ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

ชุดเอกสารกำกับดูแลและการปฏิบัติตามมาตรฐาน PCI DSS สำหรับธุรกิจตัวแทนท่องเที่ยว (Travel Agent)

เอกสารชุดนี้จัดทำโดย **ดร.นิพนธ์ นาชิน** ผู้ตรวจประเมินมาตรฐาน **PCI DSS** หรือ QSA เพื่อเป็นแนวทางเชิงนโยบาย กระบวนการ และแบบฟอร์มที่จำเป็นสำหรับธุรกิจตัวแทนท่องเที่ยว (Travel Agent) ในประเทศไทย ให้สามารถดำเนินงานด้านการรับชำระเงินด้วยบัตรได้อย่างสอดคล้องตามมาตรฐาน PCI DSS ลดความเสี่ยงจากการรั่วไหลของข้อมูลบัตร และยกระดับการกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

สารบัญ

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

1. วัตถุประสงค์และขอบเขตการใช้งาน

เอกสารชุดนี้จัดทำขึ้นเพื่อเป็นแนวทางมาตรฐานสำหรับธุรกิจตัวแทนท่องเที่ยว (Travel Agent) ในการกำหนดนโยบาย ขั้นตอนปฏิบัติ แผนงาน และแบบฟอร์ม/หลักฐานที่จำเป็น เพื่อให้การรับชำระเงินด้วยบัตรเป็นไปตามมาตรฐาน PCI DSS ตลอดจนลดความเสี่ยงจากการรั่วไหลของข้อมูลบัตร (Cardholder Data) และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง

ขอบเขตครอบคลุม:

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่เกี่ยวข้องกับการรับชำระเงิน การออกใบแจ้งหนี้ การจัดการคำสั่งจอง หรือการเข้าถึงระบบที่เกี่ยวข้องกับการชำระเงิน
- ช่องทางรับชำระที่องค์กรใช้งาน เช่น Payment Link/Payment Gateway, MOTO (รับข้อมูลผ่านโทรศัพท์แล้วกรอกในระบบธนาคาร/PSP), เครื่องรับบัตร (EDC/POI) หากมี
- ระบบสนับสนุน ได้แก่ อีเมลองค์กร ระบบแชทที่ใช้สื่อสารลูกค้า (ใช้ได้เฉพาะส่งลิงก์/ข้อมูลทั่วไป), เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, และคลาวด์ที่ใช้งาน

หมายเหตุ: เอกสารนี้ไม่ทดแทนข้อกำหนดเชิงเทคนิคของผู้ให้บริการธนาคาร/PSP และควรใช้งานร่วมกับข้อกำหนดสัญญา/คู่มือของผู้ให้บริการดังกล่าว.

2. คำจำกัดความและหลักการสำคัญ

2.1 คำจำกัดความหลัก

- CDE (Cardholder Data Environment): บุคคล กระบวนการ และเทคโนโลยีที่จัดเก็บ ประมวลผล หรือส่งผ่านข้อมูลผู้ถือบัตร
- CHD (Cardholder Data): ข้อมูลผู้ถือบัตร เช่น หมายเลขบัตร (PAN) และข้อมูลที่เกี่ยวข้องตามนิยาม PCI
- SAD (Sensitive Authentication Data): ข้อมูลยืนยันตัวตนที่อ่อนไหว เช่น CVV/CVC, Track data, PIN/PIN block ซึ่งห้ามจัดเก็บภายหลังการทำรายการ

2.2 หลักการสำคัญ

องค์กรกำหนดหลักการสำคัญ (Mandatory Rules) ดังต่อไปนี้ และถือเป็นข้อห้ามเด็ดขาด:

12. ห้ามขอ รับ หรือจัดเก็บข้อมูลบัตรผ่านช่องทางที่ไม่ปลอดภัย (เช่น Line/WhatsApp/Facebook/Email ที่ไม่มีการควบคุม หรือการส่งภาพบัตร/การพิมพ์เลขบัตรในแชท).
13. ห้ามจัดเก็บ SAD ทุกชนิด โดยเฉพาะ CVV/CVC/Track data/PIN ไม่ว่ากรณีใด ๆ (รวมถึงห้ามจดบันทึก ห้ามถ่ายภาพ ห้ามคัดลอก และห้ามส่งต่อ).
14. ให้ใช้ช่องทางรับชำระที่ลดขอบเขต PCI (เช่น Payment Link/Hosted Payment Page ของธนาคารหรือ PSP) เป็นช่องทางหลัก และให้ข้อมูลบัตรถูกกรอกโดยลูกค้าในระบบของผู้ให้บริการเท่านั้น.
15. หากจำเป็นต้องทำ MOTO ให้พนักงานกรอกข้อมูลลงในระบบธนาคาร/PSP ทันที และต้องมีการควบคุมการสนทนา/การบันทึกเสียงอย่างเคร่งครัด.
16. การเข้าถึงระบบที่เกี่ยวข้องกับการชำระเงินต้องมีการยืนยันตัวตนหลายปัจจัย (MFA) และใช้บัญชีผู้ใช้เฉพาะบุคคลเท่านั้น.

3. แบบจำลองการรับชำระสำหรับ Travel Agent และสิ่งที่อนุญาต/ห้ามทำ

3.1 ช่องทางรับชำระที่แนะนำ

- Payment Link / Hosted Payment Page: องค์กรสร้างลิงก์ชำระเงินจากธนาคาร/PSP และส่งให้ลูกค้าเพื่อกรอกข้อมูลบัตรด้วยตนเอง
- การรับชำระผ่านช่องทางที่ธนาคาร/PSP ให้บริการโดยตรง โดยองค์กรไม่สัมผัสข้อมูลบัตร (No-touch)

3.2 ช่องทางรับชำระที่จำกัด (ใช้เมื่อจำเป็น)

- MOTO (Mail Order/Telephone Order): พนักงานรับข้อมูลผ่านโทรศัพท์และกรอกในระบบธนาคาร/PSP ทันที โดยห้ามบันทึก CVV และห้ามเก็บข้อมูลบัตรไว้ในรูปแบบใด ๆ

3.3 ช่องทางต้องห้าม

- รับข้อมูลบัตรผ่านแชท/อีเมล/เอกสารแนบ/รูปภาพ และนำไปประมวลผลหรือจัดเก็บต่อ

- ถ่ายภาพบัตร เก็บ PAN/CVV ในไฟล์ Excel/Google Sheets/CRM/โน้ต/กระดาษทั่วไป/ระบบ ticketing
- อัดเสียง/บันทึกสนทนาที่มีข้อมูลบัตร โดยไม่มีมาตรการ masking หรือการปิดการบันทึกตามที่ผู้ให้บริการรองรับ

3.4 ตารางตัวอย่าง 'อนุญาต/ไม่อนุญาต' (ใช้สื่อสารกับทีม)

สถานการณ์	อนุญาต	ไม่อนุญาต
ลูกค้าขอจ่ายด้วยบัตร	ส่ง Payment Link ให้ลูกค้ากรอกข้อมูลเอง	ขอให้ลูกค้าพิมพ์เลขบัตร/CVV ในแชท
ลูกค้าขอจ่ายทางโทรศัพท์	ทำ MOTO โดยกรอกทันทีใน PSP/ธนาคาร	จด CVV ไว้ก่อนแล้วค่อยกรอกภายหลัง
ลูกค้าส่งรูปบัตรมาแล้ว	แจ้งให้ลูกค้าลบและลบข้อความ/ไฟล์ทันที พร้อมบันทึกเหตุการณ์	บันทึกรูปไว้เพื่อสะดวกในอนาคต
ต้องส่งหลักฐานการชำระให้บัญชี	ส่ง Transaction ID/Reference/ใบยืนยันจากธนาคาร (ไม่มี PAN เต็ม)	ส่งภาพหน้าจอที่มี PAN เต็ม หรือ CVV

4. โครงสร้างการกำกับดูแล (PCI Compliance Program Charter) และบทบาทหน้าที่

องค์กรต้องกำหนดโครงสร้างการกำกับดูแลและผู้รับผิดชอบด้าน PCI DSS อย่างชัดเจน เพื่อให้การกำหนดขอบเขต การจัดทำนโยบาย การรวบรวมหลักฐาน การติดตามการแก้ไข และการรายงานผู้บริหารเป็นไปอย่างต่อเนื่อง.

