ความปลอดภัยทางไซเบอร์และการปกป้องข้อมูล

เป้าหมายและผลการดำเนินงาน

เป้าหมายระยะยาวปี 2573

บริษัทฯ ได้รับการรับรองด้านความปลอดภัยทางไซเบอร์และความเป็นส่วนตัวของข้อมูลตามมาตรฐานระดับสากล



ผลการดำเนินงานปี 2568: บรรลุตามเป้าหมายระยะยาว โดยบริษัทฯ ได้รับการประเมินคะแนน NIST ติดต่อกันเป็นปีที่ 3 โดยมีคะแนน 4.22 (ค่าเฉลี่ยระดับประเทศ เท่ากับ 1.91)



100% ของบริษัทฯ ผ่านเกณฑ์ความปลอดภัยทางไซเบอร์และข้อมูลส่วนบุคคลตามมาตรฐานเครือเจริญโภคภัณฑ์และหน่วยงานภายนอก

- ข้อร้องเรียนการคุกคามทางไซเบอร์ = **0** ราย
- ข้อร้องเรียนข้อมูลส่วนบุคคลรั่วไหล = **0** ราย
- จำนวนลูกค้า พนักงาน และคู่ค้าที่ได้รับผลกระทบจากการละเมิดข้อมูลส่วนบุคคล = **0** กรณี
- **100%** ของพนักงานบริษัทฯ ได้รับการฝึกอบรมหรือสร้างความตระหนักด้านความปลอดภัยทางไซเบอร์และการหลอกลวงทางอีเมล (Phishing Email)
- **100%** ช่องทางการเข้าถึงข้อมูลของบริษัทฯได้รับการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์
- **100%** เว็บไซต์และแอปพลิเคชันบนอุปกรณ์สื่อสารของบริษัทฯได้รับการทดสอบด้านความปลอดภัยทางไซเบอร์

ความเสี่ยงและโอกาส

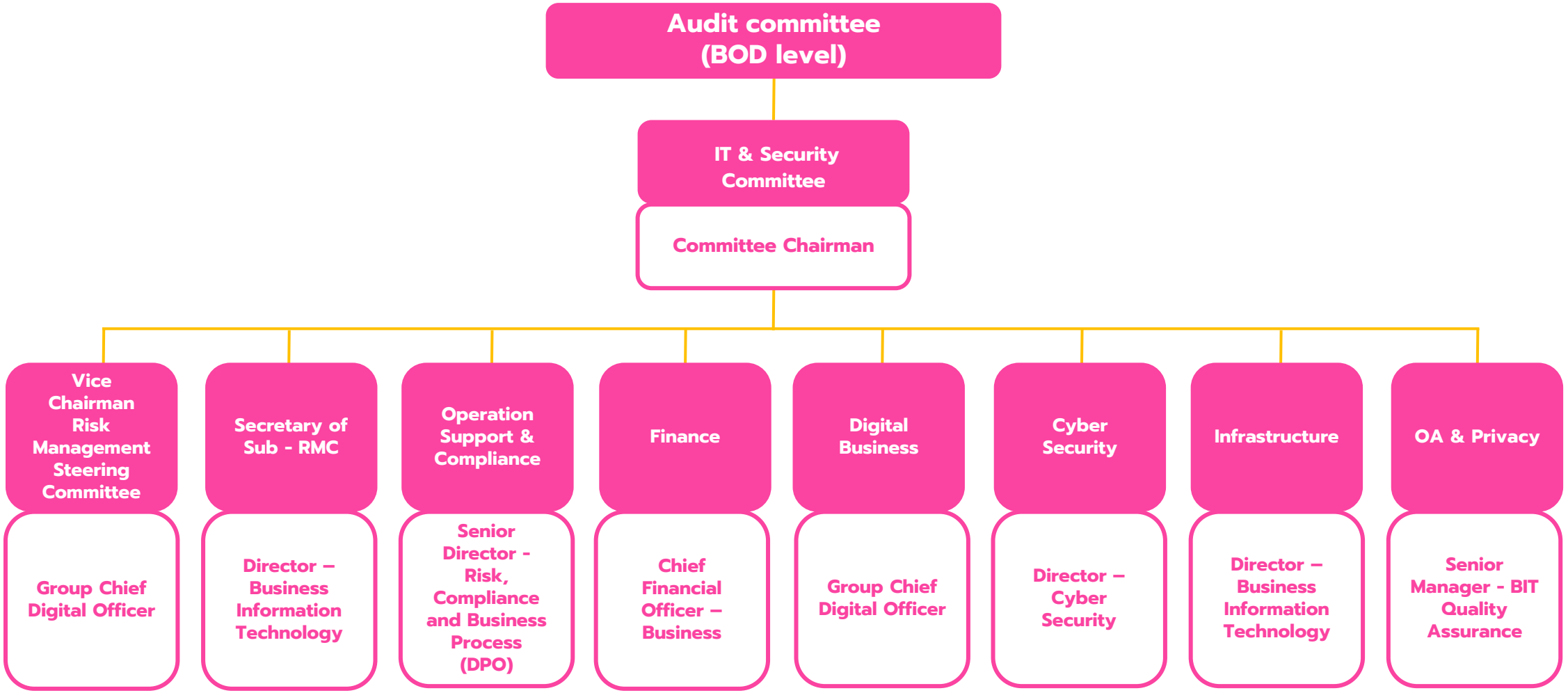
การดำเนินธุรกิจในปัจจุบันจำเป็นต้องนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้งาน เพื่อเพิ่มประสิทธิภาพการดำเนินงานให้รวดเร็ว แม่นยำ และมีความสร้างสรรค์มากขึ้น อย่างไรก็ตามการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจนั้น นำมาซึ่งความเสี่ยงที่จะถูกโจรกรรมข้อมูลหรือถูกคุกคามทางไซเบอร์ บริษัทฯ จึงมุ่งมั่นที่จะยกระดับความปลอดภัยทางไซเบอร์ และพัฒนาระบบการปกป้องข้อมูลส่วนบุคคลอย่างต่อเนื่อง เพื่อสร้างความเชื่อมั่นให้แก่ลูกค้า และผู้มีส่วนได้เสียตลอดห่วงโซ่คุณค่า

นโยบายและแนวทางการดำเนินงาน

บริษัทฯ ให้ความสำคัญต่อความปลอดภัยทางไซเบอร์และข้อมูลส่วนบุคคล โดยเริ่มจากการประเมินความเสี่ยงเพื่อเตรียมแผนรับมือต่อภัยคุกคามทางไซเบอร์ที่มีหลากหลายรูปแบบ และประกาศนโยบายแก่พนักงานในบริษัทฯได้รับทราบอย่างทั่วถึง เพื่อเป็นแนวปฏิบัติสำหรับสร้างความตระหนักทางไซเบอร์และมุ่งสู่ความปลอดภัยของข้อมูล ตามมาตรฐานระดับสากล ISO 27001 ตลอดจนมาตรฐานตามเครือเจริญโภคภัณฑ์

การบริหารความปลอดภัยทางไซเบอร์

ความปลอดภัยทางไซเบอร์เป็นส่วนหนึ่งของคณะกรรมการจัดการการบริหารความเสี่ยง โดยมีคณะกรรมการบริษัท (BOD) เป็นประธาน เพื่อการมีส่วนร่วมในกระบวนการด้านกลยุทธ์ในส่วนของความปลอดภัยทางไซเบอร์ และมีทีมผู้บริหารระดับสูงที่มีพื้นฐานด้านไอที (Chief Information Technology Officer CIO) ทำหน้าที่ดูแลกลยุทธ์ด้านความปลอดภัยทางไซเบอร์ของบริษัท



โครงสร้างนโยบายความปลอดภัยทางไซเบอร์

บริษัทฯ ปรับปรุงนโยบายความปลอดภัยทางไซเบอร์ให้เป็นปัจจุบัน และครอบคลุมแนวทางปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์มากขึ้น



การบริหารความปลอดภัยทางไซเบอร์



การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์



การรับมือต่อความเสี่ยงด้านความปลอดภัยทางไซเบอร์



การบริหารความต่อเนื่องทางความปลอดภัยไซเบอร์



การสร้างความตระหนักด้านความปลอดภัยทางไซเบอร์

โปรแกรมการจัดการความปลอดภัยทางไซเบอร์

ขอบเขตและการดำเนินการ	ผลลัพธ์ปี 2568
แผนความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัยของข้อมูล	• ปฏิบัติตามกรอบมาตรฐาน ISO 22301 เพื่อเตรียมความพร้อมรับมือกับวิกฤตต่าง ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อการดำเนินงานหลักของธุรกิจ รวมถึงมาตรการบริหารความเสี่ยงของบริษัท ในปี 2025 มีการจัดฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ จำนวน 2 ครั้ง” • ดูรายละเอียดเพิ่มเติม หน้า 7 (แผนความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัยไซเบอร์)
การวิเคราะห์ข้อบกพร่องด้านความมั่นคงปลอดภัยของข้อมูล	• ผ่านการวิเคราะห์ข้อบกพร่องด้านความมั่นคงปลอดภัยของข้อมูล (Verification and Vulnerability Analysis by External Party)
การตรวจสอบระบบการจัดการความมั่นคงปลอดภัยของข้อมูลโดยผู้ตรวจสอบจากภายนอก	• การประเมินประจำปี NIST Function บริษัทฯ ได้คะแนน 4.22 จาก 5 ซึ่งเป็นคะแนนสูงสุดในจำนวน 202 บริษัทที่เข้าร่วมการประเมิน • การตรวจสอบภายนอกโดย KPMG ในด้าน IT Controls Review
กระบวนการรายงานและส่งต่อเหตุการณ์ ความเสี่ยง หรือกิจกรรมที่น่าสงสัยสำหรับพนักงาน	• **100%** พนักงานได้รับการฝึกอบรมและสื่อสารนโยบาย ข้อมูล และแนวทางปฏิบัติ ผ่านการฝึกอบรมการสื่อสารภายในองค์กรและป้ายประชาสัมพันธ์
การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	• **100%** พนักงานได้รับการฝึกอบรมและสื่อสารนโยบายความปลอดภัยทางไซเบอร์
ข้อร้องเรียนการคุกคามทางไซเบอร์	• **0** กรณี

การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์

ปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์มีความซับซ้อนมากขึ้น บริษัทฯ จึงประเมินความเสี่ยงใน 5 มิติ ครอบคลุมช่องทางเข้าถึงข้อมูลของบริษัท ตั้งแต่ สำนักงานใหญ่ แอปพลิเคชัน โทรศัพท์มือถือ เว็บไซต์ ศูนย์กระจายสินค้าของบริษัทฯ และคู่ค้า

แนวทางการประเมินความเสี่ยง	ขอบเขตการประเมินความเสี่ยง
การเชื่อมต่อกับเครือข่ายสาธารณะ	เซิร์ฟเวอร์ของบริษัทฯ
การฟิชชิ่งและมัลแวร์เรียกค่าไถ่	พนักงานของบริษัทฯ
การโจรกรรมเอกลักษณ์บุคคล	ผู้ดูแลระบบและพนักงานของบริษัทฯ
การโจมตีห่วงโซ่อุปทาน	กลุ่มบุคคลที่ 3 (ด้านเทคโนโลยีสารสนเทศ)
การรั่วไหลของข้อมูล	พนักงานของบริษัทฯ

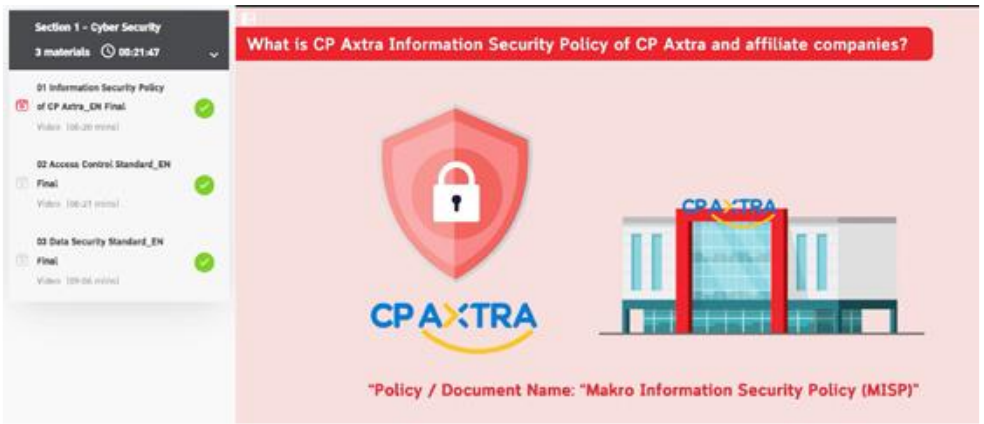
การสร้างความตระหนักรู้ และอบรมด้านความปลอดภัยทางไซเบอร์

ความตระหนักของพนักงานต่อการคุกคามทางไซเบอร์ เป็นองค์ประกอบสำคัญเพื่อสร้างความปลอดภัยของระบบสารสนเทศ และป้องกันการรั่วไหลของข้อมูล บริษัทฯ จึงมีแนวทางการสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ ประกอบด้วย การอบรมและสื่อสารเพื่อสร้างความตระหนัก (Awareness Communication) ระบบการแจ้งเตือนให้เกิดความตระหนัก (Awareness Response) และการตรวจสอบความตระหนัก (Awareness Testing)

ความปลอดภัยด้านไซเบอร์เป็นหนึ่งในความรับผิดชอบของพนักงานทุกคน โดยนำมาเป็นเกณฑ์ประเมินผลงานประจำปีและโบนัสสิ้นปีสำหรับพนักงานทั้งในระดับเจ้าหน้าที่ไปจนถึงระดับผู้จัดการที่ต้องได้รับการทบทวนการปฏิบัติงานตามระเบียบที่เกี่ยวข้องกับนโยบายความปลอดภัยทางไซเบอร์และการปกป้องข้อมูล

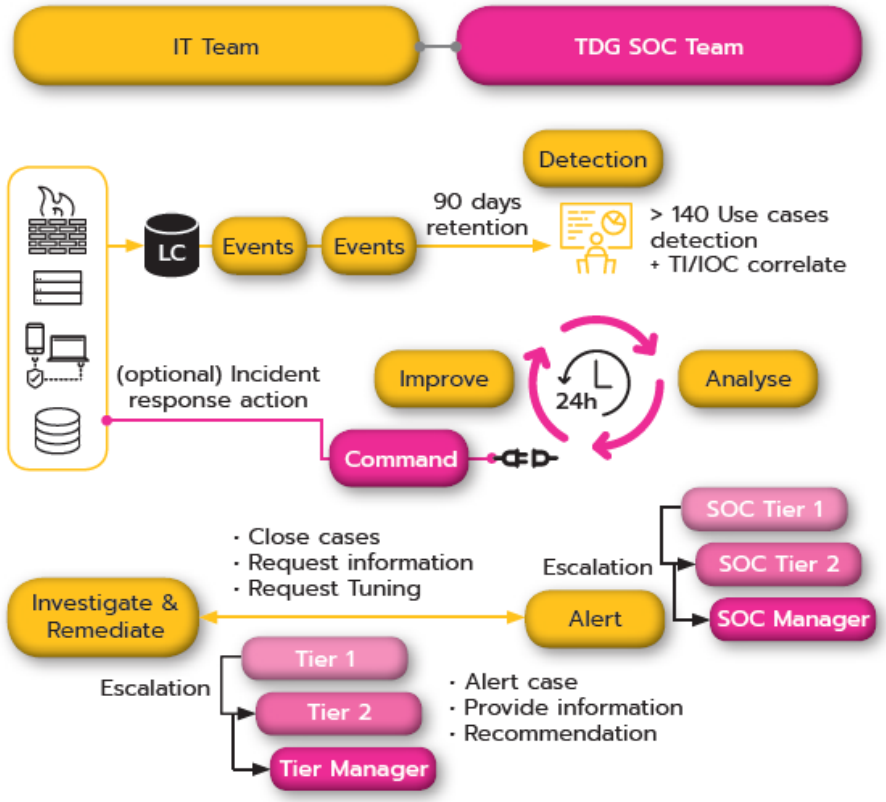
การเข้าถึงนโยบาย	• **100%** ของพนักงาน สามารถเข้าถึงนโยบายผ่านทางเว็บไซต์สื่อสารภายในขององค์กร
การสื่อสาร	• **100%** ของพนักงาน ได้รับการอบรม และสื่อสารให้ข้อมูลนโยบายและแนวทางปฏิบัติผ่านการฝึกอบรมช่องทางอีเมล และกระดานข่าวสารภายในองค์กร
การแจ้งเตือน	• **100%** ของพนักงาน ได้รับการแจ้งเตือนการรั่วไหล • ของข้อมูลบนอินเทอร์เน็ต และอีเมลที่มีความเสี่ยงต่อการโจรกรรมข้อมูล
การตรวจสอบ	• จำลองสถานการณ์โจรกรรมข้อมูล (Phishing Test) เพื่อตรวจสอบความตระหนักของพนักงาน
ระเบียบข้อปฏิบัติ	• **100%** ของพนักงาน รับทราบข้อปฏิบัติความปลอดภัยทางไซเบอร์ และการปกป้องข้อมูลก่อนเข้าสู่ระบบทุกครั้งคอมพิวเตอร์ก่อนดังภาพด้านล่าง





โครงการ "รักษาความปลอดภัยทางไซเบอร์ตลอด 24 ชั่วโมง หรือ Security Operation Center (SOC)"

บริษัทฯ เห็นถึงความเสี่ยงต่อการถูกคุกคามทางไซเบอร์ จึงจัดตั้งทีมดูแลรักษาความปลอดภัยทางไซเบอร์ ตลอด 24 ชั่วโมง หรือ Security Operation Center (SOC) เพื่อเฝ้าระวัง ติดตามและตอบสนองต่อภัยคุกคามในด้านต่าง ๆ ได้ทันท่วงที ตามกำหนดของ SLA และมาตรฐานความปลอดภัยสารสนเทศตามมาตรฐานของเครือเจริญโภคภัณฑ์

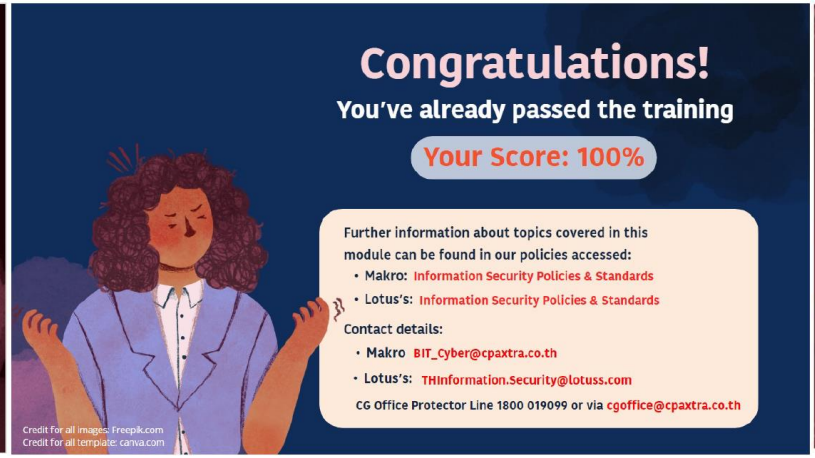


ฝึกอบรม เสริมสร้างความตระหนักด้านความปลอดภัยทางไซเบอร์

บริษัทฯ จัดฝึกอบรมเพื่อสร้างความตระหนัก ตามนโยบายด้านความปลอดภัยทางไซเบอร์แก่พนักงานทุกคนเป็นประจำทุกปี ซึ่งหลักสูตรดังกล่าวให้ความรู้เกี่ยวกับ วิธีสังเกตรูปแบบและลักษณะการหลอกลวง 4 ประการ ได้แก่

1) เนื้อหาของอีเมลกระตุ้นอารมณ์
2) ลิงค์เชื่อมโยงไม่ถูกต้อง
3) ชื่ออีเมลผู้ส่งไม่ถูกต้อง
4) ไฟล์แนบไม่ถูกต้อง รวมถึงให้คำแนะนำในการตอบกลับอีเมลหรือเหตุการณ์ที่น่าสงสัยทุกครั้งที่พบ





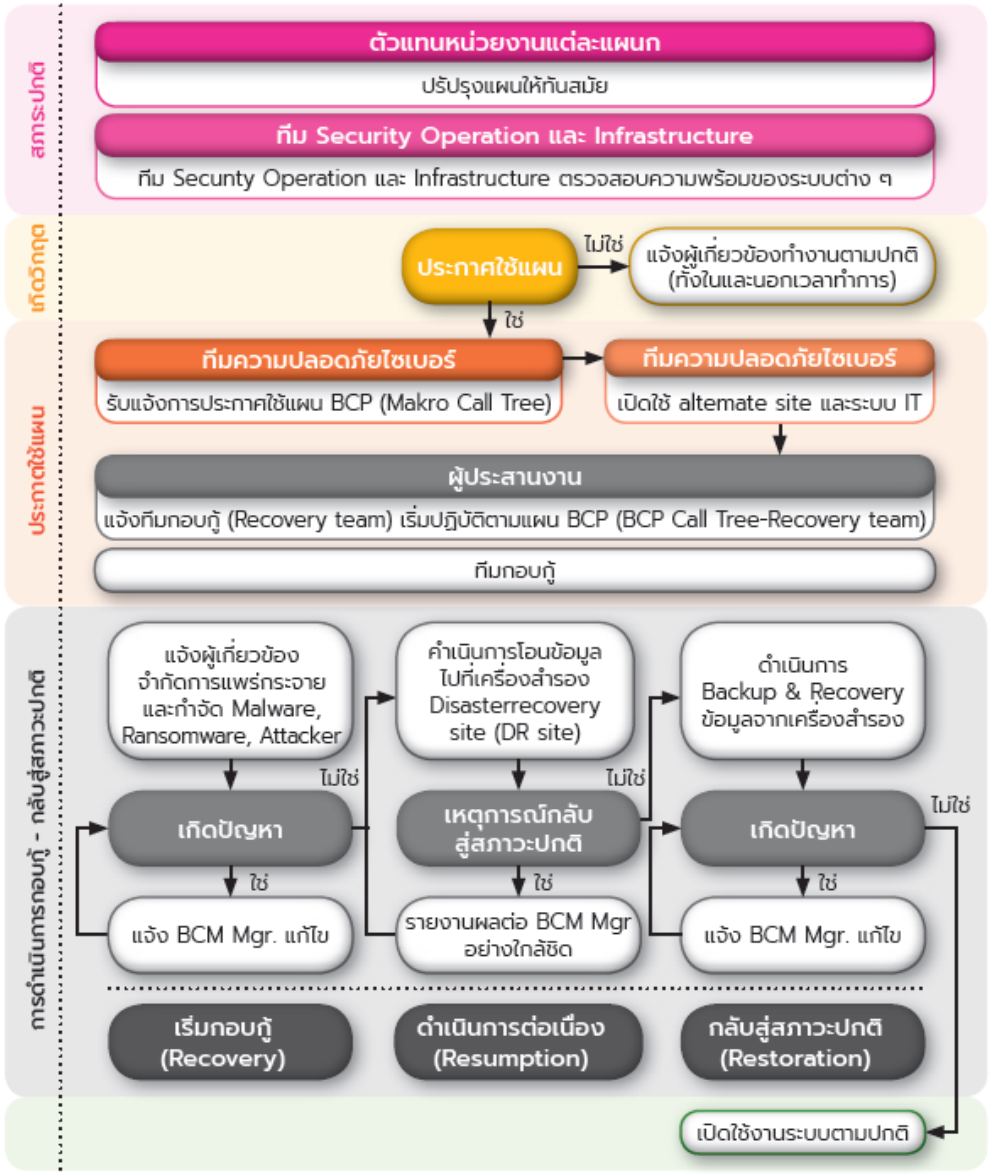


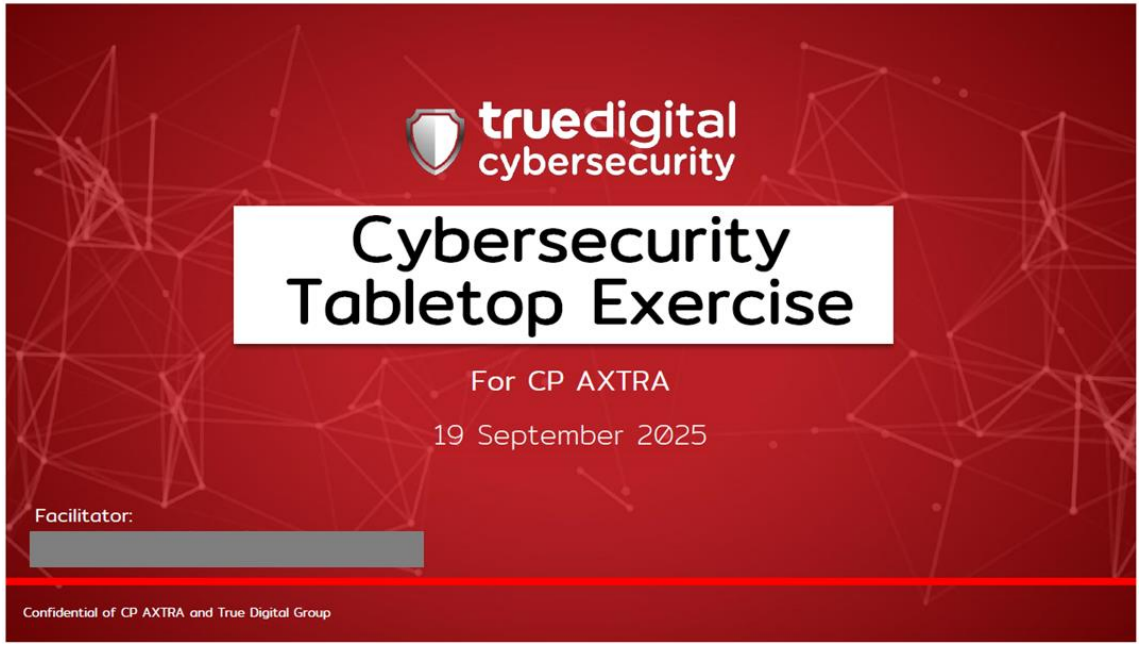


- **2,953** คน จำนวนพนักงานที่เข้าร่วมการอบรม (**100%**)
- **2,110** คน จำนวนพนักงานที่เข้าร่วมการทดสอบหลอกลวงทางอีเมล
- **73%** ของจำนวนพนักงาน ไม่กระทำการใด ๆ กับการหลอกลวงทางอีเมลและ **4%** รายงานการหลอกลวงทางอีเมล

แผนบริหารความต่อเนื่องทางความปลอดภัยทางไซเบอร์

ตามกรอบมาตรฐานสากล ISO 22301 เพื่อเตรียมความพร้อมรับมือวิกฤตการณ์ต่าง ๆ ที่อาจเกิดขึ้นที่ส่งผลกระทบต่อธุรกิจ และเพื่อเป็นแนวทางการบริหารความเสี่ยงของบริษัท ซึ่งในปี 2568 บริษัทฯมีการฝึกซ้อมตอบสนองเหตุการณ์จำลองภาวะฉุกเฉินทางไซเบอร์ (BCP) ไปแล้วสองครั้ง





"การจำลองสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์หรือเหตุการณ์การละเมิดข้อมูลส่วนบุคคลที่อาจเกิดขึ้นภายในองค์กร จัดทำขึ้นเพื่อทดสอบแผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan) และการประสานงานระหว่างทีมงาน เพื่อให้มั่นใจว่าองค์กรมีความพร้อมในการรับมือได้อย่างมีประสิทธิภาพเมื่อเกิดเหตุการณ์จริง"

การตรวจสอบและการวิเคราะห์ช่องโหว่โดยบุคคลภายนอก

บริษัทฯ ได้ดำเนินการตรวจสอบและวิเคราะห์ช่องโหว่ จากหน่วยงานภายนอกโดย NIST เพื่อตรวจสอบประสิทธิผลของระบบการจัดการกระบวนการด้านความปลอดภัยทางไซเบอร์ และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

หน่วยงานตรวจสอบภายใน

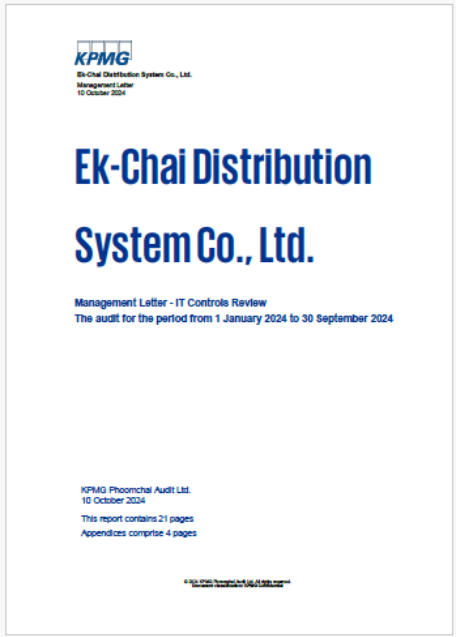

Internal Audit & Advisory

IT Application Control
Smart One and Smart Soft (2024-9)

June 2024

Distribution	
Stakeholders	Dr. Viriya U., Wipak T., Malai B., Panu P., Angsuthon S., Sakrit N.
For Information	External Auditor, Risk Management
Internal Audit Contacts	Busakorn R., Pongsatorn P., Niracha I.

โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและระบบการจัดการได้รับการตรวจสอบ


KPMG

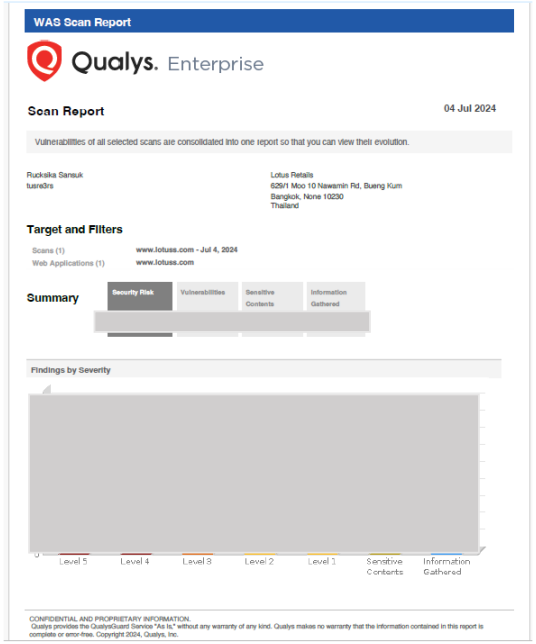
Ek-Chai Distribution System Co., Ltd.

