่ได้รับผลกระทบอย่างรวดเร็ว ▪ การสื่อสารภายในเพื่อประสานงาน และการแจ้งเตือนผู้มีส่วนได้ส่วนเสียตามแผนที่กำหนด ▪ การปฏิบัติตามกฎหมายและข้อบังคับ เช่น การแจ้งเหตุรั่วไหลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ▪ ปรับปรุงแผน BCP/DRP/IRP ให้เป็นปัจจุบัน

2. การวิเคราะห์ช่องโหว่ด้านความมั่นคงปลอดภัยของข้อมูล

กรณี/เหตุการณ์	มาตรการ
2.1 การประเมินช่องโหว่ระบบงานทั่วไป (Vulnerability Assessment)	▪ ระบบเทคโนโลยีสารสนเทศของบริษัท มีการใช้งานฟีเจอร์ Vulnerability Management ซึ่งเป็นฟังก์ชั่นตรวจจับช่องโหว่โดยอัตโนมัติของ Microsoft Defender
2.2 การทดสอบความมั่นคงปลอดภัยของระบบงานสำคัญ (Penetration Testing)	▪ การทดสอบการเจาะระบบโดยผู้เชี่ยวชาญ ยังไม่มีการดำเนินการในปี 2568 โดยจะดำเนินการทดสอบตามแผนงานในปี 2570
2.3 การจัดอันดับความมั่นคงปลอดภัยของเว็บไซต์ (Security Rating)	▪ ดำเนินการประเมินระดับความปลอดภัยของเว็บไซต์เป็นประจำ โดยประสานงานกับผู้ให้บริการ Hosting เพื่อตรวจสอบความเสี่ยงและปรับปรุงระบบให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยของบริษัทฯ

3. การตรวจสอบภายใน

บริษัทฯ ให้ความสำคัญต่อการบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของข้อมูลในทุกกระบวนการที่เกี่ยวข้อง โดยดำเนินการตามมาตรฐานสากลที่ได้รับการยอมรับ เพื่อเสริมสร้างความมั่นใจในการให้บริการทั้งภายในและภายนอกองค์กรและการดำเนินงานเป็นไปตามมาตรฐาน, นโยบาย และกฎหมายที่เกี่ยวข้อง จึงได้มีการจัดทำการตรวจสอบภายในเป็นประจำอย่างสม่ำเสมอโดยการตรวจสอบภายใน (Internal Audits) ดำเนินการ 1 ครั้ง ในเดือนมกราคม และ ตรวจสอบโดยบุคคลภายนอกในเดือนกรกฎาคม โดยการตรวจสอบจะดำเนินการภายใต้ขอบเขตมาตรฐาน ISO 9001 จากจำนวนระบบ IT ทั้งหมด 3 บริการ คือ Microsoft 365, Business Plus และ โครงสร้างพื้นฐานด้านสารสนเทศ

4. การตรวจสอบโดยหน่วยงานภายนอกอิสระ

บริษัทฯ ให้ความสำคัญต่อการบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของข้อมูลในทุกกระบวนการที่เกี่ยวข้อง โดยดำเนินการตามมาตรฐานสากลที่ได้รับการยอมรับ เพื่อเสริมสร้างความมั่นใจในการให้บริการทั้งภายในและภายนอกองค์กร

บริษัทฯ ได้มอบหมายให้ที่ปรึกษาผู้เชี่ยวชาญและหน่วยงานผู้ตรวจประเมินจากภายนอกเข้ามาดำเนินการตรวจสอบ ทบทวน และให้ข้อเสนอแนะในการปรับปรุงอย่างต่อเนื่อง จนนำไปสู่การผ่านการรับรองมาตรฐานที่เกี่ยวข้อง ดังนี้:

