Oneida County
Information Technology Acceptable Use Policy
Adopted by the Oneida County Board of Legislators
March 8, 2017

1. Overview

All Oneida County electronic communications systems, including, but not limited to wired/ wireless/smart telephones, desktop/laptop/tablet computers, facsimile machines, copy machines, network file servers, network or system peripherals, computer data and program files, e-mail and Internet accessibility, as well as software furnished to employees are to be used for **business purposes only.**

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Oneida County. This policy also addresses unacceptable use. These rules are in place to protect the User and Oneida County. Unacceptable or inappropriate use of County resources exposes Oneida County to security risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information (data), electronic and computing devices, and network resources to conduct Oneida County business or interact with internal networks and business systems, whether owned or leased by Oneida County, New York State, the User, or a third party. All Users with access to the County network and County data are responsible for exercising good judgment regarding appropriate use of information (data), electronic devices, and network resources in accordance with Federal and State law as well as Oneida County policies, collective bargaining agreements, and local laws and regulation.

This policy applies to all Users of the Oneida County Network, New York State Network/Applications and Sheriff's Department Network working at Oneida County. Any person, organizational entity, or automated process that accesses a County system for legitimate government purpose, as authorized by the County of Oneida, including but not limited to employees, contractors/vendors, consultants, temporaries, all personnel affiliated with third parties and other workers at Oneida County, including but not limited to employees, contractors/vendors, consultants, temporaries, all personnel affiliated with third parties and other workers at Oneida County, shall be considered Users. This policy applies to all equipment that is owned or leased by Oneida County, New York State or any third party including User owned equipment being used in conjunction with any County network and any business related activity.

4. Policy

4.1 General Use and Ownership

4.1.1 Oneida County routinely issues desktop and mobile equipment/devices to Users to facilitate performance of job duties. This equipment includes but is not limited to desktop and laptop Personal Computers (PCs), tablet PCs, printers, wireless devices such as phones and hot spots as well as RSA tokens and external storage devices. All equipment used for Oneida County business purposes, whether leased or owned by Oneida County or New York State is considered the property of Oneida County and must be immediately surrendered to the cognizant County IT department by the User upon separation from the County or when requested to do so by the User's Department Head or the Oneida County Chief Information Security Official (CISO).

4.1.2 At no time may any User save or store County data, including but not limited to word documents, databases, images, voice/video records etc. to a device owned by an entity other than Oneida County or New York State. Use of non-County or non-State owned equipment to conduct County business is subject to the approval of the Department Head and the CISO. Users who wish to use any computing device not owned by the County or State to access County email or data must contact the Department Head and the cognizant County IT department to ensure appropriate approvals and access controls are implemented. Non-County and non-State devices used to conduct County business must be brought to the cognizant County IT prior to User separation from the County to ensure no County data resides on the device.

4.1.3 It is the responsibility of the User to promptly report the theft, loss or unauthorized use of Oneida County wireless or computing equipment or peripherals to the cognizant County IT department.

4.1.4 It is the responsibility of the User to maintain all computing and wireless equipment

issued by the County in good working order. Mobile devices are to be kept charged and ready to use in an emergency. Software patches and updates to all equipment are to be made promptly. Assistance with patches and updates to mobile devices is available by contacting the cognizant County IT department.

4.1.5 It is the responsibility of the User to promptly report damage to equipment.

4.1.6 It is the responsibility of each User to promptly report the theft, loss or unauthorized disclosure of Oneida County proprietary information.

4.1.7 Users may access, use or share County data only to the extent it is authorized and necessary to fulfill assigned job duties. Access to data for unauthorized purposes is strictly forbidden.

4.1.8 For security and network maintenance purposes, authorized individuals within Oneida County may monitor equipment, systems, data and network traffic at any time. Users shall have no expectation of privacy regarding the use of any Oneida County electronic communication systems, devices or resources. Oneida County intends to monitor all electronic communication systems including but not limited to computer files, email and Internet use without prior notice to Users. Monitoring pursuant to this policy of any and all electronic communications, computer files, email or Internet usage within a department which is subject to a legally recognized privilege or confidentiality requirement shall be done only by the Department Head or IT personnel authorized by the CISO.

4.1.9 Oneida County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.1.10 Oneida County may restrict or discontinue access to some or all Internet resources at any time without prior notice to individual Users. Any such restrictions put in place by the cognizant County IT department, and the necessity therefore, shall be discussed with the Department Head.

4.2 Security and Proprietary Information (data)

4.2.1 All mobile and computing devices that connect to the County or Sheriff's network must be entered into a Mobile Device Management System.

4.2.2 System level and User level passwords must comply with the Oneida County Password Policy. Providing network access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices including both mobile and desktop units must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.

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

4.2.5 Users must use extreme caution when opening email attachments or clicking on web links as they may contain malware. Users must immediately contact their cognizant County IT department for assistance if they believe they have mistakenly opened an email or clicked a link containing malware.

4.3 Unacceptable Use

The following activities are prohibited. Select Users may be exempted from these restrictions during the course of their legitimate job responsibilities (i.e. network 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 any User of Oneida County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Oneida County-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 company 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 Oneida County.

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 Oneida County or the end User does not have an active license is strictly prohibited. Oneida County prohibits the illegal duplication of software and documentation. Privately owned or non-standardized software may not be installed on any Oneida County computer or network without the written approval of the Department Head and the CISO. Accessing data, a server or an account for any purpose other than conducting Oneida County business, even if you have authorized access, is prohibited.

3. Users are not permitted to use any code or password issued to another employee in order to access, view or retrieve information from any computer, network file server, network or system peripheral, email account, Internet site, computer or program file either inside or outside the County's or Sheriff's network system.

4. Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes Information Technology staff, supervisors, co-workers as well as family and other household members when work is being done at home. Sharing of passwords is strictly prohibited in all cases.

6. Using an Oneida County computing asset (data, device or other component of the IT environment) 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.

7. Making fraudulent offers of products, items, or services originating from any Oneida County account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User 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 (data) for malicious purposes.

10. Port scanning or security scanning is expressly prohibited without prior written approval from the CISO.

11. Executing any form of network monitoring which will intercept data not intended for the User's host, unless this activity is a part of the User's normal job/duty.

12. Circumventing User authentication or security of any host, network or account.

13. Introducing honeypots, honey-nets, or similar technology on the Oneida County network.

14. Interfering with or denying service to any User other than the User's host (for example, denial of service attack).

15. 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.

16. Providing information (data) about, or lists of, Oneida County Users to parties' outside Oneida County.

17. 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).

18. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

19. Unauthorized use, or forging, of email header information.

20. 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.

21. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

22. Use of unsolicited email originating from within Oneida County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Oneida County or connected via Oneida County's network.

23. Users shall not download, view, store or forward pornographic images or any other obscene materials, with the exception of any such materials deemed necessary and appropriate for the specific work purpose as determined by the Department Head.

24. Oneida County prohibits the use of computers, email, Internet, wireless or any other electronic communication system in ways that are disruptive, offensive or harmful to others. Therefore, sexually explicit messages, cartoons and jokes are prohibited. This misuse shall also include, but is not limited to ethnic slurs, racial comments, off-color jokes or anything which may be construed as harassment, disrespect of others or may lead to the creation of a hostile work environment.

25. Oneida County's electronic communications systems may not be used by any User for the purposes of soliciting contributions or funds or benefits of any kind for private, not for profit or policy agency, cause, project or fundraising activity.

5. Misc.

Conflicting provisions contained in collective bargaining agreements, to the extent required by law, shall supersede this Policy. Where collective bargaining agreements are silent, this Policy may be applied. In the event that any provision of this Policy or application thereof shall be held invalid, this act shall not be construed to affect the validity of any other provision, or application thereof of this Policy.

Any violation of this policy may result in prosecution under Federal, New York State or Local Law as well as disciplinary procedures as set forth in labor agreements or under Section 75 of the Civil Service Law.

Printed Name: _____

Signature: _____

Date: _____