Privileged Access Management Policy

Expanse Learning Group

Oct 2023

Author:	Patrick Taylor	**Version**	**2**	**Review Date:**	Oct 2024

1. Scope

This policy applies to all staff and contractors of Expanse Learning who are responsible for setting up and maintaining privileged accounts related to Expanse Group electronic information resources. Resources include user workstations as well as servers, databases, applications, and systems managed both on-premises and in the cloud.

2. Policy

a) System Approval and Authorisation

Default Password Changes

All vendor-supplied default passwords must be changed before any computer or communications system is used for Expanse Group business.

Unnecessary Software

Software features that could be used to compromise security, and that are clearly unnecessary in the Expanse Group computing environment, must be disabled at the time when software is installed on multi-user systems.

Password Categorisation

- **User Account Passwords**
  A password is a "secret" that allows the use of an account. A user account is typically tied to a unique individual, for example, an Azure Active Directory user account. Therefore, that password determines a human identity, and the password is the secret known by the human that connects that human to the system. A goal is to strive for as few user account passwords per human user as possible; ideally, a single user account password should be maintained per human user.
- **Privileged Account Passwords**
  Privileged account passwords provide administrative or specialised levels of access to enterprise systems and sensitive data, based on higher levels of permissions. A privileged account can be associated with a human being or non-human IT system, such as:
  - **Service accounts**, which run application services such as Windows Services, scheduled tasks, batch jobs, and Application Pools within IIS and Azure.
  - A**pplication accounts**, which include database logins, certificates for software signing, embedded build script passwords, configuration files, and application services used during software development
  - **System administrator accounts used to** manage databases
  - **Domain administrator accounts, used to** manage servers and control Azure Active Directory users, as well as local domain accounts at the workstation level
  - **Root accounts used** to manage Unix/Linux platforms

b) Password Composition

Role-Based Password Length

The minimum length for fixed passwords, or passwords created by users, must be set to six for handheld computers, eight for all network-connected computers, and ten for administrator and other privileged user IDs.

c) User Account Password Complexity

All user-chosen passwords for user accounts must meet the following complexity requirements:

- Must contain at least one alphabetic, one numeric and one symbol character.
- Must be at least 8 characters in length.
- Ideally passphrases should be used to increase length. Increased length provides more security than complexity and is easier for a human to memorize.

  For example:
  1) lf@j7asFd! versus 2) Blue5Chandelier2@
  The seven extra characters in (2) make it 64 trillion times stronger than (1).

d) Privileged Account Password Complexity

These passwords should be optimized for the maximum lengths of the platform. Random passwords should be generated between 80 and 127 characters in length to provide the maximum security.

The following requirements should be followed for privileged account passwords:

- Maximize the possible length of password for each platform.

- Passphrases *should not be used* to avoid memorization.
- Should have a complete mix of upper case, lower case, numbers, and symbols.

e) Seed for Generated Passwords for Privileged Accounts

If system-generated passwords are used, they must be generated using the low order bits of system clock time or some other very frequently changing and unpredictable source.

f) Null Passwords Always Prohibited

At no time, may any Systems Administrator or Security Administrator enable any user ID that permits password length to be zero (a null or blank password).

g) Enforce Password Complexity

All passwords must meet the above complexity requirements and this complexity must always be checked automatically at the time that the password is created or changed.

h) Password History and Change Interval

User Account Password Changes

User passwords must be changed at least once every 90 days. Users may be required to change passwords, or this may be done automatically.

User Account Maximum Password Changes

Users must not be permitted to change their password within seven days of their previous change. This requirement is only helpful for passwords that users are memorizing (user accounts) and is used to prevent users from changing the password multiple times back to a previously used password (therefore defeating the requirement to change the password).

Privileged Account Password Changes

All privileged accounts must be automatically required to change their passwords at least once every 90 days. This time interval should be set based on an internal risk assessment for any potential disruption to the business. A domain admin account password change would have zero disruption to the business and is very high risk. These accounts should have their passwords changed as often as possible – ideally after every use to reduce exposure to abuse, misuse, or exploits such as Pass-the-Hash attacks.