Management Letter - IT Controls Review
The audit for the period from 1 January 2024 to 30 September 2024

KPMG Phoomchai Audit Ltd.
10 October 2024

This report contains 21 pages
Appendices comprise 4 pages

การวิเคราะห์ช่องโหว่จากหน่วยงานภายนอก


WAS Scan Report

Qualys. Enterprise

Scan Report 04 Jul 2024

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Rucksika Sansuk
tusre3rs

Lotus Retails
629/1 Moo 10 Nawamin Rd, Bueng Kum
Bangkok, None 10230
Thailand

Target and Filters

Scans (1) www.lotuss.com - Jul 4, 2024
Web Applications (1) www.lotuss.com

Summary

Security Risk | Vulnerabilities | Sensitive Contents | Information Gathered

Findings by Severity

Level 5 | Level 4 | Level 3 | Level 2 | Level 1 | Sensitive Contents | Information Gathered

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2024, Qualys, Inc.

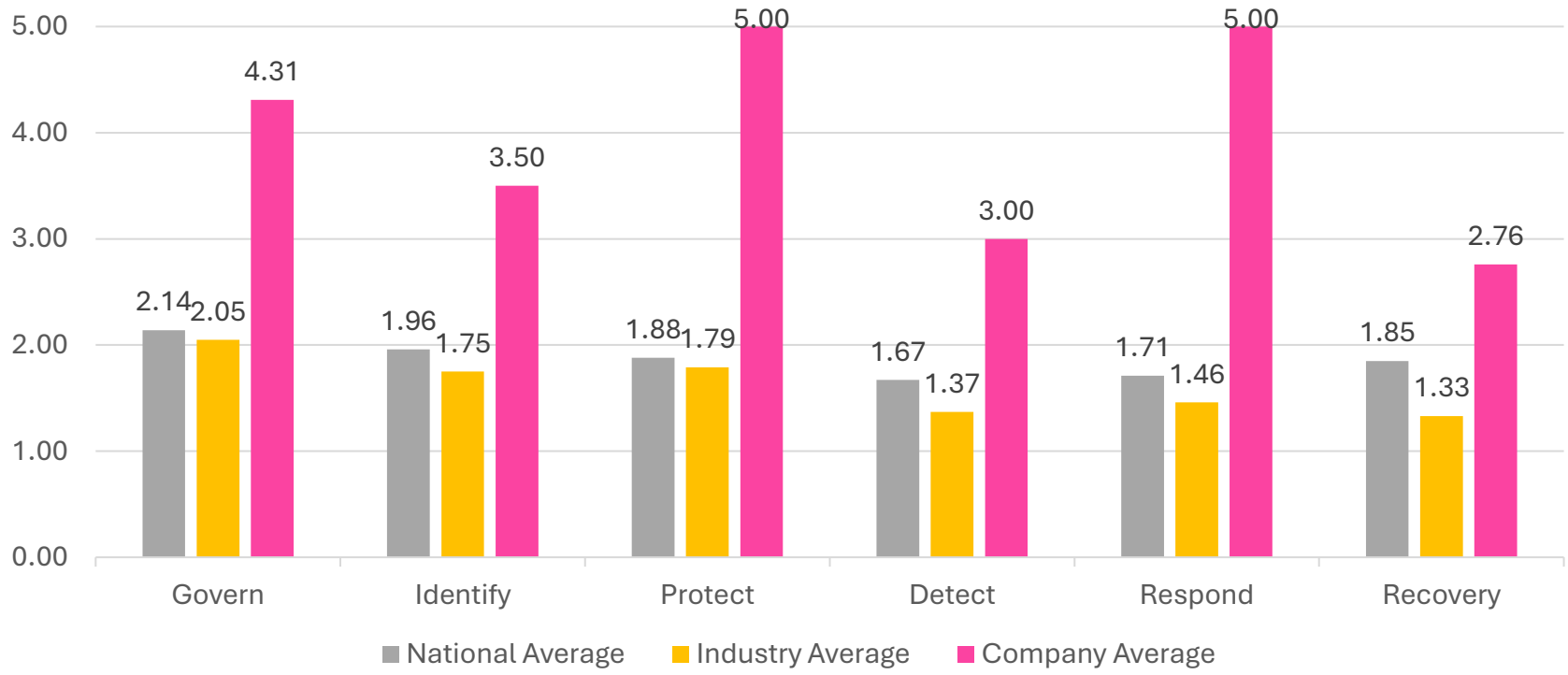
จำลองเหตุการณ์เจาะระบบเครือข่ายคอมพิวเตอร์จากหน่วยงานภายนอก

" ดูรายละเอียดเพิ่มเติม หน้า 10"

การจัดอันดับ ตาม NIST Function

บริษัทฯ ยังเข้าร่วมโครงการวัดระดับความมั่นคงปลอดภัยไซเบอร์ กับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) โดยใช้กรอบการทำงานด้านไซเบอร์ หรือ NIST Cybersecurity frameworkจัดกลุ่มคะแนนความมั่นคง โดยโครงการนี้เป็นการตรวจสอบตาม NIST Function ทั้ง 6 มิติ ประกอบไปด้วย Govern, Identify, Protect, Detect, Respond และ Recovery โดยผลการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของบริษัทฯ ได้คะแนน **4.22** จาก 5 คะแนน ซึ่งจัดอยู่ในกลุ่มบริษัทที่มีคะแนนเฉลี่ยระดับสูงสุด จากทั้งหมด 202 บริษัท

Score 4.22
Above NIST Function Average Rating



การทดสอบความปลอดภัยของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (เจาะระบบเครือข่ายคอมพิวเตอร์)

บริษัทฯ ว่าจ้างบริษัทที่ปรึกษา ภายนอก เพื่อทดสอบความปลอดภัยแบบ End-to-End ของบริษัทฯและบริษัทในเครือ โดยการทดสอบความปลอดภัย เครือข่าย และโครงสร้างพื้นฐาน ผ่านโครงการ Red Teaming โดยเจาะระบบตาม Cyber Kill Chain and MITRE ATT&CK Methodologyทดสอบความปลอดภัย Web Application ผ่านโครงการ Web Penetration Testingตาม OWASP Top 10 and Web&API Security Methodology การทดสอบความปลอดภัยMobile Application ผ่านโครงการ Mobile Penetration Testing ตาม OWASP Top 10 and Mobile Security Methodology

