BRAINTREE POLICE DEPARTMENT
Policy and Procedure

Information Technology and Data Security

2019-73

Date of Issue: 06/10/2019 Review Date : Revised:	Issuing Authority: Chief Paul Shastany
Certification Standards: Accreditation Standards: **11.4.4; 41.3.7 a-b; 82.1.6 a-d** Optional Accreditation Standards:	

Purpose

The purpose of this policy is to communicate to all Town of Braintree employees their responsibilities for proper use of Town information technology systems and resources, including computers, telephones, pagers, facsimile (fax) machines, voice mail, e-mail, Internet and intranet services. This policy will ensure that use of these resources is consistent with general Town policies, applicable laws and position responsibilities.

Policy

The Town of Braintree provides information technology communications systems and resources to employees for business purposes. All such systems and resources, and all communications and data transmitted by, received from, or stored in these systems, are the property of the Town, and may be accessed and retrieved by the Town at any time, when deemed appropriate. Therefore, employees should have no reasonable expectation of privacy in e-mail transmitted, received and stored on and/or through the Town's system.

Employees are prohibited from using the Town's information technology resources for anything other than Town business purposes. Unacceptable use of such resources includes, but is not limited to: infringing on any intellectual property rights; intercepting communications intended for other persons; accessing or sharing sexually explicit or obscene materials; propagating computer viruses or other harmful programs; distributing chain letters; furthering any

illegal act; or engaging in any other activities for purposes unrelated to the user's job.

The Town retains the right to review, audit, intercept, assess, and disclose all messages created, received or sent over the electronic mail system as necessary. Reasons for such actions include, but are not limited to: system maintenance; preventing or investigating allegations of system abuse or misuse; compliance with legal or regulatory requests for information; and ensuring that the Town's operations continue appropriately during an employee's absence.

Each individual user is responsible for complying with this and all other relevant policies when using Town information technology resources. Use of these same resources in violation of this policy or other applicable Town policies may result in disciplinary action.

Procedure

Internet and E-mail Access

Access to the Internet and Internet E-mail will be granted to employees with a legitimate business need. In order for an employee to access the Internet, the Information Technology Department must receive prior written authorization from the appropriate Department Head.

Management and Administration of Internet Usage

The Town has the capacity to record each Web access, chat, newsgroup, or e-mail message, as well as each file transfer into and out of the network. Internet activity will be monitored and analyzed to assure adherence to Town policies.

Internet facilities and computing resources must not be used knowingly to solicit, harass or otherwise offend, or for any unsuitable or unlawful purpose. Therefore, employees are prohibited from sending e-mail messages containing sexual implications, racial or gender slurs, or any comment that offensively addresses creed, age, disability, veteran status or any other characteristic protected by federal, state, or local law. The display of any kind of sexually explicit image or document on any Town system is a violation of the Town's Discriminatory Harassment in the Workplace Policy. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using the Town's network resources. Use of any Town resource for illegal activity will result in discipline, up to and including discharge.
The Town of Braintree uses independently supplied software to identify inappropriate or sexually explicit Internet sites. The Information Technology Department at Braintree Electric Light Department (BELD) will attempt to block access of all known sites. If

an employee accidentally discovers a connection to one of these sites, he/she must disconnect immediately and should report the situation to BELD by opening a Help Desk Ticket.

Any software and/or files downloaded via the Internet into the Town's network will become the property of the Town of Braintree. Any such file and/or software is limited to use consistent with respective licensing and applicable copyrights. In addition, these files must be scanned for virus infection before use.

No employee may use Town facilities knowingly to download or distribute pirated software or data.

Employees are prohibited from installing software or other files or manipulating or altering of current software running on town-owned computers, mobile, desktop or handheld computers with the permission of BELD. **[41.3.7 a,b]**

No employee will transfer software, unauthorized or unlicensed, or data from any source, including any on-line sources, into any department computer and/or workstation without approval of BELD. **[11.4.4]**

Braintree Police personnel shall not, on their own without proper authorization and support, alter their user access level or permission, attempt to access services not specifically allowed, deprive other authorized users of resources or access, or any way intervene in the operation and function of software, hardware, or services. Users will not alter the user interface, functionality, or capacity of the software or equipment, nor will they install or attempt to install additional software; including both unauthorized and unlicensed software. **[41.3.7a, b] [11.4.4]**

No employee may use the Town's Internet facilities to deliberately propagate any virus, worm, Trojan horse or trap door program code.

Only those employees or officials who are authorized to speak to the media or to public gatherings on behalf of the Town of Braintree may speak/write in the name of the Town to any newsgroup or chat room. Other employees may participate in newsgroups or chats in the course of business only when relevant to their duties but they must do so as individuals speaking only for themselves. Employees must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the Town of any commercial product or service.

The Town of Braintree retains copyright to any material posted to any forum, newsgroup, chat or Internet web page by any employee in the course of his/her duties.

No employee, contractor, or other agent working for the Town of Braintree shall use the Town's Internet facilities to perform duties for their own outside business.

Technical

User ID's and passwords must be used for Internet resources. The Town of Braintree policy prohibits the sharing of User ID's or passwords to access the Internet or e-mail.

BELD maintains an automated quality control system for such passwords which conducts an audit of personnel passwords at least once a year. **[82.1.6. d]**

Employees should schedule large file transfers or mass mailings for off-peak times.

Security

The authority has installed proxy servers and software to assure the safety and security of its networks. Any employee who attempts to disable, defeat, or circumvent any Town security facility may be subject to discipline up to and including immediate discharge.

Employees are reminded that it is against Town of Braintree policy to reveal confidential Town information. Files containing Town-Sensitive data that is transferred in any way across the Internet must be encrypted.

Computers that use modems to create independent Internet connections sidestep the Town's network security mechanisms and threaten the security of internal networks. Attackers can use such private connection to breach security.

Only those Internet services and functions with documented business purposes for the Town will be enabled at the Internet firewall.

Social Networking sites may not be accessed by employees on Town-owned computers.

Cell Phones

Town issued cell phones shall be used for Town business only.

Employees may not text while driving a vehicle under any circumstances.

Employees should refrain from talking on the cell phone while driving unless it is unavoidable. Whenever possible, pull over safely to use the cell phone.

Data Backup

Data Files, such as word processing, e-mail, spread sheets, will be backed up if they are stored on the Department server. Backup of data not stored on the server is the responsibility of each user. The department cannot be held responsible for lost data due to system failure caused by power outage or other problems with the system that may cause an unexpected shutdown. **[82.1.6 a]**

BELD is responsible for backing up all department computer files on a computer server located at the police station in the computer room. Such files are backed up daily. This data is then transmitted to a server located at BELD. Access to the both rooms and servers is limited to authorized personnel. **[82.1.6 a-c]**

Network Security

Network security is the responsibility of all users. Employees may use the police department network only for legitimate purposes. Servers and routers are located within the Braintree Police Department and at BELD. Access to the servers is limited to BELD IT personnel, the Chief of Police and personnel authorized by the Chief of Police or his/her designee. **[82.1.6 b-c]**

Supervised access to the network by vendors and contractors may be allowed on an as need basis and only with permission of the Chief of Police or his/her designee.

Laptops installed in police vehicles and the servers in the Communication Center are to be used only for the police purposes. Unprofessional comments will not be transmitted from them. This department and other agencies keep a record of transmissions. No software may be loaded on this system without authorization of the person in charge of computers. Use of any disk or CD not authorized is strictly forbidden. **[41.3.7 a]**