



# AI Acceptable Use 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.*

<b>Policy Title:</b>	AI Acceptable Use Policy
<b>Policy Owner:</b>	Anderson Anthony, Chief Security Officer
<b>Effective Date:</b>	August 5, 2024
<b>Revised Date:</b>	-

# Contents

<b>1 Purpose</b>	<b>5</b>
<b>2 Scope</b>	<b>5</b>
<b>3 Definitions</b>	<b>5</b>
<b>4 Acceptable Use of AI</b>	<b>5</b>
4.1 General Principles . . . . .	5
4.2 Prohibited Activities . . . . .	6
<b>5 Data Privacy and Security</b>	<b>6</b>
5.1 Data Protection Measures . . . . .	6
5.2 Data Minimization and Retention . . . . .	6
<b>6 Bias and Fairness</b>	<b>6</b>
<b>7 Transparency and Accountability</b>	<b>7</b>
7.1 Transparency Requirements . . . . .	7
7.2 Accountability and Oversight . . . . .	7
<b>8 Training and Awareness</b>	<b>7</b>
<b>9 Policy Compliance and Enforcement</b>	<b>7</b>
9.1 Compliance Monitoring . . . . .	7
9.2 Disciplinary Actions . . . . .	7
<b>10 Policy Review and Update</b>	<b>8</b>
<b>11 References</b>	<b>8</b>
<b>12 Policy History</b>	<b>8</b>
<b>13 Free Use Disclaimer</b>	<b>8</b>

# 1 Purpose

The purpose of this AI Acceptable Use Policy is to outline the responsible and ethical use of artificial intelligence (AI) technologies within CloudStrategik Consulting. This policy aims to ensure that AI is used in a manner that upholds the company's values, respects individual rights, and complies with legal and regulatory requirements.

# 2 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and third-party partners who use or manage AI technologies at CloudStrategik Consulting. It covers all AI applications, tools, and systems, including both internally developed and third-party solutions.

# 3 Definitions

- **Artificial Intelligence (AI):** The simulation of human intelligence processes by machines, particularly computer systems, including learning, reasoning, and self-correction.
- **AI Applications:** Software or systems that utilize AI technologies to perform tasks such as data analysis, decision-making, or automation.
- **Sensitive Information:** Data that requires protection due to its confidential nature, including personal identifiable information (PII), financial records, and proprietary data.
- **Ethical AI Use:** The practice of using AI in a manner that is fair, transparent, and respects the rights and dignity of individuals.

# 4 Acceptable Use of AI

## 4.1 General Principles

AI technologies should be used in a manner that aligns with CloudStrategik Consulting's values and ethical standards. All users must:

- Use AI tools only for legitimate business purposes and in a manner consistent with this policy.
- Respect the privacy and confidentiality of data processed by AI systems, ensuring that sensitive information is protected at all times.
- Avoid using AI in ways that could lead to discrimination, bias, or other unfair outcomes.
- Ensure transparency in AI processes, providing clear information about how AI systems are used and their decision-making criteria.

## 4.2 Prohibited Activities

The following activities are prohibited when using AI technologies at CloudStrategik Consulting:

- Using AI to generate or disseminate false or misleading information.
- Employing AI systems to impersonate individuals or entities without their consent.
- Utilizing AI to engage in or facilitate illegal activities, including but not limited to fraud, cyber-attacks, and unauthorized surveillance.
- Sharing or inputting sensitive information into public AI platforms or third-party solutions outside the company's control.
- Manipulating or tampering with AI systems in a way that undermines their integrity or intended functionality.

## 5 Data Privacy and Security

### 5.1 Data Protection Measures

AI systems must be designed and operated to protect the privacy and confidentiality of all data. This includes implementing appropriate technical and organizational measures, such as:

- Encryption of sensitive data at rest and in transit.
- Access controls to restrict data access to authorized personnel only.
- Regular audits and assessments to ensure compliance with data protection standards.

### 5.2 Data Minimization and Retention

Data processed by AI systems should be limited to what is necessary for the intended purpose. Personal data should not be retained longer than required and must be securely disposed of when no longer needed.

## 6 Bias and Fairness

AI systems must be developed and deployed in a manner that promotes fairness and minimizes bias. CloudStrategik Consulting commits to:

- Regularly testing AI systems for biases and taking corrective actions where necessary.
- Providing training and resources to employees on identifying and mitigating biases in AI applications.
- Ensuring diverse perspectives are considered in the development and deployment of AI technologies.

## 7 Transparency and Accountability

### 7.1 Transparency Requirements

Users of AI systems must ensure that the processes and outcomes are transparent. This includes:

- Clearly documenting the purpose and functionality of AI systems.
- Providing explanations for AI-driven decisions, especially in contexts that significantly impact individuals.
- Maintaining records of AI system inputs, outputs, and decision-making criteria.

### 7.2 Accountability and Oversight

CloudStrategik Consulting will establish oversight mechanisms to ensure responsible AI use. This includes:

- Assigning responsibility for AI governance to a designated team or individual.
- Conducting regular reviews and audits of AI systems and their usage.
- Reporting and addressing incidents involving unethical or unauthorized AI use.

## 8 Training and Awareness

All employees and relevant stakeholders must receive training on the ethical and responsible use of AI. This training will cover:

- The principles outlined in this policy.
- Identifying and mitigating biases in AI systems.
- Safeguarding data privacy and security.
- Reporting and responding to unethical AI practices.

## 9 Policy Compliance and Enforcement

### 9.1 Compliance Monitoring

Compliance with this policy will be monitored through regular audits and assessments. The Security Team and designated AI governance personnel are responsible for enforcing compliance and addressing any violations.

### 9.2 Disciplinary Actions

Violations of this policy may result in disciplinary actions, up to and including termination of employment or contractual agreements. Legal actions may also be pursued if applicable.

## 10 Policy Review and Update

This policy will be reviewed annually or as necessary to address new developments in AI technologies, legal requirements, and ethical standards. Updates will be communicated to all employees and relevant stakeholders.

## 11 References

NIST AI Risk Management Framework, ISO/IEC 27001, GDPR

## 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](mailto:Anderson@cloudstrategik.com)