Lunenburg Police Department

Policy Number: 1.29	Subject: Lunenburg Police C.J.I.S. Use
Issue Date: 03/14/2016 Revised Date: 10/19/2021 Effective Date: 03/14/2016	Massachusetts Police Accreditation Standards Referenced: N/A
Issuing Authority: *Chief Thomas L. Gammel*	

I. PURPOSE

The safety and well-being of each employee and citizen who comes in contact with the Lunenburg Police Department electronically is a vital concern to the Town. Electronic mail and computers in general offer an easy, efficient, and rapid means of communication, but should be used with care. Additionally C.O.R.I. information received via computers needs to be protected against intrusion or improper dissemination. The purpose of establishing this policy is to:

A. Detail how to respond to a potential security incident, intrusion attempt, etc.
B. Maintain a secure workplace for all employees.
C. Detail how to properly use the CJIS and Town of Lunenburg systems.
D. Illustrate how C.O.R.I information must be handled.
E. Decrease liability exposure from employee actions.
F. Demonstrate how to use workstations and Internet connectivity in a secure manner
G. Manage use of computer systems.
H. Detail how to properly maintain ID(s) and password(s), as well as any other C.O.R.I. data.
I. Prevent unlawful or wrongful actions against fellow employees or citizens either directly or indirectly through the use of computers.

II. DEFINITION

Electronic Communications is defined as any transfer of signs, signals, writings, images, sounds, data, or intelligence that is created, sent, forwarded, replied to, distributed,

broadcast, stored, held, copied, downloaded, displayed, viewed, read, printed, or otherwise transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system. This term expressly includes, but is not limited to, emails, attachments to emails, text messages, recorded voicemail messages, web sites visited, computer files, and data files, and data files sent over the intranet or Internet, or sent by wired or wireless communication.

III. Ownership: Hardware, Software, and Information

A. Purpose:

1. The Town will provide a computer workstation to select employees as a condition of employment. These computers, however, remain an asset of the Town and should be used for business purposes only. Consistent with Federal Law, the Town reserves the right to enter, search, disclose, and monitor both computer files and computer-related activities with or without advance notice for any business purpose.
2. Since the Town is a public entity, all records (except those specifically excluded by law) whether in electronic or hardcopy form, are subject to the Freedom of Information Act and open to public inspection. Employees must remain cognizant of this fact whenever they create a computer file. File-level password protection does not imply that a user's messages, memos, documents, or other files, either active or deleted, are private. E-mail accounts and their content, including Internet accounts, are also considered property of the Town of Lunenburg. The content of email should be considered the same as any other written public document, as any statement sent via email may subject the Town and the author to the same liabilities as a written public statement.

IV. C.J.I.S.

A. Purpose

To establish guidelines for the proper operation of fixed, mobile, and portable criminal justice information system (CJIS) workstations, and to ensure the lawful handling of Criminal Offender Record Information (CORI) information generated from or maintained within the CJIS network.

B. System Use

1. The use of a CJIS workstation is for criminal justice purposes only. These include the commission of official criminal justice duties (i.e. investigations, bookings, warrant entry etc.), qualifying an individual for employment within a criminal justice agency, and qualifying an individual to determine his/her eligibility to possess a firearms license.

2. The use of a CJIS workstation for non-criminal purposes including transactions conducted for public and private educational establishments, municipal agencies, town government officials, etc. is strictly prohibited and is punishable by a fine, suspension of services and/or incarceration.
3. Each operator shall immediately report any damage to a CJIS workstation to one's supervisor.
4. It is this agency's responsibility to report an inoperable CJIS workstation to the Office of Technology as soon as possible. Workstation operators may be held responsible for damage done to a CJIS workstation. Should the work station be the property of the Town of Lunenburg, the Office of Technology should be notified.
5. No CJIS equipment including CJIS workstations, mobile data workstations or personal digital assistant/palm pilots shall be modified or altered in any way from its set up configuration, unless it is done by a representative of the Office of Technology or the device's contract vendor, and then only with notification to, and concurrence of, the DCJIS.
6. Each agency must ensure that any and all CJIS information passing through a network segment is protected pursuant to FBI CJIS Security Policy.

V. Background Check Requirements for access to CJIS

A. Background checks shall be required for all personnel with access to CJIS. A fingerprint-based criminal history check shall be submitted to the Massachusetts State Police State Identification Section (SIS) and to the FBI for all employees, contractors or vendors with direct terminal or physical access to criminal justice information or criminal justice information systems.

B. This shall include agency personnel or volunteers, state, city or town information technology personnel, and vendors or contractors. These fingerprint-based background checks *shall be performed at least once every two years, except for vendor or contractor personnel, who shall be checked annually.* Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJIS processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

C. It is recommended vendor and contractor background re-investigations be conducted every five years. *It shall be the policy of the Lunenburg Police Department to re-investigate every two years.*
D. *Individuals with convictions for felony offenses shall not be permitted access to CJIS or any other system or source to which CJIS provides access.* If it is found that an individual with access has a conviction for a felony offense, the agency shall notify the CSO at DCJIS. In addition, access privileges shall be immediately

terminated. Failure to comply with 803 CMR 7.04 may result in loss of agency access to CJIS or other sanctions by the CSA or FBI.

E. Individuals with convictions for misdemeanor offenses may be permitted access to CJIS or any other system or source to which DCJIS provides access, but only upon the approval of the CSO. An agency seeking a waiver shall submit a written request to the CSO at DCJIS.

F. *Only those users that are authorized by the agency head and have been trained, tested, and certified regarding CJIS policy and compliance may have access to CJIS or to information obtained from CJIS or any other system.*

VI. SYSTEM ACCESS

A. Certification:
   1. All operators of CJIS workstations shall be trained, tested, and certified under procedures set forth by the DCJIS before using a workstation and shall be re-certified biannually (2 years) thereafter. As part of the re-certification process fingerprints shall be submitted at time of re-certification.
   2. Each CJIS workstation operator shall use one's assigned password when accessing the CJIS network and shall not give this password to anyone under any circumstances. No one shall use the network under another individual's password.
   3. All operators shall log on to the network at the beginning of one's work day and shall log off at the end of one's work day to ensure that transactions are logged under the appropriate user name. This will prevent one operator from being held responsible for another operator's CJIS transactions. Appropriate care will be taken to not allow any unauthorized access to CJIS.

B. Revocation of Rights and Privileges:
   1. In the event of a suspension it will be up to the Chief of Police to determine if the member's rights to the building and CJIS/Town computer system should be revoked.
   2. In the event of termination, the members rights to the building, and access to all secure areas and equipment shall be immediately revoked. The Office of Technology personnel shall be notified (via e-mail) immediately so access to the following can be removed:
      a. Removal of rights to secure areas, Lenel Security system and transponder retrieved;
      b. Removal of rights from Windows/IMC/Citrix;
      c. Removal from the Town of Lunenburg E-Mail systems;
      d. Removal from town Web Sites.

VII. REMOTE ACCESS

A. Purpose: The purpose of this policy is to define standards for connecting to Town of Lunenburg's network from any host. These standards are designed to minimize the potential exposure to Town of Lunenburg from damages which may result from unauthorized use of Town of Lunenburg resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

B. Scope: This policy applies to all Town of Lunenburg employees, contractors, vendors and agents with a computer, workstation, or similar device used to connect to the Town of Lunenburg network. This policy applies to remote access connections used to do work on behalf of Town of Lunenburg. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

C. Policy: In the event of software problems or if an end user requests technical assistance, remote access shall be permitted for technical support person(s) where it is deemed impractical or untimely to troubleshoot or correct in person. The remote session must be documented or recorded electronically.

D. It is the responsibility of Town of Lunenburg employees, contractors, vendors and agents with remote access privileges to Town of Lunenburg's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Town of Lunenburg.

VIII. CORI

A. Purpose
   1. The Massachusetts Public Records Law (G.L. c. 4, § 7) gives the public the right of access to most records maintained by a government agency. However, CORI information, including that which is obtained from the CJIS network is exempt from public access under the CORI Law (G.L. c. 6, §§ 167-178).
   2. CORI is data compiled by a criminal justice agency concerning an identifiable individual and which relates to the nature of an arrest, criminal charge, judicial proceeding, incarceration, rehabilitation or release, and may include a juvenile tried as an adult. Under 803 CMR, only those officials and employees of criminal justice agencies, as determined by the administrative heads of such agencies, shall have access to CORI. Criminal justice employees are eligible to receive CORI as needed during the course of their official duties.
   3. Reasons for conducting a board of probation (BOP) check may include, but is not limited to:
      a. An investigation

b. An arrest
c. An individual applying for criminal justice employment
d. Local licensing purposes (i.e. where the police department is the licensing agency) and door-to-door sales people where the municipality requires the police department to regulate, and
e. Firearms licensing purposes.

4. The officer may share CORI with other officers or criminal justice agencies when an investigation is being conducted, however, the dissemination must be logged in the agency's secondary dissemination log with the date, time, individual checked, purpose, officer's name, and the agency and agent to whom the information was given.
5. Many non-criminal justice agencies have been authorized by the DCJIS to receive CORI information under G.L. c. 172 (a). Such authorization was given to these agencies in writing, and a copy of this letter should be provided by these requesting agencies to the agency or police department that will be providing the requested CORI information, to print the form.
6. All other requests for CORI shall be referred to the Chief's office.
7. To lawfully obtain CORI and to then furnish the information to any person or agency not authorized to receive is unlawful and may result in criminal and/or civil penalties (G.L. c. 6, § 177 and § 178).
8. All complaints of CORI being improperly accessed or disseminated shall be handled as a citizen complaint and the Chief shall be advised of the matter. The complainant shall also be advised that they may file a complaint with the DCJIS by calling (617) 660-4760.

B. Security of C.O.R.I Information

1. Users must ensure that information obtain via CJIS, including CORI, is secure.
2. DO NOT: Leave a computer terminal, including Mobile Data
3. Terminals/Computers, unattended while logged in; share logins and/or passwords;
4. Allow documents to be left out in the open to be viewable by all whom pass your workstation.
5. Terminal screens must not be viewable from public spaces or by unauthorized individuals
6. File cabinets and records rooms must be secured and locked when unattended
7. The policy of the Lunenburg Police Department is the following: Users will make every attempt to ensure the computer is either logged off or secured (CTRL/ALT/DELTE- lock this computer/workstation) when not under your direct control (meaning in same room as your workstation/computer).

IX. IMPROPER ACCESS AND DISSEMINATION OF MASSACHUSETTS REGISTRY DATA

A. Concerning the use of the Massachusetts Criminal Justice Information System (CJIS) to access driver's license information:

1. Access to personal information contained in motor vehicle records, including driver's license files, is governed by the Federal Driver Privacy Protection Act ("DPPA") that is contained in 18 USC §§ 2721-2725. 18 USC § 2721 (b) (1) permits the use of motor vehicle administration (RMV) data "for use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions." 18 USC § 2722 makes it unlawful to access RMV data by any means (CJIS or otherwise) by any government or law enforcement agency for a non-official purpose. Individuals that violate the DPPA are subject to a criminal fine under 18 USC § 2723 and may be civilly liable to the data subject of the record that was improperly accessed pursuant to 18 USC § 2724
2. Additionally, Mass law has a provision relative to unauthorized access of computer systems. M.G.L. c. 266, §120F states that "[w]hoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, *shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both.*
3. ***The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.***" CJIS is the state's criminal justice computer system." Even if a police officer was authorized to access CJIS for official use in the normal course of his/her duties, after gaining access to the system he/she would know that using it for non-law enforcement purposes is not permitted.

B. Sanctions and Penalties

Improper Access to, and/or Dissemination of, information contained in, or obtained from, CJIS may result in any of the following:

1. Loss of CJIS access privileges and/or terminal Civil fines and penalties issued by DCJIS per M.G.L. c. 6, § 168 and 178, from $1,000 up to $5,000 per violation
2. Fines imposed by 28 C.F.R. 20.25, up to $11,000
3. Criminal Prosecution per M.G.L. c. 6, §178 and M.G.L. c. 266, s. 120F Driver Privacy Protection Act: DPPA- 18 U.S.C. s. 2721
4. ***Suspension and/or Termination from the Lunenburg Police Department.***

X. LUNENBURG POLICE VISITOR LOG POLICY

A. Purpose

1. The purpose of the Lunenburg Police Department visitor log is to identify individuals who are entering the restricted area of the department and to verify that they have a valid purpose to be in the restricted area of the department.
2. A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJIS and associated information systems. *The restricted area of the Lunenburg Police Department is designated as any interior location beyond the lobby, training room or the public interview room off the lobby. All other areas of the station are restricted to authorized personnel only.*
3. A police vehicle shall be considered a physically secure location. For the purposes of this Policy, a police vehicle is defined as a Criminal Justice Conveyance or any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of the FBI/CJIS Security policy section 5.9.13.

B. Physical Access Authorizations

All authorized personnel with access to a physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) shall be issued credentials (Key Fob/transponder) which will monitor access to these locations (building entry, lock up, evidence, armory etc). *The Lunenburg Police Department utilizes the Lenel system which controls authorization levels and records access to secure areas (evidence, armory, and lockup). This system is located in the dispatch area.*

C. Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access. This is accomplished via the DSX system, unescorted visitors and unauthorized personnel shall check in at dispatch prior to entry.

D. Access Control for Display Medium

The agency shall control physical access to information system devices that display Criminal Justice Information, (CJI) and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

E. Visitor Control Who Needs To Sign In

Individuals who are permitted access to the restricted area of the Lunenburg Police Department and will not be escorted by a department member. This includes, but is not limited to, the following:

1. Any individual who is not authorized to enter via Lenel security. (Lenel entry security generates a date/time stamp and electronic signature upon entry to the building).

F. Who Does Not Need To Sign In

The following individuals do not need to sign in as visitors at the Lunenburg Police Department:

1. Immediate family members;
2. Members of other law enforcement agencies;
3. Members of other entities that work with the Lunenburg Police (i.e. DCF, etc.);
4. Bail clerk;
5. Anyone who is escorted by a member of the Lunenburg Police Department.

G. Identification Required – What is Acceptable

Individuals, who are entering the restricted area and are required to sign in, shall show an ID unless they are personally known to the dispatcher who is granting them access (i.e. Town of Lunenburg Employees.). An individual, who is required to show an ID, may show a driver's license or a company ID card. Should a dispatcher become concerned that the ID he/she is being shown is not valid or questionable; the dispatcher shall refer the matter to the shift supervisor or the OIC.

H. Access Records

The Lunenburg Police Department shall maintain visitor access record to the physically secure location (except for those areas officially designated as publicly accessible) shall include:

1. Name and Agency of the visitor
2. Method used to identify visitor
3. Date and time of access and departure times
4. Purpose of visit
5. Name of Lunenburg Police employee visited

I. **Waiver of the ID Requirement – By Supervisor or OIC**

1. *A supervisor or OIC may waive the ID requirement for a person entering the restricted area of the station.* Should the ID requirement be waived, the

dispatcher on duty when the requirement is waived should note in the log "waived by" and the supervisor's name or badge number.

2. These records shall be maintained for a minimum of one year. Designated officials within the department shall review the access records for accuracy and completeness.

XI. C.J.I.S. RECORDS DESTRUCTION POLICY

A. Destruction of C.O.R.I Information

Any information obtained via CJIS must be shredded (cross cut) prior to disposal, under no circumstances should this information be simply thrown into the trash.

B. Electronic Media Sanitization and Disposal

The Lunenburg Police Department shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. ***Electronic media which cannot be re-written shall be preferred method (CD-R, DVD-R) for the Lunenburg Police Department use.*** Inoperable electronic media shall be destroyed (cut up, shredded, etc.). Officers shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

XII. NETWORK THREATS EXPLAINED

A. Purpose

The threats that will be discussed in this section concern the way you use your workstation, access restricted zones within the network, and the way you handle sensitive information. I will attempt to cover all the possible threats, discuss their importance in detail, and provide you various effective ways to manage them.

B. Passwords

Each employee is expected to keep his or her password confidential. Under no circumstances should a password be disclosed to anyone. If you suspect someone has discovered your password or have any knowledge of violations, please contact the Technology Department. Passwords should be "cryptic" to avoid easy detection. Avoid using child names, pet names, birthdays, telephone numbers, or motor vehicle registrations.

C. System Access to Network

1. Staff needs to be fully aware of their responsibility to keep their User ID and password as secret as possible, and it's all because this is the first line of defense within any system: the identification of the user. It is completely forbidden to share his/her ID and password with ANYONE including family members.
2. No matter how safe you might think your password is, you are not allowed to store them on any bits of paper; you must do your best and memorize it instead. Another common mistake that must not be overlooked is the horrifying fact that most of the users tend to hide these notes under the keyboard, or on some "secret" place, as they call it, around their desk; another activity that is completely forbidden due to obvious reasons. Someone could easily find the "secret" hiding place and get acquainted with vital data.

D. Password Creation

1. *Passwords must be made up of a mixture of lower-case (small) letters, upper case (capital) letters, numbers, and at least one special character, such as (!@#$%^&*()_+|);*
2. *The minimum length of the password must be at least 8 characters;*
3. *Do not use the same password on several computers and/or services as once revealed, it would compromise the security within all the others.*
    a. **Good Password Examples:**
        i. Ona327(sA
        ii. @865DapzI
        iii. 93Sow#-aq
    b. **Bad Password Examples**
        i. aaa123bbb
        ii. abcdefg
        iii. 76543210
4. The first *bad password* is a terrible one, and any properly configured cracking program will retrieve it in a matter of minutes, and let's not even mention the second and the third one. The user with the last password (76543210) obviously thought it would be an easy to remember password, as well being a secure one, as it is a long(ish) one; but what the user does not know or realize is the fact that most cracking programs will find it in a matter of seconds (as the password follows a specific numerical pattern).

E. Strong Passwords Creation Tips

1. Use the first letters of a quote, song, etc., for example "Something takes a part of me..." would be 'Stpm'

2. Join two words, include a number, as well as a special character, for example 'run4life#';

F. Password Maintenance Best Practices

1. The proper maintenance of sensitive data such as the User ID and password are a responsibility of every staff member.
2. Do NOT share your User ID(s) and password(s) with anyone including family members. It is your responsibility to keep the data as secret as possible;
3. Do NOT store your User ID(s) and password(s) on any loose bits of paper, sticky (post-it) notes, whiteboards, flip charts, etc.;
4. Do NOT hide your User ID(s) and password(s) under the keyboard, or at any other would be "secret" hiding place. Do your best and memorize it;
5. Do change your password(s) following the stated password renewal period in the security policy;
6. Before entering your User ID and password, make sure no one is watching you, to avoid the so-called" shoulder surfing" technique.
7. Before using your User ID and password on a third-party computer, make sure it is well protected, and free of Trojans and key loggers.

G. Network Account Security

1. It is the responsibility of the user to ensure the security of their network account. Network account passwords are the responsibility of the user and should remain confidential.
2. User accounts and internet access may be terminated at the discretion of the Chief of Police or his/her designee, if a violation of system or network security occurs. The Chief of Police or his/her designee may monitor account activity at any time. Users should report to a Supervisor, any communications they receive via the Town's E-mail system which violate these rules.

XIII. SOFTWARE INSTALLATION

Freeware or any other type of software, obtained or downloaded from unknown or untrustworthy sources could easily affect the Town of Lunenburg's Network security, exposing critical business data and/or corrupting sensitive ones. A lot of users tend to install such programs (from screen savers to games and funny cartoons in Flash) as they put it, for various personal needs and activities; to entertain, have something nice to look at or relax them. At the same time, they do not realize the potential threats they are exposing the Town of Lunenburg's systems and networks to, from malicious software (viruses/Trojans/worms) to legal actions against the Town for installing (possibly) pirated software on the company workstation(s). Files downloaded from the Internet, copied from a CD or a floppy coming from an unknown source, or anything else that has not been reviewed by the TEO or MIS Department or not been scanned for potential

malicious code could actually be classified as untrustworthy, unknown and dangerous. Freeware applications, due to their nature of origin, are a significant source of threat and should be approached with caution. Majority of users do not have the ability to install any new programs that might either expose sensitive information, waste valuable bandwidth, or corrupt critical data. If users need new software installed for business use, they should contact the Technology Department instead of undertaking such action themselves.

A. Removable Media (CD's, floppies, tapes, flash drives, etc.)

1. Removable media such as CD's (Compact Disks), floppies (Floppy Disks) and even tapes(backup/ADR/DAT/DLT tapes) can be defined as another possible entry point for dangerous and malicious files entering the Town of Lunenburg's network or endangering the security of a single workstation. On the other hand, these can also be used to illegally copy sensitive data on, after which it would be easy to walk out of the premises with the stolen information. *Only authorized personnel (written permission by Chief of Police) may copy sensitive data onto a removal media medium for use outside of the Lunenburg Police Department. At no time should CORI data be placed onto removable media without encryption.*
2. Malicious software (viruses/trojans/worms) also use removable media to spread; some take advantage of the auto-run feature of the CD (automatically executing the auto-start file on the CD, which could be a destructive one), others still use "classic" methods like diskettes to get the workstation infected with a malicious program. To prevent possible viruses, please contact the Technology department before inserting removable media into Town computers.

B. Viruses

1. *"Viruses will continue to be a very serious threat to critical business data, and will continue to evolve, becoming more sophisticated, dangerous and devastating."*
2. Viruses result in damage and/or potential loss of critical business data, documents, projects, and business plans, presentations employees have been working on, along with any other personal data stored on the computer will be damaged, or, more than likely, are destroyed. By getting to know the devastating effects that viruses may have, employees will be much more aware on the subject, and will more than likely understand the importance of the topic, and the risks for both the Town of Lunenburg and their home PC's.
3. Anti-Virus scanners will not detect every new virus. Employees must know that they can reduce the risk, and properly manage the danger. The Town of Lunenburg's anti-virus software allows for centralized automatic updates, these updates are scheduled on a regular basis to ensure the software detects the latest viruses/trojans/worms (known to our AV vendor's lab).

C. Malicious Code Best Practices

1. Do NOT run any files without first scanning them, no matter what the file extension is, i.e. (.exe, .bat, .com, .doc, etc.);
2. Do NOT download any files and/or programs from unknown sources; if in doubt, contact the Technology Department as soon as possible;
3. Do NOT open attachments, even if they were sent by a friend or family member; verify first that indeed, he/she has sent you the file, but nevertheless scan before you open/run anything;
4. Do NOT run any programs you have found on diskettes/CD's around your desk if you are not completely sure that they are yours; someone might have placed it there specially for you to "find it and check it out";
5. If downloading is allowed, limit it to the minimum; if you need a specific application or something else, always contact the Technology department for further information BEFORE you download and installing something;
6. Scan (full system scan) your system at least once per week with your default AV scanner software;
7. If you detect suspicious activity, do not delete the e-mail received and contact the Technology Department as soon as possible;
8. If you have any doubts regarding malicious software (viruses/trojans/worms), contact the Technology Department immediately. This way you will prevent any potential devastating mishaps, due to inappropriate and erroneous handling of dangerous and harmful incidents.

D. Encryption

1. Encryption can be defined as another "must implement" measure that will not only keep our sensitive and critical information secured against a potential attacker, but also protect us from a lot of trouble if eventually a security breach does occur.
2. Encryption can be defined as another "must implement" measure that will not only keep our sensitive and critical information secured against a potential attacker, but also protect us from a lot of trouble if eventually a security breach does occur. *The Lunenburg Police system utilizes 128 bit encryption for all mobile computers.*

E. System Backups

Disaster recovery (DR) plans are essential for the continuity of the Lunenburg Police Department as well as the proper functionality of the current processes. Sooner or later, employees inevitably face the problem where a system crashes, no matter of the OS used, but this can be dealt with promptly. The assets that must be backed up on a regular basis are all servers and computers that are vital to the everyday operations of the Lunenburg Police Department. The responsible

individuals are the Technology Department Staff, whom must ensure that the data being backed up is encrypted, can easily be restored, and is current. The backups should be stored, but are not limited to, a fireproof safe, or vault. The Lunenburg Police Department back up tapes are stored off sight at the Town Hall.

F. Software Piracy

Software piracy is a crime and will not be tolerated. Software provided by the Town to its employees is licensed for use on the town's computers only. Employees are not allowed to install the software on their home computer. Moreover, they are forbidden from distributing the software to friends and or associates. Likewise, employees are not allowed to install any software on the Town's computers without the consent of the Police Chief, his/her designee, or the Technology Department. These procedures allow us to prevent infection by computer viruses or corruption by "buggy" software. Under the current system, any attempts, successful or unsuccessful, to write to the registry of the computer (install software) is logged. This log is checked regularly by the Technology Department. This tells who, what, where, and when an attempt was made to install software.

XIV. ELECTRONIC MAIL

Electronic Mail is provided to increase both productivity and the dissemination of information. While it eliminates the common business problem of "telephone tag," its use must retain a level of business decorum. Employees must insure that messages sent and/or received via this mechanism are not threatening, offensive, frivolous, or brusque.

E-mail has become a common way for employees and other businesses to communicate with each other. Since this is the case, we encourage the use of e-mail in completing day to day activities that are beneficial to the town.

Some things that people should be aware of are e-mails with files that are attached to them. These files, especially if the recipient does not know who sent it, should not be downloaded due to the potential threat of viruses that might be contained within the file. In most cases even if you might know the person sending you the file, they might not realize that it could be a virus being sent to you, so please be cautious. This not to say that all files attached to e-mails have viruses but they must be checked to ensure they do not. If you are unsure about an e-mail attachment, please do not hesitate to call the Technology Department regarding any questions concerning this issue. *The Lunenburg Police Departments current policy is that if the user is unsure about the attachment, we will save the file to a floppy disk and properly scan the file for viruses. If the attachment checks out with no problems, the file can then be used on the network. This process is done not only to protect the computer that you are working on, but to protect the network from damaging viruses that could potentially spread throughout the network.*

A. E-mail Use Best Practices

1. Please confirm with the sender (i.e. via phone) that indeed an attachment has been sent. This will also reduce the risk of running a program that has been e-mailed out automatically (unknown to the originator) via some kind of malicious application that has made use of the mail account(s) and/or mailing system of the sender;
2. Do not use the Town's e-mail accounts for registration purposes of any kind, and do not use it while posting messages in web forums or newsgroups. Employees may want to create one, special (possibly aliased) account for this purpose only;
3. Do not use the Town's e-mail system for running your own business, excessive personal mailing, sending large attachments, thus wasting valuable bandwidth;
4. Do not respond to chain letters, or any other sort of spam using the Town's e-mail systems; if in doubt, contact the Technology Department office;
5. Never forward any Town data to external e-mail accounts (i.e. send a work document to your home email account, so to work on it further from home that evening), without first checking with your supervisor.
6. The proper use of the E-mail system will continuously be monitored and the users should be aware that they could be held liable for illegal activities, such as spamming, sending and receiving illegal content, etc.

XV. GETTING AN ACCOUNT

A. The Account Request Process

1. Network Access Definition - Network access includes viewing Web sites, sending and receiving electronic mail, transmitting or receiving flies, and running Internet applications.
2. Accounts Request Process – Network accounts will be issued after the following criteria have been met:
3. A Network User Account Request Form must be completed and signed by the employee and have department head approval.
4. The justification for employee use section must be filled in by the department head. The completed Request Form should be forwarded to the Technology Department which will be reviewed by the T. D. and Chief of Police for approval. Upon approval, the Technology Department will contact the employee to initiate their account.

XVI. INTERNET USE

The Technology Department, at the direction of the Chief of Police, has the authorization to monitor employee activity on the Internet to ensure proper use. The Town has the right

to notify the appropriate authorities if it discovers evidence of any possible illegal activities.

A. Internet Threats Explained

One of the greatest security risks to the Town of Lunenburg is Internet connectivity, and its misuse through (uninformed) employees. It is a fact that most employees will surf to sites that are strictly prohibited, and most probably will end up downloading malicious files and/or hostile code from hacker sites somehow. Any of these activities could impact the productivity of the police department, especially if one thinks about the recovery process of trying to rectify the mistakes made by staff. Employees do not need to download anything at all to get the computer infected with a virus, Trojan or even a worm but just visiting the site is enough to cause a problem.

B. Web Browsing

Web browsing represents a threat to the security of the workstation, as well as to the whole Town. Being exposed to the dangers of web browsing is very easy as hostile scripts could be downloaded, and executed automatically; all it takes, for example, is an outdated version of the web browser. Employees should be able to make a distinction between sites that are classified as allowed, prohibited or potentially dangerous, and try to avoid visiting prohibited ones. Care must be taken with Flash movies, etc. and if ever a hint of a problem occurs, the Technology Department must be contacted immediately. There are web sites in the wild, that could attempt to scan/flood the Town's network, just by visiting them; another variant to this (theoretical, but very possible) scenario is using some kind of scanning service to check the security of his/her workstation, thus wasting valuable bandwidth. Something like this will invariably produce more work for the Technology Department and the computer systems probably will register the usage of this service as a possible break-in attempt.

C. Unacceptable Use of the Internet

1. Solicitation of non-town business or use of the Internet for personal gain is prohibited.
2. Use of the Internet; for any purposes which violate a federal, state, or local law. This includes use of copyrighted material (text, picture, or sound) which may be available on the Internet.
3. Use for access to, and distribution of pornographic or sexually-explicit material, on-line gambling, or usage in a sexually harassing manner.

D. Wireless Communications

Wireless networking is a technology that allows computers and other electronic devices to have network connectivity using radio waves instead of wires. While this opens up new possibilities for mobile connectivity, it must be remembered that the wireless network is a resource made available for the benefit of the Town of Lunenburg employees. The use of all computers, mobile devices, and other wireless devices is subject to the Computer and Electronic Communications Policies. The purpose of this policy is to secure and protect the information assets owned by the Town of Lunenburg. The Town of Lunenburg provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. The Town of Lunenburg grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Town of Lunenburg wireless network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Technology department are approved for connectivity to a Town of Lunenburg wireless network.

E. Scope

1. All employees, contractors, consultants, temporary and other workers at the Town of Lunenburg, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the Town of Lunenburg must adhere to this standard. This standard applies to all wireless infrastructure devices that connect to the Town of Lunenburg network or reside on a the Town of Lunenburg site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.
2. The Town of Lunenburg Technology Department must approve exceptions to this policy in advance.

F. Requirements

All wireless infrastructure devices that connects to the Town of Lunenburg network or provides access to the Town of Lunenburg's information must:

1. Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
2. Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

G. CJIS Security Policy Compliance

Criminal Justice Information System Incidents shall be reported forthwith to the DCJIS Information Security Officer (ISO). Incidents include, but are not limited to:

1. A breach of Computer Security
2. A breach of Information Security.
3. The ISO will report the incident to DCJIS within 48 hours either by mail at:
   Massachusetts Department of Criminal Justice Information Services
   ATTN: Information Security Officer
   200 Arlington Street, Suite 2200
   Chelsea, MA 02150

   Or by EMAIL at: cjis.support@state.ma.us

H. Enforcement

This policy is part of the Computer and Electronic Communications Policy and failure to conform to the policy is a violation of the Computer and Electronic Communications Policy. Any employee found to have violated the policy may be subject to disciplinary action, up to and including termination of employment. Any violation of the policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the Town of Lunenburg.

XVII. REQUESTS FOR SERVICE (REPAIRS)

A. Service Request can be submitted via e-mail. This process will allow more flexibility and response times for the Technology Department. Upon submitting a request for service via email, your request will be automatically assigned to the appropriate personnel for response.
B. Also, you will automatically receive a series of possible solutions that the end user can implement. The person or persons assigned to fix or service your request will also receive this list of possibilities and will respond to your request by e-mail. This process will allow for easier tracking of hardware and software problems and allow for identification of equipment that may be classified as problematic. The Technology Department will respond to these requests prior to written requests not only to promote its use, but also because of the rapid notification and immediate availability of possible solutions.
C. As in the past, emergency requests will receive the highest priority, and users with emergencies which cause work stoppages can directly telephone the Technology Department. It is pertinent; however, you also submit an e-mail to allow for proper logging and tracking of the problem.