4.1 มาตรฐาน ISO 9001

4.2 มาตรฐาน ISO 14001

5. กระบวนการรายงานและส่งต่อเหตุการณ์

พนักงานและผู้ใช้งานสามารถแจ้งเหตุการณ์ที่น่าสงสัยหรือปัญหาด้านความมั่นคงปลอดภัยสารสนเทศ ผ่านช่องทางที่บริษัทฯ กำหนด ได้แก่ Hotline Call 02-0199490 ต่อ 3142-3144 หรืออีเมลถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ttw_pdpa@ttwplc.com หรือผู้ดูแลระบบความปลอดภัยไซเบอร์ support@ttwplc.com

ข้อมูลที่ได้รับจะถูกบันทึกในระบบจัดการเหตุการณ์ (Incident Management System) และส่งต่อให้หน่วยงานที่รับผิดชอบ รวมถึงทีมบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อดำเนินการตรวจสอบ วิเคราะห์ และแก้ไขปัญหาอย่างเร่งด่วน เมื่อเหตุการณ์ได้รับการจัดการเรียบร้อยแล้ว จะดำเนินการตามขั้นตอนหลังเหตุการณ์ตามแผนที่กำหนด เช่น จัดทำรายงานติดตามผล และประชุมถอดบทเรียนเพื่อป้องกันการเกิดซ้ำ

การป้องกันภัยคุกคามต่อทรัพย์สิน ข้อมูล และระบบสารสนเทศ

บริษัทฯ ได้ดำเนินการตามนโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ ซึ่งมีการดูแลอย่างครอบคลุม ดังนี้

1. ความรับผิดชอบด้านความปลอดภัย (Security Responsibilities) บริษัทฯ จะต้องให้มีการแบ่งหน้าที่ความรับผิดชอบที่ชัดเจนในการพัฒนา การนำไปใช้ และการติดตามเกี่ยวกับความปลอดภัยสารสนเทศ ตลอดจนมีการปรับปรุงการทำงานให้ดียิ่งขึ้น

2. การแบ่งประเภทของสินทรัพย์และการควบคุม (Asset Classification and Control) บริษัทฯ จะต้องจัดให้มีการทำทะเบียนทรัพย์สินทุกประเภท ทั้งสินทรัพย์ที่มีตัวตน และทรัพย์สินที่ไม่มีตัวตน พร้อมทั้งมีการมอบหมายความเป็นเจ้าของในทรัพย์สินดังกล่าวให้หน่วยงานที่เกี่ยวข้อง โดยเจ้าของทรัพย์สินจะต้องรับผิดชอบในการปฏิบัติตามแนวการปฏิบัติความปลอดภัย เพื่อให้มีการควบคุมที่เหมาะสมในการนำทรัพย์สินต่างๆ ของบริษัทฯ ไปใช้งาน

3. ความปลอดภัยด้านบุคลากร (Personnel Security) บริษัทฯ จะต้องจัดให้มีมาตรการในการควบคุมที่เหมาะสมเพื่อให้มั่นใจได้ว่าพนักงาน คู่สัญญา และที่ปรึกษาที่จ้างมาทำงานให้บริษัทฯ มีความตระหนักและให้ความสำคัญตลอดจนการปฏิบัติเกี่ยวกับความปลอดภัยด้านสารสนเทศที่ดีพอ

4. ความปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security) บริษัทฯ จะต้องจัดให้มีมาตรการในการควบคุมเกี่ยวกับความปลอดภัยด้านกายภาพและสภาพแวดล้อมตามความเหมาะสมกับคุณค่าของทรัพย์สินที่บริษัทฯ มีอยู่

5. การจัดการระบบสื่อสารและการดำเนินการ (Communications and Operations Management) บริษัทฯ จะต้องจัดให้มีการนำระบบงาน และระบบเครือข่ายเทคโนโลยีสารสนเทศไปใช้งาน เพื่อความมั่นใจว่าระบบดังกล่าวจะสามารถใช้งานได้ตามหลัก 3 ประการ คือ
   - 5.1 ระบบพร้อมที่จะเรียกใช้งานได้เมื่อต้องการ
   - 5.2 ระบบจะสามารถเข้าถึงได้โดยผู้ที่มีสิทธิ์เท่านั้น
   - 5.3 ระบบมีความถูกต้อง น่าเชื่อถือ โดยระบบดังกล่าวจะต้องได้มาตรฐานของการปฏิบัติงานที่ได้รับการยอมรับเป็นไปตามข้อกำหนดต่างๆ ของบริษัทฯ

6. การควบคุมการเข้าถึงข้อมูล (Access Controls) บริษัทฯ จะต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลในทุกระบบงาน และระบบเครือข่ายของบริษัทอย่างปลอดภัย โดยให้เจ้าของทรัพย์สินเป็นผู้รับผิดชอบในการตัดสินใจอนุญาตให้มีการเข้าถึงข้อมูล

7. การพัฒนาและการดูแลระบบงาน (Systems Development and Management) บริษัทฯ จะต้องจัดให้มีการประเมินความเสี่ยงของระบบงาน และระบบเครือข่ายที่มีจัดหาใหม่ รวมทั้งเมื่อมีการเปลี่ยนแปลงอย่างมีนัยยะสำคัญต่อระบบปัจจุบัน โดยที่หน้าที่งานเกี่ยวกับความปลอดภัยของระบบดังกล่าว ให้ถือเป็นส่วนหนึ่งของกระบวนการพัฒนาระบบงานและระบบเครือข่าย

8. การจัดการเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ (Information Security Incident Management) บริษัทฯ จะต้องมั่นใจได้ว่าเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และจุดอ่อนที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ ได้รับการรายงานไปยังผู้ที่เกี่ยวข้องและมีกระบวนการรองรับการแก้ไขปัญหาได้อย่างทันท่วงที อีกทั้งมีการติดตามและทบทวนเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าการบริหารจัดการความเสี่ยงที่มีประสิทธิภาพ เพื่อลดผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ

9. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) บริษัทฯ มีการกำหนดมาตรฐานการควบคุมการใช้บริการอย่างเหมาะสม รวมทั้งมีการจัดทำสัญญาอย่างเป็นลายลักษณ์อักษร ซึ่งระบุเงื่อนไขการให้บริการมาตรฐานของการปฏิบัติงานขั้นต่ำ และการรักษาความปลอดภัยของข้อมูล (ขั้นตอนการควบคุม IT Outsourcing)

มาตรการดูแลรับมือกรณีเกิดการคุกคามทางไซเบอร์

บริษัทฯ มีการจัดทำแผนการบริหารจัดการเหตุการณ์ไม่ปกติ (Incident Management) โดยแผนกเทคโนโลยีสารสนเทศ จะเน้นไปในส่วนของการทำงานทางด้านเทคโนโลยีสารสนเทศ ว่าจะสามารถจัดการกับปัญหาที่เกิดขึ้นได้อย่างไรให้สามารถกลับคืนสู่สภาวะปกติให้ได้เร็วที่สุด

การรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์

ปัจจุบันเทคโนโลยีและระบบสารสนเทศ เป็นเครื่องมือสำคัญต่อการขับเคลื่อนธุรกิจและองค์กรให้มีความก้าวหน้าและรวดเร็ว รวมทั้งการเปลี่ยนแปลงธุรกิจให้เข้าสู่สังคมดิจิทัล (Transformation) ทำให้ธุรกิจและองค์กรเหล่านั้นต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มากขึ้น การรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ จึงมีบทบาทที่สำคัญต่อธุรกิจและองค์กรเป็นอย่างมาก การมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ที่มีความรัดกุมต่อระดับความเสี่ยง เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์รวมถึงการบริหารความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือเทคโนโลยีสารสนเทศ เพื่อช่วยเพิ่มความมั่นใจและมั่นคงต่อผู้ใช้บริการทั้งภาครัฐและภาคประชาชน

การบริหารความเสี่ยงด้านการจัดการข้อมูลและระบบเทคโนโลยีสารสนเทศ

การจัดการบริหารความเสี่ยงด้านการจัดการข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ มีทั้งในส่วนของการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance : PM) อาทิเช่น การมีระบบป้องกันการบุกรุกทางคอมพิวเตอร์ (Fire Wall) และโปรแกรมการป้องกันไวรัส (Antivirus) รวมทั้งการกำหนดนโยบาย (Policy) ในการเข้าถึงข้อมูลที่สำคัญของบริษัทฯ ในส่วนของการบำรุงรักษาเชิงแก้ไขปรับปรุง (Corrective Maintenance) มีการสำรองข้อมูล (Backup Solution) ในการกู้คืนข้อมูล รวมทั้งการทำประกันตัวชุดอุปกรณ์ที่สำคัญที่สามารถเปลี่ยนตัวใหม่หรือทดแทนตัวที่ชำรุด ภายใน 24 ชั่วโมง

บริษัทฯ ให้ความสำคัญต่อการดูแลความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ และการป้องกันภัยคุกคามทางไซเบอร์ จึงกำหนดให้ประเด็นความเสี่ยงด้านความปลอดภัยของข้อมูลจากการโจมตีทางไซเบอร์ในรูปแบบที่เปลี่ยนแปลงไปเป็นความเสี่ยงที่เกิดขึ้นใหม่ ซึ่งได้ระบุรายละเอียดเกี่ยวกับประเด็นความเสี่ยง ผลกระทบต่อองค์กรหรือผู้มีส่วนได้ส่วนเสีย และมาตรการลดความเสี่ยง ไว้ตามประเด็นด้านความยั่งยืนหัวข้อ การบริหารจัดการความเสี่ยงด้านความยั่งยืน (ESG)

การสื่อสารเพื่อสร้างความตระหนักรู้ภายในองค์กร

บริษัทฯ ให้ความสำคัญกับพนักงานและผู้ปฏิบัติงานในการเพิ่มความรู้และทักษะในการใช้งานระบบเทคโนโลยีสารสนเทศและดิจิทัลเทคโนโลยี โดยมีกิจกรรมดังนี้

1. มีการจัดทำข้อมูลความรู้ทางด้าน Cyber Security และส่งเมล์สื่อสารให้แก่พนักงานรับทราบข้อมูลข่าวสารทุกเดือน และมีการ Update ข้อมูลของโปรแกรมต่างๆ โดยเจ้าหน้าที่ IT ได้เข้าไปให้ความรู้และตอบข้อสงสัยขณะเข้าไป PM เครื่องคอมพิวเตอร์ให้กับพนักงาน
2. ตรวจสอบแจ้งพนักงานและผู้บังคับบัญชาตามสังกัด เมื่อตรวจพบการใช้งานที่ไม่เหมาะสม เช่น โปรแกรมที่ไม่ได้รับอนุญาตหรือเข้าเว็บไซต์ที่มีความเสี่ยง

โปรแกรมการจัดการด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

1. การตรวจสอบภายนอกอิสระของโครงสร้างพื้นฐานและ/หรือระบบการจัดการความปลอดภัยของข้อมูล กรุณาให้ชื่อและมาตรฐานที่ใช้ (ยกตัวอย่าง เช่น ISO 27001, ISO 9001)
2. การฝึกอบรมความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ปี 2568 กรุณาระบุ (ยกตัวอย่างหลักสูตร)
   - 2.1 หลักสูตร Cyber Security Awareness โดยมีวัตถุประสงค์เพื่อ สร้างความตระหนักรู้ด้าน Cyber Security ขั้นพื้นฐานให้กับผู้ใช้ระบบงานคอมพิวเตอร์ของบริษัทฯ
   - 2.2 หลักสูตร Fortinet Certified Fundamentals in Cyber Security โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบมีความรู้และทักษะในการบริหารจัดการภัยคุกคามทางไซเบอร์ขั้นพื้นฐาน
   - 2.3 หลักสูตร Introduction & Requirement for ISO/IEC 27001:2022 โดยมีวัตถุประสงค์เพื่อเข้าใจแนวคิดและหลักการของมาตฐาน ISO27001:2022 เพื่อนำมาปรับใช้ในการกำหนดแนวทางปฏิบัติงานด้านสารสนเทศของบริษัทฯ ภายใต้การรักษาความปลอดภัยทางไซเบอร์