Communication Security 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:	Communication Security Policy
Policy Owner:	Anderson Anthony, Chief Security Officer
Effective Date:	August 5, 2024
Revised Date:	-

Contents

1 Purpose

The purpose of this Communication Security Policy is to establish guidelines and procedures for protecting the confidentiality, integrity, and availability of communication systems and data within CloudStrategik Consulting. This policy aims to ensure secure communication channels and protect sensitive information from unauthorized access, alteration, or disclosure.

2 Scope

This policy applies to all employees, contractors, and third parties who utilize CloudStrategik Consulting's communication systems, including email, instant messaging, voice, video, and data transmission. It covers all forms of communication, whether internal or external, and applies to both physical and electronic communication channels.

3 Definitions

- **Communication Systems**: The hardware, software, networks, and protocols used for transmitting information within and outside of CloudStrategik Consulting.
- **Sensitive Information**: Information that, if disclosed, could cause harm to the company, its employees, customers, or partners. This includes but is not limited to personal data, financial information, intellectual property, and proprietary business information.
- **Encryption**: The process of converting information into a secure format that can only be accessed by authorized parties.

4 Secure Communication Channels

4.1 Email Security

- Employees must use company-provided email accounts for all work-related communications.
- Emails containing sensitive information must be encrypted before sending.
- Phishing and spam emails should be reported to the IT department immediately.

4.2 Instant Messaging and Collaboration Tools

- Approved instant messaging and collaboration tools should be used for internal communications.
- Sensitive information should not be shared over unsecured messaging platforms.

4.3 Voice and Video Communication

- Secure communication platforms should be used for voice and video calls, especially when discussing sensitive information.
- Calls should be conducted in private areas to prevent unauthorized listening.

5 Data Protection and Encryption

- Sensitive information must be encrypted during transmission and storage.
- Employees must use strong passwords and two-factor authentication for accessing communication systems.
- Any portable devices used for communication (e.g., laptops, smartphones) must have security measures in place, such as device encryption and remote wipe capabilities.

6 Monitoring and Logging

CloudStrategik Consulting reserves the right to monitor and log communications for security and compliance purposes. Monitoring includes the inspection of emails, messaging services, and other forms of communication. Logs will be maintained to ensure that communication channels are used appropriately and securely.

6.1 Scope of Monitoring

- Monitoring will focus on detecting unauthorized access, data breaches, and misuse of communication systems.
- Logs will include details such as the time, date, sender, recipient, and content of communications, as well as any attachments.

6.2 Data Retention and Access

- Communication logs will be retained for a minimum of one year or as required by law.
- Access to these logs will be restricted to authorized personnel only, and any access will be logged and audited regularly.

7 Incident Response

Any suspected breach of communication security, such as unauthorized access or data leakage, must be reported immediately to the IT department. An investigation will be conducted, and appropriate actions will be taken to mitigate the impact of the incident and prevent future occurrences. The response will include:

- Assessing the nature and scope of the incident.

- Containing and mitigating the effects of the incident.
- Notifying affected parties and stakeholders as appropriate.
- Reviewing and updating security measures to prevent similar incidents.

8 Compliance and Enforcement

All employees, contractors, and third parties are required to comply with this policy. Non-compliance may result in disciplinary action, including termination of employment or contractual relationship. Regular audits will be conducted to ensure adherence to this policy and to identify areas for improvement.

9 Training and Awareness

CloudStrategik Consulting is committed to providing regular training and awareness programs on communication security. This includes:

- Annual training sessions for all employees on recognizing and responding to security threats.
- Specialized training for IT and security staff on the latest security practices and technologies.
- Periodic updates and reminders about the importance of secure communication practices.
- Providing resources and support for employees to report suspicious activities and potential security breaches.

The training programs aim to foster a culture of security awareness and to ensure that all personnel understand their responsibilities in protecting company communications and data.

10 Policy Review

This policy will be reviewed annually or as needed to ensure its effectiveness and alignment with current security standards and regulatory requirements. Changes to this policy will be communicated to all employees and relevant stakeholders.

11 References

NIST 800-53 Rev 5: SC-5, SC-7, SC-8, SC-9, SC-13, SC-15

12 Policy History

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

13 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