Incident handler's journal

Date: 23-08-2024	**Entry: 001** Initial vulnerability assessment of public-facing PostgreSQL database
Description	The company’s cloud-hosted PostgreSQL database has been publicly accessible (port 5432) without any authentication or filtering since launch. It stores ~1.4M records of customer PII and supports marketing campaigns responsible for ~35% of monthly revenue. This constitutes a high-severity misconfiguration.
Tool(s) used	Manual assessment, Nmap (for port visibility confirmation), Nessus (vulnerability scanning), PostgreSQL CLI, and SIEM logs (for access review).
The 5 W's	**Who** caused the incident? Misconfiguration was introduced at launch by DevOps; no formal security review occurred. **What** happened? Database open to the public with default roles, no authentication, and no encryption in place. **When** did the incident occur? Ongoing since company launch—approx. 3 years of exposure. **Where** did the incident happen? Cloud-hosted PostgreSQL cluster serving global access via open port 5432. **Why** did the incident happen? Security controls were not implemented due to initial startup speed prioritization and lack of cybersecurity staffing.
Additional notes	Immediate remediation is required to avoid GDPR violations, potential breach, and financial losses. First four controls (P1–P4) must be prioritized within 10 business days. Recommend integrating quarterly NIST SP 800-30 assessments moving forward.