b

IT126 -   
Access Control Provisioning and Deprovisioning Procedure

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.03 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[1](#_Toc57632980)

[Document Control iii](#_Toc57632991)

[Audience 4](#_Toc57632992)

[Scope 4](#_Toc57632993)

[Principles 4](#_Toc57632994)

[Compliance 16](#_Toc57632995)

[Enforcement 16](#_Toc57632997)

[Revision History 16](#_Toc57632998)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | July 10th, 2020 |
|  |  |  |
|  |  |  |

## Document Sensitivity Level

Confidential

Audience

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff in this policy).

Scope

This procedure describes the request and approval process for obtaining privileges for a user account, an administrative account, a role-based account, or access to a service or process account.

Principles

• The principle of least privileges applies: To the extent possible, accounts should be granted sufficient privileges to perform the approved business function and no more

• Where a person has multiple accounts or has the ability switch to a privileged account, the least privileged account will be used for the normal day to day non-privileged activities. The privileged account should only be used when the elevated privilege is required

• Personal accounts and the passwords to those accounts may not be shared.

• Role-based accounts may be used sparingly as appropriate and only for executing functions of the particular role, see the Data Protection Standards for more details

In this context, a role-based account is an account that performs a given function required for a given role but is not associated with a particular individual.

• All requests must be reviewed and approved from both a business and a technical perspective. The business approval confirms that the account requested is needed to perform a require business function and the technical approval confirms that the privilege requested is required to achieve the approved business need.

• Both the business and technical approvers should be managers as close to their respective areas of approval as practical to ensure that they have the requisite business and technical knowledge required to properly perform their duties.

• Separation of duties must be maintained: The person with the authority to approve a request should not be the person that fulfills the request.

Data Custodians are responsible for:

• Executing the approved account definition/modification/removal request, after validating that appropriate approvals have been granted

• Ensuring the audit and event logging is properly configured and functioning normally, and that all required audit documentation is readily available

• Conduct quarterly internal system audits of system accounts and maintain documentation accordingly

The Information Security Office is responsible for:

• Defining the general account management processes (this document)

• Consulting with system owners on system-specific account management processes Working with system owners to define and document appropriate audit procedures

• Conducting appropriate periodic audits of system accounts and the account management process

General Account Management Lifecycle

The general account management lifecycle includes several steps:

**Account request and provisioning**

1) New account/privilege request is made using the Signifi’s ticketing system (email to it@signifi.com for internal or support@signifi.com for external requests)

2) Request is sent to requestor’s manager for business approval

3) Request is sent to the appropriate Data Trustee for approval if appropriate

4) Request is sent to the technical manager of the system in question for technical approval

5) Request will be forwarded to Information Security in cases where Restricted Use data may be present on the system or where specific memberships, trainings, or certifications are required for access to data on the system

6) Final approval is sent to the Data Custodian for implementation

Account Review

1) For every Signifi maintained system, a list of active accounts with privileged access will be provided to the appropriate business approvers for review and updating on an annual basis.

2) For any Signifi maintained system that contains information belonging to a give Data Trustee, the above report is to be forwarded to that Trustee or along with comments from the appropriate business approvers explaining the business need for the account/privilege. (This is to support the annual audit requirements of the Data Trustees, etc.)

Account Auditing / Management Process Auditing

1) Information Security will review random systems and accounts on a random, periodic basis to ensure that this procedure is adhered to and that:

• there is a request for every account with elevated privilege, role-based account, or service/process account

• the request was approved both by a business and technical manager

• the request is compliant with applicable regulation, policy, best practice the granted privileges were indeed required for the approved business use requests for temporary privileges are expired on the agreed expiration date every account is held by a person still at Signifi the account holder’s business function still requires the granted privilege other tests as may be appropriate

2) Auditing will be conducted on a random sample of accounts and tickets, focusing on recent requests but including older requests as well.

Account Deprovisioning

1) Account/privilege removal request is made using Signifi’s ticketing system by the person’s manager or designee or automated process.

2) Request is sent to technical manager of the system in question for information and routing

3) The technical manager will send the request to the Data Custodian for implementation.

4) Such accounts or privileges must be removed in a timely fashion following notification; generally, within a few business days unless a specific timeframe is requested.

Making the Request

Requests will be made, recorded, processed and archived using the workflow features of Signifi’s service management solution, currently QuickBase (QB). Privileged access may be granted permanently only if that specific person’s job duties routinely require that level of access, otherwise, the access will be temporary. Privileged access is dependent on the specific person’s job duties, not the duties of the person’s group. Temporary accounts and privileges must expire within 45 days or less; if more time is required, an extension may be requested on the original ticket.

Request Fields for Accounts with elevated privileges

Name:

Signifi login:

Department:

Type of Request (indicate all that apply):

* I need an account created for me and given administrative privileges (e.g. sudo)
* I have an account but need to be given administrative privilege (e.g. sudo)
* I need a multi-machine administrator account created (e.g. username-adm)
* I have an administrator account but need it authorized for a specific system
* I need access to an existing administrative account (e.g. root, administrator)

What server(s) or database(s) do you need access to?

Is this request for temporary or permanent access?

* Temporary
* Permanent (due to job duties)

If temporary, what is the end date:

If permanent, describe job responsibilities that require ongoing access:

Business Owner:

- Name:

- Approval granted: Yes No

Technical Owner:

- Name:

- Approval granted: Yes No

- If no, what level of privilege is granted:

- Highest level of classification of data on the system: Restricted Use – Confidential – Internal – Public

- Does this system contain data that requires trustee approval: Yes No

- What data:

Data Trustee:

- Name:

- Approval granted: Yes No

Request Fields for Role-based Accounts, or access to Service or Process Accounts:

How will the account be accessed? [Shared password, Certificate or Identity Keys, Sudo]?

If this request is being made for a named group of individuals, what is the name of the group:

List the individuals that will have access to the account:

If the account will be accessed by automated processes, what are they and what system(s) are they running on?

Requested name for the service/process account:

Explain what access is needed and the business reason for this access:

Business Owner:

- Name:

- Approval granted: Yes No

Technical Owner:

- Name:

- Approval granted: Yes No

- If no, what level of privilege is granted:

- Highest level of classification of data on the system: Restricted Use – Confidential – Internal – Public

- Does this system contain data that requires trustee approval: Yes No

- What data:

Data Trustee:

- Name:

- Approval granted: Yes No

Request Approval

Prior to creation of the account or granting of new privileges, the request must be approved from both a business and a technical perspective. Approvers should be managers as close to their respective areas of approval as practical to ensure that they have the requisite business and technical knowledge required to properly perform their duties.

The request must first be approved by the requestor’s manager. This person is responsible for understanding and approving the business need for the request.

The request is then forwarded to the appropriate technical manager. This person is responsible for understanding what level of privilege is required to achieve the business objective and approving access to that level only. This person also determines:

1. If the system contains information for which access must be approved by a Trustee

2. If the system contains Restricted Use information

If the system contains information for which access must be approved by a Trustee, the technical manager forwards the ticket to the appropriate Trustee for review and approval.

If the system contains Restricted Use information, the technical manager forwards the ticket to Information Security who confirms that the requestor has signed the appropriate confidentiality agreements, taken appropriate training, and/or holds appropriate credentials for accessing the resource.

Privilege requests will be approved as follows:

|  |  |
| --- | --- |
| Service | Technical Component Owner |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Implementation

Approved requests are forwarded to the appropriate Data Custodian who verifies that the request has been properly approved and creates the requested account and/or grants the approved privilege.

• Accounts intended for individuals should be part of the Global UID system and should use Kerberos authentication, if possible.

• Service/Process accounts may be defined locally. If the account is to be accessed via a password, the password should follow Signifi password policy guidelines.

Root access

Administrative privilege (e.g. root, administrator account) to Signifi servers is restricted to Data Custodians and Information Security personnel unless special permission is granted by Information Security. If Administrator privilege is needed by anyone else, the request is made using the form and process described in this procedure, and an end date must be provided.

Account Review

Annual review of account on a system will be facilitated and documented for the following major services:

|  |  |
| --- | --- |
| Service | Service Owner |
| Signifi Vision | QA/Ops Manager |
| Signifi Production Servers | IT Manager |
| Signifi Production Virtualization Infrastructure | IT Manager |
| Signifi Office Systems and Network | IT Manager |
| Signifi Production Database Access | QA/Ops Manager |
| Remote Access Platform | Service Manager |

Account Auditing / Management Process Auditing

Security of a system is the responsibility of the Technical Component Owner and Data Custodians, with reference to Information Security for process and configuration guidelines and requirements.

