Title 2. Employment – Chapter 215
Technology Resources Law
Rule #001 – Acceptable Use

1.1 Purpose and Authority

1.1-1. *Purpose.* The purpose of this rule is to provide guidelines and techniques to promote effective use of the Nation's Digital Technology Systems. It applies to all of the Nation's systems located on, or accessed from, Nation properties and systems provided by the Nation for use in the Nation's business.

1.1-2. *Policy.* It is the policy of the Nation to provide sophisticated computer and communications systems to support official business activities, enabling effective and timely communication among staff, customers, partners, and vendors. This rule establishes expectations for all staff regarding the access, use, and disclosure of information via the Nation's Information Systems, which are to be used solely for official business purposes in accordance with these guidelines and other relevant policies.

1.1-3. *Authority.* The Technology Resources Law delegates rulemaking authority to the Digital Technology Services Department pursuant to the Administrative Rulemaking law.

1.2. Adoption, Amendment and Repeal

1.2-1. This rule was adopted by the Oneida Business Committee in accordance with the procedures of the Administrative Rulemaking law.

1.2-2. This rule may be amended or repealed by the Digital Technology Services Department and/or the Oneida Business Committee pursuant to the procedures set out in the Administrative Rulemaking law.

1.2-3. Should a provision of this rule or the application thereof to any person or circumstances be held as invalid, such invalidity shall not affect other provisions of this rule which are considered to have legal force without the invalid portions.

1.2-4. In the event of a conflict between a provision of this rule and a provision of another rule, internal policy, procedure, or other regulation; the provisions of this rule shall control.

1.2-5. This rule supersedes all internal department rules, regulations, policies, or other requirements relating to acceptable use as referenced in the Technology Resources Law.

Commented [SH1]: This rule supersedes all internal department rules, regulations, policies or other requirements and supplements the acceptable use referenced in the Technology Resources Law.

Commented [CL2]: This rule cannot supersede or conflict with the Technology resources law.

1.3. Definitions

1.3-1. This section shall govern the definitions of words and phrases used within this rule. All words not defined herein shall be used in their ordinary and everyday sense.

(a) "Nation" means the Oneida Nation.

(b) "Confidential data" means any information that the Nation is obligated by law, policy, or regulation to protect from unauthorized access, use, disclosure, modification, or destruction.

(c) "Personal use" means any technology resource use that is conducted for purposes other than accomplishing an authorized activity or official business of the Nation.

(d) "Technology resources" means any tools, systems, and applications that use technology to fulfill their purposes. Technology resources may include, but are not limited to, computers, tablets, telephones, facsimile machines, photocopiers, networks, virtual applications, and software, such as internet connectivity and access to internet services and electronic mail.

(e) "Staff" means any individual who uses the technology resources of the Nation, including but not limited to employees, independent contractor personnel, interns, members of boards, committees or commissions, volunteers, guests, and visitors.

1.4. Facilities and Equipment

1.4-1. The Nation maintains facilities, equipment, and communication systems (e.g., telephones, email, computers, fax machines) to enhance operational efficiency. These systems, provided at the Nation's expense, are for official business only. Access is granted based on job responsibilities, and use is subject to this rule.

1.4-2. Staff shall not remove equipment or software from the Nation's premises or use personal equipment for official business without prior express consent from the employee's senior level manager or director.

1.4-3. Alternate internet service provider connections to the Nation's network are prohibited unless approved by management and secured by appropriate security devices.

1.5 Information Access, Content, and Use

1.5-1. *Technology and Resources*. The Nation invests in advanced technology to support official business. All staff with access to technology resources shall read, understand, and comply with this rule.

15-2. *Business Use*.

(a) Information Systems are owned by the Nation and shall be used exclusively for business purposes, serving customer interests, and supporting normal operations.

(b) Staff decisions to use these systems should be based on sound business practices, reducing costs, or improving services measurably, while maintaining a professional image.

(c) Staff using the Nation's accounts act as representatives of the Nation and shall avoid damaging the organization's reputation.

1.5-3. *Acceptable Use*. Use of the Nation's facilities, equipment, or systems is limited to acceptable use as defined in this rule. Incidental personal use is permitted if it is not excessive, does not interfere with job performance, consume significant resources, or disrupt other staff activities, as determined by the Nation.

Commented [CL3]: Staff isn't defined - but employee and user are. Should employee or user be used instead?

Commented [CL4]: Use shall instead of must or will throughout law.

Commented [CL5]: Should staff be employee or user?

1.5-4. *Professional Conduct*. Staff shall conduct official business consistent with the Nation's mission and comply with tribal, state, and federal laws, maintaining standards of integrity, accountability, and legal sufficiency.

1.5-5. *Information Accuracy*.

(a) Staff shall disseminate current, accurate, complete, and compliant information.

(b) Information shared through technology resources shall be handled with the same level of care as other forms of communication. Users should ensure that content respects intellectual property rights, including copyrights, trademarks, and trade secrets.

(c) Staff using Internet information for strategic business decisions shall verify its integrity, ensuring the source is regularly updated and valid.

1.5-6. *Confidential and Proprietary Information*.

(a) Staff shall protect confidential and proprietary information.

(b) Questions regarding the appropriate use of technology resources or handling of information, staff should consult their area manager or director for guidance.

(c) Staff shall not discuss the Nation's business prospects, financial condition, or future products with third parties unless publicly disclosed by the Nation.

(d) Unauthorized disclosure of confidential or proprietary information may result in legal action.

1.5-7. *Public Accessibility*.

(a) Designated staff may make information publicly accessible after management review to verify accuracy and appropriateness.

(b) Publicly accessible information shall be periodically reviewed to remove inaccurate, inappropriate, or nonpublic content.

1.6. Protecting Confidential Information

1.6-1. *Importance and Procedures*. Maintaining confidentiality is critical to the Nation's success. Staff shall follow appropriate procedures to protect confidential information, exercising caution when communicating externally, as electronic communications are not fully secure.

Commented [CL6]: What are the specific procedures?

1.6-2. *Data Classification*. Confidential data shall be marked with designations such as "Confidential," "Do not reproduce," or "Do not forward." Emails containing confidential information shall include "Confidential" in the subject line.

Commented [CL7]: What constitutes confidential data?

1.6-3. *Access Restrictions*.

(a) Access to directories containing sensitive or confidential data is restricted.

(b) Unauthorized attempts to bypass restrictions, including hacking, violate this rule and may lead to disciplinary action, including termination or legal action. Hacking may also violate the Federal Electronic Communications Privacy Act (18 U.S.C. 2510).

1.6-4. *Privacy of Communications*. Staff shall respect the privacy of messages received, securing voicemail and email accounts with proper password protection, closing messages after reading, and deleting unnecessary messages.

1.6-5. *Internet Privacy*.

(a) The internet does not guarantee privacy. Staff shall exercise caution when transferring sensitive material online by using secure methods (e.g., encrypted channels, approved platforms) and avoiding public or unsecured networks. This helps prevent unauthorized access or third-party interception.

(b) Staff shall not place the Nation's materials—such as copyrighted software, internal correspondence, or other proprietary content—on publicly accessible internet-connected devices or platforms without prior approval from their area manager or director.

1.7. Copyrighted Information

1.7.1. *Intellectual Property Rights*.

(a) The Nation respects intellectual property rights. Staff shall comply with license terms for copyrighted material (e.g., literature, software, graphics) and not assume availability on electronic systems permits downloading or dissemination.

(b) Unauthorized or illegal use of third-party intellectual property, including downloading copyrighted software, video, or audio clips, is prohibited.

(c) Employees/users shall consult with management if unsure about use of third=party intellectual property.

1.7-2. *Trademark and Copyright Notices*.

(a) The Nation's trademarked or copyrighted material shall be properly marked.

(b) Staff shall not remove third-party trademark or copyright notices.

1.7-3. *Software Use*.

(a) Software use shall comply with the Nation's licensing agreements.

(b) Copying software, loading personal software, or downloading Internet software without permission is prohibited.

(c) Software and firmware shall be digitally signed using a recognized, approved certificate.

(d) All Nation-owned software remains with Nation upon staff departure.

1.8. Privacy and Monitoring

1.8-1. *Expectation of Privacy*. Staff have no reasonable expectation of personal privacy regarding data, communications, or activities on the Nation systems, which may be monitored, accessed, or reviewed by authorized personnel without notice to ensure compliance with policies, legal requirements, and security protocols.

