MATT BACAK'S CHECKLIST

Checklist 15 - Managing User Privileges

Project Name: _____ **Date:** _____

		Yes	No
	Privileged user accounts are highly targeted by hackers owing to the high level of authorized access to confidential data, as well as administrative authorities to download critical data. To minimize risks associated with the hacking of users with privileged access, it is crucial to manage user privileges. One of the best practices associated with managing user privileges is limiting users' access to accounts and ultimately minimizing the number of privileged accounts. Essentially, the principle of minimal privilege enhances your organization's cybersecurity in the sense that the scope and impact of a cyber-attack is minimized in case of an attack. Privileged users are authorized to perform significantly sensitive tasks within an organization such as the installation of systems' hardware and software, changing passwords for other users, make necessary changes to IT infrastructures, and log in to computers and machines. This therefore gives them access to critical and privileged information and in the event of an attack on such users' accounts; the results can be fatal for the company in terms of loss of data. Consider the following best practices for managing user privileges.		
1	Withhold access to local administrator accounts.	☐	☐
2	Develop formal approval processes for authorized access to domain admin accounts.	☐	☐

Notes

MATT BACAK'S CHECKLIST

Checklist 15 - Managing User Privileges

3 Establish policy based controls to minimize user privileges. ☐ ☐

4 Develop training programs to enlighten users on suspicious behavior. ☐ ☐

5 Closely monitor privileged user accounts frequently. ☐ ☐

6 Automate governance to limit user privileges. ☐ ☐

7 Set expiration dates on the privileged user accounts. ☐ ☐

8 Subject privileged user accounts to higher protocols and scrutiny. ☐ ☐

9 Change default login details and passwords for new systems, applications, and networks. ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 15 - Managing User Privileges

10

Establish least privilege policies. ☐ ☐

11

Reinforce limited access policies for all workers. ☐ ☐

12

Limit access to activity logs. ☐ ☐

13

Reinforce password policies. ☐ ☐

14

Separate your audit and accounting systems from your core networks. ☐ ☐

15

Delete or inactivate redundant user accounts. ☐ ☐

16

Reinforce personnel screening. ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 15 - Managing User Privileges

17

Develop standards for access controls and user identification. ☐ ☐

18

Avoid authorizing access to all data systems. ☐ ☐

19

Prohibit users' ability to download applications or software without permission. ☐ ☐

Notes