In order to ensure that the agreed processes and procedures are being properly followed, Information Security will periodically audit the systems, procedures and request tickets.

Setting up the system to properly support auditing (and security) is the responsibility of Information Security.

Security Event Logging

Systems must be configured to properly log audit data. At a minimum, the following events should be logged and reported:

• Successful authentications for all services, including shell access.

• Failed authentications for all services, including shell access.

• System-specific security events

• Access to privileged accounts such as root, including use of programs like sudo.

• Setting network adapters to “promiscuous mode” (where auditing is supported by the OS)

• FTP Activity: Connect, authenticate, read, write, close

• Application-appropriate log files

Security Event Alerting

The system should be configured to send system and security events and information to an external log collection/aggregation/analysis solution where applicable:

• Appropriate log excerpts (for example: /audit/trail and /var/adm/daemon)

• Attempts to delete or write to log files outside of the auditing system

File Integrity Monitoring

Systems should use file integrity monitoring tools (where available) to detect additions, changes to, and deletions of critical system files. The reports generated by these tools should be reviewed routinely by the local systems administrator for indications of unauthorized changes. Information Security may periodically audit these reports as well.

Log Review

Security logs should be reviewed regularly by system administrators. Automated and manual techniques may be used as appropriate.

Access should be reviewed regularly to confirm a normal and expected pattern of use of root access. Unexpected use of root access must be explained and understood by the technical manager of that system who may escalate findings to Information Security if appropriate.

Creation and Maintenance of Auditing Procedures

Information Security will work with Data Custodians to develop, document and maintain the procedures required to properly review and protect the Signifi systems.

The procedures will be reviewed and updated as required.

Security Process and Account Auditing

Each quarter at a randomly selected, unannounced time, Information Security will perform an audit of a sample of systems and requests. The audit will be conducted on a random sample of accounts and tickets, focusing on recent requests and events but including older requests and events as well.

Responsibilities of Information Security

• For a sample of at least 3 machines that may be randomly selected:

Confirm that requests (Service Now tickets) exist for each account with privileged access to that machine

Review the sudoers file output to confirm a normal and expected pattern of use of root access

• For a sample of at least 3 recently expired requests for temporary access:

Confirm that the access has been removed in accordance with the requested expiration date documented in request

• For a sample of at least 5 requests:

Confirm that the request was approved both by a business and technical manager and, if appropriate, the Data Trustee and Information Security

Confirm that the approved business need was valid

Confirm that the approved privileges were indeed required for the approved business reason

• For at least 3 randomly selected people:

Review the list of all systems on which that person has escalated privileges.

Confirm that the person is still employed by Signifi and is still in an organizational position and role where such privileges are appropriate. (This is to help confirm that access removal requests are being submitted appropriately.)

Confirm with that person’s manager and the system technical owner that such access is still appropriate. (This step is intended to understand and curb patterns of unwarranted privilege escalation.)

• Other tests as appropriate

Account Deprovisioning & Privilege De-escalation

Managers are responsible for submitting a ticket requesting an appropriate change in account or privilege status when a person’s job function changes, they transfer to another department, or they leave Signifi. To ensure the security of our systems, this process must be accomplished in a timely fashion.

Temporary accounts must be expired by the requested date or within 30 days, whichever is sooner.

Service Management Request Fields

Name:

Signifi login:

What accounts or privileges need to remove on which systems/databases?

Changing Passwords for Service/Process/Root/Administrator Accounts

When a person that has a password or authentication token (ssh key, e.g.) for a service/process account no longer requires access, such as might result from changing positions or terminating employment, his or her manager is responsible for submitting a ticket requesting the password or token be changed. Due to the potential sensitivity of such accounts, it is preferred that the request be made in advance of change in responsibility (provide the effective date). If this is not possible, the request must be made within 1 business day following the change.

Compliance

This policy will be officially monitored for compliance by the IT department director and may include random and scheduled inspections.

Enforcement

All instances of non-compliance will be reviewed by the employee’s department director. The department director, with the assistance of the Human Resources department has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2020-06-22 | First version | Muhammad Nasir |
| 1.01 | 2020-07-07 | Update to Signifi standards and particulars | Razvan Anghelidi |
| 1.02 | 2020-12-02 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |