Information Technology Security Policy
Nashville Police Department
Version 1.0

Table of Contents

1. Introduction

1.1 Aim of the policy

This document states the Information Technology security policy of the Nashville Police Department. This policy includes computer services and associated devices, networks and communications facilities. This document is meant to provide detail with respect to Nashville Police Department resources. This policy states the conditions of use of Nashville Police Department Information Technology Services IT facilities, the rights and responsibilities of users and administrators and the methods used to implement the policy.

The aim of this policy is to ensure:

- The provision of uninterrupted IT services.
- The integrity and validity of data.
- An ability to recover effectively and efficiently from disruption.
- The protection of all Nashville Police Department Information Technology Services, IT assets including data, software and hardware.
- Define security standards for users, IT staff, and vendors.
- Identify items required by HIPAA, LEIN, or other state or federal agency's to be in compliance.

1.2 Scope of the Policy

Security can be defined as "the state of being free from unacceptable risk". Risk for the Nashville Police Department IT concerns the following categories of losses:

- Confidentiality of Information.
- Data integrity.
- Assets.
- Efficient and Appropriate Use.
- System Availability.

Confidentiality refers to the private department information or electronic private health information.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disk fails, or subtle, as when a character in a file is inappropriately altered.

The assets that must be protected include:

- Computer and Peripheral Equipment.
- Communications Equipment.
- Computing and Communications Premises.
- Supplies and Data Storage Media.
- System Computer Programs and Documentation.
- Application Computer Programs and Documentation.
- Information/Data.

- HIPAA, LEIN, and other data resources protected by local, state, federal statue.

Efficient and appropriate use ensures that the Nashville Police Department IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

The potential causes of these losses are termed “threats”. These threats may be human or non-human, natural, accidental, or deliberate.

1.3 Policy Implementation

The Nashville Village Council has adopted the Information Technology Security Policy to govern the use of department resources, including IT resources, and reserves the right to change any portion of it at any time.

There are 3 groups involved with the implementation of the Information Technology Security Policy:

- The Chief of Police,
- The Network Administrator
- Village of Nashville Council

Except as provided by this policy, the Department Heads are responsible for determining and enforcing appropriate use of department resources, including IT resources, by employees or contractors under their supervision and control. Department Heads may establish standards of appropriate use which are more stringent than defined in this policy.

Where authorization by the Network Administrator is required, the Department Head is responsible for issuing guidelines for obtaining such authorization. The guidelines may include the delegation of authorization to others.

1.4 Risk assessment

Periodically Network Administrator's or an approved third party vendor shall carry out a risk assessment. The aim of such an assessment is to estimate Nashville Police Department Information Technology Services potential vulnerability, to ensure that security measures being taken are sufficient to reduce the risk to acceptable levels and to estimate the costs associated with achieving an appropriate level of security.

The potential risks include:

- Users with higher than necessary levels of access.
- Terminals not logged off correctly.
- Shared user-ids and passwords.
- Errors.
- Disaffected employees.

- Lack of security awareness.
- Unauthorized access.
- Viruses.
- Remote access.
- Lack of control over changes made to services and/or data.
- Legal consequences of security breaches.
- Fire.
- Water.
- Sabotage.
- Risks associated with Internet access.
- Public embarrassment.

2. IT Security Procedures

2.1 Physical Security

Access to secure areas, including computer rooms and closets, shall be restricted to authorized staff through the use of passwords, locks or access-control devices. Visitors to such areas shall be permitted only under the supervision or authorized by the Network Administrator, Chief of Police, or designated staff.

When services are required from the Department of Public Works or contractors for repair and maintenance of the building, the Department of Public Works will notify the Chief of Police either via email or verbally of all work to be done, when it is scheduled and how long it will take to complete. These areas to include:

- Nashville Police Department Office
- Nashville Police Department Garage

2.2 Hardware

The Network Administrator shall maintain a current inventory of all computers and peripheral equipment.

The effect of electrical power outages and fluctuations on mission critical services shall be protected by the installation of an uninterrupted power supply (UPS), Power Generator and or surge protection devices. The Network Administrator shall be adequately protected against fire and water damage.

- The following standards of physical security of strategic platforms must be met:
- Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- Air temperature and humidity must be controlled to within acceptable limits.

2.3 Software

All materials associated with any computer system, including software and printed materials, which are not in the public domain, must be treated in accordance with any applicable copyright agreements and

restrictions. Such material must be licensed (if required) in an appropriate manner and may be obtained only in a legal manner from a legal source. The Network Administrator shall maintain a current inventory of all license software and periodically inform departmental managers of any licensing violations.

Users will not use the facilities of any computer system for storing, accessing or otherwise using any material which in any way infringes a copyright agreement. Old or obsolete software should be destroyed.

2.4 Data Security

The use of a computer system supplies the user with information about the computer system, as well as information about Nashville Police Department IT. This information is essentially private to Nashville Police Department IT, in some cases, essential for the user to know in order to carry out useful work. Therefore, a trust relationship exists between the user and Nashville Police Department IT.

A user will not use any account or otherwise attempt to gain access to any information that he/she is not to possess or authorized to access. A user will not use a computer system, or otherwise attempt to access any file or device, to disclose information that he/she is not to possess.

It is the responsibility of Network Administrator to manage department network resources. Therefore, Network Administrator must have full access to all application/system data. Network Administrator has both an ethical and professional responsibility not to access, view, distribute, or use any data not required to complete an assigned job function.

2.5 Internet Security

All users must read and sign the Nashville Police Department Internet/Email Usage Policy(APPENDIX A) to gain access to the internet or be issued an email address.

- The Internet will be treated as a potentially hostile environment.
- All data packets and connection requests will be controlled by the firewall.
- Only explicitly permitted traffic is allowed through the firewall. All other traffic is rejected.
- All traffic passing through the firewall can be logged and audited.
- Packet filtering will be used with rules which keep the risk to a minimum.
- Where possible, access by outside users will be restricted.
- Any computing devices located outside the firewall will have installed firewall filtering software to ensure that those systems have the necessary protection from external hostile attacks.
- Publicly available computing devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers shall be located within an established DMZ.

2.6. Intrusion Detection

Within the boundaries of the Nashville Police Department Network, intrusion protection is required to prevent:

- Unauthorized individuals from indiscriminately connecting any computing devices into any access point of the network
- Unauthorized access of staff and external hostile threats to the Nashville Police Department Technology Resources

Only those computers belonging to the Nashville Police Department will be allowed to function when connected to the Nashville Police Department network. Visiting personnel wishing to access the network must have authorization from the IT director, who must apply to other then predefined public PC's.

On a weekly basis, network administrators will review access logs of failed login attempts for all systems capable of recording login failure events. Excessive failures or obvious attempts at gaining unauthorized access will be reported to Network Administrator/Chief of Police.

2.7. Remote Access

External connections to resources located within the Nashville Police Department network is discouraged due to security implications.

If employees, partner agencies, or vendors require remote access then the acceptable method of connection shall be a connection this is FIPS 140-2 compliant.

Employees and vendors are responsible for ensuring that their computers are running current Anti-virus protection on any computing device before establishing a remote access connection to the Nashville Police Department technology resources.

If third party remote control applications are used, strong passwords shall be required. The application shall only be active when required and terminated upon disconnection; furthermore, the Nashville Police Department employee responsible for the pc running the remote connection software shall not leave any remote access connection running unattended.

Unless the prior approval of the Network Administrator has been obtained, staff may not establish modems; Internet or other external network connections that could allow access to the Nashville Police Department Technology resources.

2.8. Malware /Virus/Spyware/Spam

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

- Any PC internal/external connecting to the county network will have current Anti-virus/Spyware protection.

- Client Anti-Virus software scans should be performed weekly and include “all files”.
- Servers Anti-Virus software scans are performed weekly and include “all files”.
- Client/Servers (anti-virus updates) files should be updated at least weekly.
- Network Administrator will check all software before installing it.
- Network Administrator will use software tools to detect and remove viruses.
- If end users suspect an active virus they shall immediately shut down their PC and contact and call the Network Administrator/Chief of Police.
- End-users will immediately delete any suspicious e-mails and if appropriate request that the sender resend the message again.
- All inbound email messages are to be scanned.

Spam is generally e-mail advertising for some product sent to a mailing list, unsolicited by the recipient. While software and filters are in place to mitigate propagation, all spam is not preventable. Users can reduce the amount of spam received by not opening unsolicted email, not clicking on pop-up windows, and by not downloading unnecessary programs. (see Appendix A)

2.9 Data Security

- Ensure the physical security of your server.
- Put a firewall between your server and the Internet.
- Always block TCP port 1433 and UDP port 1434 on your perimeter firewall. If named instances are listening on additional ports, block those too.
- Isolate services to reduce the risk that a compromised service could be used to compromise others.
- Run separate SQL Server services under separate Windows accounts.
- Create Windows accounts with the lowest possible privileges for running SQL Server services.
- Use NTFS.
- Always install the latest service packs and security patches.
- Run SQL Server services with the lowest possible privileges.
- Use Enterprise Manager to associate services with Windows accounts.
- Always use strong passwords for all SQL Server accounts.
- Set login auditing level to failure or all.
- Enable security auditing of Sysadmin actions, fixed role membership changes, all login related activity, and password changes.
- Remove sample databases from production servers.
- Back up all data according to what has been defined in the Information Security Policy and store copies in a secure off-site location.
- Test disaster recovery system.
- Reduce the surface area of your system that is exposed to attack by running only those services and features needed in your environment.
- Restrict membership of the sysadmin fixed server role to a few trusted individuals.
- Ensure that you use complex passwords for all SQL Server accounts.
- By default, only members of the sysadmin role can execute xp_cmdshell. You should not change this default.
- Do not grant execute perITsion on xp_cmdshell to users who are not members of the sysadmin role.
- Do not enable the guest account.
- Add MBSA to your weekly maintenance schedule, and follow up on any security recommendations that it makes.

- Periodically scan for accounts with NULL passwords and remove them or assign them strong passwords.
- Delete unused accounts.

2.10 Windows Operating System Security

The following items are performed by the Network Administrator.

- Use Windows Update/Patch Management and install the latest service packs and critical updates.
- Configure Automatic Updates to automatically notify you of the availability of new security fixes. If possible, configure Automatic Updates to automatically download updates and install them without manual intervention.
- Keep up with the latest security patches by using the GFI Languard

Use the Baseline Security Analyzer to scan and evaluate the security of your system.

2.11 Wireless Networking

Wireless networks present some security considerations, basic security recommendations specific to wireless networks. The following rules for use of wireless network shall apply:

- Turn off the broadcast SSID function, except for public internet access.
- Firewall all Wireless connections away from CJIS Network
- Change the SSID name
- Change the administrator password
- Ban rogue access points
- Limit the number of DHCP addresses assigned
- Encryption (WPA2 AES 256bit)

3. Users

3.1. Responsibilities

Users' responsibilities include:

- Ensuring that confidentiality and privacy of data is maintained.
- Safekeeping of their user-id and password.
- Ensuring the security of their terminal by logging off or locking it when it is left unattended. All windows workstations will automatically lock after 20 minutes of inactivity.
- Ensuring the security and privacy of print-outs produced from Nashville Police Department computer services.
- Compliance with all relevant Local, State, Federal, such as HIPPA, CJIS.
- Compliance with the provisions of this policy, and Nashville Police Department policies and procedures.

3.2. Confidentiality and Non-disclosure statement

Before performing any work on department machines or the department network, vendors must sign the Confidentiality and Non-disclosure agreement(APPENDIX E). Vendors must ensure that all personnel involved with any project shall be advised of the confidential nature of the information contained within Nashville Police Department network resources.

3.3 Password management

Passwords are a primary defense mechanism on many computer services. Careful selection of passwords improves security. Individual users are responsible for the robustness and maintenance of their own passwords. Individual users are responsible for the defense of any accounts held by them. The following rules for use of passwords shall apply:

- Passwords must be used where possible.
- Passwords must be at least 8 characters in length.
- A newly-issued password must be changed as soon as possible after issue.
- Passwords must be changed regularly, not to exceed 90 days.
- Passwords must not be displayed next to the terminal, under keyboard, or any other place other then a locked door.
- Users when logging on must not permit anyone to see their password being entered.
- Passwords must not be disclosed to others.
- Passwords should not be easily associated with a particular user.
- Users will not save passwords electronically within applications.
- A user who realizes that a password has been compromised shall change the password, if possible. The user is required to report all details of the breach to the Network Administrator/Chief of Police support staff.
- Passwords shall be checked to ensure that they comply with guidelines and are non-trivial.
- All system-level passwords must be updated on the global password list held by the Network Administration.