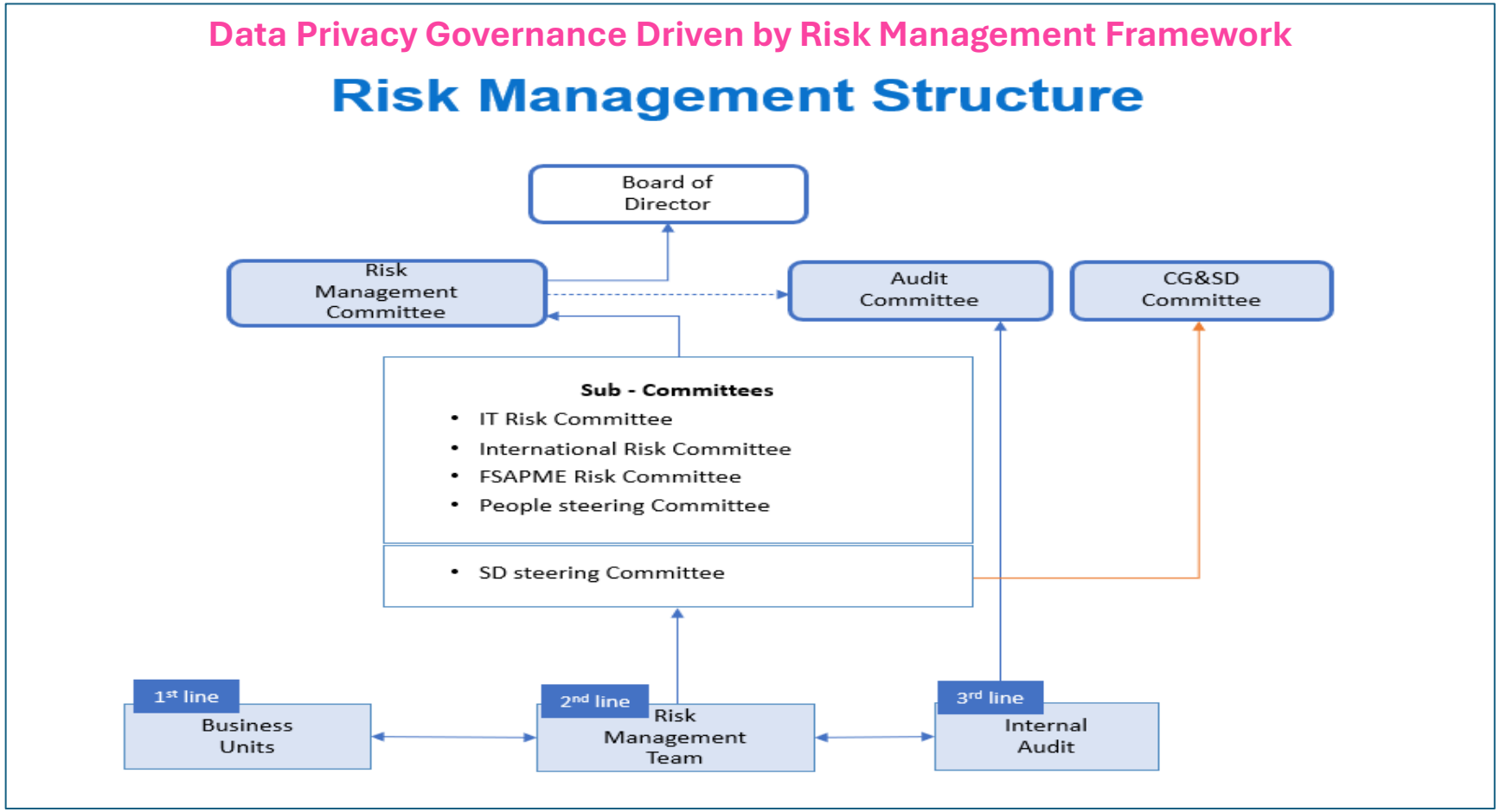
ผลลัพธ์ ปี 2565:

- **100%** ระบบความปลอดภัยทางไซเบอร์ ผ่านการทดสอบทุกหัวข้อ
- ไม่พบเหตุการณ์การโจมตีทางไซเบอร์



การคุ้มครองข้อมูล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) และคณะกรรมการ มีหน้าที่ควบคุมดูแลการเก็บรวบรวมข้อมูลส่วนบุคคล การใช้ และการเปิดเผย ตลอดจนนำเสนอรวบรวมผลการดำเนินงาน และความเสี่ยง ต่อคณะกรรมการจัดการการบริหารความเสี่ยง เพื่อดำเนินการประเมินความเสี่ยงขององค์กรประจำปี ตลอดจนให้คำปรึกษา และสื่อสารให้ทั่วทั้งองค์กรทราบถึงระเบียบปฏิบัติบทลงโทษทางวินัยที่เกี่ยวข้อง และมาตรการแก้ไข พร้อมและการเยียวยาผู้ได้รับผลกระทบ



เอกสารกำกับดูแลด้านความเป็นส่วนตัวของข้อมูล

ประกอบด้วย นโยบาย ขั้นตอน คู่มือ และแนวปฏิบัติที่เป็นกรอบการดำเนินงานของบริษัทในการคุ้มครองข้อมูลส่วนบุคคล เอกสารเหล่านี้กำหนดบทบาทและความรับผิดชอบ ให้แนวทางการปฏิบัติงานและรับรองการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนนบุคคล รวมถึงมาตรฐานสากลที่เกี่ยวข้อง ทั้งนี้เอกสารดังกล่าวถือเป็นรากฐานส าคัญในการส่งเสริมความรับผิดชอบ ความโปร่งใส และความสม่ำเสมอในการบริหารจัดการข้อมูลส่วนบุคคลทั่วทั้งองค์กร

เอกสารกำกับดูแลด้านความเป็นส่วนตัวของข้อมูล (Privacy Governance Documents) มีผลบังคับใช้กับทั้งบริษัทและบริษัทย่อยทั้งหมด รวมถึงมูลนิธิหรือกองทุนที่บริษัทได้จัดตั้งขึ้น หรือจะจัดตั้งขึ้นในอนาคต นอกจากนี้ยังครอบคลุมถึงซัพพลายเออร์(ในกรณีที่เกี่ยวข้อง) ผ่านข้อผูกพันตามสัญญา และต้องปฏิบัติให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

รายละเอียดเพิ่มเติม

https://www.cpaxtra.com/en/personal-data-protection-policy



การบริหารและจัดการข้อมูลส่วนบุคคล



นโยบายความเป็นส่วนตัวสำหรับลูกค้า



นโยบายความเป็นส่วนตัวสำหรับคู่ค้าธุรกิจ



นโยบายความเป็นส่วนตัวสำหรับนักลงทุน



การขอรับความยินยอม (Consent)



นโยบายคุกกี้ (Cookie Policy)



นโยบายความเป็นส่วนตัวสำหรับกล้องวงจรปิด

1. ประมวลผลข้อมูลส่วนบุคคลอย่างเป็นธรรมและถูกต้องตามกฎหมาย
2. ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ที่ได้แจ้งไว้ในการเก็บรวบรวม ใช้ หรือเปิดเผย
3. ตรวจสอบให้แน่ใจว่าการประมวลผลข้อมูลส่วนบุคคลมีความเหมาะสม เกี่ยวข้อง และไม่เกินความจำเป็น
4. ดูแลให้ข้อมูลส่วนบุคคลมีความถูกต้องและเป็นปัจจุบันอยู่เสมอ
5. ไม่เก็บรักษาข้อมูลส่วนบุคคลไว้นานเกินกว่าระยะเวลาที่จำเป็น
6. ประมวลผลข้อมูลให้สอดคล้องกับสิทธิของเจ้าของข้อมูลในการเข้าถึงและแก้ไขข้อมูลของตนเอง
7. มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้มั่นคงปลอดภัย
8. ห้ามโอนข้อมูลส่วนบุคคลไปยังประเทศที่มีมาตรฐานการคุ้มครองข้อมูลไม่เพียงพอ เว้นแต่จะได้รับความยินยอมหรือเป็นไปตามที่กฎหมายกำหนด
9. ใช้ข้อมูลส่วนบุคคลอย่างถูกต้องและไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลบุคล

ระบบบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคล

เพื่อให้สามารถบริหารความเสี่ยงด้านความเป็นส่วนตัวได้อย่างมีประสิทธิภาพ บริษัทฯ ได้จัดตั้งโครงการกำกับดูแลการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัว (Privacy Compliance Program) ซึ่งเป็นหนึ่งในโครงการสำคัญเพื่อบรรเทาความเสี่ยงด้านความเป็นส่วนตัวที่ได้รับการจัดให้เป็นหนึ่งในความเสี่ยงระดับองค์กร โครงการนี้สะท้อนถึงความมุ่งมั่นของบริษัทในการระบุ จัดการ และติดตามความเสี่ยงด้านความเป็นส่วนตัวอย่างเหมาะสมในทุกหน่วยงานที่เกี่ยวข้อง

บริษัทฯ ดำเนินมาตรการเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และลดความเสี่ยงจากการรั่วไหลของข้อมูลส่วนบุคคล โดยสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) บริษัทฯ ให้ความสำคัญสูงสุดกับการคุ้มครองข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลได้ (Personally Identifiable Information: PII) และได้ประกาศใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลอย่างครอบคลุม พร้อมเอกสารแนวทางประกอบเพิ่มเติมนอกจากนี้บริษัทยังนำเครื่องมือบริหารจัดการข้อมูล เช่น ระบบจัดประเภทและติดฉลากข้อมูลตามระดับความลับ (Data Classification and Labelling) และระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention: DLP) มาใช้เพื่อช่วยตรวจจับและป้องกันความเสี่ยงจากการรั่วไหลของข้อมูลโดยอัตโนมัติ