1.8-2. *Monitoring and Inspection*.

(a) The Nation reserves the right to access, inspect, or search all Information Systems, including directories, files, emails, and communication systems, without prior notice. Monitoring may occur to:

(1) Prevent transmission of discriminatory, harassing, or offensive messages.

(2) Detect illegal material or unlicensed software.

(3) Ensure communication tools are not used for unauthorized or disruptive purposes.

(4) Investigate allegations of impropriety.

(5) Access information in staff absence.

(6) Respond to legal proceedings or court orders. Staff refusing to cooperate with legitimate inspections or provide passwords may face disciplinary action, including termination. The Nation may restrict or cancel staff access to systems at any time.

1.8-3. *System Ownership*.

(a) All messages, data, and applications on Information Systems are Oneida Nation property, subject to third-party intellectual property rights.

(b) The Nation may access, review, copy, delete, or disclose data for legitimate business purposes.

1.9. Storing and Archiving Information

1.9-1. Electronic data is subject to routine backups and archival procedures, retaining copies for extended periods. Deleting data does not ensure privacy, as archives remain property of the Nation and may be used for business purposes.

1.9-2. Staff may need to preserve data for litigation or investigations per the Data Retention Rule. Staff shall regularly delete or archive files to manage disk space, avoiding large file transfers during prime hours to minimize network impact.

Commented [CL8]: Is this existing, or a rule that is going to be drafted?

1.10. Employee Usage

1.10-1. *Compliance*. Staff shall comply with this rule. Violations of this rule may result in disciplinary action, including termination or legal action.

1.10-2. *Prohibited Activities*.

(a) Personal use of technology resources for financial gain or soliciting for non-business purposes (e.g., political, religious causes) is prohibited.

(b) Inappropriate use of technology resources includes accessing, storing, or transmitting sexually explicit, illegal, or disruptive materials (e.g., defamatory, obscene, or harassing content)

(c) Sending threatening, slanderous, or anonymous messages, or misrepresenting identity, is prohibited.

(d) Staff shall not copy or transfer files without permission, disable virus protection, circumvent security mechanisms, or share confidential information externally.

(e) Staff shall cooperate with authorized investigations.

(f) If offensive material is accessed, staff shall disengage immediately.

(g) The Nation is not responsible for offensive content on external servers.

1.10-3. System Awareness. Staff shall:

(a) Protect equipment from food and/or drink and know fire suppression equipment locations.

(b) Keep unauthorized people away from equipment and data. Question strangers in areas.

Commented [CL9]: What does this mean exactly?

(c) Report security violations, including unauthorized data changes or loss, to management immediately.

1.11. Email Etiquette

(a) Email is for official business. Use of the Nation's accounts for personal email use should be limited to occasional use.

(b) Staff shall:

(1) Use descriptive subject lines and include contact information in signatures.

(2) Acknowledge receipt of important emails, even if unable to respond immediately.

(3) Delete read or sent emails to conserve storage.

(4) Avoid sending unnecessary or large emails to preserve network resources.

(5) Refrain from harassing, offensive, anonymous, or all-caps messages, avoiding terse or rude tones.

(6) Proofread messages, prioritize appropriately, and send to relevant recipients only.
(7) Exercise caution with unencrypted emails and attachments, as email is generally not secure.
(8) Reply carefully, avoiding unintended "Reply all," and consider sender's intentions before forwarding.

1-12. Enforcement

1.12-1. Violations of this rule may result in disciplinary action, up to and including termination, and potential legal action.

1.13. References

1.13-1. References include:

(a) COBIT APO01.02, APO01.11, APO07.03, APO07.05, APO13.01, APO13.02, DSS04.05
(b) GDPR Article 32
(c) HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv)
(d) ISO 27001 7.3, A.5.4, A.5.10, A.5.12-13, A.6.3-4, A.8.16
(e) NIST SP 800-37 3.3
(f) NIST SP 800-53 AT-3.2, CA-3.4, PS-3.16
(g) NIST Cybersecurity Framework ID.AM-6, ID.GV-2, DE.DP-2
(h) PCI 12.1.1

End.

Original effective date: [add effective date established by authorized entity] (Certified by LOC on)