OFFICE OF THE CISO
UNIVERSITY of WASHINGTON

Risk Advisory:
The Use of Shared Accounts by Individuals to Access Data

Shared accounts are used for various reasons, but their use comes with a level of risk. It is important to understand those risks to determine if the use of a shared account is appropriate for a given set of circumstances, and to put in place appropriate safeguards when using them.

What is a Shared Account?

A shared account is an account that can be accessed by multiple individuals to accomplish a single shared function, such as supporting the functionality of a process, system, device or application. Most UW NetID accounts are used as individual user accounts, but they can also be configured and designated as shared accounts. Because NetIDs can be granted access to a wide range of systems and information, it is important to determine when the use of a shared account is acceptable and when it poses a security or compliance risk.

Security Risks Associated with Shared Accounts

Auditing

The use of a shared account by multiple people limits the ability to monitor or audit who has used the account at any given time. Shared accounts may also offer partial or full anonymity to those that use them. This can be problematic for tracking who accessed a system or made system changes, and who viewed or modified data. The use of shared accounts by individuals to access sensitive information may also violate contractual or regulatory requirements. For example, in general, shared accounts should not be used by individuals to access Protected Health Information (PHI)[1]. Exceptions must comply with UW Medicine Information Security Standards including but not limited to SS-01, SS-03, and SS-07.[2]

Password Management

Adequately managing the password for a shared account can be difficult because the password must be shared with multiple people. Care must be used to distribute the password in a secure manner, and the password must immediately be changed when someone who used the account no longer needs access. The more people that know a password, the more likely the password could become compromised.

Shared Account Best Practices

- Justification. Why do you need to use a shared account? The decision to use a shared account should be made with oversight from the security team, regulatory bodies, IT management, and system administrators.
- Shared accounts should be documented to include who has access to the account, who is responsible for managing the account, what the account will be used for, and how long the account is needed.
- Generally speaking, a shared account should not be used by a person if they can use their individual account instead..

[1] For an overview of the HIPAA technical security requirements see *HIPAA Security Standards: Technical Safeguards,* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
[2] UW Medicine Security Standards: https://depts.washington.edu/uwmedsec/restricted/security-governance/information-security-standards/

- Access to a shared account should not be given to anyone that does not need to use it.
- Shared accounts should be audited regularly.
- Shared accounts should use strong passwords.
- Passwords for shared accounts should be changed whenever a user of the account no longer needs to use it (examples: job function change, offboarding, etc.).
- Shared accounts should be used in conjunction with a password management system. Ideally, one that keeps the password secret from its users and also records who accessed the account, when it was used, and the system it was used to access.
- Shared accounts should be disabled when not in use. For example, if a vendor uses a shared account to access a system to provide support, the account should be disabled by default and only enabled when the vendor needs to carry out support services, with a new password given each time.
- Shared accounts, like all accounts, should only have the minimal level of access necessary to complete the specific tasks associated with its use.
- If possible, set up automatic alerting for when 'high value' shared accounts are used.

Alternatives to Shared Accounts

If the use of an individual account is not appropriate for a given situation, consider using user-assigned secondary accounts instead of a shared account. Example: Jane Smith logs on to her laptop with her UW NetID *'janedoe'*. Following best security practices, Jane's user account does not have local administrative rights on the laptop. However, there are times when Jane needs administrative rights on the laptop to install software. Instead of assigning admin rights to the '*janedoe*' account or using the local administrator account, a secondary account is created called '*janedoe-admin*' that Jane can use just for installing software or completing tasks that specifically require admin rights.

In instances where multiple people need to log on to a computer with administrative rights, rather than use a single shared administrative account, create individual secondary accounts with administrative rights and use them only when necessary.

For questions about this advisory, please contact ciso@uw.edu.