Appendix H

Acceptable Use of Town Computer Equipment Policy

1. Overview

The Town of New Paltz's intentions for publishing an Acceptable Use of Town Computer Equipment Policy are not to impose restrictions that are contrary to the established culture of openness, trust, and integrity. The Town of New Paltz is committed to protecting their employees, partners, and the municipality from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the Town of New Paltz. These systems are to be used for business purposes in serving the interests of the municipality, and of our constituents and taxpayers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Town of New Paltz employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the Town of New Paltz. These rules are in place to protect the employee and the Town of New Paltz. Inappropriate use exposes the Town of New Paltz to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct the town's business or interact with internal networks and business systems, whether owned or leased by the Town of New Paltz, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at the Town of New Paltz and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Town of New Paltz policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Town Hall, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Town of New Paltz.

4. Policy

4.1 General Use and Ownership

4.1.1 The Town of New Paltz proprietary information stored on electronic and computing devices whether owned or leased by the Town of New Paltz, the employee or a third party, remains the sole property of the Town of New Paltz. You must ensure through legal or technical means that proprietary information is protected.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of the Town of New Paltz proprietary information.

4.1.3 You may access, use, or share the Town of New Paltz proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on

personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within the Town of New Paltz may monitor equipment, systems, and network traffic at any time.

4.1.6 The Town of New Paltz reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

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

4.2.3 Postings by employees from a Town of New Paltz email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Town of New Paltz, unless posting is in the course of business duties.

4.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.2.5 All town hall servers will be remotely backed-up daily and stored off-site.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of the Town of New Paltz authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Town of New Paltz-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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

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

3. Accessing data, a server or an account for any purpose other than conducting the Town of New Paltz business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others.
7. Remote access to town computer/server.

Using the Town of New Paltz computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any the Town of New Paltz account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Town of New Paltz is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Town of New Paltz network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. 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.
17. Providing information about, or lists of, the Town of New Paltz employees to parties outside the Town of New Paltz.

4.3.2 Email and Communication Activities

When using government resources to access and use the Internet, users must realize they represent the municipality. Whenever employees state an affiliation to the municipality, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the municipality".
Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

1. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
2. Unauthorized use, or forging, of email header information.
3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of anytype.

5. Use of unsolicited email originating from within the town's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any servicehosted by the Town of New Paltz or connected via the town's network.

6. Posting the same or similar non-business-related messages to large numbers ofUsenet newsgroups (newsgroup spam).

4.3.3 Social Media

1. Employees shall not engage in any social media activity that may harm or tarnish the image, reputation and/or goodwill of the Town of New Paltz and/or any of its employees.Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when engaging in social media activity or otherwise engaging in any conduct prohibited by the Town of New Paltz's *Anti-Harassment* policy.

2. Employees may also not attribute personal statements, opinions, or beliefs to the Town ofNew Paltz when engaged in social media activity. If an employee is expressing their beliefs and/or opinions on social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Town of New Paltz. Employees assume any and all risk associated with social media activity.

3. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the Town of New Paltz's trademarks, logos and any other theTown of New Paltz intellectual property may also not be used in connection with any social media activity.

5. Policy Compliance

5.1 Compliance Measurement

The Town of New Paltz Town Board will verify compliance to this policy through various methods, including but not limited to, internal and external audits, and feedback through/by/tothe IT consultant.

5.2 Exceptions

Any exception to the policy must be approved by the Town of New Paltz Town Board inadvance.

5.3 Non-Compliance

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

Signature: _____ Date: _____