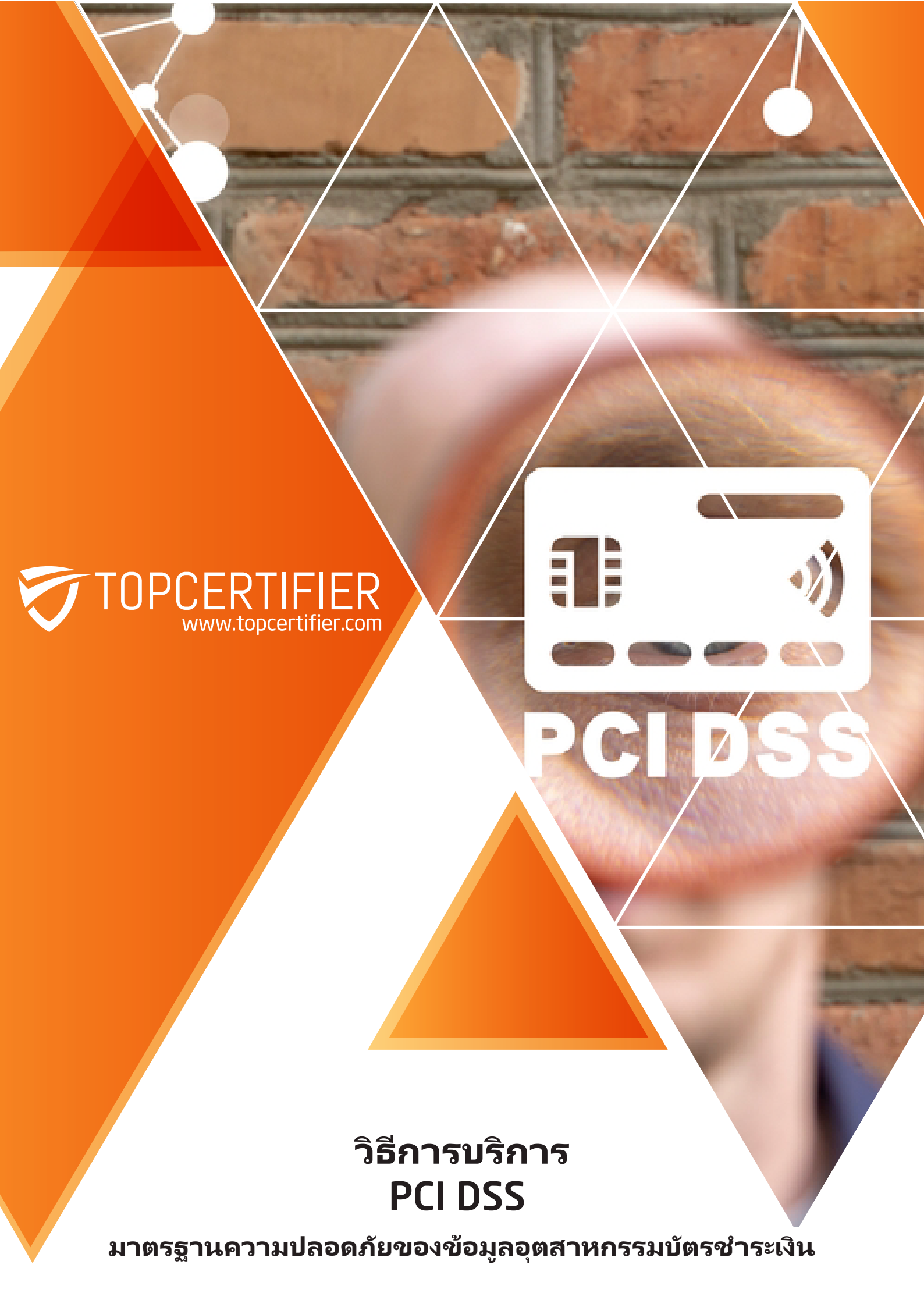

TOPCERTIFIER
www.topcertifier.com

วิธีการบริการ
PCI DSS

มาตรฐานความปลอดภัยของข้อมูลอุตสาหกรรมบัตรชำระเงิน

TOPCERTIFIER
www.topcertifier.com

บทนำ PCI DSS

TOPCertifier นำเสนอรายการตรวจสอบการวิเคราะห์ช่องว่าง PCI DSS แบบง่ายเพื่อช่วยคุณระบุพื้นที่ทีองค์กรของคุณอาจต้องได้รับการปรับปรุงเพื่อให้สอดคล้องกับ PCI DSS (Payment Card Industry Data Security Standard) รายการตรวจสอบนี้มีพื้นฐาน กรอบการทำงานสำหรับการประเมินความสอดคล้องของคุณกับ PCI DSS และทำหน้าที่เป็นก้าวแรกในการประเมินการปฏิบัติตามของคุณ

