pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Commonwealth Data Center Privileged User Identification and Access Management Policy

Number
ITP-SEC038

Effective Date
September 06, 2017

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
April 2024

1. Purpose

This Information Technology Policy (ITP) provides guidelines for Commonwealth IT Data Centers and applications to establish appropriate controls for the administration and monitoring of Privileged User access to the hosted systems and data they contain. This includes the identification, Authorization, and Authentication of Privileged Users, programs, processes, and Service Accounts that access these systems.

2. Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Definitions

Administrative Accounts: Accounts used by a specific Privileged User having administrative level role(s), with access to all standard user and privileged operations. These can be, but are not limited to, accounts which manage other user accounts and roles, accounts which can bypass an application and directly modify the contents of the application's backend database, accounts with universal access to all the application's data regardless of its nature (including PII, PHI, etc.), or accounts which can uninstall or reconfigure server software. Users of these accounts are not necessarily IT staff but may be business managers administering agency application access and privileges for other workers.

Break-the-Glass Account: An account used in emergency situations, based upon pre-staged user accounts, managed in a way that can make them available with reasonable administrative overhead. Typically, these accounts are created, and the user ID and passwords locked away in a cabinet, desk, or sealed envelope, so that their use is restricted, and it is obvious when they have been used.

Commonwealth Data Center (Data Center): Facilities used to host Commonwealth IT assets and data. These include the Enterprise Data Center (EDC) and Pennsylvania Compute Service (PACS) as well as agency owned facilities.

Least Privilege: Least Privilege refers to the security objective of granting users only those accesses they need to perform their official duties. Data entry clerks, for example, would not normally have any need for administrative level access to the database they use.

Role-based access control (RBAC): The idea of establishing standard levels of access – "permissions" – to the various computing resources and networks of an organization that are tailored to specific employee roles, or job functions, rather than to individuals.

Service or Operational Accounts: Generally, system-to-system or application-to-application accounts having administrative level roles. For example, an application which updates or creates records in a backend database would use a Service Account with appropriate database privileges to do so.

System Accounts: Built-in system or application accounts having administrative level roles. Some examples include *root* in Linux/Unix systems, *Administrator* in Windows systems, or in SQL Server.

4. Objectives

- Provide security requirements for the use of Privileged User accounts to access computer applications, systems, and data.
- Provide a level of standardization and uniformity throughout the agencies regarding the use and protection of Privileged User accounts.
- Satisfy federal compliance requirements and other external requirements, where possible.

5. Policy

IT and application administrators are responsible for management of Privileged Users and accounts. This management includes appropriate user identification, authentication, and authorization, including appropriate level of access, to systems, applications, and data.

Note: *This function of IT and application administrators makes them Privileged Users themselves and subject to the guidelines enumerated in this ITP.*

Privileged User management addresses three general types of accounts:

- Administrative

- Service or Operational
- System

In each instance, the improper use of these privileged accounts can result in serious consequences, intentional or not, such as the corruption or loss of data or improper disclosure of data. Privileged accounts shall be properly secured and monitored to avoid their misuse.

This policy applies to all types of privileged accounts listed above and generically referenced in this section as "accounts".

- Accounts shall meet or exceed all requirements set forth in *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*.
- Accounts shall uniquely identify and authenticate users, processes, or groups who make use of the account.
- Accounts shall be granted the Least Privilege needed by the user, process, or group who makes use of the account.
- Accounts privileges and access shall be based on RBAC principles, not on attributes such as user ID or employee number.
- An inventory of all privileged accounts shall be maintained by the agency and kept current as new systems or applications are brought online.
- Semi-annual scans of the infrastructure and applications shall be done to discover any unreported accounts with elevated or excessive privileges. The agency may choose to do this manually or through an approved tool of their choice.
- Account usage shall be monitored and audited. The resulting records shall be subjected to applicable enterprise and agency data retention schedules.
- These privileged accounts and access rights will be reviewed every six months and adjusted as needed.

The below sections apply to the specific types of privileged accounts enumerated above.

5.1 Administrative Accounts

- For assigned administrative tasks regularly requiring the use of a privileged account, particularly for desktop, server, or other infrastructure access (routers, firewalls, etc.), the user shall be assigned a separate account, distinct from the user's everyday account. This privileged account shall be reserved and restricted only for the privileged access use cases and will not be used for routine duties such as HR activities, sending or receiving email, or Internet usage.
- Where needed, non-privileged accounts may be temporarily elevated to a privileged status. Such actions shall be documented including date and time, who, and for what circumstances. The elevated privileges shall be removed once the need no longer exists.
- Passwords on Administrative Accounts are governed by *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*. It is required that these passwords be a minimum of 12 characters including at least one each of uppercase, lowercase, numbers, and special characters.
- Appropriate background checks, up to and including fingerprinting through the PA State Police, shall be performed on each user prior to them being

granted use of any privileged account.
- Privileged accounts shall be disabled or removed (subject to audit requirements or investigations) immediately upon separation of the user.
- All Privileged Users shall agree to and sign the *IT Administrator Acceptable Use Policy* per *Management Directive 245.18 Amended, IT Administrator Acceptable Use, Auditing and Monitoring*.
- In cases where remote access to the systems is required from outside of the COPA network, VPN or other encrypted network access shall be used. The user shall be authenticated using multifactor authentication.

5.2 Service or Operational Accounts

- If used, Break-the-Glass Accounts shall be named appropriately (e.g., breakglass01). The passwords shall be a minimum of 12 characters including at least one each of uppercase, lowercase, numbers, and special characters, and locked away in a sealed envelope. The use of these accounts shall be logged, including date and time, who, and for what circumstances. The passwords will be changed immediately after use.
- Service or other such accounts shall be managed per *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication* and documented in either the system or application design documents.

5.3 System Accounts

- The use of built-in or default accounts shall be minimized only to cases where there are no other alternatives.
- Where possible, they shall be disabled . If disabling is not possible, they shall be renamed to something other than the default.
- Default passwords shall be changed and managed per *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*.

6. Reporting of Non-Compliant Systems and Applications

In the case of non-compliant systems or legacy applications, the non-compliance shall be reported to the agency security officer and the Commonwealth CISO as part of the agency's security assessment, per *ITP-SEC023, Information Technology Security Assessment and Testing Policy*. The report will include details as to the Privileged User policies, the type of data stored on the system or accessed by the application, any compensating controls, and any plans for the revision or replacement of the system or application.

7. Responsibilities

7.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

7.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

7.3 Third-party vendors, licensors, contractors, or suppliers shall:

Ensure default application or hardware passwords are changed and managed to meet the Commonwealth's standards set forth in *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*.

8. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/Glossary.aspx*
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*
- *Management Directive 245.18 Amended, IT Administrator Acceptable Use, Auditing and Monitoring*
- *ITP-ACC001, Information Technology Digital Accessibility Policy*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*
- *ITP-SEC009, Minimum Contractor Background Checks Policy*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC023, Information Technology Security Assessment and Testing Policy*
- *ITP-SEC031, Encryption Standards*
- *NIST Special Publication SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations*
- *NIST Special Publication SP 800-63-3 Digital Identity Guidelines*
- *NIST Special Publication SP 800-63C Digital Identity Guidelines: Federation & Assertions*
- *NIST Special Publication SP 800-63B Digital Identity Guidelines: Authentication & Lifecycle Management*
- *NIST Special Publication SP 800-192 Verification and Test Methods for Access Control Policies/Models*
- *NIST Federal Information Processing Standard (FIPS) 200 Minimum Security Requirements for Federal Information and Information Systems*

9. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

10. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

11. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy Waiver Review Process* for guidance.

Please note: The waiver request shall state why the standard Privileged User policy cannot be used. Details are required about the application, server, and network connections. Network diagrams shall be included to illustrate the security components that will mitigate the proposed Privileged User policy. Any waiver that is granted will be valid for a period of not more than one (1) year and will be void if the application or system undergoes a substantial revision or replacement. Despite the existence of the waiver, the non-compliant system or application shall be reported to the Commonwealth CISO as part of the agency's security assessment as prescribed above in Section 6 and detailed in *ITP-SEC023, Information Technology Security Assessment and Testing Policy*.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	09/06/2017	Base Policy	N/A
Revision	06/19/2018	Removed unnecessary Purpose language Clarified 6.1 to include desktop and example infrastructure assets	N/A
Revision	10/19/2021	• Added Offices and third-party vendor language to Scope. • Updated Definitions Section • Updated references and included links. Added Responsibilities section.	N/A
Revision	04/25/2023	• Scope updated to include any entity connecting to the Commonwealth Network. • Replaced definitions with links to glossary where applicable • References updated • Minor grammatical and formatting updates	Revised IT Policy Redline <04/25/2023>