Workstation Use and Security Policy

ROWAN UNIVERSITY POLICY

Title: Workstation Use and Security Policy
Subject: Information Security
Policy No: ISO: 2013:03
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Assistant Vice President and Chief Information Security Officer
Date Adopted: 07/01/2013
Last Revision: 07/12/2021
Last Review: 07/12/2021

I. PURPOSE

The purpose of this policy is to specify the appropriate security controls and minimum requirements for Rowan University's workstations to ensure the security of information on the workstation and information the workstation may have access to.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Chief Information Security Officer shall implement and ensure compliance with this policy. The Vice Presidents, Deans, and other members of management shall implement this policy in their respective areas and ensure that all members of their respective organizations follow the administrative, physical, and technical safeguards defined in this policy.

III. APPLICABILITY

This policy applies to all members of the Rowan University community and any other parties, who use, work on, or provide services involving Rowan University workstations and information systems.

IV. DEFINITIONS

Refer to Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy.

V. POLICY

1. Rowan University’s workstations are provided by Information Resources & Technology (IRT) for official use to support the administrative, academic, and research needs of the university.
2. IRT is responsible for defining the baseline security controls and minimum standards and configurations for all workstations. All workstations are required to utilize the baseline security controls and safeguards defined and managed by IRT.
3. The minimum security controls and requirements for all workstations should include but is not limited to the following:
    a. Antivirus
        i. Workstations must have antivirus software installed, configured so that the virus definition files are current, routinely and automatically updated, and the antivirus software must be actively running on these workstations.

ii. All files on workstations will be scanned periodically for viruses per the schedule established by IRT.

b. Encryption

i. All workstations must be encrypted

c. Removable Media

i. All access to read or write to removable media, such as external hard drives, USB flash drives/thumb drives, rewritable DVDs and CDs must be blocked.
ii. Shipments of removable media containing information classified as sensitive must be done using a courier that can track shipments and provide proof of receipt.

d. Anti-Theft

i. All workstations that support the appropriate hardware and software requirements for anti-theft deterrent software must be configured with this software

e. Data Storage and Backup

i. Users must not save information classified as Confidential, Private, or otherwise considered sensitive or privileged information on workstations.
ii. Users are provided with access to Shared Drives and Google Drive for data storage. However, some files such as Outlook email archives are automatically stored locally on workstations.
iii. Users and business units should consult with IRT and the Office of Ethics, Compliance and Corporate Integrity regarding what kind of security is appropriate for the sensitive information they store on their local workstations.
iv. Users and business units are responsible for ensuring a backup of their data exists and should consult with IRT for guidance on backing up any data as not all locations on a workstation are backed up
v. Sensitive information should be saved in folders with access limited to those individuals authorized to access the information.
vi. Data access entitlements must be reviewed and handled according to the University's Acce ss Control Policy

f. Workstation Login and Logon Banners

i. A user ID and password must be required to use the workstation. This user ID must tie back to a user and thus generic local or network accounts are not permitted
ii. Logon Banners are required and must state: "I understand and acknowledge that this system is the property of Rowan University and is for authorized activity only. By using this system, I acknowledge notice of, and agree to comply with, Rowan University's Acceptable Use Policy available at go.rowan.edu/aup."
iii. Workstation screen lock out policies must be enforced to lock idle workstations after 15 minutes of inactivity

g. Workstation Privileges

i. Elevated Rights are only provided to full time Faculty members on their workstation
ii. Administrator access on a workstation is a privilege and will only be granted when a clear business need is established and standard university services or an alternative solution cannot support the user's business needs.
iii. IRT reserves the right to revoke without notice local administrator privileges if access is deemed to present a risk to Rowan electronic information or information systems.
iv. IRT will periodically reassess workstation privileges including administrator access and at their discretion revoke the entitlement (without notice) or offer an alternative solution to meet the user's needs.

h. Physical Controls

i. Workstations that provide access to or use of sensitive information or information systems should not be located in publicly accessible areas.

ii. If a workstation must be located in a public area, physical and technical safeguards must be employed to protect against unauthorized access and to ensure the workstation is secured from theft
iii. Workstation monitors should face away from public viewing or use privacy screens to protect the sensitive information that is displayed on the workstations

i. Software Updates

i. Workstations must be rebooted every 30 days to ensure operating system and application software updates are installed.
ii. Users are responsible for checking with IRT to validate that any software updates that are not provided by IRT are from an approved source

