

## Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
<b>Authorization /authentication</b>	<i>The incident occurred on 10/03/2023 at 8:29:57 am (5 days ago). The device used was the computer Up2-NoGud, which had the IP 152.207.255.255. After comparing the IP address with the list of all employees, the IP led to a former legal attorney, Robert Taylor Jr.</i>	<i>Robert Taylor Jr. had the authorization level of an admin; however, he had stopped working for the company on 12/27/2019, which indicates that proper measures to deprovision the user were not taken, and his access to the system was not removed after his departure, allowing this incident to occur.</i>	<i>The company should implement the principle of least privilege, ensuring that user access is appropriately restricted based on their role. Additionally, users should be properly deprovisioned upon departure, and regular checks should be performed to verify whether users still require access. For example: 1-User accounts should expire after 30 days. 2-Contractors should have limited access to business resources. 3-Enable MFA.</i>