Network Security Policies Manual

Zero Day Inc – Media Company

ITNW 2350 ENTERPRISE NETWORK – CAPSTONE PROJECT

TEAM MEMBERS:

Michele Reynolds

Christian Bertinot

Darleen Espinales

Anthony Goulet

Juan Cruz

Nathan Vazquez

Table of Contents

1.0 PURPOSE

The purpose of this document is to provide an overview of the security requirements of Zero Day Inc.'s network and describe the controls in place or planned to keep data secure and accessible. This document also defines responsibilities and expected behavior of all individuals who access the system.

2.0 RESPONSIBLE ORGANIZATION

The roles and responsibilities of the personnel involved with the Risk Management Framework (RMF) are summarized in the paragraphs below.

2.1 CHIEF INFORMATION OFFICER

The Chief Information Officer (CIO) is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems security policies, standards, guidelines, and procedures.

2.2 SECURITY MANAGER

The Security Manager (person in charge of physical security and individual safety) is responsible for coordinating investigations into any alleged computer or network security compromises, incidents, or problems with the IT Infrastructure Services director.

2.3 SYSTEM ADMINISTRATOR

System administrators are responsible for acting as local information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. They also are responsible for reporting all suspicious computer and network-security-related activities to the Security Manager. System administrators also implement the requirements of this and other information systems security policies, standards, guidelines, and procedures.

3.0 GENERAL DESCRIPTION

Zero Day Inc. provides information resources to employees in support of the mission of delivering quality media services to the public.

Zero Inc. expects all stewards and custodians of its administrative information to manage, access, and utilize this information in a manner that is consistent with the Zero Day's need for security and confidentiality. Zero Day administrative functional areas must develop and maintain clear and consistent procedures for access to Zero Day Inc.'s administrative information, as appropriate.

4.0 POLICIES

The purpose these policies have been developed is to help avoid costly misconfigurations, gain full visibility into Zero Day's network and ensure continuous compliance. It ensures that there are clear processes, and the processes are followed by all employees and visitors that uses the network at Zero Day Inc., keeping it safe and making it easier to manage network security.

All users should be aware that the data they create on the network remains the property of Zero Day Inc. Users should have no expectations of expressed or implied privacy. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. As with all privileges, it is the responsibility of the user to use this service appropriately and in compliance with all Zero Day policies and procedures, Texas state law, and Federal laws.

Zero Day reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.1 GUEST POLICY

Guest WIFI Wireless Networking Acceptable Use Policy

Zero Day Inc. is offering this guest Wi-Fi wireless Internet service (the "Service") according to this Guest Wi-Fi Wireless Networking Acceptable Use Policy (the "Policy") as a free, non-public service to its visitors for the duration of their official visits. All users of this Service must agree to the terms of this Policy by clicking the ACCEPT button below. We do not guarantee the Service or specific rates of speed. We also have no control over information obtained through the Internet and cannot be held responsible for its content or accuracy. Use of the service is subject to the user's own risk. We reserve

the right to remove, block, filter, or restrict by any other means any material that, in our sole discretion, may be illegal, may subject us to liability, or may violate this Policy. We will cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violations of this Policy may result in the suspension or termination of access to the Service or other resources, or other actions as detailed below.

Responsibilities of Service Users:
Users are responsible for ensuring they are running up-to-date anti-virus software on their wireless devices. Users must be aware that, as they connect their devices to the Internet through the Service, they expose their devices to: worms, viruses, Trojan horses, denial-of-service attacks, intrusions, packet-sniffing, and other abuses by third-parties. All visiting users and computers must receive approval from the **Zero Day Inc.** IT department before connecting and using our guest Wi-Fi services. Users must respect all copyrights. Downloading or sharing copyrighted materials is strictly prohibited. The running of programs, services, systems, processes, or servers by a single user or group of users that may substantially degrade network performance or accessibility will not be allowed. Electronic chain letters and mail bombs are prohibited. Connecting to "Peer to Peer" file sharing networks or downloading large files, such as CD ISO images, is also prohibited. Accessing another person's computer, computer account, files, or data without permission is prohibited. Attempting to circumvent or subvert system or network security measures is prohibited. Creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system is prohibited. Using any means to decode or otherwise obtain restricted passwords or access control information is prohibited. Forging the identity of a user or machine in an electronic communication is prohibited. Saturating network or computer resources to the exclusion of another's use, for example, by overloading the network with traffic such as emails or legitimate (file backup or archive) or malicious (denial of service attack) activity, is prohibited. Users understand that wireless Internet access is inherently not secure, and users should adopt appropriate security measures when using the Service. We highly discourage users from conducting confidential transactions (such as online banking, credit card transactions, etc.) over any wireless network, including this Service. Users are responsible for the security of their own devices.