ประสิทธิผลของมาตรการดังกล่าวได้รับการติดตามและรายงานผลอย่างสม่ำเสมอ โดยมีการเก็บสถิติต่าง ๆ เช่น จำนวนพนักงานที่เข้ารับการประเมิน จำนวนพนักงานที่พบการละเมิดข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล และตัวชี้วัดประสิทธิภาพอื่น ๆ ที่เกี่ยวข้อง ผลการติดตามทั้งหมดจะถูกรวบรวมและรายงานภายใต้กรอบการบริหารความเสี่ยงของบริษัท เพื่อให้เกิดความรับผิดชอบ (Accountability) และการพัฒนาอย่างต่อเนื่องให้สอดคล้องกับแนวปฏิบัติในระดับสากล

บริษัทฯ ส่งเสริมวัฒนธรรมการกล้าแสดงออกอย่างสร้างสรรค์ (Speak-up Culture) โดยจัดให้มีช่องทางการแจ้งเบาะแสที่ปลอดภัยหลายช่องทางสำหรับพนักงานและซัพพลายเออร์เพื่อให้สามารถรายงานเหตุหรือข้อกังวล รวมถึงประเด็นด้านการคุ้มครองข้อมูลส่วนบุคคล ได้อย่างเป็นความลับและไม่เปิดเผยชื่อ ทั้งนี้บริษัทฯ ยังจัดให้มีช่องทางการรายงานผ่านบุคคลที่สาม (Independent Third Party) เพื่อเพิ่มความโปร่งใสและความเชื่อมั่นรายงานทุกกรณีจะได้รับการดำเนินการด้วยความเคร่งครัดในเรื่องการรักษาความลับ โดยบริษัทฯ มีความมุ่งมั่นอย่างชัดเจนในการไม่ตอบโต้ผู้แจ้งเบาะแส (Non-retaliation) และให้การคุ้มครองสิทธิของผู้แจ้งเบาะแสอย่างเต็มที่

สิ่งที่ดำเนินการ	ผลลัพธ์ ปี 2568
บูรณาการอยู่ในระบบการบริหารความเสี่ยง	• บริษัทฯ ได้บูรณาการนโยบายความเป็นส่วนตัวเข้ากับกรอบการบริหารความเสี่ยงในระดับกลุ่มธุรกิจ โดยมีคณะกรรมการบริหารความเสี่ยง (RMSC) ซึ่งอยู่ภายใต้การกำกับดูแลของคณะกรรมการตรวจสอบ ทำหน้าที่สนับสนุนการดำเนินงานตามกรอบการบริหารความเสี่ยงองค์กร รวมถึงการกำกับดูแลความเสี่ยงด้านความเป็นส่วนตัว ซึ่งถือเป็นหนึ่งในความเสี่ยงสำคัญของบริษัทฯ ทั้งนี้การดำเนินงานของ RMSC เป็นไปตามแนวปฏิบัติสากล เพื่อเสริมสร้างการบริหารความเสี่ยงเชิงรุก ความรับผิดชอบในทุกหน่วยงาน และสร้างความมั่นใจให้แก่คณะกรรมการตรวจสอบและคณะกรรมการบริษัทว่าความเสี่ยงสำคัญได้รับการกำกับดูแลอย่างมีประสิทธิภาพ • **100%** ได้รับการประเมิน และได้จัดทำแผนลดความเสี่ยง (Mitigation Plan) อย่างครบถ้วน
มาตรการทางวินัยในกรณีที่มีการฝ่าฝืน	• **100%** ของพนักงานได้รับการประเมินการปฏิบัติตามนโยบายของบริษัท รวมถึงนโยบายความเป็นส่วนตัว โดยการประเมินความปฏิบัติตามข้อกำหนดนี้เป็นส่วนหนึ่งของกระบวนการทางวินัยและการประเมินผลการปฏิบัติงานประจำปี รวมถึงการพิจารณาโบนัสปลายปี • **100%** ของพนักงาน คู่ค้าและผู้รับเหมา ได้รับการสื่อสารเกี่ยวกับเหตุการณ์ ละความรับผิดชอบในการป้องกันการรั่วไหลของข้อมูลส่วนบุคคล ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) • หากบุคลากรของบริษัทฝ่าฝืนหรือไม่ปฏิบัติตามนโยบาย แนวปฏิบัติ หรือมาตรการต่าง ๆ โดยตรงหรือโดยอ้อม บุคลากรดังกล่าวจะถูกดำเนินการทางวินัยตามข้อบังคับการทำงานของบริษัท
การตรวจประเมินความสอดคล้องของนโยบายความเป็นส่วนตัวโดยหน่วยงานภายนอก	• ได้รับการตรวจสอบโดยหน่วยงานภายนอก (3rd party audite CLICK HERE *to external audit report on web*
การตรวจประเมินความสอดคล้องของนโยบายความเป็นส่วนตัวโดยหน่วยงานภายใน	• **100%** การดำเนินโครงการกำกับดูแลการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัว ได้รับการตรวจสอบภายใต้แผนตรวจสอบภายในประจำปี

การตรวจสอบโดยหน่วยงานภายนอก ผลการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล โดยPDPC สคส.

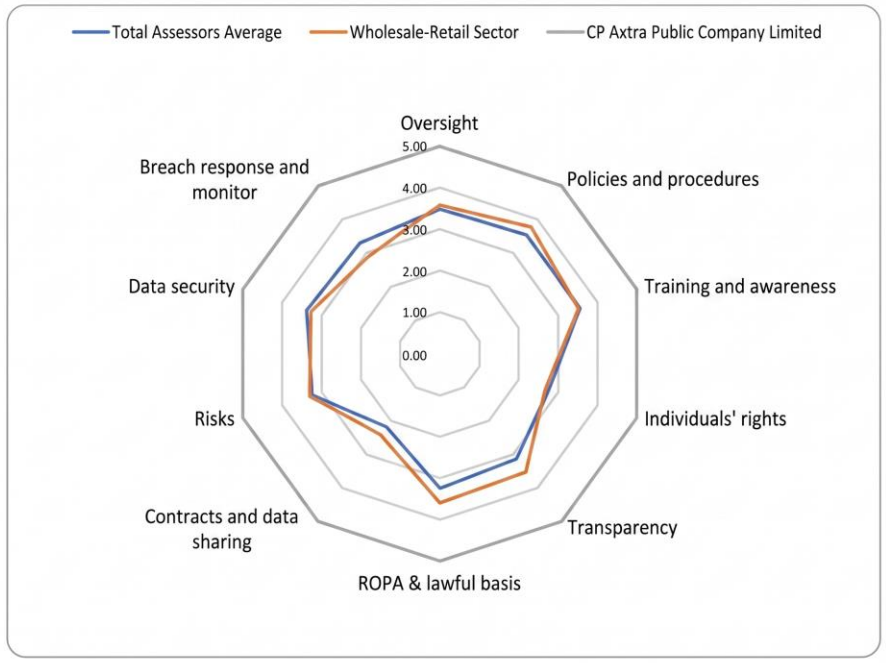
รายงานผลการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล

(Privacy Maturity Model)

บริษัท ซีพี แอ็กซ์ตร้า จำกัด (มหาชน)

External privacy policy compliance audit report:
Office of the Personal Data Protection Commission
Personal Data Protection Level Assessment Report (Privacy Maturity Model)
CP Axtra Public Company Limited.