ส่วนที 1: ความปลอดภัยของข้อมูล

- เป็นข้อมูลบัตรชำระเงินที่ได้รับการเข้ารหัสอย่างเหมาะสมระหว่างการส่งและการจัดเก็บ
- เป็นข้อมูลการตรวจสอบสิทธิ์ที่ละเอียดอ่อน เช่น หมายเลข CVV ซึ่งไม่ได้จัดเก็บไว้หลังการอนุญาต
- มีนโยบายในการรักษาความปลอดภัยข้อมูลผู้ถือบัตรและข้อมูลการตรวจสอบสิทธิ์ที่ละเอียดอ่อนหรือไม่

ส่วนที 2: ความปลอดภัยของเครือข่ายและไฟร์วอลล์

- มีการตรวจสอบและอัปเดตการกำหนดค่าเครือข่ายและกฎไฟร์วอลล์เป็นประจำ
- มีแผนภาพเครือข่ายที่แสดงการไหลของข้อมูลผู้ถือบัตรหรือไม่
- มีนโยบายและขั้นตอนด้านความปลอดภัยสำหรับการรักษาความปลอดภัยโครงสร้างพื้นฐานเครือข่ายหรือไม่

ส่วนที 3: การควบคุมการเข้าถึง

- สิทธิ์การเข้าถึงของผู้ใช้ถูกจำกัดตามความจำเป็นทางธุรกิจหรือไม่
- คือการรับรองความถูกต้องแบบหลายปัจจัยที่ใช้สำหรับการเข้าถึงเครือข่ายระยะไกล
- บัญชีผู้ใช้จะถูกปิดการใช้งานทันทีเมื่อมีการยุติหรือมีการเปลี่ยนแปลงบทบาท

ส่วนที 4: การจัดการความเปราะบาง

- Are security patches applied promptly to address vulnerabilities
- is there a process for vulnerability scanning and penetration testing
- Are critical security patches reviewed and prioritized based on risk

ส่วนที 5: นโยบายและขั้นตอนด้านความปลอดภัย

- มีการจัดทำเอกสารและเผยแพร่นโยบายและขั้นตอนด้านความปลอดภัยที่ครอบคลุม
- มีโครงการฝึกอบรมจิตสำนึกด้านความปลอดภัยให้กับพนักงานหรือไม่
- มีการตรวจสอบและอัปเดตนโยบายความปลอดภัยตามความจำเป็นหรือไม่

ส่วนที 6: การติดตามและการบันทึก

- กิจกรรมด้านความปลอดภัยและบันทึกได้รับการตรวจสอบและติดตามอย่างสม่ำเสมอ
- มีกระบวนการแจ้งเตือนกิจกรรมที่น่าสงสัยแบบเรียลไทม์หรือไม่
- มีการกำหนดขั้นตอนการตอบสนองต่อเหตุการณ์และการรายงานหรือไม่

ส่วนที 7: การตอบสนองต่อเหตุการณ์

- มีแผนตอบสนองต่อเหตุการณ์โดยสรุปขั้นตอนในการจัดการกับเหตุการณ์ด้านความปลอดภัยหรือไม่
- พนักงานได้รับการฝึกอบรมเกียวกับวิธีการรับรู้และรายงานเหตุการณ์ด้านความปลอดภัยหรือไม่
- มีกระบวนการที่จัดทำเป็นเอกสารสำหรับการวิเคราะห์และปรับปรุงหลังเหตุการณ์หรือไม่

ส่วนที 8: การรักษาความปลอดภัยทางกายภาพ

- มีการควบคุมการเข้าถึงทางกายภาพเพื่อป้องกันการเข้าถึงข้อมูลผู้ถือบัตรโดยไม่ได้รับอนุญาต
- คือการเข้าถึงพื้นที่ปลอดภัยที่ถูกจำกัดและตรวจสอบ
- มีการเฝ้าระวังวิดีโอและบันทึกผู้เยียมชมสำหรับพื้นที่ละเอียดอ่อนหรือไม่

ส่วนที 9: ผู้ให้บริการบุคคลที่สาม

- ผู้จำหน่ายบุคคลที่สามได้รับการประเมินการปฏิบัติตามข้อกำหนดของ PCI DSS หรือไม่
- มีข้อตกลงเป็นลายลักษณ์อักษรกับผู้ให้บริการเพื่อให้มันใจในการปกป้องข้อมูลของผู้ถือบัตร
- มีกระบวนการในการติดตามและประเมินแนวทางปฏิบัติด้านความปลอดภัยของบุคคลที่สามหรือไม่

โปรดทราบว่ารายการตรวจสอบนี้ให้ภาพรวมระดับสูง และจำเป็นต้องดำเนินการ การวิเคราะห์อย่างละเอียดตามกระบวนการและบริบทขององค์กรของคุณโดยเฉพาะ นอกจากนียังเป็น แนะนำให้ร่วมมือกับผู้เชียวชาญหรือทีปรึกษาของ PCI DSS เพื่อดำเนินการอย่างครอบคลุม การวิเคราะห์ช่องว่างสำหรับองค์กรของคุณ