Decorative sidebar

**N**etwork **S**ecurity **P**olicies **M**anual

**Zero Day Inc-Media Company**

ITNW 2350 Enterprise Network-capstone project

Team members

Regan stubbs

faustino Gonzales

Timothy Zellers

Jake Calvert

James Baker

| **Table of Contents** | | Page |
| --- | --- | --- |
| 1.0 | Purpose | 1 |
| 2.0 | Responsible Organization | 1 |
| 3.0 | General Description | 2 |
| 4.0 | Policies | 2 |
| 4.1 | Guest Policy | 2 |
| 4.2 | Authentication: Password Policy | 3 |
| 4.3 | Network Security Policy: Firewall, Router Switch Client, Server, Wireless | 4 |
| 4.4 | Remote Access: Encryption, VPN, RDP | 5 |

**1.0 PURPOSE**

The purpose of this document is to provide an overview of the security requirements of the system and describe the controls in place or planned, for meeting those requirements. This document also delineates responsibilities and expected behavior of all individuals who access the system.

**2.0 RESPONSIBLE ORGANIZATION**

The GIYMP Team is the organization currently under contractual agreement with Zero Day, Inc.   The Gyimp Team is tasked with the responsibility of implementing, updating, and enforcing all approved company policies.

**Gyimp organization contacts:**

Regan Stubbs Cyber Security Anylist 456-987-8910 rsstubbs@gyimp.com

Faustino Gonzales Coding/ Programming 456-987-3210 [fgonzales@gyimp.com](mailto:fgonzales@gyimp.com)

Jake Calvert Coding/ Pentester 456-987-9632 [jcalvert@gyimp.com](mailto:jcalvert@gyimp.com)

Timothy Zellers Pentester 456-987- 6598 tzellers@gyimp.com

James Baker Cyber Security Anylist 456-987-3687 jbaker@gyimp.com

The organization responsible for enforcing policies is the Zero Day INC. Technology (IT) Department. The individual who has been assigned responsibility for the security of the network system is John Doe, Chief Information Security Officer (CISO). He can be reached at 555-555-5555 or [john.doe@company.com](mailto:john.doe@company.com).Information System Owner: Information System Owner: Jane Smith, Director of IT Operations, 123 Main Street, [janesmith@company.com](mailto:janesmith@company.com), 555-123-4567. Authorizing Official:Authorizing Official: William Johnson, Vice President of Operations, 456 Oak Avenue, [williamjohnson@company.com](mailto:williamjohnson@company.com), 555-987-6543.

**3.0 GENERAL DESCRIPTION**

Zero Day Inc. is a media-based company specializing in marketing, web hosting and development, publishing, and broadcast services for local and national customers. The company is committed to protecting the company from illegal or gaming actions by individuals, either knowingly or unknowingly. Zero Day Inc. experienced rapid growth which resulted in the acquisition of a new location to meet the high demands of media services.

**4.0 POLICIES**Zero Day Inc. systems are to be used for business purposes in serving the interests of the company, employees, and customers in the support of normal business operations. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. The company network requires high-level security for the company network, employees, and customers.

Policies in 4.x policies define how employees, subcontractors and visitors will conduct their activities; these policies are broken down into four electronic information security goals:

1. Protect the internal network by establishing employee policies and guidelines
2. Enable safe access to the internet from Guest connections in the Guest Wi-Fi network
3. Establish password and authentication policies

Define wireless access policy for employees and guests

**4.1 Guest Policy**

Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the major application or general support system.

OVERVIEW This policy outlines the rules and guidelines for guests accessing the Company Network System. A guest is defined as any individual who is not an employee or a contractor of the company.

Purpose/Objective The purpose of this policy is to ensure that guests accessing the Company Network System do not pose a security risk to the organization. This policy aims to protect the confidentiality, integrity, and availability of the network and its resources.

Applicability This policy applies to all guests accessing the Company Network System.

POLICY

1. Guests must be authorized by an employee of the company before accessing the network.
2. Guests must agree to comply with all company policies and procedures related to network security.
3. Guests must use a temporary account created by the IT Department to access the network.
4. Guests must be supervised by an employee of the company while accessing the network.
5. Guests must only access network resources that are necessary to complete their work.

RELATED DOCUMENTS

1. Acceptable Use Policy
2. Information Security Policy

**4.2 Authentication Policy / Password Policy**

Authentication Policy - Zero Day Inc.

1. Purpose The purpose of this Authentication Policy is to establish guidelines and procedures for ensuring the secure authentication of users accessing Zero Day Inc.'s systems, applications, and data. This policy aims to protect the confidentiality, integrity, and availability of company resources.
2. Scope This policy applies to all employees, contractors, and third-party users who access Zero Day Inc.'s systems, applications, and data. It covers all devices, including but not limited to computers, laptops, mobile devices, and any other equipment used for accessing company resources.
3. Authentication Methods Zero Day Inc. supports the following authentication methods: a. Password-based authentication: Users are required to enter a unique password to authenticate themselves. b. Multi-factor authentication (MFA): In addition to passwords, MFA is strongly encouraged and may be mandatory for certain systems or applications. MFA methods may include the use of tokens, biometrics, or other secure means of authentication.
4. Password Security and Complexity a. Password Complexity:
   * Passwords must be at least 8 characters long.
   * Passwords must include a combination of uppercase and lowercase letters, numbers, and special characters.
   * Passwords must not contain common words, personal information, or easily guessable sequences.

b. Password Protection:

* Users must not share their passwords with anyone, including colleagues or supervisors.
* Passwords should not be written down or stored in an easily accessible manner.
* Users must change their passwords every 90 days or as per the system/application requirements.
* Reusing passwords from other systems or applications is strictly prohibited.

c. Account Lockouts:

* After six consecutive failed login attempts, the user's account will be temporarily locked.
* The account can be unlocked by contacting the IT support team or by using the self-service account recovery process.

1. Account Management a. User Provisioning:
   * User accounts must be provisioned based on the principle of least privilege.
   * User access rights should be reviewed and updated regularly to ensure appropriate access levels.

b. Account Termination:

* User accounts must be promptly disabled or removed upon termination of employment or contract.
* Termination procedures must ensure the removal of all access privileges.

1. Monitoring and Compliance Zero Day Inc. will periodically review and audit authentication practices to ensure compliance with this policy. Violations of this policy may result in disciplinary action, including but not limited to suspension, termination, or legal consequences.
2. Policy Review This policy will be reviewed annually or as necessary to align with evolving security requirements, industry best practices, and regulatory compliance.

Password Policy - Zero Day Inc.

1. Purpose The purpose of this Password Policy is to establish guidelines for the creation, protection, and management of strong and secure passwords used within Zero Day Inc.'s systems, applications, and networks.
2. Password Creation a. Password Length: Passwords must be at least 12 characters long. b. Complexity: Passwords must include a combination of uppercase and lowercase letters, numbers, and special characters. c. Avoid Common Passwords: Passwords must not contain common words, personal information, or easily guessable sequences. d. Password Managers: The use of password managers is strongly encouraged to generate, store, and manage complex passwords securely.
3. Password Protection and Usage a. Password Sharing: Users must not share their passwords with anyone, including colleagues or supervisors. b. Password Storage: Passwords should not be written down or stored in an easily accessible manner. c. Periodic Change: Users must change their passwords every 90 days or as per system/application requirements. d. Password Reuse: Reusing passwords from other systems or applications is strictly prohibited.