Limitations of Wireless Network Access:
We are not liable for any damage, undesired resource usage, or detrimental effects that may occur to a user's device and/or software while the user’s device is attached to the Service. The user is responsible for any actions taken from his or her device, whether intentional or unintentional, that damage or otherwise affect other devices or users of the Service. The user hereby releases the Company from liability for any loss, damage, security infringement, or injury which the user may sustain as a result of being allowed access to the Service. The user agrees to be solely responsible for any such loss, infringement, damage, or injury.

4.2 Authentication Policy / Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Zero Day's network.

This policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that belongs to Zero Day or has access to the Zero Day network.

Poor, weak passwords have the following characteristics:

a) The password contains less than eight characters
b) The password or a subset of the password is a word found in a dictionary (English or foreign)
c) The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

a) Contain between 8 and 32 characters
b) Contain both upper- and lower-case characters (e.g., a-z, A-Z)
c) Contain at least one number (e.g., 0-9)
d) Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
e) Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
f) Does not contain personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or another phrase.

Users will be allowed 3 failed password attempts before being locked out of a system or service. Account lockout occurs when someone tries to log on unsuccessfully several times in a row. We can usually assume that a legitimate user might type his or her password incorrectly once or twice, but not numerous times. Thus, numerous failed logons can indicate that someone is trying a brute-force password attack. If you are locked out of your account, contact your system administrator.

Compliance with the password security policy will be monitored with audits every 60 days.

4.3 Wireless Policy

Overview

Wireless networking poses a significant risk that can be exploited. To protect the systems with wireless access points, strong authentication and strong encryption is required.

Configuration Requirements

Zero Day Inc. will follow the guidelines laid out in Guidelines for Securing Wireless Local Area Networks.

Disable all network interfaces that are not authorized for any use

a) Disable bridging (passing traffic between the networks)
b) Configure host-based network security tools (e.g., host-based firewalls, host-based intrusion
    a. detection and prevention systems) to prevent multiple network interfaces from being used at one time.
c) Authentication of users and devices along with strong encryption will be used.

5.0 Network Security Policy

Overview

Introduction

The Network Security Policy applies to the IT Dept. Employees to ensure best practices are used to ensure confidentiality, integrity and availability of ZeroDay network, and its customers data.

Purpose/Scope of this Policy

1. The purpose of this policy is to ensure the security of the **Zero Day Inc.** network. To do this **Zero Day Inc.** will:
    a) Ensure Availability
    b) Ensure that the network is available for Users;
    c) Preserve Integrity
    d) Protect the network from unauthorized or accidental modification;
    e) Preserve Confidentiality
    f) Protect assets against unauthorized disclosure.

2. The purpose of this policy is also to ensure the proper use of the **Zero Day Inc.** network and make Users aware of what **Zero Day Inc.** deems as acceptable and unacceptable use of its network.

3. Willful or negligent disregard of this policy may be investigated and dealt with under the **Zero Day Inc.** Disciplinary Procedure.

4. This policy applies to all networks managed by **Zero Day Inc.** used for:

    a) The storage, sharing and transmission of non-clinical data and images;
    b) The storage, sharing and transmission of clinical data and images;
    c) Printing or scanning non-clinical or clinical data or images;
    d) The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images.

The Policy

The Network Security Policy for **Zero Day Inc.** is described below:

The **Zero Day Inc.** information network will be available when needed and can be accessed only by legitimate Users. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, **Zero Day Inc.** will undertake the following:

a) Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures;
b) Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
c) Implement the Network Security Policy in a consistent, timely and cost-effective manner.
d) Where relevant, **Zero Day Inc.** will comply with:

-Copyright, Designs & Patents Act 1988
-Access to Health Records Act 1990
-Computer Misuse Act 1990
-The Data Protection Act 1998
-The Human Rights Act 1998
-Electronic Communications Act 2000
-Regulation of Investigatory Powers Act 2000
-Freedom of Information Act 2000
- Environmental Information Regulations 2004 (EIRs)
-Health & Social Care Act 2008

The Trust will comply with other laws and legislation as appropriate

5.1 Firewall Policy

Overview

A firewall is one element of security used in Zero Day Inc.'s network. It reduces the threat of outsiders either damaging network systems or using the systems as an entry point for illegal access to other systems. A firewall does not prevent malicious or illegal activities from inside the firewall. However, to increase network security, Zero Day, Inc. will follow NIST's Guidelines for Firewall Policy.

Configuration Requirements

The firewall will be configured:

(Egress filtering):

i. Default denies all to exit DMZ except sources that are DMZ inside/outside traffic and denies all to exit the internal network except sources that are inside/outside internal network traffic to prevent IP spoofing attacks.
ii. SMTP and POP connections are limited to only the third-party email servers in use by Zero Day, Inc.
iii. DNS queries are limited only to Server DC1 in the NOC

(Ingress filtering):

i. Block incoming loopback packets and RFC 1918 networks

– 127.0.0.0

– 10.0.0.0 – 10.255.255.255

– 172.16.0.0 – 172.31.0.0

– 192.168.0.0 – 192.168.255.255

a) If there are no rules defined for a Zero Day network address, then traffic to or from that address must be denied by default.
b) Access to the Zero Day network must be blocked during the start-up procedure of the firewall. The firewall Operating System will be configured for maximum security.
c) The underlying operating systems of firewall hosts must be configured for maximum security, including the disabling of any unused services. The firewall product suite must reside on dedicated hardware.
d) Applications that could interfere with or compromise the security and effectiveness of the firewall must not be allowed to run on the host machine. The initial build and configuration of the firewall must be fully documented.
e) If any component of the firewall fails, the default response will be to immediately prevent any further access, both "outbound" as well as "inbound". ***See Definitions for further information.***

f) Periodic penetration testing will be performed rather than a conventional audit to assess the overall security of the network environment and verify that firewall rulesets are performing as intended

5.2 Router / Switch Policy

Overview

This document describes a required minimal security configuration for all routers and switches

connecting to a production network or used in a production capacity at or on behalf of Zero Day, Inc.

Configuration Requirements

Describes a minimal security configuration for all routers and switches connected to the network at or on behalf of the Zero Day's Inc Network.

Services that should be disabled

- IP directed broadcasts
- Incoming packets at the router/switch sourced with invalid addresses
- TCP small services – Echo, Chargen, Discard, Daytime
- UDP small services – Echo, Chargen, Discard
- All web services running on the router
- All source routing
- Autoconfiguration

Unless justified the services should be disabled

- Discovery protocols
- Scripting environments, for example the TCL shell

The following services must be configured

- Password encryption

Telnet not to be used across the network unless there is a secure tunnel protecting the communication path. Use SSH version 2 for the management protocol.

Every network switch including all company VLANS must meet the following configuration standards:

- No user accounts configured on the switch
- The enable password on the switch must be kept in its secure encrypted form. Must have the enable password set to the current switch password as to not cause further confusion
- MAC level address locking enabled if available

- Be able to generate an SNMP trap if the link drops and is re-established if the feature is available
- Disable a port or group of ports if new or unregistered MAC addresses appear on a port if available
- ALL Switches, Routers, and Firewalls are located in a lockable rack in a location where physical access is limited to authorized persons only

5.3 Server / Client Policy

Overview

Client/server systems often store data and perform processing on both the server and the client, meaning contingency planning for this type of system needs to address potential disruptions to the server, clients, and the connectivity between clients and server components of the system.

Configuration Requirements

Operating System configuration should be in accordance with approved **Zero Day Inc.** guidelines.

Services and applications that will not be used must be disabled where practical.

Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

Servers should be physically located in an access-controlled environment.

Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

• All security related logs will be kept online for a minimum of 1 week.

• Daily incremental tape backups will be retained for at least 1 month.

• Weekly full tape backups of logs will be retained for at least 1 month.

• Monthly full backups will be retained for a minimum of 2 years.

Security-related events will be reported to the CIO and IT director, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts

5.4 Wireless

Overview

This policy addresses the wireless connection of **Zero Day Inc.** owned devices in remote locations.

Purpose

The purpose of this policy is to secure and protect the information assets owned by **Zero Day Inc.** and to establish awareness and safe practices for connecting to free and unsecured Wi-Fi, and that which may be provided by **Zero Day Inc. Zero Day Inc.** provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. **Zero Day Inc.** grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

Zero Day Inc. Wi-Fi Network

The **Zero Day Inc.** Wi-Fi network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it. For employee business use, it is designed to be a supplement to, and not a substitute for, the production wired local area network. For non-employees, it is also provided as a convenience, primarily as a way for members to access **Zero Day Inc.** online products and services. Staff may easily demonstrate **Zero Day Inc.** online products and services to members or prospects.

Microwaves, cordless telephones, neighboring APs, and other Radio Frequency (RF) devices that operate on the same frequencies as Wi-Fi are known sources of Wi-Fi signal interference. Wi-Fi bandwidth is shared by everyone connected to a given Wi-Fi access point (AP). As the number of Wi-Fi connections increase, the bandwidth available to each connection decreases and performance deteriorates. Therefore, the number and placement of APs in a given building is a considered design decision. Due to many variables out of direct **Zero Day Inc.** control, availability, bandwidth, and access is not guaranteed.

The **Zero Day Inc.** Wi-Fi network and connection to the Internet shall be:

- Secured with a passphrase and encryption, in accordance with current industry practice Passphrases will be of appropriate complexity and changed at appropriate intervals, balancing security practice with the intended convenient business use of the Wi-Fi
- Physically or logically separate from the **Zero Day Inc.** production wired local area network (LAN) and its resources. All Wi-Fi AP/Routers must be cabled to a switch for any user to move beyond Wi-Fi.
- Provided as a convenience for the use of **Zero Day Inc.** employees, their vendors while visiting **Zero Day Inc.**, the members of **Zero Day Inc.**, and other visitors with **Zero Day Inc.**'s express permission via provision of an appropriate passphrase

- Optionally provided to members and qualifying visitors, by **Zero Day Inc.** staff, with the provision of an appropriate passphrase and may be accessed only with the agreement to acceptable use policy statements provided online or in a written or verbal format
- Used for access to the **Zero Day Inc.** production LAN only for business use and with the approved use of a **Zero Day Inc.** issued virtual private network (VPN) connection

Zero Day Inc.'s Wi-Fi service may be changed, the passphrase re-issued or rescinded, the network made unavailable, or otherwise removed without notice for the security or sustainability of **Zero Day Inc.** business

Public Wi-Fi Usage

When using Wi-Fi on a mobile device in a public establishment, there are precautions that should be followed.

Do:

- As with any Internet-connected device, defend your laptop, tablet, phone, etc. against Internet threats. Make sure your computer or device has the latest antivirus software, turn on the firewall, never perform a download on a public Internet connection, and use strong passwords.
- Look around before selecting a place to sit, consider a seat with your back to a wall and position your device so that someone nearby cannot easily see the screen.
- Assume all Wi-Fi links are suspicious, so choose a connection carefully. A rogue wireless link may have been set up by a hacker. Actively choose the one that is known to be the network you expect and have reason to trust.
- Try to confirm that a given Wi-Fi link is legitimate. Check the security level of the network by choosing the most secure connection, even if you have to pay for access. A password-protected connection (one that is unique for your use) is better than one with a widely shared passphrase and infinitely better than one without a passphrase.
- Consider that one of two similar-appearing SSIDs or connection names may be rogue and could have been setup by a hacker. Inquire of the manager of the establishment for information about their official Wi-Fi access point.
- Avoid free Wi-Fi with no encryption. Even if your website or other activity is using https (with a lock symbol in your browser) or other secure protocols, you are at much greater risk of snooping, eavesdropping, and hacking when on an open Wi- Fi connection (such as at Starbuck's, McDonald's, some hotels, etc.).
- Seek out Wi-Fi connections that use current industry accepted encryption methods and that generally will require the obtaining of a passphrase from the establishment.
- Consider using your cell phone data plan for sensitive activities rather than untrusted Wi-Fi, or your own mobile hotspot if you have one or have been provided with one.
- If you must use an open Wi-Fi, do not engage in high-risk transactions or highly-confidential communication without first connecting to a virtual private network (VPN).

- If sensitive information absolutely must be entered while using a public network, limit your activity and make sure that, at a minimum, your web browser connection is encrypted with the locked padlock icon visible in the corner of the browser window, and make sure the web address begins with https://. If possible, save your financial transactions for when you are on a trusted and secured connection, at home, for instance. Passwords, credit card numbers, online banking logins, and other financial information is less secure on a public network.
- Avoid visiting sites that can make it easier or more tempting for hackers to steal your data (for example, banking, social media, and any site where your credit card information is stored).
- If you need to connect to the **Zero Day Inc.** network and are authorized to do so, choose a trusted and encrypted Wi-Fi AP or use your personal hotspot. In every case, you must use your **Zero Day Inc.** `-provided VPN at all times. The VPN tunnel encrypts your information and communications and besides, hackers are much less likely to be able to penetrate this tunnel and will prefer to seek less secure targets.
- In general, turn off your wireless network on your computer, tablet, or phone when you are not using it to prevent automatic connection to open and possibly dangerous APs. Set your device to not connect automatically to public or unknown and untrusted networks.

Finally,

Do Not:

- Leave your device unattended, not even for a moment. Your device may be subject to loss or theft, and even if it is still where you left it, a thief could have installed a keylogger to capture your keystrokes or other malware to monitor or intercept the device or connection.
- Email or originate other messages of a confidential nature or conduct banking or other sensitive activities, and definitely not when connected to an open, unencrypted Wi-Fi.
- Allow automatic connection to or connection to first Wi-Fi AP your device finds, as it may be a rogue AP set up by a thief. Rather, choose the one that is known to be the network you expect and have reason to trust.

5.5 Remote Policy: Encryption, VPN, RDP

Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of the **Zero Day Inc.** policy, we must mitigate these external risks the best of our ability.

Purpose

The purpose of this policy is to define rules and requirements for connecting to **Zero Day Inc**'s network from any host. These rules and requirements are designed to minimize the potential exposure to **Zero Day Inc.** from damages which may result from unauthorized use of **Zero Day Inc.** resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical **Zero Day Inc.** internal systems, and fines or other financial liabilities incurred as a result of those losses.

Scope

This policy applies to all Zero Day Inc. employees, contractors, vendors, agents, and guests with a **Zero Day Inc.**-owned or personally-owned computer or workstation used to connect to the **Zero Day Inc.** network. This policy applies to remote access connections used to do work on behalf of **Zero Day Inc.**, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to **Zero Day Inc.** networks.

Policy

It is the responsibility of **Zero Day Inc.** employees, contractors, vendors, agents, and guests with remote access privileges to **Zero Day Inc.**'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to **Zero Day Inc.**

General access to the Internet for recreational use through the **Zero Day Inc.** network is strictly limited to **Zero Day Inc.** employees, contractors, vendors, agents, and guests (hereafter referred to as “Authorized Users”). When accessing the **Zero Day Inc.** network from a personal computer, Authorized Users are responsible for preventing access to any **Zero Day Inc.** computer resources or data by non-Authorized Users. Performance of illegal activities through the **Zero Day Inc.** network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access.

Authorized Users will not use **Zero Day Inc.** networks to access the Internet for outside business interests.

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (ie VirtualPrivateNetworks (VPNs) and strong pass-phrases. For further information see the *Authentication / Password Policy.*

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a **Zero Day Inc.** -owned computer to remotely connect to **Zero Day Inc.**'s corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct **Zero Day Inc.** business must be approved in advance by **Security Blanket** and the appropriate business unit manager.

4.1.5 All hosts that are connected to **Zero Day Inc.** internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.

4.1.6 Personal equipment used to connect to **Zero Day Inc.** 's networks must meet the requirements of **Zero Day Inc.** -owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to* **Zero Day Inc.** *Networks*.

Policy Compliance

Compliance Measurement

Zero Day Inc. will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

Exceptions

Any exception to the policy must be approved by Remote Access Services and the **Security Blanket** Team in advance.

Applicability.

- *All employees*
- *Subcontractors*
- *Guests / Visitors*
- *Departmental administrators*
- *Business managers*
- *Administrative staff*
- *Financial staff*

6.0 FAILURE TO COMPLY

Any users found to have violated this policy may be subject to:

- Oral or written warnings.
- Revocation of access rights
- Suspension with pay.
- Suspension without pay.
- Demotion or departmental transfer
- Termination.

7.0 DEFINITIONS

Assured File Transfer **(AFT)** -the process of moving a file or files from a higher classification system to a lower classification system.

Authorization to Operate (ATO) -the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Continuous Monitoring-a technology and process that IT organizations may implement to enable rapid detection of compliance issues and security risks within the IT infrastructure. sometimes referred to as ConMon or Continuous Control Monitoring (CCM) provides security and operations analysts with real-time feedback on the overall health of IT infrastructure, including networks and applications deployed in the cloud.

