

**Backup and Recovery Management**

Policy Template

Customer Name

Author Name: Gouri Mahendru

Version: 2.1

Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Summary of Changes | Author | Approved By |
| 1.0 | 10-Apr-14 | Initial Document | Sujatha | Sekar T |
| 1.01 | 1-May-17 | Change GAVS logo | Emmanuel F | Sekar T |
| 2.0 | 20-Jan-23 | Revised Policy Statements (section 5.0) | Gouri Mahendru | Sekar T |
| 2.1 | 16-Mar-23 | Updated as per new GS Lab | GAVS document format | Gouri Mahendru | Sekar T |

|  |
| --- |
| Statement of Confidentiality |
| This GS Lab (Great Software Laboratory) and/or GAVS (GAVS Technologies) artefact and/or document and/or presentation is strictly confidential. It contains proprietary information intended only for recipients.  The recipient acknowledges and agrees that: (i) this artefact and/or document is not intended to be distributed ii) the recipient does not have the right to implement, copy, reproduce, fax, publicly divulge, or further distribute it, in whole or in part in any form, without seeking the express written permission from GS Lab and GAVS.  Any unauthorized use of the contents of this artefact and/or document and/or presentation in any manner whatsoever, is strictly prohibited. The artefact and/or document and/or presentation represents GS Lab’s and/ or GAVS’s current product offerings and best practices which are subject to change without notice. Please note that GS Lab and GAVS collaborate in relation to some of its offerings.  All third-party trademarks used herein belong to their respective owners and may be protected by law. This artefact and/or document and/or presentation only refers to such trademarks under the doctrines of nominative and descriptive fair usage to illustrate and explain concepts without implying violation of any legal constraints. If improper activity is suspected, all available information may be used by GS Lab and /or GAVS for any remedy or for lawful purpose. |

Table of Contents

[**1.** **Purpose** 4](#_Toc130481205)

[**2.** **Scope** 4](#_Toc130481206)

[**3.** **Definitions** 4](#_Toc130481207)

[**4.** **Applicable Laws, Regulations, and Industry Standards** 4](#_Toc130481208)

[**5.** **Policy Statements** 4](#_Toc130481209)

[**6.** **Relevant Procedures** 5](#_Toc130481210)

[**7.** **Non-compliance** 6](#_Toc130481211)

## **Purpose**

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to ensure recovery mechanisms are in place to help safeguard the information assets of [Company Name]. The policy helps prevent the loss of data in case of accidental deletion or corruption, system failure or disaster, and security breaches, as well as permitting timely restoration of information and business processes should such events occur. This policy is also used for the management of secure backup and restoration processes on appropriate backup media.

## **Scope**

Define to whom and to what systems this policy applies. List the employees required to comply or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions that are out of scope, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This policy refers to the backup and recovery of all data and is inclusive of data outside of [Company Name] stored in a cloud service, and/or held on a mobile computing device.

This policy applies to staff who may be creators and/or users of such data. The policy also applies to third parties who access and use [Company Name] systems and IT equipment or who create, process, or store data owned by [Company Name].

This policy applies to all employees, managers, contractors, vendors, business partners, and any other parties who have access to company data including backup or recovery service providers.

## **Definitions**

Define any key terms, acronyms, or concepts that will be used in the policy or accompanying procedures. A standard glossary approach is sufficient. An example definition:

## **Applicable Laws, Regulations, and Industry Standards**

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Dividing this section into subsections may be required depending on the length or complexity of the policy. Mapped regulations can be edited based on policy requirements.

|  |  |
| --- | --- |
| Guidance | Section |
|  |  |

## **Policy Statements**

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Subdividing this section into subsections may be preferable, depending on the length or complexity of the policy.

|  |  |  |
| --- | --- | --- |
| # | Policy Statement | Mapped Regulations/Standards |
|  | Data must be backed up, maintained, and tested to support recovery requirements. | NIST CSF: PR. IP-4  NIST 800-53: CP-2, CP-2(1), CP-2(2), CP-2(3), CP-2(4), CP-2(5), CP-2(8), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-9, CP-10, CP-10(2), CP-10(4)  ISO27002: 8.13  CIS: 11.1, 11.2  HIPAA: §164.308(a)(7)(ii)(A), §164.308(a)(7)(ii)(B), §164.310(d)(2)(iv) |
|  | Backups must be tested to ensure that they are effectively taking place and can be recovered. | NIST CSF: ID.SC-5, PR. IP-4, PR. IP-10  NIST 800-53: CP-4, CP-9, CP-9(1), CP-9(2), CP-9(3), CP-9(5)  ISO27002: 8.13  CIS: 11.5  HIPAA: §164.308(a)(7)(ii)(A) |
|  | Any backup or recovery service providers must meet defined security requirements. | NIST CSF: PR. IP-4,  NIST 800-171: 3.8.9  NIST 800-53: CP-6, CP-6(1), CP-6(3), CP-9, CP-9(8)  CMMC: MP. L2-3.8.9  SOC2: CC6.7  ISO27002: 8.10, 8.13  CIS: 11.3  PCI3: 9.5,9.5.1  PCI4: 9.4.1, 9.4.1.1, 9.4.1.2 |
|  | Data backups must be protected against ransomware and other threats. | NIST CSF: PR. IP-4  NIST 800-53: CP-6, CP-6(1), CP-9(8)  SOC2: CC6.7  ISO27002: 8.7  CIS: 11.3, 11.4 |
|  | Disaster recovery and business continuity plans must include procedures for recovering critical security services. | NIST CSF: ID.BE-5, PR. IP-9, PR.PT-5  NIST 800-53: CP-2, CP-2(1), CP-2(3), CP-2(8), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4)  ISO27002: 5.29  HIPAA: 164.308(a)(7)(ii)(C), §164.310(a)(2)(i) |
|  | **InfoSec in Business Continuity Planning** | |
|  | Resiliency requirements for security services must be defined and implemented. | NIST CSF: ID.BE-5, PR.PT-5  NIST 800-53: CP-1, CP-2  ISO27002: 5.29  PCI3: 10.8, 10.8.1  PCI: 10.7.1, 10.7.2, 10.7.3  HIPAA: 164.308(a)(7)(ii)(C), §164.308(a)(7)(ii)(E), §164.310(a)(2)(i) | |
|  | Security continuity must be tested as part of disaster recovery and business continuity testing. | NIST CSF: PR. IP-10  NIST 800-53: CP-3, CP-3(1), CP-4, CP-4(1), CP-4(2)  ISO27002: 5.29  HIPAA: §164.308(a)(7)(ii)(D) | |

## **Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. It is a best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

## **Non-compliance**

Clearly describe consequences (legal and/or disciplinary) for employee noncompliance with the policy. It may be pertinent to describe the escalation process for repeated noncompliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Client Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Client Name] policies
2. Termination of employment
3. Legal action according to applicable laws and contractual agreements