Password History

On all multi-user Expanse Group computers, system software or security software must be used to maintain an encrypted history of previously chosen fixed passwords. This history must contain at least the previous thirteen passwords for each user ID.

i) Account Lockout and Compromised Passwords

Maximum Login Attempts

All Expanse Group computer systems that employ fixed passwords at log on must be configured to permit only five attempts to enter a correct password, after which the user ID is deactivated.

Lockout Duration

All accounts that have been disabled for incorrect logon attempts must remain inactive for at least 15 minutes.

Lockout Notification

The security team must be notified of all disabling of accounts for incorrect logon attempts so that investigation can occur if necessary and anomalies can be detected.

Password Changes After Privileged User Credential Compromise

If a privileged user credential has been compromised by an intruder or another type of unauthorized user, all passwords on that system and any related systems must be immediately changed.

Fixed Password Change Confirmation

System administrators must be immediately notified when fixed passwords are changed or updated outside of the central privileged access management system.

j) Acceptable Use of Privileged Accounts

User Account Password Sharing

User account passwords must never be shared or revealed to anyone other than the authorised user. If they are shared, then they are no longer considered a user account since the identity of the user is not known.

Privileged Account Password Sharing

Privileged account passwords should not be shared, and each privileged account must have a unique password. Passwords for privileged accounts can be shared among administrators only if controls are in place to know which administrator is using the account at any one time. This must include full auditing and non-repudiation mechanisms.

Password Display and Printing

The display and printing of account passwords must be masked, suppressed, or otherwise obscured so that unauthorised parties will not be able to observe or subsequently recover them. Any display of a privileged account password to a user must be audited and the password should be changed after it has been used.

k) Privileged Account Approval

Privileged Account Requirements

All privileged accounts on Expanse Group systems must employ greater security than non-privileged accounts. This includes longer more secure passwords and greater audit accountability.

Privileged User Account Approval

The creation or modification of privileged user accounts must be approved by at least two individuals: the system owner and an authorized member of the Information Technology department. System administrators must not be allowed to create other privileged accounts without authorization. At Expanse these individuals are the CEO (System Owner) and Head of Shared Services (Super Admin)

Number of Privileged User IDs

The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

Role-Based Account Privileges

To facilitate secure management of systems, wherever possible, privileged accounts must be defined based on the specific role of the system administrator.

l) Privileged Account Construction

Privileged User ID Construction

All privileged user IDs on Expanse Group computers and networks must be constructed according to the Expanse Group user ID construction standard, and must conform to one of the following:

- Must clearly indicate the responsible individual's name
- Must clearly define the account (i.e., purpose of the account, type of account, etc.)
- Must be managed in a system that can clearly associate a single user account to each use of the privileged account to document accountability for the use of the privileged ID

Service Account Governance

User IDs for service accounts and other application accounts should also follow the Expanse Group naming convention and requirements outlined in section 3.8.1 above.

Generic User IDs

User IDs must uniquely identify specific individuals. Generic user IDs based on job function, organizational title, or role, descriptive of a project, or anonymous must be avoided wherever possible.

Re-Use of User IDs

Each Expanse Group computer and communication system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a worker, contractor, or customer terminates their relationship with Expanse Group.

Separate System Administrator User IDs
System administrators managing computer systems with more than one user must have at least two user IDs, one that provides privileged access and is logged, and the other that provides the privileges of a normal user for day-to-day work.

m) Privileged Access Management

Central Automated Management
All privileged accounts on Expanse Group systems must be managed by a central system. This system must provide an audit trail that tracks specific additions, changes, and deletions.

Integration with Native Directories
Any privileged access management system must integrate with native operating system account management systems or directory services, such as Azure Active Directory.

Integration with Strong Authentication Methods
Any privileged access management system must integrate with strong authentication methods, such as multi-factor authentication, to ensure the identity of the user in addition to their directory authentication.

