

IT115  
Hardware Decommissioning Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.02 |
| 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](#_Toc34931253)

[Introduction 4](#_Toc34931254)

[Principles 4](#_Toc34931255)

[Scope 5](#_Toc34931256)

[Policy Objectives 5](#_Toc34931257)

[Implementation 5](#_Toc34931258)

[Disposal/Destruction of Physical Media 6](#_Toc34931259)

[Identification of IT Equipment Assets 6](#_Toc34931260)

[Asset Tags 7](#_Toc34931261)

[Disposal Criteria 7](#_Toc34931262)

[Removal / Reformatting of Storage Disks 7](#_Toc34931263)

[Software/Sanitization/Destruction 8](#_Toc34931264)

[Reuse and redistribution of IT Equipment 8](#_Toc34931265)

[Certification and Audit 8](#_Toc34931266)

[Asset Inventory 8](#_Toc34931267)

[Data Backup 8](#_Toc34931268)

[IT Asset Roles and Responsibilities 9](#_Toc34931269)

[IT Manager/Information Security/Approved Third Party 9](#_Toc34931270)

[Enforcement 11](#_Toc34931271)

[Revision History 11](#_Toc34931272)

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 | February 25th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Information and IT equipment are vital assets to any organization, and virtually all of our activities involve creating or handling information in one form or another via the IT equipment we use. The Hardware Decommissioning Policy and its associated policies are concerned with managing the secure disposal of IT equipment assets which are owned by the Signifi and are no longer required.

Principles

This policy defines the roles and responsibilities of staff in ensuring the secure disposal of Signifi IT equipment.

* All Signifi employees, part-time and temporary workers, trainees, contractors and vendors who use information assets have a responsibility to handle them appropriately and in accordance with their classification
* Signifi information assets should be made available to all who have a legitimate need for them
* The integrity of information assets must be maintained at all times. Information assets that are used in conjunction with the IT asset must also be accurate, complete, timely and consistent with other related information and events.

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. This policy applies to all Signifi resources owned, leased, or supported by Signifi, or any outside entity that has signed a Vendor Access Agreement with Signifi.

Policy Objectives

* To define the responsibilities of individuals for the secure disposal of Signifi IT assets
* To provide a rigorous and consistent process to ensure Signifi IT assets which are deemed “end of life” or to be recycled, are securely wiped before being redistributed or leaving the Signifi premises e.g. PCs, laptops, mobile phones and other devices that process and store Signifi data.
* To provide advice on the appropriate methods of destruction of physical media.
* To ensure sensitive information assets stored via the IT equipment is sufficiently backed up, copied and/or removed prior to being disposed of.
* To ensure an auditable trail of disposal/destruction is evidenced.

Implementation

Procedures will be put in place to ensure effective use of the Signifi IT Hardware Decommissioning Policy. These procedures include:

* Clear identification of Signifi information assets and protection in line with the asset classification scheme.
* Implementation of procedures for the disposal of Signifi IT assets.
* Ensuring that disposal procedures are adhered to.
* Provision of certification and audit trail for asset disposal.

Disposal/Destruction of Physical Media

The Signifi has a number of cross-cut shredders and confidential waste disposal locations, which must be used to dispose of hardcopy sensitive information assets which are no longer needed.

This removes the need for staff of the Signifi to store unwanted information assets within their workspace areas and improves efficiency.

For all other asset types such as, but not limited to:

* CDs
* Floppy discs
* Video tapes
* X-Rays
* Microfiche records
* Paper-based and hardcopy documents

please contact the IT department and they will help with the disposal.

Identification of IT Equipment Assets

IT equipment and devices that have the ability and capability to store Signifi information and sensitive data include:

* PCs
* Laptops
* Mobile phones
* Multi-Functional Devices - printers/scanners
* Servers
* USB memory sticks and external hard drives

Asset Tags

All Staff should be aware of the origin of the IT equipment being used to fulfil Signifi business activities. All IT equipment which has been purchased via a Signifi account must have an asset tag assigned to it. Where practical, the asset tag will be physically visible on the equipment stipulating that it is the property of the Signifi.

Please Note:

In the event that you are unsure of the origins, responsibility and ownership of IT systems or equipment, contact the Signifi IT Helpdesk Team.

Disposal Criteria

In the event that sensitive information and IT assets are no longer needed for Signifi purposes and cannot be securely wiped the equipment may need to be physically destroyed.

Removal / Reformatting of Storage Disks

IT equipment disposal must be managed by IT department manager and approved delegates only. Deleting visible files is not a sufficiently secure method of wiping equipment - data recovery software could be used by a new owner to “undelete” such files.

Similarly, formatting the whole hard disk or storage device may not prevent the recovery of redundant data as it is possible for disks to be “unformatted”.

Software/Sanitization/Destruction

Any IT assets leaving Signifi premises must comply with licenses and copyright law. IT department manager must ensure that all Signifi licensed software or operating systems are removed.

Reuse and redistribution of IT Equipment

IT department manager will undertake the necessary secure procedures to ensure any sensitive data is removed before IT equipment is redistributed.

Certification and Audit

Successful deletion and destruction must be evidenced, and certification must be obtained and recorded at all times.

Asset Inventory

Details must be recorded and updated within the IT department manager’s inventory database to ensure the Signifi has an up-to-date record of active IT assets.

Data Backup

It is the explicit responsibility of the owner/requestor of the IT asset to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

IT Asset Roles and Responsibilities

**Requestor**

All IT disposal requests must be requested via an IT Disposal Request Form ,which is completed and submitted to IT department manager.

**Please Note:**

All mandatory fields must be completed prior to submission. Failure to supply the relevant

information may defer or delay collection/disposal. IT department manager will only carry out the secure disposal of the IT assets detailed within the initial request. Any additional IT assets will require a separate request.

IT Manager/Information Security/Approved Third Party

Once the disposal request has been received, IT department manager will schedule a collection with the requestor.

IT department manager will ensure:

* All Urgent disposal requests will be physically reviewed, picked up and stored within IT department storage and disposed of in a secure manner within an agreed timescale
* All Scheduled disposal requests will be picked up and disposed of in a secure manner within an agreed timescale
* Certification of secure disposal will be obtained
* The redistribution or disposal of IT assets will be recorded in the asset inventory database

In the event of a significant disposal request, IT department manager may request that Facilities Management collect and transfer the IT assets to the appointed IT department storage.

Approved Third Party Supplier/Service Provider (Licensed) Where a licensed third-party service provider is to undertake secure disposal/destruction on behalf of the Signifi, its department manager will ensure the Signifi disposal criteria can be satisfied, and all confidential or sensitive information is securely sanitized and safeguarded.

It is imperative that a formal contract, due diligence and security review of the third-party supplier is undertaken at least on an annual basis to ensure Signifi requirements are satisfied.

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 | 2020-02-26 | Minor updates | Seenan Bunni |
| 1.02 | 2020-12-04 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |