Incident handler's journal

Date: 01-04-2025	**Entry: 001** Initial investigation of recent customer data breach.
Description	A data breach occurred, exposing users' personal information (names, addresses). The incident was traced to insecure access controls and missing network defenses.
Tool(s) used	
The 5 W's	**Who** caused the incident? Likely an external attacker exploiting weak access controls and default credentials. Internal behavior (shared passwords) increased risk. **What** happened? The attacker accessed the production database and exfiltrated sensitive customer data. There were no firewall rules or MFA to prevent access o detect anomalies in time. **When** did the incident occur? Detected on April 1, 2025. **Where** did the incident happen? Access was made through the public-facing web portal, targeting the backend database. **Why** did the incident happen? Shared passwords violated AC-2 (Account Management) Default admin credentials violated IA-5(1) (Password Management) No MFA violated IA-2 (Identification and Authentication) No firewall traffic filtering violated SC-7 (Boundary Protection)
Additional notes	Full forensic investigation is ongoing. Temporary containment measures: forced credential rotation, MFA rollout initiated, emergency firewall rules deployed. Recommend mapping corrective actions to NIST CSF: PR.AA, PR.PS, DE.CM, RS.MI. Incident will be reported to stakeholders as per RS.CO.