Password Vault Encryption
Expanse Group must maintain any credentials stored in a central management system within an encrypted password vault, using strong encryption algorithms that meet compliance and/or regulatory requirements.

Privileged Account Inventory
Expanse Group must maintain an inventory of all accounts with privileged access on production information systems.

Account Inventory Update
The privileged account inventory must be updated at least quarterly to identify new or changed accounts.

Inactive Account Maintenance
All accounts must be created with an expiration date. All inactive accounts over 90 days old must be either removed or disabled.

Disaster Recovery
Any privileged access management system must be configured to utilise robust backup, recovery, and availability methodologies to ensure resiliency and availability of the credentials stored within the system as well as the timely recovery of the system in the event of a system failure.

n) Third-Party Privileged Accounts

Third-Party User ID Expiration
Every privileged user ID established for a non-employee or third-party application must have a specified expiration date with a default expiration of 30 days when the actual expiration date is unknown.

o) Local Administrative Privileges

Employee Workstations
Users should not try to access local administrator accounts on their individual workstations. In accordance with a least privilege policy, the default local administrator account should be treated as a failsafe in the event of damage/theft or loss.

p) Application Development

Special Application Accounts
All development applications and systems that require privileged access, including DevOps tools, containers, and microservices, must use secure privileged accounts.

Secret IDs or Passwords
Developers must not build or deploy secret user IDs or passwords that have special privileges that are not clearly described in the generally available system documentation.

Hard-Coded Passwords in Software

Passwords must never be hard coded in software developed by or modified by Expanse Group workers or contractors.
Third-Party Repositories
Credentials used in the application development process must never be stored in remote repositories, such as GitHub.

Test Account Removal
Test data and accounts used during development and testing must be removed before a production system becomes active.

q) Privileged Account Logging

Privileged System Commands Traceability
All privileged commands issued on computer and communication systems must be traceable to specific individuals with comprehensive logs.

Privileged User ID Activity Logging
All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs, including third-party vendors, must be securely logged on our MIS (Databridge).

Privileged User ID Activity Log Review
All logs recording privileged ID activity must be reviewed at least quarterly via periodic management reports.

Privileged User ID Activity Log Correlation
All logs recording privileged ID activity must be aggregated into Databridge for privileged accounts or a Security Information and Event Management (Databridge) to correlate privileged ID activity to other security events, log entries, and related non-privileged ID activity.

Privileged User ID Session Logging
In addition to event logging, all activity on privileged accounts must be logged via session or keystroke recording.

r) Application Control

Whitelisting
Only trusted applications should be allowed to be installed or executed automatically. Those not on Expanse Group's whitelist will be subject to review and approval.

Blacklisting
Specific applications known or suspected to contain malicious code may be added to a blacklist and not allowed to be installed or executed.

3. Disciplinary Action

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Expanse Group reserves the right to notify the appropriate authorities of any unlawful activity and to cooperate in any investigation of such activity. Expanse Group does not consider conduct in violation of this policy to be within an employee's scope of employment. Accordingly, to the extent permitted by law.

Impact of non-compliance

Staff:	Disciplinary action
Student:	Not Applicable
Legislation/organisational:	Reputational damage, statutory and non-regulated compliance. ICO Fines
Compliance lead:	Shared Services (ICT)
Policy Reference:	ELGR-ISTM-POL-0005
Version:	2
Agreed policy location:	Company Intranet
Review Schedule:	Annual
Does the policy require Governor approval?	No

Approval

Prepared by	***Approved by***	***Counter Signatory***
Patrick Taylor	Scott Roberts (Assoc. CIPD)	Tony Brown
20/10/2023	20/10/2023	20/10/2023
IT Coordinator	Head of Shared Services	CEO

Version Control

Version	***Date***	***Revision***	***Review Date***
1	10/02/2023	First Issue	10/02/2024
2	20/10/2023	Policy Reviewed	20/10/2024
3			
4			
5			