3.4 Account Security

Department heads are required to notify the Network Administrator when a user account or security profile needs to be disabled or deleted. Accounts should be disabled or deleted when a employee leaves or situations where the employee will be gone for an extended period of time. In most all circumstances the account should be disabled or deleted on the last day of the employees' service to the department.

If an employee leaves or a temporary employee needs access to the department network. The employee will notify the Network Administrator an account will be created. All temporary employee accounts will have an expiration date that is provided by the department.

Department heads should request account changes with the Network Administrator to implement any security changes for employees in their department.

3.5 E-mail Disclaimer

When an employee sends out e-mail with HIPAA or other sensitive information the following (or similar) disclaimer must be add to the end of the transmission. ***CJIS Information is exempt from this as no CJIS data is to be transmitted via EMAIL.***

Disclaimer:
This electronic message, including any attachments, is confidential and intended solely for use of the intended recipient(s). This message may contain information that is privileged or otherwise protected from disclosure by applicable law. Any unauthorized disclosure, dissemination, use or reproduction is strictly prohibited. If you have received this message in error, you must delete it permanently and notify the sender immediately.

3.6 Data Backup

An appropriate regular backup schedule shall be implemented to protect all data and software. A sufficient number of backups of all data and software shall be stored off-site to protect against major damage at one location.

Data on each user's workstation is not backed up. Users should save all valuable information on servers that are backed up as part of the backup procedure.

3.7 Disciplinary Actions

Department resources generally, and IT resources specifically, may be provided to employees exclusively to assist in the efficient and effective day to day operations of offices, departments, and agencies. Misuse of department resources may result in discipline, up to and including immediate discharge and, where appropriate, civil and/or criminal liability.

4. Security Management

The responsibility for the Network Administrator of information security procedures must be assigned to specific personnel in such a way that the procedures can be implemented and monitored while still guaranteeing that the overall security of Nashville Police Department Information Technology Services computing facilities is not compromised.

The overall responsibility for the management of the security of data rests with the Network Administrator. As part of the security procedures, access to all services must be monitored on a continuing basis and audit trails or access logs maintained. It is in the interest of all account holders that Network Administrator negates or minimizes any potential or actual security breach. The Network Administrator may disable an account without notice, regardless of whether the account itself is suspected of misuse.

All other accounts owned by the account holder may also be disabled without notice.
The Network Administrator decides the nature and period of account suspension.

Mission critical applications shall require individual users authentication and provide Intruder lockout after three unsuccessful logon attempts.

Terminals which are logged in and inactive for an extended period of time, and which are not being used to process or monitor foreground or background tasks, must be automatically logged off and the details logged for later review.

Department heads shall review any application with electronic protected health information and the level of security assigned to their employees.

4.1 Security Breaches

When appropriate, The Network Administrator will refer any incident involving a possible breach of State, Federal or International law for investigation. The Network Administrator will give that authority all reasonable assistance requested.

If a security breach occurs in which a person or organization external to the Nashville Police Department is involved as a potential victim of the breach, the Nashville Police Department will refer to the external party the details specific to that party.

If a security breach involves facilities strictly internal to the Nashville Police Department. The Nashville Police Department may follow the appropriate department disciplinary procedures.

Security Incident Reviews

The person who carries out the technical investigation of a security breach shall submit a report to the Network Administrator/Chief of Police outlining the following details (where possible):

- The general nature of the security breach.
- The general classification of people involved in the security breach, (such as external client, privileged staff member).
- The computer services involved in the security breach.
- The details of the security breach.
- The impact of the security breach.
- Unrealized, potential consequences of the security breach.
- Possible courses of action to prevent a repetition of the security breach.
- Side-effects of those courses of action.

Remedial action should be taken on the basis of this report, when appropriate.

The following steps are listed in the order that they should be taken. Once a breach is confirmed, these steps should be taken as urgently as possible. If a particular step is not appropriate to the breach, then the reader should ignore it and move to the next step.

