Generative AI Incident Response 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:	Generative AI Incident Response Policy
Policy Owner:	Anderson Anthony, Chief Security Officer
Effective Date:	August 5, 2024
Revised Date:	-

Contents

1 Introduction

The Generative AI Incident Response Policy outlines the procedures for identifying, managing, and responding to incidents involving Generative AI (GAI) systems. This policy is designed to minimize the impact of incidents on the organization, ensure the security and integrity of GAI systems, and align with the NIST Risk Management Framework (RMF) principles.

2 Purpose

The purpose of this policy is to establish a structured approach for responding to GAI incidents. It aims to ensure timely identification, containment, and resolution of incidents, thereby minimizing potential harm to the organization and its stakeholders.

3 Scope

This policy applies to all employees, contractors, and third parties involved with GAI systems within the organization. It covers incidents related to data breaches, security vulnerabilities, ethical concerns, and any other issues affecting GAI systems.

4 Definitions

- **Generative AI (GAI)**: AI models capable of generating new content, including text, images, and audio.
- **Incident**: An event that disrupts normal operations, compromises security, or causes harm.
- **NIST RMF**: A structured process developed by NIST for managing information security and privacy risks.

5 Incident Response Framework

The incident response framework includes the following phases, aligned with the NIST RMF:

5.1 Preparation

Preparation involves establishing policies, procedures, and response plans to effectively manage incidents. This includes training personnel, identifying critical assets, and establishing communication protocols.

5.2 Identification

Identifying incidents involves monitoring GAI systems for anomalies, security breaches, or ethical concerns. It requires the use of monitoring tools, user reports, and automated alerts to detect potential incidents.

5.3 Containment

Containment strategies are employed to limit the impact of an incident. This may involve isolating affected systems, restricting access, and implementing security controls to prevent further damage.

5.4 Eradication

Once an incident is contained, eradication involves removing the cause of the incident. This includes addressing vulnerabilities, removing malicious content, and ensuring systems are secure.

5.5 Recovery

Recovery focuses on restoring affected systems and operations to normal. This may involve restoring data from backups, reconfiguring systems, and verifying the integrity of GAI models.

5.6 Post-Incident Review

A post-incident review is conducted to analyze the incident, assess the effectiveness of the response, and identify areas for improvement. This phase includes documenting lessons learned and updating response plans.

6 Roles and Responsibilities

6.1 Incident Response Team (IRT)

The IRT is responsible for managing the incident response process. This includes coordinating response activities, communicating with stakeholders, and ensuring compliance with policies and regulations.

6.2 IT and Security Teams

IT and Security Teams are responsible for implementing technical controls, monitoring GAI systems, and assisting in incident detection and response.

6.3 Legal and Compliance Teams

Legal and Compliance Teams ensure that incident response activities comply with legal and regulatory requirements. They are also responsible for addressing any legal implications of incidents.

6.4 All Employees

All employees are responsible for reporting incidents, adhering to security policies, and participating in incident response training.

7 Incident Reporting and Communication

All incidents must be reported to the IRT immediately. The IRT will assess the severity of the incident and determine the appropriate response. Communication protocols will be established to keep stakeholders informed throughout the incident response process.

8 Monitoring and Continuous Improvement

Continuous monitoring of GAI systems is essential for early detection of incidents. The organization will use advanced monitoring tools and techniques to track system performance, detect anomalies, and identify potential security threats. The incident response process will be reviewed and updated regularly to incorporate lessons learned and adapt to evolving risks.

9 Training and Awareness

The organization will provide regular training and awareness programs for employees on incident response procedures, GAI risks, and security best practices. This training will include simulations and drills to ensure preparedness for real incidents.

10 Policy Review and Maintenance

This policy will be reviewed annually or as needed to ensure its effectiveness and relevance. Updates will be made based on changes in technology, regulatory requirements, and organizational needs.

11 References

NIST Risk Management Framework, NIST SP 800-53

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