Incident handler's journal

Date: 10/03/2023	**Entry: 001**
Description	Unauthorized access by a former employee account with administrative privileges that should have been deactivated in 2019.
Tool(s) used	SIEM (Security Information and Event Management) tool for activity logging and anomaly detection.
The 5 W's	**Who** caused the incident? Robert Taylor Jr. **What** happened? An inactive account with admin privileges was used to access the system. **When** did the incident occur? 10/03/2023 at 8:29:57 AM **Where** did the incident happen? Device: Up2-NoGud, IP Address: 152.207.255.255 **Why** did the incident happen? The account was not deactivated after the end date (12/27/2019). Weak access controls, lack of RBAC (Role-Based Access Control), no automated deprovisioning, and no alerting contributed to the incident.
Additional notes	Recommendations include enforcing RBAC, enabling automated account deactivation, implementing MFA (Multi-Factor Authentication), conducting regular access reviews, and assigning clear access control ownership.