Village of Dansville
Electronic Devices & Information Technology Security Policy

1. PURPOSE.

The purpose of this policy is to define appropriate user behavior, describe the tools and guidelines needed to protect data and information systems, and to provide measures to be used in the event of system breaches and policy violations.

2. SCOPE.

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Village business or interact with internal networks and business systems, whether owned or leased by the Village, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers of the Village of Dansville are responsible for exercising good judgment regarding appropriate use of information, electronic devices and network resources in accordance with Village of Dansville policies and standards, and local laws and regulations.

This information security (infosec) policy is intended not to impose restrictions that are contrary to the Village of Dansville's established culture of openness, trust and integrity. Infosec is committed to protecting Village of Dansville employees, partners and the municipality from illegal or damaging actions by individuals, either knowingly or unknowingly.

Web-based systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and Internet browsing are the property of the Village of Dansville. These systems are to be used for business purposes in serving the interests of the Village, its partners and customers, and its citizens in the course of normal operations.

Effective security is a team effort involving the participation and support of every Village of Dansville employee and associate who deals with information and/or information systems. It is the responsibility of every computer user to know the guidelines, rules and regulations, and to conduct their activities accordingly.

The Village of Dansville reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3. DEFINITIONS.

BLOGGING – To maintain or add new entries to a blog, a website containing a writer's or group of writers' own experiences, observations, opinions, etc., and often having images and links to other websites.

ENCRYPTION OR ENCRYPTED DATA – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

HACKER – A person who uses computers to gain unauthorized access to data.

HONEYPOT – A honeypot is a computer system that is set up to act as a decoy to lure cyber-attackers, and to detect, deflect or study attempts to gain unauthorized access to information systems.

HONEYNET – A network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.

INFORMATION RESOURCE – The data and information assets of an organization, department or unit.

MALWARE – Software that is intended to damage or disable computers and computer systems.

PEER TO PEER FILE SHARING (P2P) – P2P file sharing allows users to access media files such as books, music, movies, and games using a P2P software program that searches for other connected computers on a P2P network to locate the desired content. The nodes (peers) of such networks are end-user computers and distribution servers (not required).

PERSONALLY IDENTIFIABLE INFORMATION – Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered.

PHISHING – The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

PLAIN TEXT – Unencrypted data.

PROTECTED DATA – See PII and PHI.

PROTECTED HEALTH INFORMATION (PHI) – Under US law any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" and can be linked to a specific individual.

SAFEGUARDS – Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

SENSITIVE DATA – Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI.

SOCIAL NETWORKING SERVICES – Online platforms that are used by people to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections.

SPAM – Unsolicited or undesired electronic messages.

SPYWARE – Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

TROJAN HORSE – Any malicious computer program that is used to hack into a computer by misleading users of its true intent.

WORM – A standalone malware computer program that replicates itself in order to spread to other computers on a network. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

4. ACCEPTABLE USE.

A. Purpose.

The purpose of acceptable use rules is to outline the appropriate use of Village of Dansville computer and related equipment and software. These rules are in place to protect the employee and Village. Inappropriate use exposes the Village to risks including virus, malware, spyware, and Trojan horse attacks that compromise network systems and services, and subject the Village to lawsuits.

B. Rules.

(1) General Use and Ownership

(a) Any Village of Dansville confidential information sensitive data stored on electronic and computing devices, whether owned or leased by the Village, the employee or a third party, remains the responsibility of the Village. Users must ensure, through legal or technical means, that the information is protected.

(b) Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Village of Dansville confidential information/sensitive data.

(c) Users may access, use or share Village of Dansville confidential information/sensitive data only to the extent it is authorized and necessary to fulfill their assigned job duties.

(d) Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Web-based systems. In the absence of such policies, employees should consult their department head.

(e) For security and network maintenance purposes, authorized individuals within or under contract with the Village of Dansville may monitor equipment, systems and network traffic at any time.

(2) Security and Confidential Information/Sensitive Data

(a) All mobile and computing devices that connect to the internal network must comply with minimum access guidelines.

(b) System-level and user-level passwords must comply with the password rules. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

(c) All computing devices must be secured with a password-protected screensaver with an automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.

(d) Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

(3) Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is an employee of the Village of Dansville authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Village-owned resources. The activities are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

(a) System and Network Activities

i. Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Village of Dansville.

ii. Unauthorized copying of copyrighted material, including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Village or the end user does not have an active license.

iii. Accessing data, a server or an account for any purpose other than conducting Village of Dansville business, even if the person has authorized access.

iv. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws.

v. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

vi. Revealing your account password to others or allowing use of your account by others unless authorized by your supervisor for a particular purpose, after which the password will be changed.

vii. Using a Village of Dansville computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

viii. Making fraudulent offers of products, items or services originating from any Village of Dansville account.

ix. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.

x. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

xi. Circumventing user authentication or security of any host, network or account.

xx. Interfering with or denying service to any user other than the employee's host.

xxi. Using any program/script/command, or sending messages of any kind with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet.

xxii. Providing information about, or lists of, Village of Dansville employees to parties outside the Village.

(b) Email and Communication Activities

i. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

ii. Any form of harassment via email, telephone or paging, whether through language, frequency or size of messages.

iii. Unauthorized use, or forging, of email header information.

iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

vi. Use of unsolicited email originating from within the Village of Dansville network or other Internet service providers on behalf of, or to advertise, any service hosted by the Village or connected to the Village's network.

c. Blogging and Social Network Services

i. Blogging and the use of social media are, in general, prohibited while on the job unless required by one's duties.

ii. Blogging by employees, whether using the Village of Dansville's property and systems or personal computer systems is subject to the terms and restrictions set forth in this policy.

iii. The Village's confidential information/sensitive data guidelines also apply to blogging. As such, employees are prohibited from revealing any Village confidential information, or any other material covered by the confidential information policy, when engaged in blogging.

iv. When authorized to blog or use social network services, an employee must ensure that he or she is not doing so in any manner that may harm or tarnish the image, reputation and/or goodwill of the Village of Dansville and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

v. Employees also may not attribute personal statements, opinions or beliefs to the Village when engaged in blogging or using social media when not working. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Village of Dansville. Employees assume any and all risk associated with blogging or use of social media.

5. INTERNET USAGE.

A. Internet Services.

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

(1) Email – Send/receive email messages to/from the Internet (with or without document attachments.

(2) Navigation – World Wide Web (WWW) services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser too. Full access to the Internet.

(3) File Transfer Protocol (FTP) – Send data/files and receive in-bound data/files as necessary for business purposes.

B. Allowed Usage.

(1) Communication between employees and non-employees for business purposes.

(2) IT technical support downloading software upgrades and patches.

(3) Review of possible vendor/government websites for product information.

(4) Reference regulatory or technical information.

(5) Research

C. Creating Websites and Facebook Pages.

Establishing websites or Facebook pages other than the official Village sites/page, must be officially approved by the Village of Dansville Board of Trustees.

All sites/pages representing the Village or departments thereof are owned by the Village. Direct responsibility for the content and the representation of the Village belongs to the department head.

All Village websites and Facebook pages must be protected from unwanted intrusion through formal security measures.

All Village websites and Facebook pages must be maintained for accuracy, appropriateness and effectiveness. The village clerk will periodically review sites/pages to ensure this and make certain they are current.

The Village's IT consultant and maintenance vendors will periodically review sites/pages for usage compliance and policy maintenance.

6. EMAIL USAGE.

A. Purpose.

The purpose of this section is to cover rules for the appropriate use of any email sent from a Village of Dansville email address. They apply to all employees, officials and agents operating on behalf of the Village.

B. Rules.

(1) All use of email must be consistent with Village of Dansville policies and procedures of ethical conduct, safety, compliance with applicable laws and governmental professional standards.

(2) All Village of Dansville email accounts should be used primarily for Village business-related purposes; personal communication is permitted on a limited basis, but non-Village related commercial uses are prohibited.

(3) All Village of Dansville data contained within an email message or an attachment must be secured according to data protection standards.

(4) Email should be retained only if it qualifies as a Village of Dansville business record. Email is a Village business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

(5) Email that is identified as a Village of Dansville business record shall be retained according to the Records Retention and Disposition Schedule MV-1.

(6) The Village of Dansville email system shall not be used for the creation or distribution of any disruptive or offensive messages, including comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Village employee should report the matter to their supervisor immediately.

(7) The Village of Dansville email system shall not be used for hacking, phishing, or any other such improper/illegal purposes.

