Village of Pleasantville Cybersecurity Policy

Adopted October 13, 2020 BOT Res 2020-209

Definition

The use of the term "Village" is in referenced to the Village of Pleasantville.

Introduction

This Cyber Security Policy is a formal set of rules by which those people who are given access to Village technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform Village users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the Village. The Cyber Security Policy describes the technology and information assets that must be protected and identifies many of the threats to those assets.

The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the Village computer systems and network.

Cybersecurity Policy Coordinators

Eric Morrissey, Village Administrator, Village of Pleasantville
P: 914-769-1940
E: administrator@pleasantville-ny.gov

Noreen Regan, Administrative Aide, Village of Pleasantville
P: 914-769-1975
E: nregan@pleasantville-ny.gov

Wayne Frick, Partner, A1 Computer Services
P: 914-495-3473
E: wfrick@a1cs.com

What We Are Protecting

It is the obligation of all users of the Village systems to protect the technology and information assets of the Village. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the Village are made up of the following components:

- Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.

- Application Software: used by the various departments within the Village. This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

Threats to Security

Employees

Employees are the biggest threat to the Village's IT network. They may do damage to systems either through incompetence or on purpose, and as such, cyber security must be layered. Mitigation efforts include the following:

- ✓ Only give out appropriate rights to systems. Limit access to only business hours.
- ✓ Don't share accounts to access systems. Never share login information with co-workers.
- ✓ When employees are separated or disciplined, remove or limit access to systems.
- ✓ Advanced – Keep detailed system logs on all computer activity.
- ✓ Physically secure computer assets, so that only staff with appropriate need can access.
- ✓ Provide notification on emails that identify when messages are received from external sources.
- ✓ Conduct training/awareness activities, such as test phishing emails and educational videos.

Amateur Hackers and Vandals.

These are the most common type of attackers on the Internet. The probability of attack is extremely high and typically crimes of opportunity. These amateur hackers are scanning the Internet and looking for security holes that have not been plugged. Web servers and electronic mail are preferred targets. Once they find a weakness they will exploit to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

Criminal Hackers and Saboteurs.

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

User Responsibilities

This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the Village.

Acceptable Use

User accounts on Village computer systems are to be used only for business of the Village and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the Village computing system and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore they are prohibited

from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the Village.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Village systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the Village IT designee. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in the Village computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

Use of the Internet

Policies governing the use of the internet can be found on pages 400-11 through 400-13 of the Village's Employee Handbook. In general, the Village will provide Internet access to employees and contractors who are connected to the internal network ***and*** who have a business need for this access.

The Internet is a business tool for the Village. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain.

Monitoring Use of Computer Systems

The Village has the right and capability to monitor electronic information created and/or communicated by persons using Village computer systems and networks, including e-mail messages and usage of the Internet. Users of the systems should be aware that the Village may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with Village policy.

Access Control

A fundamental component of the Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management &

supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed every (90 days).
- User accounts will be frozen after (5) failed logon attempts.
- Logon IDs and passwords will be suspended after (30) days without use.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the Village.

Supervisors / Managers shall immediately and directly contact the Village's IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must contact the Village's IT consultant, A1CS at support@a1cs.com to get a new password assigned to their account.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between the Village and all third-part companies and other entities required to electronically exchange information with Village.

"Third-party" refers to vendors, consultants and business partners doing business with the Village, and other partners that have a need to exchange information with the Village. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the Village. Third-party vendors will ensure that only authorized users will be allowed to access information on the Village network. The third-party will not allow Internet traffic or other private network traffic to flow into the network.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved by the Village.

Connecting Devices to the Network

Only authorized devices may be connected to the Village's network(s). Authorized devices include PCs and workstations owned by the Village that comply with the configuration guidelines of the Village. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-Village computers that are not authorized, owned and/or controlled by Village.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's.