4.1 บทบาทหลัก (แนะนำ)

บทบาท	ความรับผิดชอบหลัก	ผู้ดำรงตำแหน่ง (ตัวอย่าง)	หลักฐาน/ผลลัพธ์
PCI Program Owner	กำกับดูแลโปรแกรม PCI, กำหนดขอบเขต, ประสานงานการตรวจ, ติดตามช่องโหว่/ประเด็น	หัวหน้าฝ่ายกำกับดูแล/IT Security	รายงานสถานะ, Evidence Register, แผนทบทวน
Payment Process Owner	ออก/บริหาร Payment Link, ควบคุม MOTO, ตรวจสอบรายการรับชำระ/การกระทบยอด	หัวหน้าฝ่ายการเงิน	Payment Link Log, รายงานธุรกรรม
IT Administrator	ดูแลอุปกรณ์/บัญชี/การตั้งค่า MFA/EDR/Patch/Log และการเข้าถึง	ผู้ดูแลระบบ IT	Inventory, Patch Log, EDR Report

บทบาท	ความรับผิดชอบหลัก	ผู้ดำรงตำแหน่ง (ตัวอย่าง)	หลักฐาน/ผลลัพธ์
HR/Training Coordinator	อบรมความตระหนักรู้, Onboarding/Offboarding, เก็บแบบรับทราบ/บันทึกการอบรม	HR/Admin	Training Record, Acknowledgement Form

4.2 รอบการประชุมและรายงาน (ขั้นต่ำ)

- ประชุมติดตาม PCI อย่างน้อยรายไตรมาส (หรือบ่อยกว่าตามความเสี่ยง/ปริมาณธุรกรรม)
- รายงานผู้บริหาร: สถานะการปฏิบัติตาม, ประเด็นค้างแก้ไข, เหตุการณ์ด้านความปลอดภัย, และแผนปรับปรุง

5. ชุดนโยบาย (Policies) ที่ต้องประกาศใช้

5.1 รายการนโยบายขั้นต่ำ

1. นโยบายการรับชำระเงินและการจัดการข้อมูลบัตร (Card Data Handling & Payment Acceptance Policy)
2. นโยบายรหัสผ่านและการยืนยันตัวตน (Password, MFA & Authentication Policy)
3. นโยบายควบคุมการเข้าถึงและการแบ่งแยกหน้าที่ (Access Control & Segregation of Duties Policy)
4. นโยบายความปลอดภัยทางกายภาพและการจัดการอุปกรณ์รับบัตร (Physical & POI/EDC Handling Policy)
5. นโยบายการป้องกันมัลแวร์/การจัดการช่องโหว่/การจัดการแพตช์ (Malware, Vulnerability & Patch Management Policy)
6. นโยบายการบันทึกเหตุการณ์และการเฝ้าระวัง (Logging & Monitoring Policy)
7. นโยบายการจัดการผู้ให้บริการภายนอก (Third-Party Service Provider Policy)
8. นโยบายการอบรมและสร้างความตระหนักรู้ (Security Awareness Policy)
9. นโยบายการวิเคราะห์ความเสี่ยงแบบมุ่งเป้า (PCI Targeted Risk Analysis Policy)
10. นโยบายการตอบสนองเหตุการณ์ (Incident Response Policy/Plan)

5.2 เนื้อหามาตรฐานที่ต้องมีในทุกนโยบาย

- วัตถุประสงค์ (Purpose) / ขอบเขต (Scope) / คำจำกัดความ (Definitions)
- บทบาทหน้าที่ (Roles & Responsibilities)

- ข้อกำหนดหลัก (Policy Statements) พร้อมสิ่งที่อนุญาต/ไม่อนุญาต
- การจัดการข้อยกเว้น (Exception Management) และบทลงโทษ (Enforcement)
- การจัดเก็บหลักฐาน (Records/Evidence) และรอบทบทวนเอกสาร (Review Cycle)

6. ชุดขั้นตอนปฏิบัติ (Procedures) ที่ต้องใช้งานจริง

6.1 ขั้นตอนรับชำระแบบ Payment Link (Preferred)

1. ตรวจสอบคำสั่งจอง ยอดชำระ และข้อมูลผู้ติดต่อ โดยห้ามขอข้อมูลบัตรผ่านช่องทางสื่อสารทั่วไป
2. เข้าระบบธนาคาร/PSP Portal ด้วยบัญชีเฉพาะบุคคล และต้องเปิดใช้ MFA
3. สร้าง Payment Link โดยระบุ (ก) ยอดชำระ (ข) สกุลเงิน (ค) วันหมดอายุลิงก์ (ง) หมายเลขอ้างอิงคำสั่งจอง
4. ส่ง Payment Link ให้ลูกค้าผ่านช่องทางที่องค์กรอนุมัติ (อีเมลองค์กร/ระบบ CRM ที่ควบคุมได้/แชทได้เฉพาะส่งลิงก์ โดยห้ามมี PAN/CVV)
5. บันทึกข้อมูลการส่งลิงก์ลงแบบฟอร์ม FRM-01 (ผู้ส่ง/ผู้รับ/เวลาส่ง/ยอด/วันหมดอายุ/สถานะ)
6. ติดตามผลการชำระจากธนาคาร/PSP และบันทึก Transaction ID/Reference (ห้ามบันทึก PAN เต็ม)
7. จัดเก็บหลักฐานเป็นไฟล์ PDF/รายงานจากธนาคาร และอัปโหลดเข้าที่เก็บหลักฐานกลางตามที่กำหนด

6.2 ขั้นตอนรับชำระแบบ MOTO (Restricted)

ใช้เฉพาะกรณีจำเป็น และต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้:

1. ห้ามเปิดลำโพงโทรศัพท์ในพื้นที่สาธารณะ/พื้นที่ที่มีบุคคลอื่นได้ยิน
2. ห้ามอัดเสียงหรือบันทึกสนทนาที่มีข้อมูลบัตร หากระบบ call recording เปิดใช้งาน ต้องกำหนดวิธีปิดการบันทึกสำหรับช่วงรับข้อมูลบัตรหรือใช้ระบบ masking ที่ได้รับอนุมัติ
3. ต้องเปิดหน้า PSP/ธนาคารให้พร้อม เพื่อกรอกข้อมูลทันที (ห้ามจด CVV ไว้ก่อน)
4. ยืนยันตัวตนลูกค้าตามขั้นตอนงานขาย/งานการเงิน (ไม่รวมการขอข้อมูลบัตรผ่านแชท)
5. แจ้งลูกค้าว่าองค์กรจะไม่จัดเก็บข้อมูลบัตร และจะกรอกข้อมูลเข้าระบบธนาคาร/PSP ทันที
6. รับ PAN/วันหมดอายุ/ชื่อผู้ถือบัตร และกรอกทันทีในระบบ PSP/ธนาคาร
7. รับ CVV/CVC และกรอกทันที (ห้ามจด ห้ามทวนเสียงดัง)

8. เมื่อทำรายการเสร็จ ให้แจ้งลูกค้าเฉพาะผลการทำรายการ และ Transaction ID/Reference
9. บันทึกการทำรายการลง FRM-02 โดยไม่บันทึก CVV และไม่บันทึก PAN เต็ม (ให้บันทึกเฉพาะ 4 หลักท้ายแบบ masked)

6.3 ขั้นตอนเมื่อได้รับข้อมูลบัตรผ่านแชท/อีเมลโดยไม่ตั้งใจ

1. ห้ามคัดลอก ส่งต่อ หรือบันทึกข้อมูลดังกล่าวในระบบอื่นใด
2. แจ้งลูกค้าด้วยข้อความมาตรฐาน (FRM-03) ให้ลบข้อมูล และเสนอช่องทางชำระที่ปลอดภัย (Payment Link)
3. ลบข้อความ/ไฟล์แนบในระบบที่สามารถลบได้ และแจ้งหัวหน้างาน/PCI Program Owner ทันที
4. บันทึกเหตุการณ์ใน FRM-10 โดยระบุเพียงข้อเท็จจริง (ห้ามบันทึก PAN/CVV)
5. ประเมินความจำเป็นในการแจ้งธนาคาร/PSP ตาม Incident Response Plan และดำเนินการตามคำแนะนำ

6.4 ขั้นตอนตรวจอุปกรณ์รับบัตร (EDC/POI) และการป้องกันการงัดแงะ

1. จัดทำทะเบียนอุปกรณ์ (FRM-04) ระบุ Serial/รุ่น/ตำแหน่ง/ผู้รับผิดชอบ
2. กำหนดความถี่การตรวจสอบ (รายวัน/รายสัปดาห์/ตาม Targeted Risk Analysis) และบันทึกผลลง FRM-05
3. ตรวจสอบซีล สติ๊กเกอร์ หมายเลข Serial ความผิดปกติของพอร์ต สายเชื่อมต่อ หรืออุปกรณ์แปลกปลอม
4. หากพบความผิดปกติ ให้หยุดใช้งานทันที แยกเก็บอุปกรณ์เป็นหลักฐาน และแจ้งธนาคาร/PSP ตาม Incident Response Plan

6.5 ขั้นตอน Onboarding/Offboarding (บัญชีผู้ใช้และอุปกรณ์)

1. Onboarding: ตรวจสอบประวัติพนักงานตาม Employee Screening Policy (ตามที่กฎหมายอนุญาต) และจัดอบรมความตระหนักรู้ก่อนให้เข้าถึงระบบสำคัญ
2. กำหนดสิทธิ์ตามหลัก Need-to-Know และแยกหน้าที่ (Sales/Finance/IT) พร้อมบันทึกใน FRM-07/FRM-06
3. บังคับใช้ MFA และตั้งค่าความปลอดภัยอุปกรณ์ (เช่น Screen lock, EDR, Auto-update) ก่อนเริ่มงาน
4. Offboarding: เพิกถอนสิทธิ์ทันทีเมื่อสิ้นสุดการจ้าง (อีเมล/PSP/CRM/คลาวด์) และเรียกคืนอุปกรณ์/โทเคน
5. ตรวจสอบและปิดการเข้าถึงที่เหลือค้าง (รวม shared mailbox/forwarding/OTP device) พร้อมบันทึกหลักฐาน

6.6 ขั้นตอนการทบทวนความปลอดภัยรายไตรมาส (Quarterly Review)

1. ทบทวนการตั้งค่า/ประสิทธิผลของการควบคุมที่สำคัญ: MFA, EDR, Patch, Access review, POI inspection, log review, TPSP compliance
2. ผู้ทบทวนต้องเป็นผู้ที่ไม่ได้ปฏิบัติหน้าที่นั้นโดยตรง (independence)
3. ต้องจัดทำบันทึกผลการทบทวน รายการประเด็น และแผนแก้ไข พร้อมการลงนามรับรอง

7. แผนงาน (Plans) และรอบการทบทวน/ตรวจสอบ

7.1 แผน PCI Compliance Roadmap (ตัวอย่าง 90 วัน)

ช่วงเวลา	กิจกรรมหลัก	ผู้รับผิดชอบ	ผลลัพธ์/หลักฐาน
สัปดาห์ 1-2	กำหนด scope, ทำ data flow, ทำ inventory (ระบบ/อุปกรณ์/บัญชี)	PCI Owner + IT + Finance	Scope doc, Inventory, Evidence Register
สัปดาห์ 3-4	ประกาศนโยบายหลัก, ตั้งค่า MFA/EDR, ปิดช่องทางต้องห้าม, สื่อสารทีม	IT + HR + Finance	Policy pack, MFA evidence, Awareness notice
เดือนที่ 2	เริ่มใช้ Payment Link เป็นหลัก, ปรับกระบวนการ MOTO, เริ่ม log review/POI inspection	Finance + Operations	FRM-01/02/05
เดือนที่ 3	ทำ Quarterly Review, สแกนช่องโหว่/patch review, ปรับปรุงเอกสารและหลักฐาน	PCI Owner + IT	Quarterly report, Patch log, Action items

7.2 รอบการทบทวนขั้นต่ำ (Retention/Review Cycle)

- ทบทวน scope และ data flow: อย่างน้อยปีละครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการชำระเงิน/ระบบ/ผู้ให้บริการ
- ทบทวนสิทธิ์การเข้าถึง (Access Review): อย่างน้อยรายไตรมาส
- ทบทวน log ที่สำคัญ: รายวันหรืออย่างน้อยตามที่กำหนดจากความเสี่ยง
- ทบทวนความสอดคล้องของ TPSP: อย่างน้อยปีละครั้ง (ขอ AOC/Attestation/สัญญา)
- เก็บหลักฐานอย่างน้อย 12 เดือน (แนะนำ) หรือเป็นไปตามข้อกำหนดสัญญา/กฎหมาย/ธนาคาร

8. แบบฟอร์มและทะเบียนหลักฐาน (Forms/Logs/Evidence Register)

