Network Security Policy

Double Good Technologies, LP

March 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.2

Table 2: Document history

Date	Comment
Oct 17 2023	Initial document

1 Purpose and Scope

1.1 Purpose

The Network Security Policy (NSP) defines specific requirements for ensuring the security and integrity of the organization's network infrastructure. It aims to safeguard sensitive data, prevent unauthorized access, and mitigate network-related risks.

1.2 Scope

This policy applies to all components of the organization's network infrastructure, including but not limited to routers, switches, firewalls, wireless access points, and related network devices. It is binding for all employees, contractors, and partners who manage or have access to the organization's network systems.

2 Background

Network security is paramount in protecting the organization's data and ensuring uninterrupted business operations. This policy outlines the specific requirements and instructions for establishing and maintaining a secure network environment.

3 Policy

3.1 Network Access Control

Access to the organization's network resources must be controlled. Users must be authenticated and authorized before gaining access.

Guest network access should be isolated from the organization's internal network to prevent unauthorized access.

3.2 Firewall Configuration

Firewalls must be implemented to filter network traffic and block unauthorized access.

Rules for allowing or denying traffic should be well-defined and regularly reviewed.

3.3 Intrusion Detection and Prevention

Intrusion detection and prevention systems (IDS/IPS) should be deployed to detect and respond to unauthorized or malicious activities.

Alerts generated by IDS/IPS must be reviewed, and appropriate action should be taken to mitigate security threats.

3.4 Network Segmentation

The network should be segmented to isolate sensitive data and limit lateral movement in the event of a breach.

Network segmentation must be designed to prevent unauthorized access to critical systems and data.

3.5 Wireless Network Security

Wireless networks should be secured with strong encryption and authentication methods.

Default credentials on wireless access points should be changed, and guest networks must be securely isolated.

3.6 Monitoring and Logging

Network traffic, logs, and security events should be monitored continuously.

Regular review of network logs and real-time alerts to identify and respond to security incidents is essential.

3.7 Network Redundancy

Redundancy should be built into the network infrastructure to ensure availability and minimize downtime.

Failover and backup systems should be tested periodically.

3.8 Compliance

The network should be regularly audited to ensure compliance with security policies, industry standards, and regulations.

Non-compliance may result in disciplinary actions.

4 Revision

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