

IT117   
Password Policy

|  |  |
| --- | --- |
| 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.*

[Document Control v](#_Toc26334739)

[Introduction 6](#_Toc26334740)

[Purpose 6](#_Toc26334741)

[Audience 6](#_Toc26334742)

[Scope 7](#_Toc26334743)

[Policy Statement 7](#_Toc26334744)

[Enforcement 11](#_Toc26334745)

[Revision History 11](#_Toc26334746)

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 | Feb 25th, 2020 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. Password authentication ensures the associate is authorized to access that system and has the appropriate permissions to do so. A strong password is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software. A poorly chosen password may result in the compromise of Signifi’s entire corporate network.

As such all users of Signifi information and/or systems are responsible for taking the appropriate steps, as outlined below, to select and secure passwords. Any Signifi computer, computer systems, computer-based applications or networks must be brought into compliance based on this policy.

Purpose

The purpose of this policy is to set the criteria for the creation of strong passwords, the protection of those passwords, and the frequency of change. The combination of a User ID and Password provides authenticated access to Signifi systems and services. In some cases, additional authentication factors, such as RSA Tokens, are also used but are beyond the scope for this policy.

Audience

This policy applies to all Signifi employees, part-time and temporary workers, trainees, contractors and vendors (“users” from now on).

Scope

This policy applies to all users which include but not limited to employees, contractors, part-time and temporary workers, trainees, service providers, and those employed by others to perform work at hosted or outsourced sites, or who have been granted access to Signifi information or systems.

Policy Statement

1. General Password Security Standard
   1. IT must ensure that workstations left unattended for 3 minutes will automatically activate a password-protected screen lock.
   2. System Administrators must not leave servers or workstations unattended for any period of time without first logging-out, locking the server or workstation via a password-protected screen lock
   3. Passwords must not be included in electronic mail messages or other forms of electronic communication unless strong encryption is employed.
   4. Passwords should also never be written down and left exposed.
   5. All first-time and reset passwords will be set to a unique value for each user, and each user must change their password upon first login.
   6. A user’s account will be disabled after a total of five (5) invalid passwords attempts.
   7. Each user must not leave their workstation unattended for any period of time without first logging-out or locking the screen via a password-protected screen lock.
2. Account Unlock or Password Reset
   1. The users who have a locked account must perform one of the following:
   * Contact the IT Service Desk
   * Wait 30 minutes for automatic reset
   * Use a password reset portal
   1. In a case where the user is unable to provide the requested information their HR representative or direct functional manager should send an email to IT Service Desk requesting for an unlocking of the account or for a password reset on the user’s behalf.
   2. All temporary employee or vendor accounts must be set to expire on the date that their contract ends.
   3. Under no condition must a user disclose their password, for any reason.
   4. Always decline the use of the “Remember Password” feature of applications when/if prompted.
   5. A Signifi Management level individual who manages the Vendor relationship may also contact the IT Service Desk on behalf of the Vendor for the purpose of unlocking an account and/or initiating a password change.
   6. Password Changes: All user passwords (e.g. network sign-on) and administrator passwords must be changed at least every ninety (90) days.
   7. System-Level Passwords: All system-level passwords (e.g. Windows service accounts, root, enable, Unix Daemons) must be known to the least number of administrators, minimum of 2.

1. Password Use
   1. Default passwords must not be used. A unique password must always be generated according to the general practices listed in this policy.
   2. All “GUEST” accounts on all systems must be disabled.
   3. Application access must not be shared with anyone.
   4. Employees must ensure that the entry of passwords is not observed by others.
   5. Employee accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that Employee.
   6. If a user account or password is suspected to have been compromised, report the incident to the IT Service Desk and change all passwords immediately.
2. Password Security
   1. Server Configuration: The system must provide password aging capability. All user passwords must be set to expire every ninety (90) days at a minimum.
   2. Password Composition: Where supported by the Operating System or application, passwords must conform to the Password Construction Standard described in section 5 below.
   3. Password Reuse: Where supported by the operating system or application, reuse of the last five (5) passwords must be prohibited.
   4. Account Lockout: The account lockout must be set to lockout with no more than five (5) failed attempts.
   5. Lockout Duration: The account will remain locked for 30 minutes or will be unlocked by an administrator.
   6. Session Timeout: If a session has been idle for more than 5 minutes, users must be required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session.
   7. Password Expiration: New account passwords or passwords reset by the systems administrator must be set to expire immediately requiring the user to change the password at the first logon. Administrator passwords to accounts that have elevated privileges (e.g. system and service accounts) linked to the administrator should be changed when the user’s employment is terminated.
   8. Default Passwords: Vendor default passwords must be removed or reset before placing a system on the Signifi network. Do not allow default passwords on a system except during the install process, initial user setup, or user re-initialization. Upon completion of these activities, the password must be changed.
   9. Default Account Names: Where possible, vendor supplied account names must be changed.
3. Password Construction
   1. Passwords are used for various purposes at Signifi. Some of the more common uses include network and email access, screen lock protection and application access.
   2. Passwords used are at least twelve (12) characters, with a maximum not less than sixty-four (64) characters long, and include all four of the following conditions of complexity:
   * One number
   * One uppercase letter
   * One lowercase letter, and
   * One special character.

Enforcement

Signifi may monitor applications/systems, devices, and network traffic at any time to ensure compliance with this policy. All instances of non-compliance will be reviewed by the 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 | 2019-12-09 | First Draft | Darace Rose |
| 1.01 | 2020-02-25 | Minor edits | Seenan Bunni |
| 1.02 | 2020-12-03 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |