pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

# Information Technology Policy

## *Commonwealth Data Center Privileged User Identification and Access Management Policy*

| **ITP Number**<br>ITP-SEC038 | **Effective Date**<br>September 06, 2017 |
|---|---|
| **Category**<br>Security | **Supersedes**<br>None |
| **Contact**<br>RA-ITCentral@pa.gov | **Scheduled Review**<br>June 2019 |

## 1. Purpose

This policy 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 Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

## 3. Objective

The objective of this ITP is to:

- 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 Commonwealth of PA (COPA) agencies regarding the use and protection of privileged user accounts
- Satisfy federal compliance requirements and other external requirements where possible.

## 4. 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. These users are not necessarily IT staff but may be business managers administering agency application access and privileges for other workers.

**Authentication** – The process of establishing confidence in the validity of a user's presented identifier, usually as a prerequisite for granting access to resources in an information system.

**Authentication Method** – The type of authentication being used to validate a user. These are categorized as:

- Something you know (e.g. PIN, password, shared information)
- Something you possess (e.g. token, smart card, digital certificate)

- Something you are (biometrics – e.g. fingerprint, voice, iris, face)

**Authorization** – The process of verifying that an authenticated user is permitted to have access to a system or application based on the user's business responsibilities.

**Break-the-Glass** – Accounts 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 userID and passwords locked away in a cabinet, desk, sealed envelope, etc. 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.

**Globally Unique Identifier (GUID)** – The Globally Unique Identifier is an alpha-numeric code which uniquely identifies a person. Two John Smiths could, for instance, both have the same userID at different times, but they would have different GUID's. User access to IT resources should be based on the GUID rather than the userID as it uniquely identifies the person. Note: Active Directory assigns a GUID to each account, this is not necessarily the same as assigning a GUID to a person.

**Identify and Access Management (IAM)** – Processes and tools used to manage user IT accounts throughout the account lifecycle. These include the creation (provisioning) of the account, management of attributes and privileges during the account's active lifetime, password management, and finally the removal (de-provisioning) of the account when that lifetime is over.

**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.

**Multi-Factor Authentication** – The use of two or more of the Authentication Methods (see above). Two-factor would employ one each of two of the methods; three-factor would employ one each of all three methods.

**Privileged Access Management (PAM)** – Processes and tools that provide IT administrators a method of managing privileged users and their accounts and access rights to IT resources. This is a specialized aspect of general Identity and Access Management. (Sometimes referred to as Privileged Account Management or Privileged User Management though these each have slightly different nuances.)

**Privileged User** – A user who has been granted elevated privileges for accessing protected physical or logical resources, including users with application administrator access or roles. Such users include, for example, security personnel or system administrators who are responsible for managing restricted physical locations or shared information technology (IT) infrastructure. These users might require access to related systems to create new user accounts, and add to or amend the privileges of other users.

**Role-based access control (RBAC)** – RBAC is 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.

**Separation of duties** – Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.

**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 *sa* in SQL Server.

## 5. General Policy

Information technology 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, and System accounts. 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 must be properly secured and monitored to avoid their misuse.

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

5.1 Accounts shall meet or exceed all requirements set forth in ITP-SEC007 *Minimum Standards for IDs, Passwords, and Multi-Factor Authentication*.

5.2 Accounts shall uniquely identify and authenticate users, processes, or groups who make use of the account.

5.3 Accounts shall be granted the least privilege needed by the user, process, or group who makes use of the account.

5.4 Accounts privileges and access shall be based on RBAC principles, not on attributes such as userID, employee number, etc.

5.5 An inventory of all privileged accounts shall be maintained by the agency and kept current as new systems or applications are brought online.

5.6 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.

5.7 Account usage shall be monitored and audited. The resulting records shall be subjected to applicable enterprise and agency data retention schedules.

5.8 These privileged accounts and access rights will be reviewed every six months and adjusted as needed.

## 6. Detailed Policy

The policies in this section apply to the specific types of privileged accounts enumerated above in §5.

### 6.1 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/receiving email, or searching/browsing the Internet.
- Where needed, non-privileged accounts may be temporarily elevated to a privileged status. Such actions shall be documented including date/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, though it is recommended 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 MD245.18 – *IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures*.
- 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.

### 6.2 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 are to be disabled (preferably) or renamed to something other than the default.
- Default passwords shall be changed and managed per ITP-SEC007.

### 6.3 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/time, who, and for what circumstances. The passwords will be changed immediately after use.
- Service or other such accounts are to be managed per ITP-SEC007 and well-documented in either the system or application design documents.

## 7. Reporting of non-Compliant Systems and Applications

In the case of non-compliant systems or legacy applications, the non-compliance will be reported to the agency security officer and the Commonwealth CISO as part of the agency's security assessment (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.

## 8. Exemptions and Waivers

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for a waiver is to be completed and submitted via the Commonwealth of Pennsylvania Policy and Procurement Action Request (COPPAR) process. Requests are to be entered via the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

The waiver request is to state why the standard privileged user policy cannot be used. Details are required about the application, server, and network connections. Network diagrams are to 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 is to be reported to the Commonwealth CISO as part of the agency's security assessment as prescribed above in §7 and detailed in ITP-SEC023 *Information Technology Security Assessment and Testing Policy*.

## 9. Related ITPs/Other References

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 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- Management Directive 210.5 *The Commonwealth of Pennsylvania State Records Management Program*
- Management Directive 245.18 *IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures*
- ITP-SEC000 *Information Security Policy*
- ITP-SEC007 *Minimum Standards for IDs, Passwords, and Multi-Factor Authentication*
- ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC020 *Encryption Standards for Data at Rest*
- ITP-SEC023 *Information Technology Security Assessment and Testing Policy*
- NIST Special Publication SP 800-53 Rev. 4 *Security and Privacy Controls*
- NIST Special Publication SP 800-63-2 *Electronic Authentication Guideline*
- 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*

## 10. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

## 11. Publication Version Control

It is the 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 are to be directed to RA-ITCentral@pa.gov.

This chart contains a history of this publication's revisions:

| Version | Date | Purpose of Revision |
|---|---|---|
| Original | 09/06/2017 | Base Policy |
| Revision | 06/19/2018 | Removed unnecessary Purpose language<br>Clarified 6.1 to include desktop and example infrastructure assets |