Title 2. Employment – Chapter 215
TECHNOLOGY RESOUCES LAW
Rule #004 – Security Awareness Training

4.1 Purpose and Authority

4.1-1. *Purpose.* A robust security program necessitates that staff are trained in security policies, procedures, and technical controls. Oneida Nation staff who manage digital information shall possess the skills required for their roles. The aim of this Security Awareness and Training Rule is to ensure that security awareness and training measures safeguard Information Resources, maintaining their availability, confidentiality, and integrity.

4.1-2. *Authority.* The Technology Resources Law delegates rulemaking authority to the Digital Technology Services Department pursuant to the Administrative Rulemaking law.

4.2. Adoption, Amendment and Repeal

4.2-1. This rule was adopted by the Oneida Business Committee in accordance with the procedures of the Administrative Rulemaking law.

4.2-2. This rule may be amended or repealed by the Digital Technology Services Department and/or the Oneida Business Committee pursuant to the procedures set out in the Administrative Rulemaking law.

4.2-3. 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.

4.2-4. 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.

4.2-5. This rule supersedes all prior rules, regulations, internal policies or other requirements relating to security awareness training as outlined in the Technology Resources Law.

4.3. Definitions

4.3-1. 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) "Department" means the DTS Digital Technology Services department which is responsible for overseeing information security policies and procedures.

(b) Digital Security Office: The area designated to oversee the security of Digital Information Resources, ensuring the security program is well-supported with adequate resources and budget.

(c) Information Resources: Digital data and information systems that are used, managed, and protected by the organization.

Commented [RN1]: I thought DTS is Digital Technology Services Department

(d) Security Awareness and Training Plan (Plan): A documented strategy outlining the process for staff security training, education, and awareness to ensure they understand their roles and responsibilities in protecting Information Resources.
(e) Information Security Management System (ISMS): A systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process.
(f) Social Engineering Attacks: Manipulative tactics used by attackers to trick individuals into divulging confidential or personal information that may be used for fraudulent purposes. Examples include phishing, phone scams, and impersonation calls.
(g) BYOD (Bring Your Own Device): A Rule that defines the use of personal devices (such as smartphones, tablets, and laptops) for work purposes, which introduces specific security risks and responsibilities.
(h) Cloud Computing Security: Measures and protocols designed to protect data, applications, and services hosted in the cloud from threats and vulnerabilities. This includes addressing multi-tenant environments, nationality issues, and different cloud delivery models.
(i) Skills Gap Analysis: An assessment process to identify the difference between the skills required for a job and the actual skills possessed by employees. This helps in developing targeted training programs to bridge the gap.
(j) Secure Authentication: Methods used to verify the identity of a user, ensuring that only authorized individuals can access sensitive information. This includes passwords, biometrics, and multi-factor authentication.
(k) Security Incidents: Events that indicate a possible breach of information security policies or failure of safeguards, which may compromise the confidentiality, integrity, or availability of information resources.
(l) DTS Department: The department responsible for preparing and distributing information security manuals and ensuring staff are aware of security policies and procedures.

4.4. Requirements and Responsibilities

4.4-1. Management Responsibilities

(a) Oneida Nation management shall prioritize effective security awareness and training.
(a) Management shall implement a robust security program with a strong awareness and training component.
(b) The Digital Security Office shall be designated to oversee the security of Digital Information Resources.
(c) The Digital Security Office shall ensure the security program is well-supported with adequate resources and budget.

Commented [RN2]: Debatable if this is possible

4.4-2. Digital Security Office Responsibilities

(b) Develop, implement, and maintain a Security Awareness and Training Plan (Plan).
(c) Ensure the Plan documents the process for staff security training, education, and awareness.
(d) Ensure staff understand their roles and responsibilities in protecting Information Resources.

(e) Maintain continuous and engaging communication relevant to the information security management system (ISMS).

4.4-3. Training and Awareness:

(a) Provide regular training, reference materials, and reminders to staff.

(b) Training topics shall include:

(1) Oneida Nation's responsibilities for protecting Information Resources.

(2) Risks to Information Resources.

(3) Identifying social engineering attacks (e.g., phishing, phone scams).

(4) Secure use of Information Resources.

(5) Information security policies, procedures, and best practices.

4.4-4. Training Requirements:

(a) New users shall attend an approved security awareness training class within 90 days of being granted access to Information Resources.

(b) Staff shall receive role-specific training and verify their understanding and compliance.

(c) Staff shall be trained to identify, report, and prevent security incidents.

(d) Staff shall understand the importance of secure authentication and proper handling of sensitive information.

(e) Security policies, procedures, and manuals shall be readily available for staff reference.

(f) Staff shall attend annual security awareness training, with attendance records maintained.

(g) Staff shall sign an acknowledgment of understanding Oneida Nation's security policies and procedures.

4.4-5. Additional Training Components:

(a) The DTS Department shall prepare and distribute information security manuals.

(b) Cloud computing security awareness training shall address multi-tenant, nationality, and cloud delivery models.

(c) Staff shall be aware of BYOD risks and responsibilities.

(d) Staff shall understand actions for standalone, lost, and misplaced equipment.

4.4-6. Digital Security Office Duties:

(a) Conduct a skills gap analysis to identify training needs and develop an education roadmap.

(b) Maintain a communication process for new security programs and updates.

(c) Ensure staff responsible for implementing security safeguards receive formal training.

(d) Provide periodic security reminders to keep staff updated on threats and best practices.

(e) Collect and incorporate training feedback into future sessions.

4.5. Enforcement:

(a) Any Staff member found to have violated this rule may be subject to disciplinary action, up to and including termination.

4.6. References:

a) COBIT EDM01.03, APO02.08, APO07.12-13, APO12.02, APO12.07, APO13.07, MEA02.11
b) GDPR Article 25, 32
c) HIPAA 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(D)
d) ISO 27001 7.3, A.5.23, A.6.3, A.8.7, A.8.16
e) NIST SP 800-37 3.3, 3.4, 3.5, 3.7
f) NIST SP 800-53 AT-2, AT-3, CP-3, IR-2, PM-13, SI-3, SI-4(24), SR-1
g) NIST Cybersecurity Framework ID.GV-1, PR.AT-1-5, DE.DP-1, RS.RP-1, RS.MI-2
h) PCI 6.2.2, 9.1.1, 12.10.4, A3.1.4

End.

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