(8) Emails which are forwarded by the user must not contain Village of Dansville confidential material/sensitive data unless the recipient is authorized to view it and has the appropriate security.

(9) Users are prohibited from using third-party email systems and storage servers, such as Google, Yahoo and MSN Hotmail, etc., to create any binding transactions, or to store or retain email on behalf of the Village. Such communications and transactions should be conducted through proper channels using Village-approved documentation.

(10) Using a reasonable amount of Village of Dansville resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work-related email. Sending chain letters or joke emails from a Village email account is prohibited.

(11) Village of Dansville employees shall not have an expectation of privacy in anything they store, send or receive on the Village's email system.

(12) The Village of Dansville may monitor emails without prior notice.

7. EMAIL RETENTION.

A. Purpose.

The email retention rules are intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered includes, but is not limited to, information that is either stored or shared via electronic mail, instant messaging, texting, tweets, or similar technologies.

All employees should familiarize themselves with the email retention topic areas.

Questions about the proper classification of a specific piece of information should be addressed to the respective department head or village clerk.

B. Scope.

All Village of Dansville email information will be categorized according to the designated Records Retention and Disposition Schedule MV-1.

8. PASSWORDS.

A. Password Construction Guidelines.

(1) Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data or the network.

(2) Guidelines

All passwords should meet or exceed the following guidelines:

Strong passwords have the following characteristics:

(a) Contain at least 12 alphanumeric characters.

(b) Contain both upper and lower case letters.

(c) Contain at least one number (for example, 0-9).

(d) Contain at least one special character (for example, !$%^&*()_+)

Poor, or weak, passwords have the following characteristics:

(a) Contain less than eight characters.

(b) Can be found in a dictionary, including foreign language, or exist in a language slang, dialect or jargon.

(c) Contain personal information such as birthdates, addresses, phone numbers or names of family members, pets, friends and fantasy characters.

(d) Contain work-related information such as building names, system commands, sites, companies, hardware or software.

(e) Contain number patterns such as aaabbb, qwerty, zyxwvuts or 123321.

(f) Contain common words spelled backward or preceded or followed by a number (for example, terces, secret 1 or 1 secret).

(g) Are some version of "Welcome123", Password123", "Changeme123".

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation or other phrase. For example, the phrase, "This May Be One Way to Remember" could become the password TmB1w2R! or another variation. (NOTE: Do not use the example as a password!)

A passphrase is similar to a password; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lower case letters, numbers and special characters.

C. Password Change.

(1) All system-level passwords must be changed on at least a quarterly basis.

(2) All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

(3) Password cracking or guessing may be performed on a periodic or random basis by the Village's IT consultant. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the password construction guidelines.

D. Password Protection.

(1) Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Village of Dansville information.

(2) Passwords must not be inserted into email messages or other forms of electronic communication.

(3) Passwords must not be revealed over the phone to anyone.

(4) Do not reveal a password on questionnaires or security forms.

(5) Do not hint at the format of the password (i.e., "my family name).

(6) Do not share Village of Dansville passwords with anyone, including family members.

(7) Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile device without encryption.

(8) Do not use the "Remember Password" feature of applications.

(9) Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

9. CLEAN DESK PROCEDURES.

A. Purpose.

The purpose of this section is to present clean desk procedures that can be an important tool to ensuring that all sensitive/confidential materials are removed from an end user workplace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to be utilized when trying to reduce the risk of security breaches in the workplace. Such procedures can also increase employees' awareness about protecting sensitive information.

B. Procedures.

(1) Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

(2) Computer workstations must be locked when the workspace is unoccupied.

(3) Computer workstations must be shut completely down at the end of the work day.

(4) Any restricted, confidential or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

(5) File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.

(6) Keys used for access to restricted, confidential or sensitive information must not be left at an unattended desk.

(7) Laptops/tablets must be either locked with a locking cable or locked away in a drawer.

(8) Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

(9) Printouts containing restricted, confidential or sensitive information should be immediately removed from the printer.

(10) Upon disposal, restricted, confidential or sensitive documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.

(11) Whiteboards containing restricted, confidential or sensitive information should be erased.

(12) Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

(13) All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

10. SOFTWARE INSTALLATION.

A. Overview.

Allowing employees to install software on Village computing devices opens the municipality up to unnecessary exposure. Unauthorized installation can result in conflicting file versions and questionable software that can prevent programs from running, introduce malware and other troubling issues (worms, spyware, phishing, etc.), cause copyright issues, and result in hacking of the Village's network.