- The Network Administrator/Chief of Police should be notified immediately.
- If the security breach involves a possible breach of State, Federal or International law, the appropriate authorities should be notified as soon as possible.
- If an organization or person external to Nashville Police Department is involved in any capacity, then the Computer Emergency Response Team (CERT) should be contacted.
- If an organization or person external to Nashville Police Department is involved as a potential victim, then that organization or person should be advised as soon as possible.

4.2 Security Audits

Regular auditing procedures shall be carried out on all computer services to check for conformance to policy, and to satisfy the requirements of the Nashville Police Department internal and external auditors. The depth and regularity of each level of audit should be outlined in the local procedures manual.

Audit procedures, of any level, may be carried out on any computer system at the discretion of the Network Administrator/Chief of Police.

In the course of the auditing procedure, the Network Administrator may delete or otherwise modify any data on any computer system that promotes an infringement of the this policy or the host configuration guidelines in the local procedures manual, in order to re-establish system security.

All unauthorized access attempts must be noted and logged. The Audit Trail/System Access Log must be reviewed daily, exception reports generated and inspected by the Network Administrator and appropriate action taken. A copy of the report of unauthorized access attempts must be produced and kept for future reference.

4.3 Disaster Recovery

A disaster recovery plan shall be implemented which takes into account the risk assessment, Nashville Police Department needs and vulnerabilities. The disaster recovery plan shall be documented and tested periodically.

4.4 Review and Amendment of Security Policy

This policy shall be reviewed at least annually and may be amended as required by the Network Administrator/Chief of Police/Village Council. When amended, each copy of the former policy shall be replaced by a copy of the new policy.

4.5 Training

The level of security that can be implemented within Nashville Police Department depends to a large extent on the understanding and co-operation of all staff. The key to good security is based on staff awareness and training Personnel who have been granted access to computer services have a responsibility for the safe keeping of data within their own area of work. Users must be aware of the ways in which the security of data can be enhanced.

To assist staff to gain an understanding of how system security can be enhanced it is necessary to:

- Define personnel policies and procedures.
- Provide education and appropriate supervision.
- Ensure an understanding of confidentiality requirements.

It is essential that all aspects of IT security, including confidentiality, privacy and procedures relating to system access, should be incorporated into formal staff induction procedures for all new staff and be

conveyed to existing staff on a regular basis. Each employee, on commencement of employment, should be made aware that they must not divulge any information that they may have access to in the normal course of their employment.

4.6 Media Protection/Transportation

All CJIS/PII shall be protected. All CJIS/PII shall stay within the confines of the Nashville Police Department. If the data is required to be transported (i.e. to Prosecutors etc.) a log shall be maintained. When applicable the data shall be encrypted with FIPS 140-2 Certified encryption.

4.7 Media Sanitization/Destruction

Any form of media that has value in reuse may be used within the Nashville Police Department or another criminal justice agency (i.e. Sheriff Department, State Police, etc.) Any media regardless of form shall not be used in a non-criminal justice agency. All retired CJIS/PII media that is no longer needed shall be melted down, or shredded beyond recognition.

APPENDIX A

Date_____

Department: Nashville Police Department User_____

Nashville Police Department
Policy Regarding the Use of
Information Technology Resources

IT resources refers to items such as personal computers, software, the county network, phones, tablets, the department provided Internet connection, the department web page and Intranet; e-mail, electronic voice and video communication, and facsimiles. This policy addresses, among other things, department access to, review or disclosure of electronic files, electronic mail and electronic voice and video communications through or stored on any part of the department's IT resources. These policies do not constitute a contract. The Department reserves the right to change them at any time.

Nashville Police Department employees must not misuse E-mail or Internet access. Nashville Police Department provides computers and computer access to its employees so that they can better perform their jobs. E-mail sent by Nashville Police Department employees must be of a nature and tone that is consistent with the standard of conduct appropriate to the workplace, and Nashville Police Department employees must not solicit or encourage others to send E-mail that fails to meet this standard. Similarly, all other file-sharing and communication across the Internet must meet this same standard of conduct.

For purposes of this policy, "E-mail" includes all electronic mail sent or received using Nashville Police Department computer equipment, regardless of whether the E-mail is transmitted or delivered by means of a Nashville Police Department local network, a Nashville Police Department-provided Internet account, or a private Internet account. Likewise, "Internet access" includes all Internet access by means of Nashville Police Department computer equipment, regardless of whether the access is through a Nashville Police Department-provided Internet account or a private Internet account.

