IT Privileged Account Policy

Privileged Access

Privileged accounts must be created whenever a user requires privileged access in the MSU IT environment. A privileged account is required when accessing resources that are managed by MSU IT and when a user must assume levels of privilege that may allow the user to expose sensitive data or circumvent security controls. Privileged access includes, but is not limited to:

- Direct server access via SSH or RDP, RD Gateway access
- Accounts for Domain/Enterprise administration
- Access to appliances in the data center network
- Access to VMware configuration or Virtual Machine consoles
- Access to data center resources via Bomgar or other remote means
- Access to data center resources via VPN connection
- Local administrator privileges on a workstation

For example, a privileged account is required when a user would need to SSH or RDP directly to a data center host. Conversely, a privileged account would *not* be needed in order to utilize an application presented by that same host to the public network (eg. e-mail, Banner). Privileged accounts may also be necessary for non-interactive purposes, such as a **service account** that requires access to data center resources in order to transfer data for integrations.

Unprivileged Access

Unprivileged access is provided by a user's MSU NetID. NetIDs provide user-level access to publicly available resources and configurations that would not allow a user to expose sensitive data or circumvent security controls. This includes but is not limited to:

- Any publicly available resources
- Web interfaces such as Workday, Banner, and Peoplesoft[1]
- E-mail systems, Google Accounts, web proxy servers
- Standard user privileges on a workstation or lab machine
- Access to public campus resources via a VPN connection

Why Privileged Accounts?

A privileged account is not a replacement for an MSU NetID, it is a *supplement*. The aim of creating a privileged account for an interactive user is to reduce the possibility that privileged resources could be exploited in the event that a user's MSU NetID is compromised.

By limiting the use of a privileged account to specific use cases, the degree of exposure for that credential is significantly reduced. For example, privileged accounts would not be used to login to public wireless networks or insecure services.

Passwords

It is imperative that passwords for privileged accounts are *completely different* from the password the user or custodian's MSU NetID. Only *temporary one-time* passwords should be

set by the administrator that is provisioning the account. These passwords must *only* be used by the user to reset their credentials. **An administrator should *never* know the password to a privileged account, unless they are the account user or custodian**.

All password changes for Privileged Accounts should be done by the users and custodians of these accounts via the Privileged Account Password Reset form (https://paper.montclair.edu). Passwords set by PAPR should adhere to the IT Password Complexity Guidelines. For more information regarding password policy, reference the IT Password Protection Policy.

Provisioning, Disabling, and Removing Privileged Accounts

All requests for provisioning, disabling, and removing privileged accounts must follow the IT Privileged Account Management Guidelines. Associated privileged accounts must be disabled immediately when an employee is separated from the University.

Defining Access

Access controls for all privileged accounts must be provided by security group membership in Active Directory. Any new groups that must be created to provide access to a new privileged account must follow the Active Directory Security Groups Standard.

Classification

Privileged accounts are classified into categories: MSU Privileged Account, Vendor Privileged Account, Local Workstation Administrator, Service Account, Domain Administrator.

For MSU users, the naming convention for a privileged account follows the convention of <*netid_suffix*>, where *netid* is their MSU NetID and *suffix* is the appropriate suffix defined below by the classification of their account. MSU users can have *more than one* privileged account depending on how many roles they require.

For non-MSU users, the first portion of their account follows the convention of last name, first initial, then suffix. In the event of two non-MSU users sharing the same first and last name, the NetID account naming convention will be followed: eg. smithj_vnd, smithjo_vnd. A non-MSU user should never have more than one classification of privileged account.

MSU Privileged Account (_prv)

Any MSU user that requires privileged access. The specific level of privileged access is defined in the account's Active Directory user object via security group membership. This is including but not limited to Windows and Linux system administrators, VMware administrators, developers in IT and other groups that need direct access to IT systems, and VPN users that are placed on a VLAN that provides direct data center access.

Vendor Privileged Account (_vnd)

Any non-MSU user that requires privileged access, regardless of the project that they are assigned to. The project that the user is assigned to will be recorded in the user object. The specific level of privileged access is defined in the Active Directory user object via security group membership

Local Workstation Administrator (_loc)

Any MSU user that requires membership in the local *Administrators* group on their workstation. This type of account should never be utilized in a server environment, and is *non-interactive.* The purpose of an _loc account is to allow a user to temporarily assume the role of Administrator on their workstation in order to install specialized software. A user must have the written consent of their supervisor, as well as MSU IT in order to qualify for local Administrator privileges.

Valid use cases for local Administrator privileges include but are not limited to developers, system engineers, system administrators and researchers. Local administrator privileges are granted to users that need to frequently install approved software without the assistance of MSU IT staff. Reference the IT Workstation Local Administrator Procedure for more information on how to provision this type of account.

Service Account (_svc)

A service account is provisioned for any non-interactive account that provides communication or data transfer between two hosts or between an MSU resource and an off-campus resource (eg. integrations with SaaS providers). Service accounts require an *account custodian*, who must be an MSU employee. Contact information for the custodian must be populated in the user object in Active Directory.

Domain Administrator

Any MSU user that requires membership in the Domain Admins group in Active Directory. This type of account only has privileges to log into Domain Controllers. The user would also have a separate *netid_prv* account for other work in the domain, that should have access control defined by other group membership (eg. *Server Admins*, *Workstation Admins, Security Admins*)

Defining Access

Access controls for all privileged accounts are provided by group membership in Active Directory. Any new groups that must be created to provide access to a new privileged account must follow the Active Directory Security Groups Standard.