Title 2. Employment – Chapter 215
TECHNOLOGY RESOURCES LAW
Rule #002 – Clear Desk/Screen

2.1 Purpose and Authority

2.1-1. *Purpose.* To improve security and confidentiality, whenever possible for papers, digital storage devices, and screens which contain sensitive or confidential information.

2.1-2. *Authority.* The Technology Resources Law delegates rulemaking authority to the Digital Technology Services Department pursuant to the Administrative Rulemaking law.

2.2. Adoption, Amendment and Repeal

2.2-1. This rule was adopted by the Oneida Business Committee in accordance with the procedures of the Administrative Rulemaking law.

2.2-2. This rule may be amended or repealed by the Digital Technology Services Department and/or the Oneida Business Committee pursuant to the procedures set out in the Administrative Rulemaking law.

2.2.3. Shall 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.

2.2-4. 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.

2.2-5. This rule supersedes all prior rules, regulations, internal policies or other requirements relating to clear desk/screens.

2.3. Definitions

2.3-1. 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) **"**Authorized Individual**"** means a person who has the proper authorization to access, handle, or remove Sensitive Information from devices that transmit or print such information.

(b) **"**Information Systems**"** means systems used to store, process, and manage information, including computers, networks, and databases.

(c) "Removable Storage Media" means devices such as flash drives, removable media, tablets, and cellular phones that can store electronic data and be physically removed from a workstation.

(d) "Secure Storage Areas" means areas where sensitive information is stored that shall remain locked or digitally secured when staff are away from their work areas.

(e) "Sensitive Information" means information (both hardcopy and electronic) that shall be protected from unauthorized access or disclosure. This includes private, non-public, or confidential data.
(f) "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.
(g) "Unauthorized Access" means access to Sensitive Information by individuals who do not have the proper authorization or clearance.
(h) "Unauthorized Disclosure" means the release or sharing of Sensitive Information to individuals who are not authorized to receive it.

2.4. Digital Security Office Responsibilities

2.4-1. The Digital Security Office shall ensure processes are in place to:
(a) Identify Sensitive Information (hardcopy and electronic) that shall be protected from unauthorized access or disclosure.
(b) Identify workstations that shall be shut down at the end of the workday and those to remain powered on at night to receive security updates.
(c) Laptops/tablets/cellular phones containing Sensitive Information shall be secured per the **Mobile Device policy**.

2.5. Staff Responsibilities

2.5-1. Oneida Staff shall ensure that:
(a) Sensitive or private/non-public electronic information is secured and/or removed from unauthorized disclosure or access when they leave their work areas. Staff who work with Sensitive Information shall have means to store information in a secure area when not in use. Staff shall check with their immediate supervisor or Oneida management if an employee is not sure what information shall be secured or what lockable storage is available.
(b) Their desk and work area is clear (clear desk) of papers and removable storage media when leaving their work area unsecured. In addition, monitors shall be cleared (clear screen) to protect against unauthorized access to information or Information Systems. Screen savers shall be automatically activated after a period of inactivity. See the **Workstation Security policy** for more information.
(c) Papers and electronically stored Sensitive Information (e.g., flash drives, removable media, tablets, cellular phones) shall be secured when Staff leave their work area. Storage areas containing Sensitive Information shall remain locked or digitally secured when Staff are away from their work areas. Keys to secure storage areas shall not be left in the lock or accessible by unauthorized personnel.
(d) Devices that transmit or print (e.g., Fax machines, printers) Sensitive Information shall have the documents immediately removed from the device by authorized staff to prevent unauthorized disclosure or access.
(e) Documents waiting to be shredded shall not be accessible by unauthorized staff.
(f) Violations to this rule may be subject to disciplinary action, up to and including termination.

2.6. References

(a) 2.6.1. COBIT EDM03.07, APO07.05, APO12.02, APO12.07, APO14.02, DSS06.07
(b) 2.6.2. GDPR Article 25, 32

Commented [JH1]: IK am not sure you have authority over hardcopy documents. This is being managed through the Open Records and Open Meetings law. This may have some impact in electronic documents also.

Commented [RN2]: Not possible in shared cubicle spaces

Commented [RN3]: Don't agree

Commented [JH4]: who is this? Is this employee or user?

Commented [JH5]: Who is this? Should it be employee or user?

(c) 2.6.3. HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(B)
(d) 2.6.4. ISO 27001 A.7.7
(e) 2.6.5.NIST SP 800-37 3.1, 3.3
(f) 2.6.6. NIST SP 800-53 AC-11, MP-2, MP-4
(g) 2,6.7. NIST Cybersecurity Framework ID.AM-6, ID.GV-4, ID.RA-3, PR.AC-2, PR.AT-1, DE.DP-2
(h) 2.6.8. PCI 9.4.1, 12.1.1

End.

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