8.1 รายการแบบฟอร์มที่แนบในภาคผนวก

1. FRM-01 Payment Link Log
2. FRM-02 MOTO Processing Log และสคริปต์สนทนามาตรฐาน
3. FRM-03 ข้อความมาตรฐานสำหรับลูกค้า (ห้ามส่งข้อมูลบัตรผ่านแชท/อีเมล)
4. FRM-04 POI/EDC Inventory
5. FRM-05 POI/EDC Inspection Log (รายวัน/ตาม TRA)
6. FRM-06 System & Account Inventory (Email/PSP/CRM/Endpoints)
7. FRM-07 Access Control Matrix และ Quarterly Access Review
8. FRM-08 Patch & EDR Status Log
9. FRM-09 Log Review Checklist
10. FRM-10 Incident Report Form
11. FRM-11 TPSP Due Diligence Checklist (AOC/Scope/Contacts)
12. FRM-12 Exception Request & Approval Form
13. FRM-13 Evidence Register (รายการหลักฐานสำหรับการตรวจ)

8.2 หลักการจัดเก็บหลักฐาน (Evidence Handling)

- จัดเก็บหลักฐานในพื้นที่เก็บกลางที่มีการควบคุมสิทธิ์ (เช่น SharePoint/Drive ขององค์กร) และเปิด MFA
- ตั้งชื่อไฟล์มาตรฐาน: YYYYMMDD_DocumentName_Unit_Version (เช่น 20260128_PaymentLinkLog_Finance_v1)
- ห้ามจัดเก็บข้อมูลบัตร (PAN เต็ม/CVV) ในหลักฐานทุกชนิด รวมถึงภาพหน้าจอ

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

ภาคผนวก A: แบบฟอร์ม (Templates)

FRM-01: Payment Link Log (บันทึกการส่งลิงก์ชำระเงิน)

วันที่	เวลา	ชื่อลูกค้า/อีเมล	Order/Booking ID	ยอดเงิน	วันหมดอายุลิงก์	สถานะ/Transaction Ref
29/01/26	10:15	กมล / kamon@ex.co	BK00124	48,500	31/01/26	PAID / TX88421

ผู้บันทึก: น.ส. ศศิธร วัฒนะ ผู้ตรวจทาน (Finance): นายกิตติพงษ์ สุขใจ วันที่ตรวจทาน: 2026-01-31

FRM-02: MOTO Processing Log และสคริปต์สนทนามาตรฐาน

สคริปต์มาตรฐาน (ให้พนักงานอ่าน):

- “เพื่อความปลอดภัย บริษัทจะไม่จัดเก็บข้อมูลบัตรของท่าน และจะกรอกข้อมูลเข้าระบบของธนาคาร/ผู้ให้บริการทันที”
- “กรุณาแจ้งหมายเลขบัตรและวันหมดอายุ ข้อมูลนี้จะใช้เพื่อทำรายการครั้งนี้เท่านั้น”
- “กรุณาแจ้งรหัสความปลอดภัย (CVV) เพื่อยืนยันการทำรายการ โดยบริษัทจะไม่บันทึกหรือเก็บรักษาข้อมูลนี้”
- “รายการเสร็จสิ้นแล้ว ขอแจ้งเลขอ้างอิงการทำรายการ (Transaction Reference) …”

บันทึกการทำรายการ (ห้ามบันทึก CVV และห้ามบันทึก PAN เต็ม):

วันที่/เวลา	ชื่อลูกค้า	ช่องทางโทรศัพท์	Booking ID	ยอดเงิน	PAN (แสดง 4 หลักท้าย)	ผลรายการ	Transaction Ref
30/01 14:40	John	+66-4455	BK00131	12,900	4455	OK	MOTO1059

FRM-03: ข้อความมาตรฐานสำหรับลูกค้า (ห้ามส่งข้อมูลบัตรผ่านแชท/อีเมล)

ข้อความสั้น (แชท):

“เพื่อความปลอดภัย บริษัทไม่รับข้อมูลบัตรผ่านแชทหรืออีเมล กรุณาอย่าส่งเลขบัตร/รหัส CVV และโปรดใช้ลิงก์ชำระเงิน (Payment Link) ที่บริษัทส่งให้เพื่อกรอกข้อมูลในระบบธนาคารโดยตรง ขอบคุณค่ะ/ครับ”

ข้อความกรณีลูกค้าส่งข้อมูลบัตรมาแล้ว:

“บริษัทขอความร่วมมือให้ท่านลบข้อความ/ไฟล์ที่มีข้อมูลบัตรดังกล่าว เพื่อความปลอดภัย บริษัทได้ลบข้อมูลที่ได้รับแล้ว และจะส่งลิงก์ชำระเงินที่ปลอดภัยให้ท่านดำเนินการต่อ”

FRM-04: POI/EDC Inventory (ทะเบียนอุปกรณ์รับบัตร)

สาขา/สถานที่	ตำแหน่งใช้งาน	ยี่ห้อ/รุ่น	Serial No.	ผู้รับผิดชอบ	วันที่รับมอบ	สถานะ
HQ	เคาน์เตอร์ 1	Ingenico M250	IGM2500-81	วราภรณ์	15/11/25	ใช้งาน

FRM-05: POI/EDC Inspection Log (บันทึกการตรวจสอบการงัดแงะ)

วันที่/เวลา	สาขา	Serial No.	ซีล/สติ๊กเกอร์ครบ	พอร์ต/สายปกติ	พบอุปกรณ์แปลกปลอม	ผู้ตรวจ	หมายเหตุ/Incident No.
31/01 09:05	HQ	IGM2500-81	ครบ	ปกติ	ไม่พบ	สมชาย	-

FRM-06: System & Account Inventory (ทะเบียนระบบ/บัญชีที่เกี่ยวข้องกับการชำระ)

รายการ	ประเภท (ระบบ/บัญชี/อุปกรณ์)	ผู้ให้บริการ	เจ้าของ	อยู่ในขอบเขต (Y/N)	MFA (Y/N)	วันที่ทบทวนล่าสุด	หมายเหตุ
PSP-FIN01	บัญชี	PSP Bank	Fin Mgr	Y	Y	31/01/26	Payment Link

FRM-07: Access Control Matrix และ Quarterly Access Review

1) ตารางสิทธิ์ (ตัวอย่าง):

บทบาท	Email	PSP/Bank Portal	CRM/Booking	Cloud Storage	หมายเหตุ

Sales	User+MFA	No	User	Limited	-
Finance	User+MFA	Admin+MFA	User	User+MFA	อนุมัติ/คืนเงิน
IT	Admin+MFA	No	Admin	Admin+MFA	ดูแลระบบ

2) Quarterly Access Review (ให้ลงนามรับรอง):

ไตรมาส: Q1/2026 ผู้ทบทวน: นายกิตติพงษ์ สุขใจ วันที่: 2026-03-31 ผลการทบทวน: [x] ไม่มีประเด็น [ ] มีประเด็น (แนบรายการ)

FRM-08: Patch & EDR Status Log

เดือน	เครื่อง/Asset ID	OS/Browser Version	Patch ล่าสุด	EDR สถานะ	ผู้รับผิดชอบ	หมายเหตุ
ม.ค. 2026	LAP-FIN01	Win11 / Ch131	27/01/26	Healthy	IT Admin	ไม่มีค้าง

FRM-09: Log Review Checklist

วันที่	แหล่ง Log	ช่วงเวลาที่ตรวจ	พบความผิดปกติ	สรุป/หลักฐานแนบ	ผู้ตรวจ	Incident No.
31/01/26	M365/PSP	30/01	ไม่พบ	แนบภาพ log	IT Admin	-

FRM-10: Incident Report Form

วันเวลาเหตุการณ์: 02/02/26 16:20 ผู้แจ้ง: พิมพ์ชนก ประเภทเหตุการณ์: ลูกค้าส่งข้อมูลบัตรผ่านแชท

ระบบ/ช่องทางที่เกี่ยวข้อง: LINE OA ผลกระทบเบื้องต้น: พบ PAN บางส่วนในแชท (ไม่มี CVV)

การควบคุมเหตุการณ์ (Containment) ที่ดำเนินการแล้ว: ลบข้อความ, แจ้งลูกค้า, แจ้ง PCI Owner

ต้องแจ้งธนาคาร/PSP หรือไม่: [x] ใช่ [ ] ไม่ใช่ ผู้ประสานงาน: กิตติพงษ์ เวลาแจ้ง: 02/02/26 16:45

บทเรียนและแผนป้องกันซ้ำ: ใช้ข้อความเตือนอัตโนมัติ, ทบทวนอบรมทีมขาย, ใช้ FRM-03 เวอร์ชันล่าสุด

ผู้รับรอง/ผู้อนุมัติการปิดเหตุการณ์: อรทัย (PCI Owner) วันที่: 03/02/26

FRM-11: TPSP Due Diligence Checklist

ชื่อผู้ให้บริการ	บริการที่ให้	อยู่ใน Scope PCI (Y/N)	หลักฐาน AOC/Attestation	วันหมดอายุ	ผู้ติดต่อ	หมายเหตุ
PSP Bank	Pay Link	Y	AOC (PDF)	30/09/26	psp@bank.co	Q3 review

FRM-12: Exception Request & Approval Form (แบบขอข้อยกเว้น)

รายการข้อยกเว้นที่ร้องขอ: ขอขยายเวลาติดตั้ง EDR บนเครื่องสำรองฝ่ายขาย 1 เครื่อง

เหตุผลและความจำเป็น: เครื่องเดิมชำรุดและอยู่ระหว่างเปลี่ยนเครื่องใหม่ ต้องใช้ชั่วคราวเพื่อรับงานลูกค้า

การประเมินความเสี่ยง/มาตรการทดแทน: จำกัดสิทธิ์ใช้งานเฉพาะอีเมลองค์กร, ห้ามเข้าระบบ PSP, เปิด Defender และติดตามทุกวัน

ระยะเวลาใช้ข้อยกเว้น: จาก 2026-02-01 ถึง 2026-02-07 ผู้รับผิดชอบ: IT Admin

อนุมัติโดย: กรรมการผู้จัดการ (ตัวอย่าง) วันที่: 2026-02-01

FRM-13: Evidence Register (รายการหลักฐานสำหรับการตรวจ)

หมวด	หลักฐาน	เจ้าของ	รอบ/ความถี่	ที่เก็บไฟล์	หมายเหตุ
Access	MFA + Review Q1	IT Admin	รายไตรมาส	/PCI/2026/Q1	masked

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

ภาคผนวก B: Audit Evidence Checklist (แนวทางรวบรวมหลักฐาน)

รายการด้านล่างเป็นตัวอย่างหลักฐานที่มักถูกขอระหว่างการตรวจประเมิน/ทบทวนภายใน (ควรเก็บแบบต่อเนื่อง):

- เอกสาร Scope Overview + Data Flow (ฉบับล่าสุด) และหลักฐานการอนุมัติ/ทบทวน
- หลักฐานการตั้งค่า MFA สำหรับ Email, Cloud, PSP/Bank Portal (ภาพหน้าจอ/รายงาน)
- Payment Link Log และรายงานธุรกรรมจากธนาคาร/PSP (ไม่มี PAN เต็ม)
- MOTO Processing Log (ไม่มี CVV) และหลักฐานการควบคุม call recording/การป้องกันการได้ยิน
- POI/EDC Inventory และ POI/EDC Inspection Log ตามความถี่ที่กำหนด (อ้างอิง Targeted Risk Analysis)
- รายงาน EDR/Anti-malware และ Patch Log ของเครื่องที่เกี่ยวข้อง
- ผลการ Quarterly Review และรายการประเด็นพร้อมสถานะแก้ไข
- รายการ TPSP และหลักฐาน AOC/Attestation/สัญญาที่เกี่ยวข้อง
- บันทึกการอบรม Security Awareness และแบบรับทราบของพนักงาน
- Incident Report (ถ้ามี) และบทเรียน/การปรับปรุงกระบวนการ

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

ภาคผนวก C: แนวทาง Mapping กับข้อกำหนด PCI DSS (สรุประดับหัวข้อ)

ตารางนี้เป็นแนวทางเชื่อมโยงเอกสาร/การควบคุมกับกลุ่มข้อกำหนด PCI DSS เพื่อใช้จัด Evidence Pack (ไม่ใช่รายการข้อกำหนดทั้งหมด).

กลุ่มข้อกำหนด	ตัวอย่างสิ่งที่ต้องทำ (Travel Agent)	เอกสาร/แบบฟอร์มที่เกี่ยวข้อง	หลักฐานตัวอย่าง
Access & Authentication	ใช้บัญชีเฉพาะบุคคล + MFA สำหรับระบบสำคัญ	FRM-07, FRM-06	ภาพหน้าจอ MFA, Access review
Card Data Handling	ห้ามเก็บ PAN/CVV ในแชท/อีเมล; ใช้ Payment Link	FRM-01, FRM-03	Payment Link logs, customer templates
Logging & Monitoring	ทบทวนเหตุการณ์สำคัญตามรอบ	FRM-09	Log review checklist
Vulnerability & Malware	EDR + Patch + สแกน/ติดตามช่องโหว่	FRM-08	EDR report, Patch log
Physical/POI	ทำ inventory และตรวจอุปกรณ์ป้องกัน skimming	FRM-04/05	POI inspection records
TPSP Management	รวบรวม AOC/Attestation และทบทวนประจำปี	FRM-11	AOC, TPSP checklist
Incident Response	มีแผนและแบบฟอร์มเหตุการณ์; แจ้งธนาคาร/PSP เมื่อจำเป็น	FRM-10	Incident report, comms log
Awareness & Training	อบรมก่อนเริ่มงานและรายปี; มีแบบทดสอบ/รับทราบ	Training record/ack	Attendance, acknowledgement

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

ภาคผนวก D: ตัวอย่างนโยบาย (Policies) สำหรับ Travel Agent เพื่อการปฏิบัติตาม PCI DSS

ภาคผนวกนี้จัดทำเป็นตัวอย่างนโยบายฉบับย่อที่สามารถนำไปปรับใช้เป็นเอกสารทางการขององค์กรได้ โดยควรกรอกข้อมูลชื่อบริษัท ผู้รับผิดชอบ และช่องทางรับชำระที่ใช้งานจริงให้ครบถ้วนก่อนประกาศใช้.

APPX-P17: นโยบายการรับชำระเงินและการจัดการข้อมูลบัตร (Card Data Handling & Payment Acceptance Policy)

เลขที่เอกสาร	PCI-TA-POL-01	**เวอร์ชัน**	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. องค์กรต้องใช้ช่องทางรับชำระแบบลดการสัมผัสข้อมูลบัตร (No-touch) เป็นหลัก ได้แก่ Payment Link/Hosted Payment Page ของธนาคาร/PSP.
2. ห้ามพนักงานขอ รับ หรือจัดเก็บข้อมูลบัตรผ่านช่องทางสื่อสารทั่วไป (เช่น แชท, อีเมล, เอกสารแนบ, ภาพถ่าย) ไม่ว่ากรณีใด ๆ.
3. ห้ามจัดเก็บ SAD ทุกชนิดโดยเด็ดขาด (รวมถึงการจดบันทึก/ถ่ายภาพ/คัดลอก/ส่งต่อ).
4. กรณี MOTO ให้พนักงานกรอกข้อมูลเข้าสู่ระบบธนาคาร/PSP ทันที และต้องไม่บันทึก CVV และไม่บันทึก PAN เต็มในเอกสาร/ระบบภายใน.
5. เอกสาร/หลักฐานการชำระเงินต้องใช้ข้อมูลที่ถูกปกปิด (Masked) และต้องไม่ปรากฏ PAN เต็มหรือ CVV ในภาพหน้าจอ/ไฟล์ PDF.
6. หากได้รับข้อมูลบัตรจากลูกค้าโดยไม่ตั้งใจ ต้องลบ/ทำลายข้อมูลนั้นทันที และดำเนินการตามขั้นตอน Incident/เหตุการณ์ (FRM-10) โดยไม่บันทึกข้อมูลบัตรลงในรายงาน.

5) ขั้นตอนปฏิบัติที่อ้างอิง

- ขั้นตอน Payment Link (ดูหัวข้อ 6.1 และ FRM-01)
- ขั้นตอน MOTO (ดูหัวข้อ 6.2 และ FRM-02)
- ขั้นตอนเมื่อได้รับข้อมูลบัตรโดยไม่ตั้งใจ (ดูหัวข้อ 6.3 และ FRM-03/FRM-10)

6) บทบาทและความรับผิดชอบ

- PCI Program Owner: กำกับดูแลการปฏิบัติตามและทบทวนหลักฐาน/ประเด็น
- Payment Process Owner (Finance): อนุมัติช่องทางรับชำระ ควบคุมการออก Payment Link และกระทบยอด

- พนักงานปฏิบัติการ/ฝ่ายขาย: ปฏิบัติตามข้อห้ามด้านข้อมูลบัตรอย่างเคร่งครัดและบันทึก Log ตามแบบฟอร์ม

7) การเก็บรักษาเอกสารและหลักฐาน

- Payment Link Log (FRM-01) และรายงานธุรกรรมจากธนาคาร/PSP: เก็บอย่างน้อย 12 เดือน (หรือเป็นไปตามสัญญา/กฎหมาย)
- บันทึก MOTO (FRM-02): เก็บอย่างน้อย 12 เดือน โดยต้องไม่ปรากฏ CVV และไม่ปรากฏ PAN เต็ม
- Incident Report (FRM-10): เก็บตามนโยบายการจัดเก็บ/ทำลายข้อมูลขององค์กร

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P18: นโยบายรหัสผ่านและการยืนยันตัวตน (Password, MFA & Authentication Policy)

เลขที่เอกสาร	PCI-TA-POL-02	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. บัญชีผู้ใช้ทุกบัญชีที่เข้าถึงระบบสำคัญ (อีเมล, คลาวด์, PSP/Bank Portal, CRM/Booking, ระบบบัญชี) ต้องเปิดใช้ MFA.
2. กำหนดให้ใช้รหัสผ่านที่มีความซับซ้อนและความยาวเพียงพอ โดยต้องห้ามใช้รหัสผ่านซ้ำกับระบบอื่นและห้ามแชร์รหัสผ่านระหว่างบุคคล.
3. ห้ามใช้บัญชีร่วม (Shared account) สำหรับการเข้าถึงระบบที่เกี่ยวข้องกับการชำระเงิน ยกเว้นได้รับอนุมัติเป็นข้อยกเว้น (FRM-12) พร้อมมาตรการควบคุมทดแทน.
4. ต้องมีการล็อกหน้าจออัตโนมัติและการยืนยันตัวตนใหม่เมื่อไม่มีการใช้งานตามช่วงเวลาที่กำหนด โดยเฉพาะเครื่องที่ใช้เข้าระบบ PSP/ธนาคาร.
5. การรีเซ็ตรหัสผ่าน/การกู้คืนบัญชีต้องมีการยืนยันตัวตนผู้ขออย่างเหมาะสม และต้องบันทึกการดำเนินการไว้เป็นหลักฐาน.

5) มาตรฐานขั้นต่ำที่แนะนำ

- รหัสผ่านยาวอย่างน้อย 12 ตัวอักษร (แนะนำใช้ Passphrase)
- ห้ามใช้รหัสผ่านที่เดาง่าย/อยู่ในรายการต้องห้าม (เช่น ชื่อบริษัท, 123456, password)
- MFA แนะนำเป็นแอปยืนยันตัวตน (Authenticator) หรือ Hardware token ตามความเหมาะสม

6) การกำกับดูแลและหลักฐาน

- ทะเบียนบัญชี/ระบบ (FRM-06) และหลักฐานเปิดใช้ MFA (ภาพหน้าจอ/รายงาน)
- ผลการทบทวนสิทธิ์รายไตรมาส (FRM-07)

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P19: นโยบายควบคุมการเข้าถึงและการแบ่งแยกหน้าที่ (Access Control & Segregation of Duties Policy)

เลขที่เอกสาร	PCI-TA-POL-03	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS
และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. การให้สิทธิ์ต้องยึดหลัก Need-to-Know และ Least Privilege โดยกำหนดตามบทบาทงาน (Role-based access).
2. ต้องแยกหน้าที่ (Segregation of Duties) ระหว่างการสร้างยอด/ออก Payment Link, การอนุมัติคืนเงิน, และการกระทบยอดบัญชี อย่างเหมาะสม.
3. การอนุมัติสิทธิ์ระดับสูง (Admin/Approver) ต้องได้รับอนุมัติจากผู้บริหาร/เจ้าของกระบวนการ และต้องบันทึกเป็นหลักฐาน.
4. ต้องทบทวนสิทธิ์การเข้าถึงอย่างน้อยรายไตรมาส และเพิกถอนสิทธิ์ทันทีเมื่อพนักงานพ้นสภาพ/เปลี่ยนบทบาทงาน.
5. ห้ามแชร์บัญชีผู้ใช้หรือใช้บัญชีส่วนบุคคลสำหรับการทำงานขององค์กร (ยกเว้นได้รับอนุมัติเป็นกรณีพิเศษ).

5) ขั้นตอนที่เกี่ยวข้อง

- Onboarding/Offboarding (ดูหัวข้อ 6.5)
- Access Control Matrix และ Quarterly Access Review (FRM-07)
- System & Account Inventory (FRM-06)

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P20: นโยบายความปลอดภัยทางกายภาพและการจัดการอุปกรณ์รับบัตร (Physical & POI/EDC Handling Policy)

เลขที่เอกสาร	PCI-TA-POL-04	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS
และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. ต้องควบคุมการเข้าถึงพื้นที่ทำงาน/อุปกรณ์ที่เกี่ยวข้องกับการชำระเงิน โดยเฉพาะบริเวณที่มี EDC/POI หรือเครื่องที่ใช้เข้าระบบ PSP/ธนาคาร.
2. หากมีอุปกรณ์ EDC/POI ต้องจัดทำทะเบียนอุปกรณ์ (FRM-04) และกำหนดผู้รับผิดชอบประจำอุปกรณ์.
3. ต้องตรวจสอบการงัดแงะ/อุปกรณ์แปลกปลอมตามรอบที่กำหนด และบันทึกผล (FRM-05).
4. ห้ามย้ายตำแหน่ง ติดตั้ง เพิ่มอุปกรณ์ หรือซ่อมแซม EDC/POI โดยไม่ได้รับอนุญาตจากผู้รับผิดชอบและธนาคาร/PSP.
5. การทำลาย/ส่งคืนอุปกรณ์ต้องเป็นไปตามข้อกำหนดผู้ให้บริการ และต้องเก็บหลักฐานการส่งคืน/ทำลาย.

5) มาตรการขั้นต่ำ

- กำหนดพื้นที่วาง EDC/POI ที่มองเห็นได้ และลดโอกาสถูกสลับอุปกรณ์
- มีรูปภาพอ้างอิงอุปกรณ์ (ยี่ห้อ/รุ่น/Serial) เพื่อใช้ตรวจเทียบ

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P21: นโยบายการป้องกันมัลแวร์/การจัดการช่องโหว่/การจัดการแพตช์ (Malware, Vulnerability & Patch Management Policy)

เลขที่เอกสาร	PCI-TA-POL-05	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. เครื่องคอมพิวเตอร์/อุปกรณ์ที่ใช้ทำงานต้องมีมาตรการป้องกันมัลแวร์ (เช่น EDR/Anti-malware) ที่เปิดใช้งานและอัปเดตตลอดเวลา.
2. ต้องติดตั้งอัปเดตความปลอดภัย (Patch) ของระบบปฏิบัติการ/เบราว์เซอร์/ซอฟต์แวร์ที่เกี่ยวข้องอย่างสม่ำเสมอ และต้องบันทึกหลักฐานการดำเนินการ.
3. ต้องมีการประเมินและจัดลำดับความเสี่ยงของช่องโหว่ (Vulnerability Risk Ranking) และกำหนดกรอบเวลาแก้ไขตามระดับความรุนแรง.
4. ห้ามปิดการทำงานของ EDR/Anti-malware หรือเปลี่ยนแปลงการตั้งค่าโดยไม่ได้รับอนุญาต.
5. ต้องมีการตรวจสอบ/ทบทวนสถานะ EDR และ Patch อย่างน้อยรายเดือน และรายงานประเด็นค้างแก้ไขให้ผู้รับผิดชอบทราบ.

5) หลักฐานขั้นต่ำ

- Patch & EDR Status Log (FRM-08)
- รายงาน/หน้าจอสรุปจากระบบ EDR/MDM
- ทะเบียนอุปกรณ์/ระบบ (FRM-06)

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P22: นโยบายการบันทึกเหตุการณ์และการเฝ้าระวัง (Logging & Monitoring Policy)

เลขที่เอกสาร	PCI-TA-POL-06	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS
และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. ระบบที่เกี่ยวข้องกับการชำระเงินต้องมีการบันทึกเหตุการณ์สำคัญ (เช่น การเข้าสู่ระบบ, การเปลี่ยนสิทธิ์, การทำธุรกรรมสำคัญ) ตามความเหมาะสมของผู้ให้บริการและระบบที่องค์กรควบคุมได้.
2. ต้องทบทวนเหตุการณ์ (Log Review) ตามรอบที่กำหนด (รายวัน/รายสัปดาห์/รายเดือน) โดยพิจารณาตามความเสี่ยงและปริมาณธุรกรรม.
3. เหตุการณ์ผิดปกติที่มีนัยสำคัญต้องถูกยกระดับเป็น Incident และดำเนินการตาม Incident Response Plan.
4. ต้องกำหนดผู้รับผิดชอบการทบทวน Log และจัดเก็บหลักฐานการทบทวน (FRM-09) เพื่อการตรวจสอบย้อนหลัง.
5. ต้องรักษาความถูกต้องของเวลา (Time synchronization) ในระบบที่องค์กรควบคุมได้ และใช้เวลามาตรฐานเดียวกันเพื่อการสืบค้นเหตุการณ์.

5) หลักฐานขั้นต่ำ

- Log Review Checklist (FRM-09) พร้อมหลักฐานประกอบ
- ผลการ Quarterly Review ที่รวมการทบทวน Monitoring controls

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P23: นโยบายการจัดการผู้ให้บริการภายนอก (Third-Party Service Provider Policy)

เลขที่เอกสาร	PCI-TA-POL-07	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS
และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. ก่อนว่าจ้างผู้ให้บริการภายนอกที่เกี่ยวข้องกับการชำระเงิน/ข้อมูล ต้องมีการประเมินความเหมาะสม (Due Diligence) และบันทึกผล (FRM-11).
2. ต้องจัดทำและรักษารายการผู้ให้บริการภายนอก (TPSP Register) พร้อมขอบเขตบริการและความเกี่ยวข้องกับ PCI.
3. ต้องขอหลักฐานการปฏิบัติตาม PCI ของผู้ให้บริการตามความเหมาะสม (เช่น AOC/Attestation/รายงานการรับรอง) และทบทวนอย่างน้อยปีละครั้ง.
4. สัญญาจ้างต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัย การแจ้งเหตุการณ์ การคุ้มครองข้อมูล และสิทธิในการตรวจสอบตามความเหมาะสม.
5. กรณีผู้ให้บริการมีเหตุการณ์ด้านความปลอดภัยที่อาจกระทบองค์กร ต้องแจ้งองค์กรภายในกรอบเวลาที่กำหนดและร่วมดำเนินการสืบสวน/แก้ไข.

5) หลักฐานขั้นต่ำ

- TPSP Due Diligence Checklist (FRM-11)
- สำเนา AOC/Attestation/สัญญา/ข้อตกลงการให้บริการ (SLA)

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P24: นโยบายการอบรมและสร้างความตระหนักรู้ (Security Awareness Policy)

เลขที่เอกสาร	PCI-TA-POL-08	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS
และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. พนักงานทุกคนที่เกี่ยวข้องกับการรับชำระเงินต้องได้รับการอบรมความตระหนักรู้ด้านความมั่นคงปลอดภัยและ PCI ก่อนเริ่มปฏิบัติงานและอย่างน้อยปีละ 1 ครั้ง.
2. เนื้อหาการอบรมต้องครอบคลุมข้อห้ามสำคัญ (เช่น ห้ามเก็บ CVV, ห้ามรับข้อมูลบัตรผ่านแชท) กระบวนการ Payment Link/MOTO และการแจ้งเหตุการณ์.
3. ต้องมีการทดสอบความเข้าใจ/แบบประเมินผล และต้องเก็บบันทึกการเข้าร่วมอบรมเป็นหลักฐาน.
4. ต้องมีการสื่อสารเตือนภัย/กรณีศึกษาอย่างสม่ำเสมอ (เช่น รายไตรมาส) ตามความเสี่ยงและเหตุการณ์ที่เกิดขึ้นจริง.