Users' responsibilities include:

- Ensuring that confidentiality and privacy of data is maintained.
- Safekeeping of their user-id and password.
- Ensuring the security of their terminal by logging off or locking it when it is left unattended. All county owned workstations automatically lock after 20 minutes of inactivity.
- Ensuring the security and privacy of print-outs produced from Nashville Police Department computer services.
- Compliance with all relevant Local, State, Federal, such as HIPPA, CJIS.
- Compliance with the provisions of this policy, and Nashville Police Department policies and procedures.

I. Prohibited Uses of IT Resources

1. Duplicating, transmitting or using software which is not in compliance with software licensing agreements and/or unauthorized use of copyrighted materials or other person's original writings.

2. Security violations including, but not limited to:

A. Accessing accounts or information within or outside the Department's computers and communications facilities for which an employee is not authorized or does not have a business need;

B. Knowingly spreading malware.

C. Transmitting confidential and/or attorney-client privileged communication and information without proper security and authority.

D. Misuse of another's password, negligent or intentional disclosure of the assigned password or any attempt to defeat the password security.

3. Modifying or altering software, programs or the standardized configuration of the equipment supplied by the Department including software, hardware, and OS system files without prior authorization from the Network Administrator.

4. Installing, removing, storing, uploading or downloading software or programs to the IT system without prior approval from the Network Administrator. All approved installations must be performed by the Network Administrator personnel or at their direction.

5. Making available a network service (FTP server, WWW server, etc.) without written permission from the Network Administrator.

6. Moving department equipment from its IT designated location to a new location without prior authorization from the Network Administrator.

7. Installing hardware or software without permission of the Network Administrator

8. Intentionally wasting IT resources by, for example:

A. Placing a program in an endless loop; or,

B. Disrupting the use or performance of Department-authorized IT resources or any other computer system or network.

C. Distributing "junk mail" such as chain letters, advertisements or unauthorized solicitations.

9. Making available any access to the Department's telecommunications equipment, computers, or associated media without written authorization from the Network Administrator.

10. Using the computer system to copy and/or transmit software programs, documents or other information protected by copyright law.

II. Prohibited Uses of E-mail and the Internet

A. Use for any purpose that violates a law of the United States or a law of the State of

Michigan.

B. Use for any purpose that violates a personnel rule, or a Nashville Police Department employment contract.

C. Use for any purpose specifically prohibited by the Department Head or Network Administrator.

D. Use which violates the security, privacy, and confidentiality policies, practices and laws of this Nashville Police Department and the State of Michigan including unauthorized release of confidential material.

E. Use or access to the intentional display or distribution of files containing the following: obscenity, profanity, pornography; expressions of animosity or bias against individuals, groups or organizations; material in violation of regulations prohibiting sexual harassment or other non-businesslike materials.

F. For the intentional display or transmission of sexual images, messages, or cartoons, as well as the use of ethnic slurs, racial epithets or anything that could be construed as harassment, gender bias, race/ethnic bias, or bias against any protected class.

G. Use for profit activities (unless specific to the mission of the Department or other government agencies).

H. Use to solicit for commercial ventures or political causes, or for private or personal business transactions, or for partisan or non-partisan political activities, or for political fund raising.

I. Use for advertising or public relations activities not specifically related to Nashville Police Department business.

J. Use for playing of games or non-business computer activities, which generate traffic or consume excessive bandwidth on any local area network.

K. Interfering with computers or computing systems, damaging software on other computers, or altering the software on the computers without authorization.

L. Seeking or obtaining information about files, documents, or other data that are private, confidential, or otherwise not open to public inspection, unless specifically authorized to do so by the file owners; or copying, modifying, or deleting such files, documents, or data without authorization.

M. Copying or downloading software in violation of copyright or license restrictions, or using evaluation copies of software in violation of license restrictions.

