## **Access Controls Breach Report**

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | * This incident was caused by *Robert Taylor Jr.* who is a *Legal Attorney* contracted to the company. * The event occurred on *10/03/2023* at *8:29:57 AM.* * The device used in the attack was a computer with the username *Up2-No-Gud* IP address *152.207.255.255.* | * The user had *Administrative* access to the system. * I do not believe that this user’s account should have been active as the user’s session at the company had ended at the time of the attack. | I recommend the following actions to prevent such an incident from occurring again:   * We should add a system which automatically deactivates a user’s account after 25 days without use. * We should implement a multi-factor authentication system to accurately verify users before being allowed access to the system. * We should set up alerts for any suspicious activity which does not align with the normal operations. |