Title 2. Employment – Chapter 215
TECHNOLOGY RESOURCES LAW
Rule #008 – Third Party Providers

8.1 Purpose and Authority

8.1-1. Purpose**.** Third party service providers are integral to supporting Oneida Nation's infrastructure and information services. In some cases, these providers may collect, store, and maintain Sensitive Information. This rule establishes guidelines to limit and control third party service providers to minimize risks such as revenue loss, liability, loss of trust, and embarrassment to Oneida Nation, while ensuring the responsible use of company information and resources.

8.1-2. Authority**.** The Technology Resources Law delegates rulemaking authority to the Digital Security Department pursuant to the Administrative Rulemaking law.

8.2 Adoption, Amendment and Repeal

8.2-1. This rule was adopted by the Oneida Nation Business Committee in accordance with the procedures of the Administrative Rulemaking law.

8.2-2. This rule may be amended or repealed by the Digital Security Department and/or the Oneida Nation Business Committee pursuant to the procedures set out in the Administrative Rulemaking law.

8.2-3. 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.

8.2-4. 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.

8.2-5. This rule supersedes all prior rules, regulations, internal policies or other requirements relating to third party providers as outlined in the Technology Resources Law.

8.3 Definitions

8.3-1. 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) Third Party Service Provider: Any external entity contracted to collect, store, process, manage, or dispose of Oneida Nation's information.

(b) Sensitive Information: Confidential or proprietary data owned by Oneida Nation or its customers.

(c) Information Resources: DTS systems, networks, applications, and data managed by Oneida Nation.

(d) Digital Security Office: The department or personnel responsible for overseeing DTS operations and third party assessments.
(e) Cyber Security Risk Assessment (CSRA): A process of identifying, analyzing, and prioritizing potential threats and vulnerabilities to an organization's information systems, data, and digital infrastructure to reduce the likelihood and impact of cyberattacks.

8.4 Digital Security Office Responsibilities

8.4-1. The Digital Security Office shall ensure:

(a) Maintain a list of all third party service providers and their services as they relate to digital technology.
(b) Retain records of assessments and audits of third party service providers.
(c) Assign a DTS point of contact to ensure compliance with this rule.
(d) Monitor and enforce third party adherence to applicable Oneida Nation policies and agreements.
(e) Cyber security risk assessments are conducted during the purchasing process and repeated as necessary such as when the scope of products, services, or technology changes.

8.5 Scope

8.5-1. This rule applies to all Oneida Nation Staff responsible for reviewing, purchasing, installing, operating, or maintaining digital information resources, and to all third party service providers handling Oneida Nation information.

8.5-2. Third party service providers with remote or on-site access to Oneida Nation systems shall comply with this rule, regardless of location.

8.6 Third Party Service Provider Requirements

8.6-1. Due Dilligence.

(a) Prior to engagement, Oneida Nation Staff shall conduct due diligence on third party service providers, including background checks, business history, and experience with similar engagements.

8.6.2. Rule Compliance.

(a) Service providers shall comply with all applicable Oneida Nation policies, including but not limited to:

(1) Acceptable Use Rule
(2) Password Policy
(3) Vendor Remote Access Rule

8.6.3. Agreement Specifications.

(a) Agreements with service providers shall include:

(1) Confidentiality clauses protecting Oneida Nation and customer information.
(2) Controlled access to Information Resources.
(3) Methods for protecting Information Resources.
(4) Acceptable processes for return, destruction, or disposal of Oneida Nation information at agreement end.
(5) Restriction of information use to the purpose of the agreement only.
(6) Prohibition on using or sharing Oneida Nation information for other purposes.

(7) Defined service levels (SLA) and change control processes.

(b) Service providers shall notify Oneida Nation within five (5) working days of a security breach, with Oneida Nation reserving the right to terminate the agreement. If customer information is involved, the provider shall cover remediation costs, including customer notifications and one year of free credit monitoring.

8.6.4. Staff Management

(a) Service providers shall provide and update a list of staff working on Oneida Nation services within 24 hours of changes.

(b) On-site provider staff shall obtain and display Oneida Nation identification badges, returning them upon departure.

(c) Staff handling Sensitive Information shall be cleared and have access activated only when needed, deactivated post-service.

8.6.5. Access Controls

(a) Remote access aacounts shall be enabled only during use and disabled when not needed, with unique credentials per client.

(b) Access to Information Systems shall be monitored and comply with the Oneida Nation Password policy.

(c) Major activities shall be logged in the Third Party Service Provider Log, including personnel changes, password updates, and milestones.

8.6-6. Security and Incident Reporting.

(a) Service provider personnel shall report security incidents to Oneida Nation immediately.

(b) Incident management responsibilities shall be outlined in the agreement if applicable.

(c) Health information handling requires online and print descriptions of security and privacy safeguards.

8.6-7. Termination Procedures.

(a) Upon staff departure or agreement termination, Sensitive Information shall be returned or destroyed within 24 hours, with written certification provided.

(b) All Oneida Nation badges, access cards, and equipment shall be surrendered immediately, with exceptions documented by management.

8.6-8. Auditing and Ethical Use.

(a) Service providers shall comply with state and Oneida Nation auditing requirements.

(b) Agreements shall include security controls (e.g., encryption, access restrictions) to prevent data breaches or misuse.

8.7 Enforcement

8.7-1. Any Oneida Nation Staff member violating this rule may face disciplinary action, up to and including termination.

8.8. References

(a) COBIT APO09.05, APO10.05, APO12.02, APO13.07, BAI02.05-06, DSS01.05, DSS05.07

(b) GDPR Article 25, 26, 28, 32

(c) HIPAA 164.308(a)(1)(ii)(A), 164.308(b)(4), 164.502(b)(1), ARRA 13404(b), ARRA 13405(b)

(d) ISO 27001 8.1, A.8.12, A.8.21, A.8.30
(e) NIST SP 800-37 3.3, 3.7
(f) NIST SP 800-53 CM-4, IR-4, PM-30, PS-7, RA-9, SA-4, SA-10-12, SA-15, SA-17, SR-1
(g) NIST Cybersecurity Framework ID.AM-4-6, ID.BE-4, ID.RA-4, ID.RM-1, ID.SC-3-4, DE.CM-6
(h) PCI 12.5.2, A1.1.1, A2.1.2-3, PCI Software Security Framework

End.

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