## Information Security Plan

## DATE: June 17, 2022

## From: Trisun

## SUBJECT: Information Security Plan

## Purpose

The purpose of this policy is to provide suggestions and information on products or other products to relevant personnel of the organization. Every program needs effective and understandable reasons.

## Policy

The country must clearly explains how to change the security risks of Cisco and services, including the timeline, actions, and responsibilities that apply equally to all customers.

## Cisco Product Security Incident Response

## We know that Internet technology is based on IP protocol. All information communication is through IP groups. All devices that need to communicate must have a unique IP address. Therefore, in order to access the Internet, the devices communicating through the Internet must have a unique global Internet address. When the network needs to access the Internet, all devices in the network have their own network addresses, which is undoubtedly the best way to realize various network applications. But this makes all devices exposed to the network, and anyone can attack. My network currently uses IPv4 protocol for network development. So far, not enough IP addresses can be used, and it is almost impossible for devices on the network to need IP addresses.

## The administrator only specifies a public Internet address, which can be converted to a port address through port address translation, and accesses the IP ports mapped to the IP pool, so that each project can map the IP of more than 60000 internal network hosts through the Internet. Therefore, the internal network address information is hidden, and the internal network devices cannot be accessed directly from the outside.

## Reporting or Obtaining Support for a Suspected Security Vulnerability

It was asked that individuals or organizations should be consulted with Cisco's security challenges. Cisco welcomes reports from independent researchers, industry organizations, suppliers, customers, and other product and security sources. The minimum date is to return security emissions. A description of the potential for vulnerabilities.

## Reference:

1. Mark, H 2021, *Cisco Security*, viewed 17 June 2022,

**< https://tools.cisco.com/security/center/resources/security\_vulnerability\_policy.html>**

1. Bruce, S 2021, *Vulnerabilities in Weapons Systems*, viewed 17 June 2022,

**<**[**https://www.schneier.com/blog/archives/2021/06/vulnerabilities-in-weapons-systems.html**](https://www.schneier.com/blog/archives/2021/06/vulnerabilities-in-weapons-systems.html)**>**

1. Patton, O 2021, *Assessing Security Risk*, viewed 17 June 2022,

**<**[**https://www.cisco.com/c/en/us/training-events/training/certifications/certifications/security.html**](https://www.cisco.com/c/en/us/training-events/training/certifications/certifications/security.html) **>**