Documents and Records Policy

CloudStrategik Consulting

Effective Date: August 5, 2024
Version: 1.0

Prepared by: CloudStrategik Consulting
Anderson@cloudstrategik.com

Confidentiality Statement

This document contains proprietary and confidential information of CloudStrategik Consulting. The information contained herein is disclosed to the recipient in confidence for the sole purpose of internal use. No part of this document may be disclosed, reproduced, or distributed without the prior written consent of CloudStrategik Consulting.

Policy Title:	Documents and Records Policy
Policy Owner:	Anderson Anthony, Chief Information Officer
Effective Date:	August 5, 2024
Revised Date:	-

Contents

1 Purpose **5**

2 Scope **5**

3 Definitions **5**

4 Objectives **5**

5 Classification of Documents and Records **6**

6 Handling of Documents and Records **6**

7 Labeling of Documents **6**

8 Retention and Disposal **6**

9 Responsibilities **7**

10 Monitoring and Review **7**

11 Policy Review **7**

12 References **7**

13 Policy History **7**

14 Free Use Disclaimer **7**

1 Purpose

This policy outlines the procedures for classifying, handling, and managing documents and records within CloudStrategik Consulting. It aims to ensure that information is properly secured, accessed, and disposed of in a manner that safeguards its confidentiality, integrity, and availability.

2 Scope

This policy is applicable to all employees, contractors, and third-party partners who engage with the company's information assets. It covers all forms of documentation, whether physical or electronic, and addresses the full lifecycle of information management, from creation to disposal.

3 Definitions

- **Document**: Any piece of written, printed, or electronic information created or received by CloudStrategik Consulting in the course of business.
- **Record**: A subset of documents that provide evidence of business activities, transactions, or legal obligations, including contracts, reports, and communications.
- **Confidential Information**: Information that could harm the company if disclosed, such as financial data and trade secrets.
- **Sensitive Information**: Personal data or other information that must be protected to avoid harm or privacy violations, including personal identifiable information (PII).
- **Public Information**: Information that is approved for public dissemination and does not pose any risk if disclosed.

4 Objectives

The key objectives of this policy include:

- Educating stakeholders on the importance of proper information classification and management.
- Providing a structured approach to handling sensitive and confidential information.
- Establishing clear guidelines for the retention and disposal of records.

5 Classification of Documents and Records

Information at CloudStrategik Consulting is classified into three primary categories:

- **Confidential**: Includes highly sensitive business information, financial data, and proprietary knowledge that could harm the company if disclosed.
- **Sensitive**: Pertains to personal data, health records, and other private information that requires protection against unauthorized access.
- **Public**: Comprises information meant for public release, such as press statements and marketing materials.

6 Handling of Documents and Records

Handling practices vary according to the classification of information:

- **Confidential**: Access is restricted to authorized personnel. Must be stored securely and transmitted using encrypted channels.
- **Sensitive**: Access is limited and requires additional security measures, including secure storage and controlled access protocols.
- **Public**: Freely accessible and may be disseminated without restrictions.

7 Labeling of Documents

To ensure clarity in classification, documents are labeled accordingly:

- **Public**: Clearly marked as suitable for public access.
- **Private**: Indicated for internal use, access restricted.
- **Restricted**: Marked for limited access, requiring higher security.

8 Retention and Disposal

The retention period for various records is defined as follows:

- **Human Resources Records**: Retain for a minimum of seven years.
- **Financial Records**: Maintain for at least twelve years.

Upon reaching the end of the retention period, documents and records must be securely destroyed to prevent unauthorized access or disclosure.

9 Responsibilities

All employees, contractors, and third parties are responsible for:

- Accurately classifying and handling documents according to this policy.
- Protecting confidential and sensitive information from unauthorized access and disclosure.
- Reporting any incidents related to unauthorized access or breaches in data security.
- Ensuring that information is accessed only for legitimate business purposes.

10 Monitoring and Review

CloudStrategik Consulting will conduct regular audits and reviews of this policy to ensure compliance and effectiveness. Monitoring involves tracking access to sensitive and confidential information and auditing adherence to the established classification and handling procedures. The policy will be updated as necessary to reflect changes in regulatory requirements or business practices.

11 Policy Review

This policy will undergo an annual review or be updated as needed to ensure continued relevance and effectiveness. All modifications will be approved by senior management and communicated to all relevant stakeholders.

12 References

NIST 800-53 Rev 5: CP-6, CP-9, MP-4, MP-6

13 Policy History

Version	Approved By	Date	Description
1.0	Anderson Anthony, Chief Information Officer	08/05/2024	Initial Policy Release

14 Free Use Disclaimer

This policy was created by CloudStrategik Consulting. All or parts of this policy can be freely used for your organization. There is no prior approval required. For assistance with typesetting, formatting, or any policy-related needs, contact us at Anderson@cloudstrategik.com