Evaluation Score 5.00 Points	Your current score is higher than the average score of all participating organizations. (Average score of all assessors is 3.18 points)	Your current score is higher than the average score in the Wholesale-Retail and Online Commerce group. (Average score for your industry group is 3.26 points)



ข้อมูลความเป็นส่วนตัวของลูกค้า

เพื่อปกป้องข้อมูลความเป็นส่วนตัวของลูกค้าไม่ให้รั่วไหลออกภายนอกบริษัทฯ หากไม่ได้มีการอนุญาตอย่างถูกต้อง และลดความเสี่ยงจากการรั่วไหลข้อมูลและรักษาประสิทธิภาพข้อมูลว่ามีความปลอดภัยขณะใช้งาน จึงมีนโยบายความเป็นส่วนตัวของบุคคลภายนอก ซึ่งครอบคลุมดังหัวข้อต่อไปนี้

- ขอบเขตของประกาศความเป็นส่วนตัว
- วิธีที่บริษัทฯ ใช้เก็บรวบรวมข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่จัดเก็บ
- วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- การเปิดเผยข้อมูลส่วนบุคคล
- การส่งหรือโอนข้อมูลไปยังต่างประเทศ
- ระยะเวลาการเก็บรวบรวมข้อมูลส่วนบุคคล
- สิทธิของลูกค้า
- การปรับปรุงข้อมูลส่วนบุคคลของลูกค้า
- มาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้า
- ข่าวสารทางการตลาด
- โปรแกรมคุกกี้(Cookies) และข้อมูลเชิงเทคนิค
- กรณีการเชื่อมต่อไปยังเว็บไซต์ของบุคคลอื่น
- การเปลี่ยนแปลงนโยบายความเป็นส่วนตัว
- การแจ้งเตือนกรณีข้อมูลลูกค้ารั่ว ไหลหรอื เกิดเหตุละเมิดข้อมูล
- ช่องทางการติดต่อ
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



https://www.cpaxtra.com/th/privacy-notice-for-customer

ผลลัพธ์ ปี 2565:

- **3%** ของข้อมูลลูกค้า ถูกนำไปใช้เพื่อวัตถุประสงค์รอง (Secondary Purpose) โดยเป็นไปภายใต้ความยินยอมและตามกรอบ PDPA

ข้อมูลความเป็นส่วนตัวของลูกค้า



1. NATURE OF INFO CAPTURED

Personal Information We Collect...

Details categories of collected data: profiles, purchase history, device info.



2. USE OF COLLECTED INFO

Purposes of Collection, Use and Disclosure

Specifies primary objectives: enhance services, operations, customer experience.



3. OPT-OUT OPTION AVAILABLE

Customer Rights (Right to Object / Withdraw)

Ensures right to decline data processing or revoke consent.



4. OPT-IN CONSENT REQUIRED

Consent Basis

Explicit and proactive consent acquired prior to data collection.



5. REQUEST ACCESS TO DATA

Customer Rights (Right to Access)

Empowers customers to request access and obtain copies of held data.



6. REQUEST DATA PORTABILITY

Customer Rights (Right to Data Portability)

Request data in structured format and transfer to another controller.



7. REQUEST DATA RECTIFICATION

Customer Rights (Right to Rectification)

Channel for correcting inaccurate or incomplete personal information.



8. REQUEST DATA DELETION

Customer Rights (Right to Erasure / Deletion)

Request deletion or anonymization under legal conditions.



9. RETENTION PERIOD

Retention Period of Customer Personal Information

Strict timeframes and criteria for data retention.



10. INFORMATION PROTECTION

Security Measures for Customer Personal Information

Rigorous cybersecurity protocols, encryption, data protection.



11. THIRD-PARTY DISCLOSURE

Disclosure of Customer Personal Information

Transparentizes conditions, purposes, and entities for data sharing.



12. MONITORING SECONDARY USE

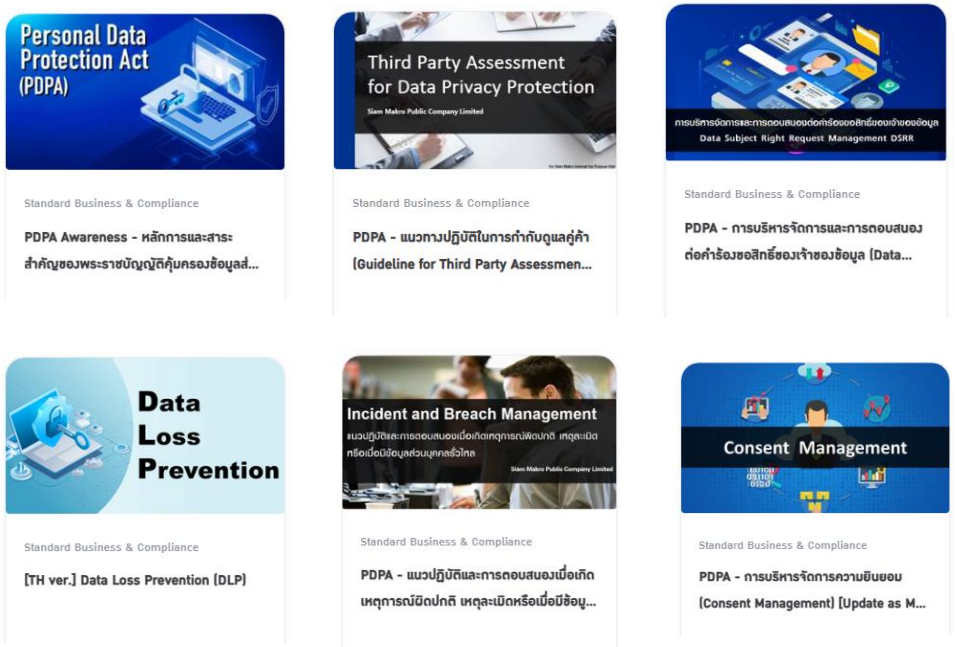
Percentage of users whose data is used for secondary purposes.

2025 RESULT: 3%

หมายเหตุ: (*) หมายถึงหัวข้อของประกาศความเป็นส่วนตัวสำหรับลูกค้าซึ่งเปิดเผยที่เว็บไซต์บริษัทฯ https://www.cpaxtra.com/th/privacy-notice-for-customer

การส่งเสริมความมุ่งมั่นของทั้งองค์กรในการคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ กำหนดให้พนักงานทุกคนต้องผ่านการอบรมประจำปี ด้านการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีอัตราการผ่านการอบรมครบ 100% นอกจากนี้ยังมีหลักสูตร e-learning หลากหลายรูปแบบให้พนักงานสามารถทบทวนความรู้และเสริมสร้างความเข้าใจด้านการคมุ้ ครองข้อมลู และการปฏิบัติตามข้อกำหนดได้ด้วยตนเองตลอดทั้งปี นอกจากนี้บริษัทฯ ยังขยายความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลไปยังซัพพลายเออร์ผ่านข้อผูกพันตามสัญญาที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) รวมถึง จรรยาบรรณของซัพพลายเออร์ (Supplier Code of Conduct) และช่องทางการสื่อสารอย่างต่อเนื่อง เพื่อส่งเสริมความเข้าใจและการปฏิบัติที่สอดคล้องกันในห่วงโซ่อุปทานด้วยการส่งเสริมการเรียนรู้อย่างต่อเนื่องให้กับพนักงาน และการเสริมสร้างความตระหนักรู้ด้านความเป็นส่วนตัว แก่ซัพพลายเออร์บริษัทฯ มุ่งมั่นให้การคุ้มครองข้อมูลส่วนบุคคลของลูกค้าและผู้มีส่วนได้ส่วนเสียเป็นไปอย่างรอบคอบ โปร่งใส และมีความรับผิดชอบ







ผลลัพธ์ ปี 2568

- **100%** พนักงานทุกคนได้รับการอบรมหลักสูตรภาคบังคับประจำปี
- **0** กรณี พนักงาน คู่ค้า และผู้รับเหมา ได้รับผลกระทบจากข้อมูลส่วนตัวรั่วไหลหรือถูกละเมิดข้อมูลส่วนบุคคล