Defined Company Objectives

Nexelus

Nexelus management is committed to provide the highest quality services by establishing, implementing and maintaining SOC I and SOC II compliance. An annual cycle will be used for setting the objectives, to coincide with the audit year. These objectives will be based upon a clear understanding of the business requirements, informed by the annual IT service management review with customers.

Company objectives specifically aligned with SOC 2 compliance requirements, focusing on data confidentiality, integrity, availability, and network performance:

Data Confidentiality Objectives

Objective 1: Implement stringent access controls (e.g., role-based access, multi-factor authentication) to ensure that only authorized personnel can access confidential data, in line with SOC 1 and SOC 2 standards.

Objective 2: Encrypt all sensitive data at rest and in transit using industry-approved encryption algorithms (e.g., AES-256) to protect confidentiality and ensure compliance with SOC 2 confidentiality principles.

Objective 3: Conduct regular confidentiality risk assessments and audits to identify vulnerabilities, document control measures, and ensure that data handling practices remain compliant with SOC 1 and SOC 2 standards.

Data Integrity Objectives

Objective 1: Implement and maintain data integrity controls, including checksums, validation rules, and version control systems, ensuring that data remains accurate, consistent, and unaltered during storage and transmission.

Objective 2: Perform regular integrity audits and implement automated monitoring tools that alerts for data discrepancies or potential breaches, allowing for prompt remediation in line with SOC 1 and SOC 2 integrity criteria.

Objective 3: Establish documented policies and procedures for maintaining data integrity throughout its lifecycle, including data input, processing, storage, and disposal, to meet SOC 1 and SOC 2 compliance requirements.

Data Availability Objectives

Objective 1: Implement a robust disaster recovery plan (DRP) and business continuity plan (BCP) that ensures critical systems and data are available during and after a disruption, in accordance with SOC 1 and SOC 2 availability requirements.

Objective 2: Guarantee system and service uptime through redundant systems, failover strategies, and geographically distributed data centers, aiming to meet a minimum of 99.9% availability.

Objective 3: Regularly test and update availability controls (e.g., backup systems, load balancers, failover protocols) to ensure they are effective and aligned with SOC 1 and SOC 2 availability criteria, mitigating risks of downtime.

These objectives are designed to meet SOC 1 and SOC 2 requirements while ensuring that the company's systems and processes remain secure, available, and reliable, protecting both the organization and its clients.