Monitoring Management Policy

Double Good Technologies, LP

January 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.2

Table 2: Document history

Date	Comment
Sep 12 2023	Initial document

1 Purpose and Scope

1.1 Purpose

The Monitoring Management Policy (MMP) defines specific requirements for information systems to establish and maintain monitoring capabilities across the organization's entire environment. Monitoring is crucial for assessing system performance, detecting issues, and ensuring security.

1.2 Scope

This policy applies to all information systems within the organization's production network. It is also binding for all employees, contractors, and partners who administer or provide maintenance for the organization's production systems, referred to as system administrators throughout this policy.

2 Background

Effective monitoring is essential for maintaining the security, reliability, and performance of information systems. This policy outlines the specific requirements and instructions for implementing a robust monitoring system.

3 Policy

3.1 Monitoring Requirements

All production systems within the organization must establish and maintain monitoring capabilities. These capabilities should include, at a minimum:

Real-time monitoring of system performance, resource utilization, and service availability. Alerting mechanisms to notify administrators of system issues or performance anomalies. Log collection and analysis to detect potential security threats. Monitoring of network traffic and data flows to identify irregularities. Regular vulnerability scanning to assess system security. ## Specific Monitoring Activities Specific monitoring activities must include, at a minimum:

Continuous assessment of system performance metrics, including CPU, memory, and disk utilization. Tracking network traffic for unusual patterns or deviations. Log collection and analysis for security incidents and audit trail maintenance. Real-time alerts on critical system or service outages. Regular vulnerability scanning to identify and address security vulnerabilities. ## Alerting and Incident Response An incident response process should be established to address alerts generated by the monitoring system. This process should include:

Timely response to critical alerts. Notification of relevant personnel when incidents occur. Incident tracking and resolution procedures. ## Cloud Environment Monitoring When using an outsourced cloud environment, monitoring should extend to cloud-based resources. Monitoring cloud environment access, utilization, and performance is essential.

3.2 Compliance Monitoring

The monitoring system should include compliance checks to ensure adherence to industry and organizational standards.

4 Compliance

This policy will be regularly audited to ensure compliance. Non-compliance may result in disciplinary action.

5 Revision

This policy will be reviewed and updated as needed to adapt to changing technology and security requirements.