N. Representing oneself as another without that other person's permission.

III. Security

Department heads, with technical assistance from the Network Administrator if necessary, have the capability to access, review, copy, modify and delete any information transmitted or stored in IT resources, including voice and e-mail messages. The appropriate department head, reserve the right to

access, review, copy, modify or delete all such information for any purpose and to disclose it to any party if legally compelled to do so, pursuant to the Freedom of Information Act, or if the Department otherwise deems it appropriate. Those voice or other IT resources files containing personal information of an employee as a result of an employee's making incidental use of the IT resources system for personal purposes, including the transmission of personal voice and e-mail messages, will be treated no differently than other files, i.e., the department heads, Network Administrator reserve the right to access, review, copy, modify, delete or disclose them for any purpose required by law, or which the department heads, deem appropriate in its discretion. Accordingly, employees should not use the IT resources system to send, receive or store any personal information that they wish to keep private. Employees should treat the IT resources system like a shared file system -- the files or messages sent, received or stored anywhere in the respective systems will be available for review by the appropriate department head, and, may be disclosed to third parties.

IV. Violations

Violations of the aforementioned guidelines listed above may result in disciplinary action up to and including termination. If necessary, the Nashville Police Department will advise appropriate legal officials of any illegal violations.

Policy Use and Acceptance Form

My signature below certifies that I have read the Policy Regarding the Use of Information Technology Resources, and that I understand, accept and will abide by the provisions stated in them.

Signature: _____

Name: _____

Department: Nashville Police Department

Date: _____

Department Head Signature: _____

Date: _____

Registered E-Mail Address: _____
(If assigned by Information Services)
The completion of this form is required for E-Mail and Internet use privileges.

Adopted by the Village Council _____

APPENDIX B
NASHVILLE POLICE DEPARTMENT CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

THIS AGREEMENT, made and entered into this ____day of _____, by and between the Nashville Police Department, a municipal corporation and political subdivision of the State of Michigan (hereinafter referred to as the "Department") and _____ (hereinafter referred to as the "Vendor").

RECITALS

WHEREAS, the Department and the Vendor have entered into a contract or a Purchase Order has been issued for products and/or services, a copy of which is attached hereto; and

WHEREAS, Vendor in the provision of such products or service, may come into contact with software licensed or owned by the Department and with the Department's; and

WHEREAS, it is understood by the Vendor that access to such software, data, network infrastructure, website and security codes is conditioned upon their being treated as confidential and that they not be disclosed to anyone other than Vendor's personnel who have a need to such access in order to provide the required products or services; and

WHEREAS, the Department and Vendor agree to such confidentiality and non-disclosure requirements which are set forth herein.

NOW THEREFORE, it is hereby agreed by the Department and Vendor as follows:

1. Confidentiality and Non-Disclosure Agreement.

It is expressly understood and agreed by the Department and Vendor that Vendor's personnel in the provision of products and/or performance of services required under the contract entered into between the Department and Vendor and/or the Department's Purchase Order for such products or services will come into contact with software licensed or owned by the Department and with the Department's data, network infrastructure, website and security codes. To the extent necessary for the provision of products and/or performance of services under the contract and/or the Department's Purchase Order, Vendor shall be given access to said software, data, network infrastructure, website and security codes necessary for fulfillment of the contract or purchase order.. All said software, data, network infrastructure, website and security codes shall be considered to be confidential and shall not be disclosed by the Vendor, persons under the Vendor's employ, or Vendor's contractors, to any third party without the prior written consent of the Network Administrator (IT). Such disclosure shall be for the limited purpose authorized by the Network Administrator and made subject to the terms and conditions of this Agreement. Upon completion of the provision of products and performance of services required by the contract or Purchase Order, the Vendor shall return and/or destroy as the Network Administrator may direct all information or data and any copies which may have been made thereof of the Department's software, data, network infrastructure, website and security codes it may have obtained under the contract or Purchase Order. If requested by the Network Administrator, the Vendor shall provide the Department with a written, signed and notarized certification that all information and copies thereof on the Department's software, data and security codes have been returned and /or destroyed as required by this Agreement.

2. Certification of Authority to Sign Agreement.

The persons signing on behalf of the parties to this Agreement certify by their signatures that they are duly authorized to sign this Agreement on behalf of said parties and that this Agreement has been authorized by said parties.

IN WITNESS WHEREOF, the authorized representatives of the parties hereto have fully signed and entered into this Agreement on the day and year first above written.

WITNESS:

Nashville Police Department

_____ _____

Date , Network Administrator

VENDOR:

_____ _____

Date