COLCHESTER POLICE DEPARTMENT

	SUBJECT: **Computer Policy**
EFFECTIVE DATE: August 4, 2020	NUMBER: GENERAL ORDER # 25
REFERENCE:	SPECIAL INSTRUCTIONS: Includes Appendices A - J
REEVALUATION DATE: ANNUAL APPROVED:	NO. PAGES: 4

POLICY: The Colchester Police Department recognizes the fact that computerization is providing a significant and essential impact on law enforcement. It also recognizes that sound policy and guidelines need to be established and adhered to in order to ensure the highest levels of security for the information under its jurisdiction. It is the policy of this department that all steps, consistent with the following procedures, will be taken to ensure system security and data integrity.

The Colchester Police Department embraces and adheres to the concepts and policies outlined in the Vermont Criminal Justice Information Systems Security Policy and Guidelines, as well as the FBI CJIS Security Policy.

CONTENTS:

I. OVERVIEW:

The Colchester Police Department strives to be a forerunner in the era of high technology and the accepted practice of computerized names, records, and other sensitive data. The age of multi-agency electronic information sharing, external database accessibility and mobile computing makes the formulation of sound internal policy governing the uses and access of such information a necessity.

Proper policy is critical to ensure accurately maintained and properly disseminated information and to ensure the integrity of the information and the department remains intact. An efficiently administered computer system can provide increased efficiency, with significant time savings, product quality enhancement, and more rapid access to critical information.

II. DEFINITIONS:

Colchester Police Department Computer System: Includes all hardware and software, both networked and non-networks, possessed and/or owned by the police department for its use in day to day activities. This includes all redundant back-up systems located both on and off site of the department.

Network: refers to a computer system that is interconnected via hardware and software.

System Administrator: The individual designated to establish, operate, and maintain the computer system

Users: All members who have been granted some degree of access to the network and possess a valid login name and password.

VIBRS System: Refers to the Vermont Incident Based Reporting System as established and maintained by the Vermont Criminal Justice Services.

CAD/RMS; Refers to the current computer aided dispatch/records management system currently utilized by the Colchester Police Department.

Mobile Data System: Refers to the use of department computers, phones, tablets, and any other digital device that is allowed access to any of the following outside the physical wall of the police department:

1. Colchester Police Department Network
2. State of Vermont VIBRS Network
3. Valcour, Spillman or other CAD/RMS system utilized by the Colchester Police Department.

III. PROCEDURES:

A. Users: All sworn and civilian personnel of the department, who are active members may be granted access to the Colchester Police Department computer system, henceforth referred to as "Network". Prior to access, the individual must successfully complete approved training in the use and responsibilities for the network. Specific access and program rights will be set based upon the individual's position and requirements.

B. Login: Refer to Appendix A, "Unique Identifier" for user login requirements.

C. Passwords: Refer to Appendix B, "Password Compliance" for password requirements

D. Advanced Authentication: Colchester Police Department Policy, as well as the State of Vermont CJIS Policy, and that of the FBI require that only authorized individuals gain access to the CJIS system. This requires advanced authentication methods, which are laid out in Appendix C, "Advanced Authentication".

E. Home Directories: Each user will be assigned a general home directory. Limits may be established for the amount of material retained in an individual's directory at the system administrator's discretion, based on system capabilities. It is the user's responsibility to ensure the directory does not exceed the specific limit. The system administrator will periodically monitor material quantity in user directories to insure limits are maintained.

F. Electronic Mail (E-Mail): The Colchester Police Department E-Mail system is for the free use of system users pursuant to the following guidelines and restrictions:

1. Material of an offensive nature is not allowed. This includes but is not limited to vulgar language and comments critical of department policy or personnel.

2. Users should be aware that the contents of E-Mail can be used as evidence in civil, criminal, and internal investigations and therefore should not contain any material which can be construed to indicate bias, prejudice, or other litigation liability which may be damaging to the department.

3. Users should be aware that system backups of E-Mail have not been deleted.

G. Mobile Data System: The mobile data system is an extension of the Colchester Police Department Network, and therefore falls under all restrictions of the network. As it exists outside the physical walls of the police facility, further requirements exist for its' safe use and to ensure data security. Refer to Appendix J, "Mobile Data System" for all additional restrictions.

H. Security: Data integrity and security is of utmost concern to the Colchester Police Department. Strict requirements have been put in place to help deter security breaches and attacks from outside the network. Refer to Appendix D, "Acceptable Computer Use" for detailed information on security.

I. Security Training: Every individual that has physical or constructive access to the network shall be subject to Data Security training on an annual basis. This rule applies to any individual that has completed a fingerprint supported background check and is allowed unescorted access to the police facility. Training will be completed on line and in the following manner:

Colchester Police Department Users: Training shall be completed as part of annual NCIC user training.

Town of Colchester Employees: Training may be completed on line at the following location: WWW.NEXTest.Com

Town of Colchester Vendors: Training may be completed on line at the following location: WWW.NEXTest.Com

J. VIBRS System: The Colchester Police Department Network allows connection to the State VIBRS system via the internet. Access to the system is regulated by the Vermont Department of Public Safety, Agency of Digital Services. All Colchester Police Department members are governed by the

VIBRS System User Policy when attached to that system. Only users who have signed a VIBRS User Agreement will be allowed access to the VIBRS network.

K. CAD/RMS: The Colchester Police Department currently utilizes three CAD/RMS Systems, with VALCOUR being the primary system in use. Spillman and Novell are utilized as archival systems to store historical information. Only users that have a signed VALCOUR agreement and have received approved training will be allowed access to the system.

L. Internet Use: The network allows access to the internet for all users. This access is strictly for law enforcement purposes. Use of the internet by department personnel is governed by the following:

1. No files of any type are to be directly downloaded to the Colchester Police Department computers without authorization from the system administrator.

2. Use of the internet opens the network up to possible virus infection (data loss, file corruption and system damage) and for this reason, all network computers have virus protection software. In the event a virus warning is received, the procedures outlined in Appendix E, "Computer Incident Response Policy" shall be followed.

3. Internet Access is further defined in Appendix F, "Protection of CJIS Data".

M. Network Firewall: The Colchester Police Department adheres to all policies issued by the Vermont Department of Public Safety, Agency of Digital Services, pertaining to the use of firewalls. Refer to Appendix H, "Network Firewall", for full statement.

N. Dial-In Access: Security concerns demand strict requirements with regards to network access from outside the physical walls of the police department. Refer to Appendix G, "Dial-In Access".

O. Disposal of Media: Media (Hard Drives, CD's, DVD's, and any other device capable of saving electronic data) shall be disposed of properly. Refer to Appendix I, "Disposal of Media" for proper procedures.

P. Revocation: In order to ensure the integrity of the system, any user who does not adhere to this policy may have their network privileges revoked. Furthermore, rights to the network as well as rights to the VIBRS network and the CAD/RMS systems may be suspended as well.

The system administrator reserves the right to immediately disable any user who is, or appears to be, compromising the integrity of the system.

#

COLCHESTER POLICE DEPARTMENT

		SUBJECT: **Unique Identifier**
EFFECTIVE DATE: August 4, 2020		
REFERENCE: GENERAL ORDER # 25, Appendix "A"		SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL	APPROVED:	NO. PAGES: 1

I. POLICY: This policy shall ensure accountability of all users that access the Colchester Police Department Network and network devices by defining the creation of a unique identifier to allow access to the network, network devices, and NCIC information.

A. General

The Colchester Police Department requires each employee that has access to the Colchester Police Network, applications, and/or NCIC for the purposes of storing, processing, and/or transmitting information shall be uniquely identified by use of a unique identifier. A unique identifier shall also be required for all persons who administer and maintain the system(s) that access agency and NCIC information and/or network. The Colchester Police requires users to identify themselves uniquely before the user is allowed to perform any action on the network and/or applications. All users IDs shall belong to currently authorized users. Identification data shall be kept current by adding new users and disabling former users. Employees shall not share their IDs with other employees, supervisors, management, or family members at any time.

B. Guidelines

The unique identification can take the form of one of the following examples:

- User's full name (JohnWDoe)
- Form of full name (SASmith)
- Badge Number (CPD180)
- Combination of name and badge number (jdoe180)
- Serial Number (1234567890)
- Other unique alphanumeric identifier.

C. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

#

COLCHESTER POLICE DEPARTMENT

	SUBJECT: Password Compliance
EFFECTIVE DATE: August 4, 2020	
REFERENCE: Appendix "B"	SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL APPROVED:	NO. PAGES: 5

POLICY: It is the policy of the Colchester Police Department to provide secure network and user accounts to facilitate law enforcement access to CJIS information. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of the Colchester Police Department 's entire computer network. As such, all Colchester Police employees (including contractors and vendors with access to the Colchester Police systems) are responsible for taking the appropriate steps, as outline below, to select and secure their password.

CONTENTS:

I. SCOPE: The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at the Colchester Police facility, has access to the Colchester Police Computer network, and /or NCIC network, or stores and non public Colchester Police information.

II. GENERAL:

1. All system-level passwords (e.g., root, enable, network administrator, application administration accounts, etc,) must be changed at least every 90 days.

2. On all systems (procured after 09/30/2005) password reuses of the last ten (10) passwords shall be prevented if the password is used for authentication.

3. All production system-level passwords must be part of the Information Security administrated global password management database.

4. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.

5. User accounts with access to NCIC privileges must have a unique password from all other accounts held by that user.

6. Passwords must not be inserted into email messages or other forms of electronic communication.

7. Where simple network management protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system" and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2)

8. All user level, system level, and NCIC access level passwords must conform to the guidelines described below.

III. PASSWORD CONSTRUCTION GUIDELINES:

1. Passwords are used for various purposes at the Colchester Police Department. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and lock router logins. Since very few systems have support for one time tokens (i.e., Dynamic passwords which are used once), everyone should be aware of how to select strong passwords.

   a. Poor, weak passwords have the following characteristics:

      - The password contains less that eight characters

      - The password is a word found in a dictionary (English or Foreign)

      - The password is a common usage word such as:

        - Name of family, pets, friends, co-workers, fantasy characters, etc.

        - Computer terms and names, commands, sites, companies, hardware, software.

        - The words "Colchester Police", "CPD", "COLPD" or any derivation.

        - Birthdays and other personal information such as addresses and phone numbers.

        - Word or number patterns like aaabbb, 111222, zyxwvts, 456321, etc.

        - Any of the above described names, words, spelled backwards.

        - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

2. Strong passwords have the following characteristics:

   - Contain both upper and lower case characters (e.g., a-z, A-Z)
   - Have digits and punctuation characters as well as letters (e.g., 0-9,!@#$%^&*()_+{}[]:";<>?)
   - Are at least eight alphanumeric characters long.
   - Are not words within any language, slang, dialect, jargon, etc.
   - Are not based on personal information, names of family, etc.
   - Passwords based on a song title, affirmation, or other phrase. For example, the phrase might be, "This May Be One Way to Remember", and the password could be, "TmB1w2R" of "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples.

IV. PASSWORD AND LOGON DELETION:

1. All passwords and/or logons that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

   - When a user retires, quits, is terminated, released, dismissed, etc.
   - Default passwords shall be changed immediately on all equipment
   - Contractor accounts, when no longer needed to perform their duties.

2. When a password is no longer needed, the following procedures should be followed:

   - Employee/Contractor will notify the Deputy Chief of Police or department designee.
   - The Deputy Chief shall ensure that the user's account will be suspended or deleted.
   - A password deletion form will be complete and filed in a secure filing system.

V. PASSWORD PROTECTION STANDARDS:

1. Do not use your user id as your password. If you do not authenticate against DPS active directory, do not use the same password for the Colchester Police Computer Network Accounts as for NCIC accounts. For example, select one password for your Windows account login and a different one for your NCIC account login. Do not share Colchester Police Department Network passwords with anyone, including administrative assistances or secretaries. All passwords are to be treated as sensitive,

confidential Colchester Police Information.

Here is a list of "do not's"

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to a co-worker
- Don't use the "Remember Password" feature of applications
- Don't write passwords down and store them anywhere in your office
- Don't store passwords in a file on any computer system without the ability to encrypt the data.
- Don't reveal password to anyone for any reason!!!!!

2. If someone demands a password, refer them to this document or have them contact the Operations Lieutenant for clarification of the policy.

3. If an account or password is suspected to have been compromised, report the incident to the Deputy Chief of Police.

4. Password cracking or guessing may be performed on a periodic or random basis by the FBI or this agency. If a password is guessed or cracked during one of these scans, the user will be required to change it.

VI. APPLICATION DEVELOPMENT STANDARDS:

Application developers must ensure their programs contain the following security Precautions:

- Should support authentication of individual users, not groups
- Should not store passwords in clear text or in any easily reversible Form

- Should provide some sort of file management, such that one user can take over the function of another without having to know that other's password

- Should support Terminal Access Controller Access Control System+ (TACACS+) Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, whenever possible.

VII. REMOTE ACCESS USERS:

Access to the Colchester Police Department Networks via remote access is to be controlled by using either a virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.)

#

COLCHESTER POLICE DEPARTMENT

		SUBJECT: **Advanced Authentication**
EFFECTIVE DATE: August 4, 2020		
REFERENCE: G.O. #25 APPENDIX "C"		SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL	APPROVED:	NO. PAGES: 2

POLICY: This policy will establish guidelines to help ensure that only authorized individuals gain access to CJIS systems via a variety of authentication methods, in an effort to preserve the confidentiality, integrity, and availability of CJIS information as it is processed.

A. General Uses and Ownership**:** Advanced authentication is achieved when a user presents, verified across the network, any combination of at least two of the following credentials:

- Something the user knows (e.g., password/pin)
- Something the user has (e.g., token, smart card or challenge card)
- Something the user is (e.g., a biometric such as a fingerprint or iris scan.)

B. Procedures: Procurement and upgrades to systems, after 9/30/2005, that are part of or access CJIS from any internets, wireless, or dial-in connection that is not physically secured shall used advanced authentication.

All mobile devices such as PDA's cell phones transmitting CJIS data, and mobile data computers which have been removed from a police vehicle shall, at a minimum also incorporate the use of a unique password or other personal identifier (PIN) as well as meet the advanced authentication requirement.

C. Acceptable Authentication: Currently the only two advanced authentication systems supported by the CSA is through the uses of RSA Secure ID cards or installed soft tokens. The RSA Secure ID Cards system utilizes a password to access the authentication system which then queries the user for a numeric identifier generated from an electronic token in the possession of the user. If this dual authentication is met, then the user is granted access to the network. This authentication takes place across the network. The Soft Token application utilizes a user name and password on software installed on a specific device, which then authenticates the user via an authentication server. A numeric identifier is then returned to the user to authenticate within the CAD/RMS software.

In order to receive access through secure ID, the individual must have the Colchester Police Department's authorization on file and the paperwork as required by the CSA, who will then make a determination as to the granting of access.

#

COLCHESTER POLICE DEPARTMENT

		SUBJECT: **Acceptable Computer Use**
EFFECTIVE DATE: August 4, 2020		
REFERENCE: G.O. #25 Appendix "D"		SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL	APPROVED:	NO. PAGES: 3

POLICY: The purpose of this policy is to outline the acceptable use of computer equipment at the Colchester Police Department. These rules are in place to protect the employee and the Colchester Police Department. Inappropriate use exposes this agency to risk, including virus attacks, compromises of the network systems and services, and legal issues.

CONTENTS:

I. SCOPE: This policy applies to employees, contractors, consultants, temporary staff, and other workers at the Colchester Police Department, including all personnel affiliated with NCIC and third parties. This policy applies to all equipment that is owned or leased by the Colchester Police Department.

II. GENERAL USES AND OWNERSHIP:

1. While the Colchester Police Department's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the Colchester Police Department. Because of the need to protect this agency's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Colchester Police Department.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

3. The Colchester Police Department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted

4. For security and network maintenance purposes, authorized individuals within the Colchester Police Department may monitor equipment, systems, and network traffic at any time.
5. The Colchester Police Department reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

III. SECURITY AND PROPRIETARY INFORMATION:

1. The user interface for information contained on the Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by department policy on the release of information. Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Please review the Colchester Police Departments Password Policy for guidance.

3. All department computers, laptops, and workstations should be secured with password-protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off when the computer is unattended.

4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops and other portable devices in accordance with the "Mobile Data Security Policy"

5. All devices used by employees that are connected by the Colchester Police Department Internet/Intranet/Extranet, whether owned by the employee or this agency, shall be continually executing approved virus scanning software with a current database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

IV. UNACCEPTABLE USE: The following activities are, in general, prohibited. Under no circumstances is an employee of the Colchester Police Department authorized to engage in any activity that is illegal under local, state, federal or international law utilizing Colchester Police Department owned resources. The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

1. Unauthorized access, copying, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.)

2. Installation of any copyrighted software for which the Colchester Police Department or end user does not have an active license.

3. Installation of any software without pre-approval and virus scan.

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

5. Revealing your account password to others or allowing use of your account by others.

6. Effecting security breaching or disruptions of network communications. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee in not expressly authorized to access, unless these duties are within the scope of their regular duties. For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, packet floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to and permission received from Chief of Police or his/her designee.

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

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

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

11. 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/Intranet/Extranet.

12. Providing information about NCIC or alist of the Colchester Police Department employees to parties outside this agency.

V. ENFORCEMENT: Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

#

COLCHESTER POLICE DEPARTMENT

	SUBJECT: Computer Incident Response
EFFECTIVE DATE: August 4, 2020	
REFERENCE: G.O. #25 Appendix "E"	SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL APPROVED:	NO. PAGES: 3

POLICY: This policy will establish guidelines to assist the Colchester Police Department in the reporting of computer related incidents. There has been an increase in the number of computer attacks into government and private organizations, regardless of whether the systems are high or low profile and it is important that this information is shared with other agencies as soon as possible. The consequences of such attacks can jeopardize human life and people's safety, expose classified and sensitive data, damage systems and disrupt computer services.

CONTENTS:

I. GENERAL:

A. Members need to be aware of the need to identify potential problems, and listed below are some indicators that an incident might be occurring (note: these do not mean an incident is occurring as the cause could be simple computer malfunction):

- Systems crash unexpectedly and without clear reason
- New files with novel or strange names appear
- Unexpected changes in file length or modification dates on files
- Unexpected data modification or deletion
- Denial of service
- Unexplained poor system performance
- Anomalies

- Suspicious probes
- Suspicious browsing
- Attempts to write to system files

II. **INCIDENT RESPONSE:** All members should be familiar with the proper procedures for dealing with an actual or a perceived incident.

A. The Colchester Police Department contact person is the Deputy Chief of Police, who should be contacted as soon as possible following the detection of an incident.

B. DO NOT POWER DOWN THE SYSTEM!

C. The suspected system(s) should be removed from network connectivity as soon as possible by unplugging the network cable from the computer.

D. Fill out the required incident report form (see attached Computer Incident Reporting Form)

E. The Department of Public Safety ISO needs to be contact as soon as possible after an incident has been detected.

III. **INCIDENT ANALYSIS AND INVESTIGATION:** The Colchester Police Department understands the need to properly document and investigate any computer incident for the purpose of determining the scope of the incident. The Town of Colchester Information Technology Manage will be contacted to review local systems, in the event of an incident, to:

- Look for modifications to system software and configurations files.
- Look for tools installed by the intruder.
- Check out other component systems for modifications.
- Check remote component systems for modifications.
- Or any other steps that may be required to determine the scope of the issue. Investigation will be conducted in such a way as to ensure the preservation and documentation of any evidence associated with the incident.

IV. **INCIDENT REPORTING FORM:** The Colchester Police will utilize a standard Computer Incident Reporting Form (see attached) to ensure the incident is appropriately documented. At a minimum this report will include the following information:

a. Description of the Incident

b. What happened?

c. How was the incident discovered?

d. Who does the incident affect?

e. When did the incident occur?

f. Why did the incident happen?

g. Where did the incident occur?

h. Resolutions identified?

i. What are the vulnerabilities and impact on other systems?

j. What is being done or should be done to correct the problem and ensure this type of incident does not recur?

k. What procedures are in place or are needed to prevent future occurrences?

V. **CONTINGENCY PLAN:** In the event of a security breach, the affected units shall immediately be taken off the network and secured until the incident has been appropriately investigated and documented. The affected units shall not be reattached to the network until threats have been neutralized, and the units cleaned and approved for reconnection.

#

COLCHESTER POLICE DEPARTMENT

SUBJECT: **Protection of CJIS Data**

EFFECTIVE DATE: **Augusts 4, 2020**

REFERENCE: G.O. #25 Appendix "F"

SPECIAL INSTRUCTIONS:

REEVALUATION DATE: ANNUAL

APPROVED:

NO. PAGES: 2

POLICY:

This policy shall ensure that necessary protocols and infrastructures are in place to provide necessary security of the CJIS systems from unauthorized Internet Access and to preserve the confidentiality, integrity, and availability of CJIS information as it is processed. This policy will define the minimum requirements that need to be implemented to ensure protection of CJIS data.

I. PROCEDURES:

The Colchester Police Department is authorized to grant Internet Access, to include dial-up access in accordance with this policy.

A. Authentication

Advanced authentication is required in accordance with CJIS Security Policy guidelines.

B. Firewalls

Firewall type devices shall protect networks in which some terminals or access devices had CJIS access and/or Internet access (e.g., peer to peer relationships, large mainframes and servers that house websites)

These devices shall implement a minimum firewall profile to provide, both from inside and outside the CJIS network, to ensure:

- a point of defense
- controlled and audited access to servers

C. Additional Protections

Additional protections shall include the following:

1. Data which is at risk on access devices and workstations shall have

residual CHIS Data removed by methods of removal, encryption, or erasure.

2. CJIS data transmitted through any Internet connection shall immediately be protected with a minimum of 128 bit encryption,

3. Internet contracts after 9/30/2005 shall support a minimum of 128 bit encryption

    - Must be NIST certified to ensure cryptographic modules meet FIPS Publications 140-2 requirements.

COLCHESTER POLICE DEPARTMENT

	SUBJECT: Remote Access
EFFECTIVE DATE: August 4, 2020	
REFERENCE: G.O. #25, Appendix "G"	SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL APPROVED:	NO. PAGES: 2

POLICY: The Colchester Police Department adopts this policy to maintain compliance with the Federal Bureau of Investigation CJIS Standards. It is further adopted to protect the Colchester Police Department's electronic information from being inadvertently compromised by authorized personnel using a dial-in/remote connection.

PROCEDURES: Authorized Colchester Police Department employees and third parties (contactors, vendors, etc,) can use dial-in or remote connections to gain access to the agency's network. Remote access should be strictly controlled, using the following criteria:

1. Users shall be authenticated by at least one of the following: strong passwords (as defined in the Password Policy), biometric, token device, certificates, smart cards, etc.

2. Dial-in users shall use a Virtual Private Network connection to gain access to the Colchester Police Department network.

3. Each authorized dial-in user shall be issued a unique identifier (as defined in Unique Identifier Policy)

4. The system shall employ log-in capabilities which include session initiation and termination messages, failed access attempts, and all forms of access violations such as attempts to access data beyond the level of authorized access.

5. Data transmitted over the dial-in segment shall be protected by 128 bit encryption.

6. Personal equipment which is used to connect to the Colchester Police Department internal network shall meet the requirements set forth in this policy.

7. All remote access hosts shall ensure the computers have the most up-to-date anti-virus software.

Any employee or third party that accesses the network through a bank of modems shall:

1. First, call the agency to have the modem turned on.

2. Second, inform agency personnel on how long they need a connection to the network.

3. Third, identify and authenticate themselves to the network and application.

4. Fourth, call agency personnel when more time is needed or the connection is no longer needed.

If the dial-in user does not call back in the given time stating that the connection is needed, the agency personnel shall terminate the connection in the stated time requested.

It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to the Colchester Police Department is not used by non-employees to gain access to the agency's information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their locations and the Colchester Police Department are literal extensions of the Colchester Police Department network, and that they provide a potential path to the agency's most sensitive information. The employee and/or third party individual must take every reasonable measure to protect the Colchester Police Department's assets and information.

NOTE: Dial-in accounts are considered "as needed" accounts. Account activity is monitored, and if a dial-in account is not used for four months, the account will expire and no longer functions. If dial-in access is subsequently required, the individual must request a new account as described above.

#

COLCHESTER POLICE DEPARTMENT

		SUBJECT: **Network Firewall Statement**
EFFECTIVE DATE: August 4, 2020		
REFERENCE: G.O. #25, Appendix "H"		SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL	APPROVED:	NO. PAGES: 1

POLICY: The Colchester Police Department will adhere to all policies issued by the Department of Public Safety, Agency of Digital Services, pertaining to the use of firewalls. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment pursuant to the Colchester Police Department's rules and regulations. CSA agency retains the right to terminate service in the event of a serious violation or failure to comply.

#

COLCHESTER POLICE DEPARTMENT

		SUBJECT: **Disposal of Media**
EFFECTIVE DATE: August 4, 2020		
REFERENCE: G.O. # 25, Appendix "I"		SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL	APPROVED:	NO. PAGES: 2

POLICY: This policy will outline the proper disposal of media at the Colchester Police Department. These rules are in place to protect sensitive and classified information, employees and the Colchester Police Department. Inappropriate disposal of Colchester Police and FBI information and media may put employees, this agency and the FBI at risk.

SCOPE: This policy applies to employees, contractors, temporary staff, and other workers at the Colchester Police Department, including all personnel with access to sensitive and classified data and media. This policy applies to all equipment that process classified and sensitive data that is owned or leased by this agency.

PROCEDURES: When no longer usable, computers, hard drives, diskettes, tape cartridges, ribbons, hard copies, printouts, and other similar media and items used to process or store classified and/or sensitive data shall be properly disposed of in accordance with measures established by the Colchester Police Department . The following procedures will be followed:

1. When no longer usable, hard copies and printouts shall be shredded.
2. Diskettes and tape cartridges shall be taken apart and shredded (ribbons, floppy disk) Any reference to material contained within the media (i.e., labels) shall be destroyed along with the containers as well.
3. The shredded remains shall be disposed of properly.

IT systems that have processed, stored, or transmitted sensitive and/or classified information shall not be released from The Colchester Police Department's control until the equipment is sanitized and all stored information has been cleared. For sensitive, but unclassified information, the sanitization method shall be approved by the Deputy Chief of Police or his/her designee. For classified systems, National Security Association approved measures shall be used. The following procedures will be followed:

1. Employees will send all hardware that processes and/or stores classified and/or sensitive data to Deputy Chief of Police to be properly disposed of. The will be disposed of hardware by one of the following methods:

a. Overwriting – an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. A minimum of three (3) overwrites are recommended.

b. Degaussing – a method to magnetically erase data from a magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

c. Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc.

Also, computers that are used to transmit classified and/or sensitive information must protect residual data. This can be accomplished with the use of integrated encryption technology. This technology uses a device or software which encrypts all data as it is written to the disk. When the user retrieves a file, the data is automatically decrypted for the owner to use. The encryption/decryption process is typically transparent to the user. Should the hard drive be removed, no useable data can be retrieved.

ENFORCEMENT: Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment pursuant to the Colchester Police Department's rules and regulations. CSA agency retains the right to terminate service in the event of a serious violation or failure to comply.

#

COLCHESTER POLICE DEPARTMENT

		SUBJECT: **Mobile Data**
EFFECTIVE DATE: August 4, 2020		
REFERENCE: G.O. #25, Appendix "J"		SPECIAL INSTRUCTIONS:
REEVALUATION DATE: ANNUAL	APPROVED:	NO. PAGES: 6

POLICY: The Colchester Police Department adopts this policy to provide guidelines and procedures for the use of Mobile Data Computers (MDC). It shall also ensure that a high degree of security exists for network associated data as it is remotely connected.

CONTENTS:

I. OVERVIEW:

Mobile Data Computers are used for communication between NLETS/VLETS, Vermont Department of Motor Vehicles records, VIBRS and Mobile Data Computer equipped cruisers as well as those computers utilizing compatible messaging services

The Colchester Police Department Mobile Data Computer System utilizes software that allows members in the field direct access to NLETS, VLETS, and NCIC information. Members could also have access to all RMS related tables, the department e-mail system, as well as several other applications deemed appropriate to meeting the needs of the department. The system has been designed to give the members in the field timely access to essential information using wireless computer network and application software. This information will be made available to the member without the need for voice interaction with the Colchester Police communication specialist.

II. DEFINITIONS:

A. Cellular Digital Packet Data (CDPD) – a method of data transmission used by VWIN which uses standard Internet Protocol.

B. Vermont Wireless Information Network:

1. VWIN is a wireless mobile data network for interested state and local Vermont government agencies which provide access to:

- VIBRS (Vermont Incident Based Reporting System)

- NCIC (National Crime Information Center)

- NLETS (National Law Enforcement Telecommunications System)
- SPIN (State Police Intelligence Network)

2. VWIN uses mobile data computers to send and receive encrypted and compress data.

3. VWIN is managed and supported by the Vermont Department of Public Safety.

4. VWIN cellular modems – CDPD modems which can be inserted into PCMCIA slots or imbedded in commercial laptops and MDC's

The scope of this policy is to define the minimum requirements that need to be implemented to ensure protection of CJIS data.

C. Mobile Data Computer (MDC) – A laptop or fixed mount version of a personal computer capable of running on battery power alone, including a car battery.

1. Mobile Data Computer (Includes integrated CDPD modem, external keyboard, external monitor and in most cases external speakers.

D. MDC System – The following equipment compromises a complete MDC system:

- in-car printer
- external antenna
- docking and mounting hardware
- software

III. SCOPE: This policy applies to employees, contractors, consultants, temporary staff, and other workers at the Colchester Police Department, including all personnel affiliated with NCIC and third parties. This policy applies to all equipment that is owned or leased by this agency.

IV. PROCEDURES:

A. Security

1. The security of the system will be the concern of all users. All NLETS/VLETS/NCIC/VIBRS/SPIN rules and regulations regarding use and disclosure of information are in full effect when operating Mobile Data Computers. The computers have been designed with both a Windows log on and password prompt as well as two factor authentication utilizing an installed soft token application requiring log-on identification/password

The connecting system will use a minimum of 128 bit encryption as required by CJIS policy. The connection system that the Colchester Police Department currently uses 128 bit encryption.

2. The person who is using the computer is responsible for insuring the security of the computer against unauthorized use. The MDC computers will not be access by anyone other than sworn agency members or authorized department representative/Agency of Digital Services Employees.

3. Each MDC is configured with a screen saver, which activates after ten minutes of inactivity. This will prevent unauthorized viewing of information on the MDC monitor.

4. Each cruiser that is equipped with a laptop will have a docking station which is lockable. When the computer is docked in the vehicle, the lock will be utilized. The keys to the lock will not be left in the lock when the computer is docked.

5. All information obtained via the MDC computers will be treated as CONFIDENTIAL and used for authorized law enforcement or criminal justice purposes only.

6. Should any of the following occur, or it is believed that it might have occurred, the member shall immediately contact the Deputy Chief of Police:

   - An unauthorized access was attempted or occurred;
   - A security breach has occurred (i.e. sensitive or confidential data has been compromised)
   - The computer has been lost or stolen

   All officers shall comply with all other Colchester Police Department Rules and Regulations regarding the loss of/or damage to equipment.

7. No confidential material will be stored on the mobile computers. All personnel will ensure that prior to the end of their shift that all sensitive or confidential data received during the shift is deleted and/or destroyed. Any paper copy of any e-mail, instant message or message received from VLETS/NLETS will be shredded as per the NCIC policy.

8. Anti-virus is in place on all Mobile Data Computers. The software must be managed in compliance with CJIS antivirus guidelines.

B. Messaging

1. MDC messaging is defined as any message sent or received from one computer to another, such as car to car, car to VLETS, VLETS to car, office pc to car or interface with CAD/RMS law enforcement records.

2. MDC messaging, CAD (Computer Aided Dispatch) messages, CAD calls and CAD access via the Verizon Air Cards are subject to the following restrictions:

   - The message shall have a reasonable communicative purpose.

   - Messages must be authored in a professional business-like manner, which would be considered acceptable as public record.

   - Messages used for personal communication to Dispatch or car to car are allowed as long as the needs of the citizens, members and co-workers are attended to first and the content is in keeping with the professionalism dictated by this policy. Personal or chat type messages between dispatch and field units or car to car, are not permitted unless directly job related.

   - The communication shall not be used to harass, annoy or alarm any recipient or third party.

   - The communication shall not contain language, acronyms or symbols representing language that would be considered offensive or obscene to a reasonable member of the public.

   - The content shall not bring discredit to any public safety employee (including co-workers) or public safety agency.

   - The content shall not bring unwarranted discredit to a member of the public.

   - The communication shall not contain any home address or telephone number of law enforcement personnel unless that employee has given express permission to transmit the information.

   - The communication shall not contain any slanderous statements toward any group, organization or individual.

   - Field units should clearly understand that information viewed and obtained is similar to other VLETS/NCIC information and any information received via the MDC shall be kept confidential.

3. MDC messages, CAD messages and CAD calls may be public record. They are logged by the Vermont Department of Public Safety system, including sender and receiver information, are archived as public record and available to the public. Any request for information that could be considered a public record should be referred to the department's records section. This does not preclude a field user from using information provided by the MDC to satisfy legitimate law enforcement purposes.

C. Maintenance / Repairs

The system design is integrated between VWIN and VLETS. System failures shall be the responsibility of the Deputy Chief of Police. He/She will provide assistance and guidance in maintaining the function of the vehicle mounted computers. System failures shall be reported through the proper chain of command. Members will utilize the radio system as apposed to the cellular telephone when the MDC computer and/or system are down.

1. Members are required to notify the Deputy Chief of Police when the MDC computer is not functioning properly. The computer will then be taken out of service until replaced/repaired.

   - The Deputy Chief of Police will be responsible for handling hardware and replacement of MDC computers.

   - The Agency of Digital Services will be responsible for handling VLETS software related problems.

   - The Colchester Police will be responsible for handling Records Management Software related problems with the appropriate provider or vendor.

D. Care and Use

1. The cruiser will remained locked at all times when not in use.

2. Nothing should be placed on top of the MDC or its components, especially any foods or drinks.

3. No software or material will be loaded into the MDC without prior approval from the Chief of Police or his/her designee.

4. Recommendations dealing with changes or improvement should be brought to the Deputy Chief of Police.

5. The MDC will not be used while the car is in motion unless the vehicle is in operation with two members. In either case, members are to call in to dispatch when leaving your assigned EQ (i.e., motor vehicle stops) Members, while utilizing the vehicle mounted MDC computers, shall be mindful of their safety at all times. Members shall position themselves to observe the stopped motorist and/or occupants at all times while entering data into the MDC. Members will take proper precaution to insure that person(s) who are unauthorized to do so do not view any confidential or sensitive material.

6. Members whose vehicles are not being used for an extended period of time will notify their supervisor to remove the laptop and store it in the office.

7. Temperature Considerations

A. When temperatures exceed 80 degrees, the rear window of the cruiser should be lowered ½ inch.

B. During the winter months and when the temperature is below 40 degrees, the cruiser should be warmed up to a temperature above 40 degrees prior to turning on the MDC.

V. ENFORCEMENT:

1. Agencies and users of Mobile Data Computers shall adhere to this policy and any other mandatory rule, policy or procedure or could be sanctions by this agency or the Department of Public Safety, Agency of Digital Services staff.

2. Sanctions could result in a loss of privileges (disconnection) by the user. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment pursuant to the Colchester Police Department's rules and regulations.

3. The Colchester Police Department or designee may impose emergency sanctions, including disconnection, if they believe there is a security threat sufficient to warrant such action.

#