

IT121

Wireless Access 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 iii](#_Toc35862381)

[Introduction 4](#_Toc35862382)

[Purpose 4](#_Toc35862383)

[Audience 4](#_Toc35862384)

[Scope 5](#_Toc35862385)

[Policy Statement 5](#_Toc35862386)

[Enforcement 9](#_Toc35862387)

[Revision History 9](#_Toc35862388)

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 (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 Jafffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | March 19th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Precaution must be taken for wireless devices due to their inherent risk. While wireless data networks are attractive for the convenience that they offer, deploying and using wireless networks securely have many challenges. Unlike traditional wired networks, access to a wireless network is not confined to the physical office space. Wireless signals penetrate walls and floors easily and it is required by IT to employ appropriate security measures to ensure that only Signifi authorized users are provided access to corporate networks. Continual protection of the Signifi information that travels over these networks is a must.

Purpose

This policy describes how wireless networks are deployed by IT and used by associates, with the goal of protecting the Signifi information and network. It outlines acceptable deployment of wireless network infrastructure, including requirements for physical connection, secure configuration, access methods and appropriate management approvals. It also addresses user acceptable practices.

Audience

This policy applies to all Signifi associates, part-time and temporary workers, trainees, contractors, and vendors.

Scope

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.

Policy Statement

1. General
   1. Wireless devices must be provisioned and deployed only by Signifi IT network staff and approved by IT Management;
   2. No user is permitted to enable or connect a wireless Access Point on any Signifi network or premises;
   3. An inventory of all wireless devices must be maintained, documented by IT and provided upon request for audit and compliance purposes;
   4. IT must monitor and protect against the latest threats on wireless devices to ensure ongoing protection of the Signifi network;
   5. Encrypt all non-console administrative access to wireless devices using strong cryptography. Use technologies such as SSH v2, IPsec v2, TLS1.2 for web-based management and other non-console administrative access;
   6. Each administrator must have unique access credentials for systems administration and must use only central authentication, authorization and accounting access control systems when accessing administrative sessions on wireless devices;
   7. All wireless devices systems clocks must be synchronized with central Network Time Protocol (NTP) servers;
   8. Wireless devices must be placed in secure areas where physical access, power supplies, temperature and humidity are controlled; and
   9. Wireless access points must be located in a secure area to prevent unauthorized physical access and modification.

1. Policy Requirements
   1. Wireless access must not be used for carrying Signifi mission critical traffic;
   2. Wireless access must not be used for supporting systems that house mission critical data;
   3. Wireless access must not be used to transmit or access Highly Confidential information or systems e.g. card data environment (PCI Secure Zone);
   4. Wireless Internet access for guests must be segregated from Corporate wired /wireless Internet access or Signifi corporate network;
   5. Connections made to corporate resources via wireless networks need to be made using secure protocols as configured by IT.

1. IT Requirements
   1. For wireless technologies, IT must maintain/conduct the following:
   2. Ensure explicit approval by authorized parties for use of wireless technologies;
   3. Must configure wireless networks to disallow all access except those explicitly permitted;
   4. Ensure authentication is in use for wireless technologies (for example token or certificate);
   5. A listing of all such devices and personnel with access;
   6. Label devices to determine owner, contact information and purpose;
   7. Ensure acceptable uses of the technology is understood by users;
   8. Ensure acceptable network locations for the technologies. Access points and controllers are to be connected to a network that is isolated from any other network (internal and DMZ), such as a separate network on a corporate managed firewall;
   9. Keep current a list of company-approved wireless products;
   10. Change the default SNMP community strings on wireless devices;
   11. Change the default passwords/passphrases on access points;
   12. Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. The methodology used by IT must adequately detect and identify any unauthorized wireless access points, including at least the following:
   13. WLAN cards inserted into existing system components;
   14. Portable wireless devices connected to system components (for example, by USB, etc.);
   15. Wireless devices attached to a network port or network device;
   16. Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks;
   17. Verify other security-related wireless vendor defaults were changed, if applicable;
   18. Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted;
   19. Verify that logs for wireless equipment are offloaded or copied onto a secure centralized internal log server or media;
   20. Segment wireless access for visitors and Signifi staff using separate Service Set Identifier (SSID);
   21. Ensure all unwanted services and unused ports on wireless devices must be disabled; and
   22. Configure wireless device to display a legal warning message prior to the logon process of administrative components.
2. Wireless Network Device Configuration
   1. Wi-Fi Protected Access 2 (WPA2) configuration must be implemented using AES 128bit strength data encryption, at a minimum;
   2. Broadcast of the SSID must be disabled;
   3. Signal strength of wireless access points must be measured and reduced to cover only the desired areas;
   4. Configuration/change control and patch management processes must be followed for access points, controllers and other wireless devices to ensure that equipment have the latest software release/versions;
   5. The wireless operating system being used must be current and supported by the manufacturer. The operating system being used must be an official manufacturer stable, general release. Beta versions are not permitted;
   6. Wireless device configurations and password files must be backed-up and protected from unauthorized access and disclosure;
   7. Access points and other wireless device configuration must be standardized to ensure consistency of operation;

Enforcement

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 | 2019-12-17 | First draft | Darace Rose |
| 1.01 | 2020-02-26 | Minor edits | Seenan Bunni |
| 1.02 | 2020-03-16 | Minor edits | Razvan Anghelidi |
| 1.03 | 2020-11-30 | Annual review | Razvan Anghelidi |
| 1.04 | 2021-12-12 | Annual review | Hadeel alzuhairi |