ENTERPRISE TRUST · DATA PROTECTION · GOVERNANCE

ความปลอดภัยของข้อมูล เริ่มจากความไว้วางใจ

สรุปแนวทางดูแลข้อมูลพนักงาน สมรรถนะ และโครงสร้างองค์กรของ **GapGroot** สำหรับผู้บริหาร HR และทีม IT

สาระสำคัญ

7 มาตรการด้าน Security & Privacy

ข้อมูลจากรายงานต้นฉบับ

จากการแยกข้อมูลระหว่างองค์กร ไปจนถึงการควบคุมสิทธิ์ การสำรองข้อมูล และช่องทางชำระเงิน โดยเรียบเรียงใหม่เพื่อช่วยให้ผู้บริหารและ HR เห็นภาพได้รวดเร็ว

สิ่งที่องค์กรควรมั่นใจ ก่อนนำแพลตฟอร์มมาใช้

01

ข้อมูลเป็นสัดส่วน

แยกข้อมูลของแต่ละบริษัทตามขอบเขตองค์กร

02

เข้าถึงตามหน้าที่

กำหนดสิทธิ์แยกพนักงาน ผู้จัดการ ผู้บริหาร และ HR

03

ตรวจสอบและกู้คืน

มีกลไกบันทึกเหตุการณ์ สำรอง และย้อนคืนข้อมูล

อ่านเอกสารนี้อย่างไร

หน้านี้สรุปภาพรวม · หน้า 2–3 อธิบายมาตรการทั้ง 7 ด้าน · หน้า 4 เป็นตารางเทียบศัพท์และรายการหลักฐานที่ควรขอประกอบการประเมินก่อนใช้งานระดับองค์กร

SECURITY FOUNDATION

4 มาตรการหลักเพื่อปกป้องข้อมูล

01–04 / 07

แนวทางที่รายงานต้นฉบับระบุว่าระบบใช้ในการควบคุมการเข้าถึงและลดความเสี่ยงระหว่างใช้งาน

01 แยกข้อมูลแต่ละองค์กร

Multi-Tenant Data Isolation

จำกัดขอบเขตข้อมูล

เข้าใจง่าย เหมือนแต่ละบริษัทมีตู้เซฟส่วนตัว เปิดได้เฉพาะกุญแจของตนเอง

รายงานระบุการใช้ Organization Boundary Isolation เพื่อแยกข้อมูลพนักงาน โครงสร้างตำแหน่ง และผลการประเมินระหว่างองค์กรที่ใช้งานระบบเดียวกัน

02 เข้ารหัสข้อมูลระหว่างส่งและจัดเก็บ

Encryption in Transit & at Rest

ลดการเปิดเผยข้อมูล

เข้าใจง่าย เหมือนส่งข้อมูลผ่านช่องทางปิดล็อก และเก็บข้อมูลสำคัญในรูปแบบที่อ่านไม่ได้หากไม่มีสิทธิ์

รายงานระบุการสื่อสารผ่าน HTTPS (SSL/TLS) และการเข้ารหัสข้อมูลที่มีความอ่อนไหวในฐานข้อมูลด้วย AES-256

03 สิทธิ์ตามบทบาทและความรับผิดชอบ

Role-Based Access Control (RBAC)

ดูเฉพาะที่จำเป็น

เข้าใจง่าย เหมือนบัตรผ่านเข้าอาคาร แต่ละบทบาทเปิดได้เฉพาะพื้นที่ที่ได้รับอนุญาต

แบ่งมุมมองของพนักงาน ผู้จัดการ ผู้บริหาร และ HR พร้อมกำหนดขอบเขตข้อมูลตามหน้าที่ และจำกัดการแสดงข้อมูลส่วนตัวในบางมุมมอง

04 ป้องกันการโจมตีที่หน้าเว็บไซต์

Web Application Firewall (WAF)

กรองคำขอผิดปกติ

เข้าใจง่าย เหมือนเจ้าหน้าที่เฝ้าทางเข้า คัดกรองกิจกรรมที่มีลักษณะเสี่ยง

รายงานระบุการใช้งาน ModSecurity และ Imunify360 รวมทั้งกฎปฏิเสธการเข้าถึงไฟล์สำรองบางประเภท เช่น .zip, .tar, .bak และ .sql

CONTINUITY & RESPONSIBLE HANDLING

ความต่อเนื่อง ความเป็นส่วนตัว และธุรกรรม

05–07 / 07

การวางระบบที่ดีควรช่วยลดผลกระทบเมื่อเกิดเหตุผิดปกติ และจัดการข้อมูลอย่างโปร่งใส

05 สำรองข้อมูลและเตรียมย้อนคืนระบบ

Automated Backup & Rollback

รับมือเหตุขัดข้อง

เข้าใจง่าย เหมือนเก็บสำเนาเอกสารสำคัญไว้ และมีแผนกลับไปยังฉบับที่ใช้งานได้

รายงานระบุการสำรองข้อมูลตามรอบ และกลไก Automated Rollback Archive ก่อนอัปเดตระบบเพื่อช่วยย้อนกลับไปยังสถานะก่อนหน้าเมื่อจำเป็น

06 คำนึงถึง PDPA และบันทึกการเข้าถึง

Privacy by Design & Audit Trail

ตรวจสอบย้อนหลัง

เข้าใจง่าย เหมือนมีทะเบียนการเข้าใช้ข้อมูลสำคัญ พร้อมกำหนดว่าใครควรเห็นอะไร

รายงานระบุการออกแบบกระบวนการยินยอม การจำกัดการแสดงข้อมูลส่วนบุคคล และ Audit Log สำหรับการเข้าถึงข้อมูลสำคัญ ทั้งนี้ การปฏิบัติตาม PDPA ต้องประเมินทั้งระบบและกระบวนการขององค์กรร่วมกัน

07 ให้ผู้ให้บริการชำระเงินจัดการธุรกรรม

Payment Gateway Separation

ลดข้อมูลบัตรในระบบ

เข้าใจง่าย เหมือนให้ผู้ให้บริการรับชำระเงินโดยตรง แทนการเก็บรายละเอียดบัตรไว้ในแพลตฟอร์ม

รายงานระบุการเชื่อมต่อกับ PaySolution สำหรับการซื้อแพ็กเกจและเครดิต AI และระบุว่า GapGroot ไม่จัดเก็บเลขบัตรเครดิตหรือรหัส PIN ในระบบของตน

สิ่งที่ควรขอให้ทีม IT ยืนยันเพิ่มเติม

BACKUP & RECOVERY

- ความถี่การสำรองข้อมูลและระยะเวลาการเก็บ
- ผลการทดสอบกู้คืนล่าสุด

PRIVACY & SECURITY

- หลักฐานการทดสอบสิทธิ์และการแยกข้อมูล
- นโยบายการเก็บ/ลบข้อมูลและการจัดการเหตุการณ์

DECISION-READY REFERENCE

ศัพท์ด้าน IT ที่ HR เข้าใจได้ทันที

Quick Reference

สรุปคำสำคัญจากเอกสารต้นฉบับให้ทีม HR และผู้บริหารใช้พูดคุยกับ IT ได้ง่ายขึ้น

มาตรการ	เปรียบเทียบให้เห็นภาพ	ประโยชน์ต่อองค์กร
Multi-Tenant Isolation	ตู้เซฟข้อมูลแยกแต่ละบริษัท	ลดความเสี่ยงที่ข้อมูลพนักงานปะปนข้ามองค์กร
SSL / TLS	ช่องทางส่งข้อมูลที่มีการเข้ารหัส	คุ้มครองข้อมูลที่ส่งระหว่างเบราว์เซอร์กับบริการ
Role-Based Access Control	บัตรผ่านที่ให้สิทธิ์ตามหน้าที่	พนักงานและผู้จัดการเห็นข้อมูลตามขอบเขต
Web Application Firewall	ระบบคัดกรองคำขอที่น่าสงสัย	ช่วยกรองการโจมตีที่ชั้นเว็บไซต์
Audit Log	สมุดบันทึกกิจกรรมดิจิทัล	ช่วยตรวจสอบเหตุการณ์ที่สำคัญย้อนหลัง
Automated Rollback	ระบบย้อนกลับไปยังสถานะก่อนอัปเดต	ลดผลกระทบเมื่อการอัปเดตเกิดปัญหา

สถานะผลตรวจตามรายงานต้นฉบับ

273
รายการทดสอบ

ระบุว่าชุดทดสอบ Backend ผ่านครบทุกกรณี

รายงานลงวันที่ 24 ตุลาคม 2026 ระบุผลทดสอบ 273 รายการ ผ่าน 100% พร้อมอ้างถึงการตรวจเว็บเซิร์ฟเวอร์ Security Headers และกระบวนการสำรองข้อมูล