Egress Filtering - controls the traffic that is attempting to leave the network. Before an outbound connection is allowed, it has to pass the filter's rules (i.e. policies). These rules are set by the administrator.

Inbound- Only specific services which support Zero Day's mission will be allowed to be accessed from the Internet. The chart below identifies the most common services used for Internet communications within the Zero Day Inc. environment.

Ingress Filtering – monitors, controls and restricts traffic entering a network with the objective of ensuring that only legitimate traffic is allowed to enter and that unauthorized or malicious traffic is prevented from doing so

Information Security Plan - A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements

Keylogger -The action of recording or logging the keystrokes on a keyboard.

Need- to-Know (NTK) - is a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Network Address Translation (NAT)- stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information.

Outbound - Allow ALL Internet traffic to hosts and services outside of Zero Day, Inc. with the exception of known security vulnerabilities. This allows anyone connected to the Zero Day Network to utilize all services on the Internet with the exception of known vulnerabilities.

Plan of Action & Milestones (POA&M) - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Risk Assessment - the identification of hazards that could negatively impact an organization's ability to conduct business.

Risk Assessment Report - The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk.

Risk Management Framework (RMF) - a template and guideline used to identify, eliminate and minimize risks.

Wi-Fi - A term for certain types of wireless local area networks (WLAN) that use specifications in the 802.11 family.

Wireless - A term used to describe telecommunications in which electromagnetic waves, rather than some form of wire, carry the signal over all or part of the communication path.

Wireless Access Point (AP) - A device that allows wireless devices to connect to a wired network using Wi-Fi or related standards.

TCP and UDP Small Services – (Also known as small servers) Services which runs on the router itself for some useful diagnostics

Echo (TCP) - Echoes back whatever you type through the **telnet x.x.x.x echo** command.

Chargen (TCP) - Generates a stream of ASCII data.

Discard (TCP) - Throws away whatever you type.

Daytime (TCP) - Returns system date and time, if it is correct. It is correct if you run Network Time Protocol (NTP), or have set the date and time manually from the exec level.

Echo (UDP) - Echoes the payload of the datagram you send.

Discard (UDP) - Silently pitches the datagram you send.

Chargen (UDP) - Pitches the datagram you send, and responds with a 72-character string of ASCII characters terminated with a CR+LF.

8.0 REFERENCE DOCUMENTS

Kuhn, D. Richard, et al. *Security Considerations for Voice Over IP Systems*. NIST, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-58.pdf.

"50 Free Cyber Security Policy Templates To Secure Your Network." *PurpleSec*, 17 May 2021, https://purplesec.us/resources/cyber-security-policy-templates/.

2510+ Business Templates. https://www.template.net/business/. Accessed 19 Feb. 2022.

Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual. Version 2.2, National Industrial Security Program Authorization Office, https://www.dcsa.mil/Portals/91/Documents/CTP/tools/DCSA_Assessment_and_%20Authorization_Process_Manual_Version_2.1.pdf.

Department of Defense, et al. *Security and Privacy Controlsfor Information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Grassi , Paul A., et al. *Digital Identity Guidelines Authentication and Lifecycle Management*. https://pages.nist.gov/800-63-3/sp800-63b.html. Accessed 19 Feb. 2022.

"Issue Specific Security Policy." *Studylib.Net*, https://studylib.net/doc/8599543/issue-specific-security-policy. Accessed 19 Feb. 2022.

Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments*. Rev. 1, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Sample Internet Usage Policy. https://www.gfi.com/pages/sample-internet-usage-policy. Accessed 19 Feb. 2022.

Scarfone , Karen, and Paul Hoffman . *Guidelines on Firewalls and Firewall Policy*. Rev. 1, National Institute of Standards and Technology (NIST) - U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf.

Souppaya , Murugiah, and Karen Scarfone. *Guidelines for Securing Wireless Local Area Networks (WLANs)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf.

Swanson , Marianne, et al. *Guide for Developing Security Plans for Federal Information Systems*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf.

8.1 POLICY CONTACTS

Michele Reynolds - MCREYNOLDS@MYMAIL.TSTC.EDU

Christian Bertinot - csbertinot@mymail.tstc.edu

Darleen Espinales - despinales@mymail.tstc.edu

Anthony Goulet - apgoulet@mymail.tstc.edu

Juan Cruz - jcruz16823@mymail.tstc.edu

Nathan Vazquez - nevazquez98859@mymail.tstc.edu