Security Group Policy

## Purpose

This policy defines the rules and guidelines for the creation, management, and usage of security groups within [Organization Name]'s cloud computing environment. The objective is to ensure the security, integrity, and availability of resources while maintaining compliance with regulatory requirements and industry best practices.

## Scope

This policy applies to all employees, contractors, and third-party service providers who are responsible for configuring and managing security groups within [Organization Name]'s cloud infrastructure.

## Responsibilities

* The [Designated Role/Team] is responsible for defining and implementing security group rules based on business requirements and security policies.
* Cloud administrators and infrastructure teams are responsible for creating, configuring, and monitoring security groups to ensure compliance with this policy.
* Users are responsible for adhering to the security group rules and guidelines when deploying and managing cloud resources.

## Security group configuration

* Security groups must follow the principle of least privilege, allowing only necessary inbound and outbound traffic.
* All inbound and outbound traffic must be explicitly defined and justified based on business requirements.
* Security group rules should be regularly reviewed and updated to reflect changes in business needs, security threats, or regulatory requirements.

## Rule definition

Each security group rule must specify:

* Protocol (e.g., TCP, UDP, ICMP)
* Port range or protocol-specific parameters (e.g., ICMP type and code)
* Source or destination IP addresses or CIDR blocks
* Action (allow or deny)

## Implicit deny

By default, all inbound and outbound traffic is denied unless explicitly allowed by a rule. This follows the principle of least privilege, where only necessary traffic is permitted.

## Scalability

Security groups can be easily applied and modified for multiple instances simultaneously. This allows for efficient management of security policies across various resources within a network.

## Dynamic updates

Changes to security group rules take effect immediately, allowing for quick adaptation to changing security requirements or network configurations.

## Required rule types for systems

#### Web servers

Inbound, outbound

#### Database servers

Inbound, outbound

#### File servers

Inbound, outbound

#### Application servers

Internal, peer

#### Remote access servers

Inbound, outbound

#### Monitoring systems

Inbound, outbound

#### Load balancers

Inbound, outbound

#### DNS servers

Inbound, outbound