

IT106   
Data Backup, Retention and Disposal Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.15 |
| 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](#_Toc25267155)

[Purpose 6](#_Toc25267156)

[Abbreviations and Acronyms 6](#_Toc25267157)

[Scope 7](#_Toc25267158)

[Roles and Responsibilities 7](#_Toc25267159)

[Policy Statement 7](#_Toc25267160)

[Policy Compliance 11](#_Toc25267161)

[Exceptions 11](#_Toc25267162)

[Enforcement 11](#_Toc25267163)

[Revision History 12](#_Toc25267164)

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 20th, 2022 |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | February 27th, 2021 |
| Shamira Jaffer | CEO | January 5th, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
|  |  |  |
|  |  |  |

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

PI Personal Information

Scope

This policy applies to:

1. All employees, contractors and agents (“Staff”) of Signifi who have access to PI or who work in proximity to media containing PI.
2. All Signifi information assets including PI, corporate data, system administration and security data (“Signifi Data”).

Roles and Responsibilities

1. The Chief Operating Officer (COO) for Signifi is responsible for the day-to-day management of this backup, retention, and disposal policy.
2. The Chief Privacy Officer (CPO) for Signifi is responsible for ensuring compliance with this policy.

Policy Statement

1. Retention of PI
   1. Signifi will establish a retention schedule for PI, consistent with the legal obligations of Signifi customers under applicable privacy and data protection legislation and documented in Signifi service-level or licensing agreements.
   2. Signifi will establish retention schedules for backup copies of PI databases created for disaster recovery and business continuity purposes, audit logs that contain PI and copies of data created for other authorized purposes, based on an assessment of business requirements.
   3. Signifi will maintain an inventory of all databases and repositories of PI held in electronic form, including backup copies created for disaster recovery and business continuity purposes, audit logs that contain PI and copies of data created for other authorized purposes.
   4. Signifi will ensure that any software or utilities (e.g. encryption programs) required to read or copy archived or backed-up PI is available for the entire period in which the PI is retained.
   5. When there is a change in technology (e.g. new version of software), Signifi will ensure that the new technology can read production and archived data, or Signifi will convert the data into a format that can be read by the new technology.
   6. If data is stored in an encrypted format, Signifi will ensure that encryption programs, algorithms and keys required to decrypt production and archived data are available during the entire retention period and retained in a secure environment.
2. Retention for Signifi Emails
   1. Signifi will store the email mailboxes of former personnel for:

• 2 years for Project Managers and Account Managers  
• 3 years for Director/Manager level  
• 5 years for C level  
• 1 year for everyone else  
after the person is no longer associated with Signifi.

1. Backup of Signifi Data
   1. Signifi will establish a data backup plan and will implement procedures to create and maintain retrievable exact copies of PI and other information assets.
   2. Adequate backup facilities will be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
   3. Signifi will maintain accurate and complete records of the backup copies and documented restoration procedures.
   4. The extent (e.g. full or differential backup) and frequency of backups will reflect the business requirements of Signifi and its customers, security requirements of the information involved in the criticality of the data to the continued operations of Signifi and its customers.
   5. Data backups will be encrypted in accordance with the Signifi Encryption Policy.
   6. Data backups will be classified in accordance with the Signifi Data Classification Policy.
   7. Backup data and media will be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.
   8. Backup information stored at the offsite backup facility should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. If the offsite backup facility is owned and operated by a third party, the Service Level Agreement should specify the level of protection required.
   9. Backup media should be tested at least quarterly to ensure that they can be relied upon for emergency use when necessary.
   10. Restoration procedures should be checked and tested at least annually to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
2. Disposal and Destruction of Signifi Data
   1. At the end of the retention period, PI and any copies of the PI that are no longer required for the purposes for which it was collected, will be destroyed or rendered anonymous.
   2. Where PI is rendered anonymous, an effective anonymization or pseudonymization algorithm and program will be applied. After anonymization or pseudonymization the source files will be destroyed in a secure manner.
   3. Signifi will determine and will document in procedures, the method(s) for destroying or permanently erasing media containing PI, application software or security critical system data.
   4. When media containing PI, application software or security critical system data is no longer required, the media will be destroyed in a complete and secure manner or will be permanently erased.
   5. When equipment that includes media or devices containing PI, application software or security critical system data is sent out for repair, reuse or disposal (e.g. hard drives, flash drives) the media or devices containing PI will be removed, destroyed or permanently erased.
   6. All Signifi subcontractors provide that, upon termination of the contract, they will return or destroy/dispose of all personal information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
   7. The methods of destruction, disposal, and reuse are reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.
   8. In case a Signifi Client (the organization that directly receives the services) terminates their contract with Signifi and no longer utilizes the Signifi services, the following actions will be taken depending on the Signifi services in use:

* Signifi will provide the customer with a copy of the database, in PostgreSQL backup format, within 7 business days from the date of termination
* Signifi will keep up the server/instance/computing environment (e.g. clientname.signivision.com) for 30 days from the date of termination to allow the Client to retrieve the information from the web portal. This is the service stop day.
* Signifi will automatically remove the Client data from its backup systems. Depending on the hosting method, the backup data will be removed after 7 days from the service stop day for dedicated servers, up to 30 days (OVH servers) or 180 days (Aptum servers) for multi-tenant.

In all cases it is solely the responsibility of the Client to maintain the safeguards required by PIPEDA once the data is transferred out of Signifi systems.

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.

Enforcement

Any violation of this Policy by an employee of Signifi is subject to disciplinary sanctions, as determined by Signifi, up to and including dismissal.

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 | 2019-12-05 | First version | Darace Rose |
| 1.1 | 2019-12-17 | Update template | Razvan Anghelidi |
| 1.11 | 2020-12-01 | Annual review | Razvan Anghelidi |
| 1.12 | 2021-01-04 | Updated section 3.8 | Razvan Anghelidi |
| 1.13 | 2021-02-27 | Added section 2 | Razvan Anghelidi |
| 1.14 | 2021-12-12 | Annual review | Hadeel Alzuhairi |
| 1.15 | 2022-12-05 | Annual review | Razvan Anghelidi |