Remote Access

Only authorized persons may remotely access the Village network. Remote access is provided to those that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to Village network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

Unauthorized Remote Access

The remote access to a Village computer or workstation that is connected to the Village LAN is not allowed without the written permission of the Village. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

Penalty for Security Violation

Upon violation of this policy, an employee of Village may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules, policies and collective bargaining agreements.

In a case where the accused person is not an employee of Village the matter shall be submitted to the Cyber Security Policy Administrators. The Village may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

Security Incident Handling Procedures

This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the Village network. Some examples of security incidents are:

- Illegal access of a Village computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a Village computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a Village web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of the Village network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or have otherwise been improperly accessed or used, should report the situation to the Cybersecurity Policy Coordinators immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security

incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

Information and Data Management

The Following relates to the handling of personal information. Personal information will be defined as any information accessed, collected, or used by the Village that identifies an individual, or can reasonably be used to identify an individual, whether directly or indirectly. Examples of Personal Information include: name, mailing address, telephone or fax number, e-mail address, employee identification number.

Information and Data Collection

The Village shall only collect information in a manner and scope that is consistent with applicable Village policy, including any privacy policy.

Information and Data Use

The Village shall only use information in a manner and scope that is consistent with applicable Village policy, including any privacy policy.

Information and Data Retention

The Village shall limit the retention of Village Information in accordance with applicable Village records and information management policies and procedures and any applicable Legal Hold Notice (any notice issued by or at the direction of Legal advising Village to retain and preserve particular categories of records indefinitely until Legal advises that retention is no longer required).

Information and Data Access

The Village shall limit access to Village Information and Village Information Systems to those Village employees, contractors, and other third parties who require such access to perform their job duties or contractual obligations or engagement terms, as applicable.

Information and Data Storage

The Village shall take reasonable steps to ensure that Village Information under its control is stored in a manner that protects the security and confidentiality of such Information, based on the sensitivity of the Village Information and in accordance with this Policy, and the applicable procedures, standards and guidelines.

Information and Data Disposal

When Village Information in paper, electronic or other form is no longer required to be retained (including Village Information stored on devices and media that are no longer to be retained), the Village Information must be properly disposed of in a manner that protects the security and confidentiality of such Village Information, based on the sensitivity of the Village Information and in accordance with this Security Policy, and the applicable procedures, standards and guidelines.

Paper records containing Confidential Information must be disposed of by shredding. Electronic media (e.g., CDs and DVDs, and hard disks, including hard disks on computers, printers and copiers) containing Confidential Information must be disposed of by shredding or degaussing the media as appropriate.

Protection Standards for Sensitive Personal Information

The Village may collect certain sensitive personal information, including Social Security numbers, in the course of our business. We protect the confidentiality of the sensitive information we collect by maintaining what we believe to be reasonable physical, electronic and procedural safeguards to protect their confidentiality.

For the purposes of this policy, sensitive personal information can be defined as follows:

> Personal Information that requires an extra level of protection and a higher duty of care based on applicable law. Examples of Sensitive Personal Information could include: credit card or bank account number, Government identification numbers, including Social Security numbers, Social Insurance numbers, passport numbers, and driver's license numbers, information on medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

The Village will enforce the following safeguards:
Personal Sensitive information must:

- Be restricted to individuals that have a defined business need.
- Be encrypted at rest and in transit.
- Never be stored on any portable media.
- Be securely disposed of if stored on paper.
- Never be left visible and unattended either on screen or in paper form.

In furtherance of this policy, the following actions are prohibited:

- accessing sensitive personal information by any person who does not have a legitimate business purpose for doing so;
- any intentional communication of a sensitive personal information to the general public and any other unauthorized disclosure to any person;
- printing an individual's sensitive personal information on an access card or tag that is necessary to access facilities, services, benefits or products;
- requiring an individual to transmit his or her sensitive personal information over the internet, unless the connection is secure or the sensitive personal information is encrypted;
- requiring a sensitive personal information or a derivative thereof to be used as an access code for authorization purposes, such as access to a website; and
- the mailing of materials displaying an individual's sensitive personal information, unless mandated by Federal or State law.