

IT114  
Data Classification 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](#_Toc26333984)

[Purpose 4](#_Toc26333985)

[Abbreviations and Acronyms 4](#_Toc26333986)

[Scope 5](#_Toc26333987)

[Roles and Responsibilities 5](#_Toc26333988)

[Policy Statement 5](#_Toc26333989)

[Policy Compliance 9](#_Toc26333990)

[Exceptions 9](#_Toc26333991)

[Non-Compliance 9](#_Toc26333992)

[Contact 10](#_Toc26333993)

[Revision History 11](#_Toc26333994)

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 26th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Purpose

The purpose of this policy is to outline the requirements for the backup, retention and disposal of Signifi’s information assets to ensure their continued integrity and availability in case of loss or destruction caused by human error, malicious activity, equipment or media failure, or a catastrophic event, such as fire, flood or earthquake. Furthermore, this policy supports any applicable legislative and business requirements for information retention.

Abbreviations and Acronyms

CEO Chief Executive Officer

CPO Chief Privacy Officer

COO Chief Operating Officer

PIPEDA Personal Information Protection and Electronic Documents Act

ISO International Organization for Standardization

PI Personal Information

Scope

This policy applies to:

All employees, contractors, and agents (“Staff”) of Signifi who have access to PI or who work in proximity to media containing PI.

All Signifi information assets including PI, corporate data, system administration and security data (“Signifi Data”).

Roles and Responsibilities

1. Responsibility for day-to-day management of the Data Classification Policy is delegated to the Chief Privacy Officer (CPO).
2. Staff are responsible for ensuring that data within their control is appropriately classified and that security safeguards commensurate with the sensitivity of the data are applied.

Policy Statement

**Data Classification Levels:**

The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. This policy applies to data in all formats or places of storage. All Signifi Data will be classified into one of four sensitivity levels, or classifications:

1. **Restricted Data (Class 4)**

Data will be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a high level of risk to Signifi, its clients or its affiliates. Examples of Restricted data include:

* Personal Information
* Data classified as PI by Federal privacy regulations
* Data protected by confidentiality agreements
* Security sensitive data (e.g. password files)

The highest possible level of security controls will be applied to restricted data.

1. **Confidential Data (Class 3)**

Data will be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could result in a significant level of risk or damage to Signifi, its employees or its affiliates. Examples of Confidential Data include:

* Corporate Intellectual Property
* Corporate Financial Data
* Corporate Human Resources Information
* Statements of Work
* Sales Agreements

By default, all Corporate Data that is not explicitly classified as Restricted or Public data will be treated as confidential data. A high level of security controls should be applied to confidential data.

1. **Internal Data (Class 2)**

Data will be classified as Internal when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to Signifi, its employees, clients or its affiliates. The types of risk include but are not limited to unsolicited sales and marketing, Examples of Internal Data include:

* Corporate Phone and Email lists
* De-identified Personal Information used for application testing

By default, all Corporate Data that is not explicitly classified as Restricted, Proprietary or Public data should be treated as Private data. Internal Data should not be made available to persons or entities outside of Signifi except as expressly permitted by the Privacy Officer. A reasonable level of security controls should be applied to internal data.

1. **Public Data (Class 1)**

Data will be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to Signifi, its employees, clients, or its affiliates. Examples of Public data include:

* Press releases
* Course information
* Case Studies and Research Publications

While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

**Determining Classification:**

The goal of information security, as stated in Signifi’s Information Security Policy, is to protect the confidentiality, integrity, and availability of Corporate Data. Data classification reflects the level of impact to the company or its clients if confidentiality, integrity, or availability is compromised.

In some situations, the appropriate classification may be more obvious, such as when federal laws require Signifi to protect certain types of data (e.g. personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide. It is an excerpt from [Federal Information Processing Standards (“FIPS”) publication 199](https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf) published by the National Institute of Standards and Technology (NIST), which discusses the categorization of information and information systems.

|  | DATA CLASSIFICATION | | | |
| --- | --- | --- | --- | --- |
| CLASSIFICATION  OBJECTIVE | PUBLIC  (CLASS 1) | INTERNAL  (CLASS 2) | CONFIDENTIAL  (CLASS 3) | RESTRICTED  (CLASS 4) |
| **Confidentiality** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | Information collected and used by Signifi in the conduct of its business, including human resources, sales, marketing, and all aspects of corporate finance. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity** Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **moderat**e adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability** Ensuring timely and reliable access to and use of information. | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **moderate** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

Policy Compliance

The Signifi team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to this policy must be approved by the CEO or CEO delegate.

Non-Compliance

1. Any violation of this Policy by an employee of Signifi is subject to disciplinary sanctions, as determined by Signifi, up to and including dismissal.
2. Any violation of this Policy by a supplier, vendor or contactor or their respective employees and agents, is subject to remedies identified in the agreement or contract. Signifi may request the removal of a supplier, vendor or contractor employee who has violated this Policy.

Contact

Chief Privacy Officer: Razvan Anghelidi

Email Address: <mailto:ranghelidi@signifi.com>

Contact Number: 905-602-7707

Address: 1705 Tech Ave Unit 3, Mississauga, ON, L4W 0A2, Canada

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 | 2019-12-10 | First version | Darace Rose |
| 1.01 | 2020-02-26 | Minor changes | Seenan Bunni |
| 1.02 | 2020-12-01 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |