****

**APPLICATION ACCESS CONTROL POLICY**

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. No.** | **Release Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 30th May 2020 | Initial draft  | Rahul Raj |  |  |
| 1.0 | 22nd July 20 | Baseline and published | Rahul Raj | Tim/Tanuj | SEPG Team |
| 2.0 | 28th Sep 20 | Update section 4 and 5 | Rahul | Tanuj | SEPG Team |
| 2.1 | 14th Jan 21 | Update section 6 as per HIPAA requirement on access control | Rahul | Tanuj/Saket | SEPG Team |

Contents

[1. Access Control Policy 4](#_Toc79413465)

[2. Scope 4](#_Toc79413466)

[3. Objective 4](#_Toc79413467)

[4. Definitions 4](#_Toc79413468)

[5. Responsibilities 5](#_Toc79413469)

[6. Access Control Implementation 5](#_Toc79413470)

[6.1 Identity Management 5](#_Toc79413471)

[6.2 Authentication Management 5](#_Toc79413472)

[6.3 Access Governance 5](#_Toc79413473)

[6.4 Privileged Account Management 6](#_Toc79413474)

[6.5 Shared Use Accounts 6](#_Toc79413475)

[6.6 Vendor or Default User Accounts 6](#_Toc79413476)

[6.7 Test Accounts 6](#_Toc79413477)

[6.8 Removal or Adjustment of Access Rights 7](#_Toc79413478)

[6.9 Access Reviews 7](#_Toc79413479)

[6.10 Access in Special Circumstances 7](#_Toc79413480)

# Access Control Policy

Information is a valuable asset and access to it must be managed with care to ensure that Confidentiality, Integrity and Availability are maintained. Access to SVAM systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

This policy outlines the rules relating to authorizing, monitoring, and controlling access to SVAM accounts, information, and information systems.

# Scope

This policy applies to any person or systems that are granted or that grant access to accounts, information or information systems owned or operated by the SVAM.

# Objective

Compliance with this policy enables consistent controls to be applied throughout the organization, minimizing exposure to security breaches. This policy aims to ensure that, by having the appropriate access controls in place, the right information is accessible by the right people at the right time and that access to information, in all forms, is appropriately managed and periodically audited.

# Definitions

* **Access Control** is the process that limits and controls access to resources of a computer system.
* **Users** are employees, consultants, contractors, vendors and authorized users accessing SVAM IT systems and its applications.
* **System** or **Application** **Accounts** are user IDs created by IT systems on applications, which are associated with specific access privileges on such systems and applications.
* **Privileged Accounts** are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include administrative and super user accounts.
* **Access** **Privileges** are systems permissions associated with an account, including
* permissions to access or change data, to process transactions, create or change settings, etc.
* **Administrator Account** is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.
* **Application and Service Accounts** are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.
* **Non-disclosure Agreement** is a contract between a consultant, contractors, vendors and the SVAM stating that the consultants, contractors, vendors will protect confidential information.

# Responsibilities

All personnel (e.g., employees, vendors and third parties) at the SVAM must abide by relevant Information Security and Access Control policies and procedures.

All SVAM account holders must:

* Only use their account and access in accordance with the SVAM GD-27-ISMS-CEI-SVAM-Computer Email and Internet Usage Guidelines
* Secure their credentials in line with the SVAM-PO-06-PP-Password Policy
* Be responsible for the systems, services, and data within their control.
* Exit services and data prior to vacating a role referring to the Separation Policy

IT Asset owners must:

* Periodically review access to their assets and investigate any anomalies. Review periods are based on the risk rating of a given asset.

Access administrators must:

* Only grant access requests that have:
	+ A request through email
	+ Adequate and appropriate justification, as confirmed by the Management
* Document all access granted

# Access Control Implementation

The following headings outline the principles around how access is managed at the SVAM:

##  Identity Management

Formal user registration and de-registration processes are implemented (PR-21-ISMS-ITO-IT Operation Process) to enable the assignment of accounts on an individual basis. This ensures accountabilities for all actions taken by employees and associate account users.

##  Authentication Management

All account, service and platform access are managed through secure Office 365 authentication controls. For more information on this please see the SVAM-PO-06-PP-Password Policy

##  Access Governance

A formal user access provisioning process is implemented to assign or revoke access rights for all user types to systems and information assets under the control of the SVAM.

This access provisioning is based on the following principles:
Access changes for employees are primarily managed through the IT Team on the request raised by Project Manager/ Delivery Head/ or Management.

* Appropriate approval is required and documented for all access requests or changes.
* Where possible, SVAM will set user accounts to automatically expire at a pre-set date. More specifically,
	+ When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
	+ User accounts assigned to contractors will be set to expire according to the contract’s expiry date.
	+ User accounts will be disabled after periodic visit by IT team in case of inactivity. This does not apply to accounts assigned to management.
* Reviews of access are performed by relevant asset owners periodically.
* These principles are agnostic of account type, service, application, or system.

##  Privileged Account Management

Privileged accounts and privileged access (see PR-21-ISMS-ITO-IT Operation Process) must be purpose driven, secure and always adhere to the principle of least privilege.

* An individual privileged user account must be created for administrator accounts instead of generic administrator account names.
* Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved.

##  Shared Use Accounts

Where possible, the use of specific network domain “security groups” should be used to share common access permissions across many users, instead of shared accounts.

Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as “guest” and “functional” accounts.

When shared accounts are required:

* Passwords will be stored and handled in accordance with the Password Policy.
* The use of shared accounts will be monitored where possible, the reason for accessing the shared user account, and the individual accessing his account. When the shared user account has administrative privileges, such a procedure is mandatory and access to the monitoring logs must be protected and restricted.

##  Vendor or Default User Accounts

Where possible, all default user accounts will be disabled or changed. These accounts include “guest”, “temp”, “admin”, “Administrator”, and any other commonly known or used default accounts, as well as related default passwords used by vendors on systems and applications.

## Test Accounts

Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner or Solution Head, through a formal request to the IT Manager or the IT Help Desk.

Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be revaluated every 90 days and approved.

Test accounts will be deleted / disabled when they are no longer necessary.

##  Removal or Adjustment of Access Rights

The access rights of all employees and associate account users to information and information processing facilities will be removed upon termination of their employment, contract, or agreement, or adjusted upon change. Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access SVAM systems.

##  Access Reviews

It is recommended that the risk relating to each individual asset is measured and given a risk rating in line with the single asset risk assessment process, outlined in the GD-08-RSM-Risk Management Guidelines. Where an access review identifies an access anomaly it will be treated as a potential incident and investigated by the asset owner and information security team.

Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

* An active account assigned to contractors, vendors or employees that no longer work for the organization.
* An active account with access rights for which the user’s role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.
* System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
* Unknown active accounts.

## Access in Special Circumstances

There are special circumstances where extra or privileged access is needed. For all cases, access to an account, the information contained within an account or information pertaining to the activity of an account, is carefully restricted and must only be carried out with the appropriate authorisation and safeguards in place.

**Appendix A** in PR-21-ISMS-ITO-IT Operation Process outlines the approach taken for special circumstances.