**4.3 Network Security Policy  
Devices: firewall, router, switch, client, server, wireless**

1. Firewalls:
   * Implement and maintain robust firewall configurations to control inbound and outbound network traffic.
   * Regularly update firewall firmware and security patches to address potential vulnerabilities.
   * Configure firewall rules to restrict unauthorized access and allow only necessary services.
   * Perform periodic security audits and log monitoring to identify and respond to potential security incidents.
2. Router:
   * Enable strong password protection for router administration interfaces.
   * Implement access control lists (ACLs) to restrict unauthorized access to the router.
   * Regularly update router firmware to patch security vulnerabilities.
   * Disable unnecessary services and ports on the router.
   * Monitor router logs for any suspicious activity or unauthorized access attempts.
3. Switches:
   * Change default passwords and implement strong authentication mechanisms for switch management.
   * Enable port security to prevent unauthorized devices from connecting to the network.
   * Disable unused switch ports to minimize attack surface.
   * Regularly update switch firmware to address security vulnerabilities.
   * Implement VLANs to segregate network traffic and enhance security.
4. Clients:
   * Implement strong password policies for user accounts on client devices.
   * Regularly update operating systems and applications with the latest security patches.
   * Deploy and maintain antivirus and anti-malware software on client devices.
   * Enable personal firewalls on client devices to protect against unauthorized access.
   * Educate users about safe browsing habits and the risks of opening suspicious email attachments or visiting malicious websites.
5. Servers:
   * Implement strong password policies for server accounts and regularly change passwords.
   * Regularly update server operating systems and applications with the latest security patches.
   * Employ intrusion detection and prevention systems to monitor and protect server environments.
   * Enable logging and monitoring of server activities to detect and respond to security incidents.
   * Implement access controls and user permissions to restrict unauthorized access to server resources.
6. Wireless:
   * Secure wireless networks with strong encryption protocols (e.g., WPA2 or WPA3).
   * Change default wireless network names (SSIDs) and enable network hiding (if applicable).
   * Implement strong, unique passwords for wireless network access.
   * Regularly update wireless access point firmware to address security vulnerabilities.
   * Enable MAC address filtering to allow only authorized devices to connect to the wireless network.

**4.4 Remote Policy  
Encryption, VPN, RDP**

1. Encryption 1.1. All remote communication and data transmission must be encrypted using strong encryption algorithms such as AES (Advanced Encryption Standard) with a minimum key length of 128 bits. 1.2. The use of encryption must be mandatory for all remote connections, including but not limited to virtual private networks (VPNs) and remote desktop protocol (RDP) sessions.
2. Virtual Private Network (VPN) 2.1. All remote access to the organization's internal network must be established through an approved VPN solution. 2.2. Only authorized personnel with a legitimate business need should be granted VPN access. 2.3. VPN connections must utilize secure protocols such as IPSec or SSL/TLS. 2.4. Multi-factor authentication (MFA) should be implemented for VPN connections to enhance security. 2.5. VPN client software and configurations should be kept up to date with the latest security patches and updates. 2.6. Remote users must disconnect from the VPN when their work is completed or when leaving their remote workstations unattended for an extended period.
3. Remote Desktop Protocol (RDP) 3.1. RDP access to internal resources should be limited to authorized personnel only. 3.2. RDP access should be granted based on the principle of least privilege, ensuring that users have access only to the resources necessary to perform their job duties. 3.3. Strong and complex passwords must be used for RDP accounts, and password sharing is strictly prohibited. 3.4. Two-factor authentication (2FA) should be implemented for RDP connections wherever possible. 3.5. Remote desktop services must be configured to enforce account lockout policies after a certain number of failed login attempts. 3.6. Regular audits and monitoring should be performed to identify and address any unauthorized RDP connections or suspicious activities.
4. General Security Guidelines 4.1. Remote devices used for accessing the organization's network must be protected with up-to-date anti-virus and anti-malware software. 4.2. Remote users should follow best practices for securing their home network, such as using strong Wi-Fi passwords and keeping network equipment firmware updated. 4.3. Remote workers must report any security incidents or potential vulnerabilities promptly to the appropriate IT personnel. 4.4. Employees must comply with all other relevant security policies and guidelines outlined by the organization.

**5.0 Failure to Comply**

Violations in any company policy:

* Guests may lose privileges on the company’s guest Wi-Fi, may be asked to leave the premises, and could face legal consequences.
* An employee found in violation of any company policy may be subject to disciplinary action, up to and including termination, illegal activity will reported to the appropriate authorities.

**This policy was created for Zero Day Media Inc- Company to get in compliance with NIST 800-18, NIST 800-30, NIST SP 800-53.**

**POLICY 516-2023**. Version: **N**etwork **S**ecurity **P**olicies **M**anual

**Effective: *5/16/******2023******Last Updated: 5/16/2023***