5) หลักฐานขั้นต่ำ

- Training Record / Attendance / ผลแบบทดสอบ
- Acknowledgement Form (แบบรับทราบหน้าที่และข้อห้าม)

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบ ผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P25: นโยบายการวิเคราะห์ความเสี่ยงแบบมุ่งเป้า (PCI Targeted Risk Analysis Policy)

เลขที่เอกสาร	PCI-TA-POL-09	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS
และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. องค์กรต้องจัดทำการวิเคราะห์ความเสี่ยงแบบมุ่งเป้า (Targeted Risk Analysis - TRA) สำหรับกิจกรรม/การควบคุมที่ PCI DSS ระบุให้พิจารณาความถี่หรือวิธีการตามความเสี่ยง.
2. TRA ต้องระบุ (ก) ขอบเขต/วัตถุประสงค์ (ข) ปัจจัยความเสี่ยง (ค) วิธีการให้คะแนน/การตัดสินใจ (ง) ความถี่ที่กำหนด และ (จ) การอนุมัติ.
3. ต้องทบทวน TRA อย่างน้อยปีละครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการ/ระบบ/ผู้ให้บริการ หรือเมื่อมีเหตุการณ์ด้านความปลอดภัย.
4. ความถี่การตรวจ POI/EDC, การทบทวน Log และกิจกรรมที่เกี่ยวข้องต้องอ้างอิงผล TRA และต้องเก็บหลักฐานการดำเนินการตามความถี่นั้น.

5) หลักฐานขั้นต่ำ

- แบบฟอร์ม Targeted Risk Analysis (เช่น Template) พร้อมการอนุมัติ
- บันทึกที่เชื่อมโยงกับความถี่จาก TRA (FRM-05, FRM-09 เป็นต้น)

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.

ALPHASEC CO., LTD.
Park Ventures Ecoplex Level 18, 57 Witthayu Rd., Lumphini,
Pathum Wan, Bangkok 10330 TEL: +662 309 3559

APPX-P26: นโยบายการตอบสนองเหตุการณ์ (Incident Response Policy/Plan)

เลขที่เอกสาร	PCI-TA-POL-10	เวอร์ชัน	1.0
หน่วยงานเจ้าของเอกสาร	ฝ่ายกำกับดูแล PCI / ฝ่ายเทคโนโลยีสารสนเทศ / ฝ่ายการเงิน	**ผู้อนุมัติ**	[กรรมการผู้จัดการ/ผู้บริหารสูงสุด]
วันที่ประกาศใช้	2026-01-28	**รอบทบทวน**	อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงสาระสำคัญ
ขอบเขตอ้างอิง	PCI DSS v4.x (แนวปฏิบัติ)	**สถานะ**	ร่าง/ใช้งาน (ตามการอนุมัติ)

1) วัตถุประสงค์

เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการควบคุมความมั่นคงปลอดภัยของข้อมูล การปฏิบัติงาน และการเก็บรักษาหลักฐาน ให้เป็นไปตามมาตรฐาน PCI DSS และข้อกำหนดที่เกี่ยวข้องของธนาคาร/ผู้ให้บริการรับชำระ (PSP) สำหรับการดำเนินงานของธุรกิจตัวแทนท่องเที่ยว.

2) ขอบเขต

- พนักงานทุกคน ผู้รับเหมา และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบ/ข้อมูลที่เกี่ยวข้องกับการรับชำระเงินด้วยบัตร
- ช่องทางรับชำระเงินทั้งหมดขององค์กร (เช่น Payment Link/Hosted Payment Page, MOTO, EDC/POI หากมี)
- ระบบสนับสนุนที่เกี่ยวข้อง (อีเมล, เครื่องคอมพิวเตอร์/มือถือทำงาน, ระบบจอง/CRM, ระบบบัญชี/การเงิน, ระบบจัดเก็บไฟล์/คลาวด์)

3) คำจำกัดความ

- CHD: ข้อมูลผู้ถือบัตร (เช่น PAN)
- SAD: ข้อมูลยืนยันตัวตนที่อ่อนไหว (เช่น CVV/CVC, Track data, PIN) ซึ่งห้ามจัดเก็บภายหลังการทำรายการ
- CDE: สภาพแวดล้อมที่มีการจัดเก็บ/ประมวลผล/ส่งผ่านข้อมูลผู้ถือบัตร
- PSP/ธนาคาร: ผู้ให้บริการรับชำระเงินหรือเกตเวย์ชำระเงินที่องค์กรทำสัญญาใช้งาน

4) ข้อกำหนดนโยบาย (Policy Statements)

1. องค์กรต้องมีแผนตอบสนองเหตุการณ์ (Incident Response Plan) ครอบคลุมการแจ้งเหตุ การควบคุมเหตุการณ์ การสืบสวน การกู้คืน และการสื่อสารกับผู้มีส่วนได้ส่วนเสีย.
2. ต้องกำหนดเกณฑ์การยกระดับเหตุการณ์ที่เกี่ยวข้องกับข้อมูลบัตร/การชำระเงิน และกำหนดช่องทางประสานงานกับธนาคาร/PSP และหน่วยงานที่เกี่ยวข้อง.
3. เมื่อเกิดเหตุการณ์ต้องบันทึกข้อเท็จจริงในแบบฟอร์ม Incident (FRM-10) โดยห้ามบันทึก PAN เต็มหรือ CVV ลงในรายงาน.
4. ต้องมีการฝึกซ้อม/ทดสอบแผนอย่างน้อยปีละ 1 ครั้ง (Tabletop Exercise) และเก็บรายงานการฝึกซ้อม.
5. หลังเหตุการณ์ต้องจัดทำบทเรียน (Lessons learned) และแผนป้องกันซ้ำ พร้อมติดตามการแก้ไขจนปิดประเด็น.

5) ขั้นตอนอ้างอิง (ขั้นต่ำ)

- การแจ้งเหตุ: พนักงาน -> หัวหน้างาน/PCI Owner -> ทีม IT/Finance -> ธนาคาร/PSP (ตามความจำเป็น)
- การควบคุมเหตุการณ์: ระงับบัญชี/เพิกถอนสิทธิ์/แยกเครื่อง/หยุดใช้งานอุปกรณ์ที่สงสัย
- การกู้คืนและติดตาม: ทำความสะอาดเครื่อง, เปลี่ยนรหัสผ่าน/โทเคน, ทบทวน Log และจัดทำรายงานปิดเหตุ

8) การจัดการข้อยกเว้น

กรณีจำเป็นต้องขอยกเว้นจากข้อกำหนดในนโยบายนี้ ต้องจัดทำคำขอข้อยกเว้น (FRM-12) พร้อมการประเมินความเสี่ยงและมาตรการควบคุมทดแทน โดยต้องได้รับการอนุมัติจากผู้บริหารก่อนดำเนินการ.

9) การบังคับใช้และบทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการฝ่าฝืนระเบียบขององค์กร และอาจมีผลต่อการดำเนินการทางวินัย รวมถึงการเพิกถอนสิทธิ์การเข้าถึงระบบ ทั้งนี้ให้เป็นไปตามข้อบังคับขององค์กรและกฎหมายที่เกี่ยวข้อง.

10) การทบทวนและปรับปรุง

นโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงกระบวนการรับชำระเงิน ระบบ ผู้ให้บริการ หรือข้อกำหนดจาก PCI/ธนาคาร/PSP รวมถึงเมื่อเกิดเหตุการณ์ด้านความปลอดภัยที่มีนัยสำคัญ.