B. Rules and Procedures.

(1) Employees, except those authorized by the mayor, may not install software or apps on Village of Dansville computing devices operating within the Village of Dansville network.

(2) Software and apps requests must first be approved by the department head and then by the Board of Trustees.

(3) The village clerk will obtain and track all software licenses for conflict and compatibility.

11. TECHNOLOGY EQUIPMENT DISPOSAL.

A. Scope.

The guidelines contained in this section apply to any computer/technology equipment or peripheral devices that are no longer needed within the Village of Dansville including, but not limited to, the following: personal computers, servers, hard drives, laptops, mainframes, smart phones or handheld computers, peripherals, printers, scanners, typewriters, compact and floppy discs, portable storage devices, backup tapes, printed materials, recording devices.

B. Technology Equipment Disposal.

(1) When technology assets have reached the end of their useful life, they must be sent to the Village Clerk for proper disposal.

(2) The Village Clerk will securely erase or have erased or shredded all storage mediums in accordance with current industry best practices.

(3) All data, including all files and licensed software, shall be removed from equipment using disk sanitizing software that cleans the media.

(4) No computer or technology equipment may be sold to any individual.

(5) No computer equipment should be disposed of via skips, dumps, landfill, etc.

(6) All electronic drives must be "cleaned". Hard drives may also be removed and rendered unreadable (drilling, crushing or shredded).

(7) Computer equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives, or any storage device, network switches, routers, wireless access points, batteries, backup tapes, recorders, etc.

(8) The village clerk may contract with a certified company for the removal and destruction of data or storage devices. The company shall provide the Village with certification that the data has been removal and/or the storage device destroyed.

(9) Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and physically destroyed.

(10) Records of the removal and/or destruction of storage devices shall be maintained by the village clerk.

12. NOTIFICATION OF BREACH.

A. Authority and Purpose.

This section of the policy is consistent with the New York State Technology Law ' 208 as added by Chapters 442 and 491 of the Laws of 2005. This policy requires notification to affected New York residents and non-residents. The Village of Dansville is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's

private information in compliance with the Information Security Breach and Notification Act and this policy.

B. Notification of Unauthorized Disclosure Required.

The Village of Dansville, after consulting with the State's Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures of its compromised data, must notify an individual when it has been determined that there has been, or is reasonably believed to have been, a compromise of the individuals private information through unauthorized disclosure.

A compromise of private information means the unauthorized acquisition of unencrypted computerized data with private information.

If encrypted data is compromised along with the corresponding key, the data is considered unencrypted and thus falls under the notification requirements.

Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

C. Methods of Notification.

The Village of Dansville will notify the affected individual directly by one of the following methods:

(1) Written notice;

(2) Electronic notice, provided that the person to whom the notice is required has expressly consented to receiving notice in electronic form and a log of each notification is kept by the municipality that notifies affected persons in such form;

(3) Telephone notification, provided that a log of each notification is kept by the municipality that notifies affected persons; or

(4) Substitute notice, if the municipality demonstrates to the state Attorney General that the cost of providing notice would exceed $250,000, that the affected class of persons to be notified exceeds500,000, or that the municipality does not have sufficient contact information. The following constitute sufficient substitute notice:

(a) Email notice when the municipality has an email address for the subject persons;

(b) Conspicuous posting of the notice on the municipality's website page, if the municipality maintains one; and

(c) Notification to major statewide media.

D. Notice to State Agencies.

(1) The Village of Dansville must notify the CSCIC as to the timing, content and distribution of the notices and the approximate number of affected persons.

(2) The Village must notify the Attorney General and the Consumer Protection Board, whenever notification to a New York resident is necessary, as to the timing, content and distribution of the notices and approximate number of affected persons.

E. Contents of Notice.

Regardless of the method by which the notice is provided, the notice must include contact information for the municipality making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

F. Notice to Consumer Reporting Agencies.

When more than 5,000 New York residents must be notified at one time, then the municipality must notify the consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.

13. APPLICABILITY.

This policy applies to all employees, contractors, consultants, temporaries, and other workers for the Village of Dansville, including all personnel affiliated with third parties. This policy applies to all equipment and software that is owned or leased by the Village of Dansville.