4. Workstation Use

a. Users must log off or lock their workstations when not in use.
b. Users must receive approval through the Information Technology Acquisition Process (ITAP) before installing software or connecting hardware that has not been issued or purchased by Rowan University.
c. Users must provide and retain proof of purchase and licenses when installing personal licensed software, unless the software is provided with a free license for use at Rowan University by the software developer. Any specialized software required must be submitted for approval through IT AP, paid for with department funds and released to the university once the user leaves the university.
d. Users must use the home drive and department shared drives (e.g. OpenArea or Google Drive) to maintain a backup of their important data.
e. Users must use a privacy screen when handling or displaying classified information on their workstation screen that could be viewed by an unauthorized user or bystander. If privacy screens are not available or practical, then ensure the monitors are in areas or at angles that minimize viewing by persons who do not need the information.
f. Users should utilize privacy shutters on web cameras to prevent the capture of classified information within the view of the camera and ensure that the privacy shutter is enabled when the camera is not in use
g. Users should take the necessary precautions to protect the data and their workstations from unauthorized use, theft, damage etc. For example, best practices include:

i. Never leaving a workstation unattended and securing workstations in the location that it is typically used
ii. When traveling, store workstations appropriately to ensure the workstations are protected
iii. Be mindful of liquids from food or drink while using the workstation

5. Workstation Minimum Software, Hardware and Network Requirements

a. Workstations must authenticate with Rowan University systems monthly to ensure compliance with all Rowan University technology policies unless special permission has been given by the Department Head and the Information Security Office.
b. Workstations are required to be brought into the campus during the annual Physical Audit of the university department
c. Workstations that are over six (6) years of age are considered end-of-life and will be removed from service.
d. Workstations, where the original operating system or the hardware are no longer supported by the manufacturer, are considered end-of-life and will be removed from service following the requirements of the Technology Ownership Policy.
e. Workstations may be rebooted or disconnected from the network if deemed necessary to:

i. Ensure a workstation's security controls comply with the requirements in V.3 and are updated and functioning correctly, such as updated antivirus definitions.
ii. Prevent propagation of malware to other networked devices or detrimental effects to the network or data.
iii. Address a security incident under the direction of the Information Security Office (ISO).

6. Workstation Auditing, Logging and Monitoring

a. Each department is responsible for working with IRT to provide and maintain an accurate and current inventory of all workstations. Annual Physical Audits of workstations are required to ensure the inventory and asset database are updated and any deviations of security controls are documented and reviewed by the Information Security Office. Workstations that deviate from Rowan University's baseline security controls and safeguards must be identified by Technology Support during the asset audit. Deviations must be documented and state:

    i. The department where the workstation resides.
    ii. The purpose of the workstation.
    iii. The workstation's serial number.
    iv. The controls and safeguards not applied to the workstation.
    v. The business justification for deviating from Rowan's baseline security controls, safeguards, and configurations.
    vi. The IRT Asset manager approving the deviation

b. Workstations must be used in accordance with the University's policies and secured against unauthorized access. In order to protect the confidentiality, integrity, and availability of Rowan University's electronic information and information systems, activity may be reviewed, logs captured, and access monitored without notification.

7. Workstation Repurpose and Disposal

    a. A workstations that is repurposed for another user or for another use must be first reviewed by IRT per university guidelines and procedures to ensure the workstation meets the minimum requirements to be in use. In addition, all data must be securely disposed of and all licensed software, hardware and security controls must be removed. Once the data is securely disposed, the workstation can be reimaged to meet the minimum requirements and the asset database must be updated accordingly to reflect the new ownership and the new use of the workstation.
    b. A workstations that is deemed end-of-life will not be supported or permitted on the network and must be disposed by IRT per university guidelines and procedures to ensure the workstation and data is securely disposed of and all licensed software, hardware and security controls are removed prior to disposal and that the asset database is updated accordingly.

8. Workstation Loss and Theft
    a. Workstations, removable media or related peripherals that are lost or stolen must be reported to the Manager, Data Owner, Department of Public Safety and the Technology Support Center.
    b. The Information Security Office must investigate the workstation loss or theft according to the Security Incident Management Policy.

9. Workstation Exceptions

    a. Exceptions to this policy can be requested if the workstation cannot meet the requirements for a specific security control or if the security control interrupts with another core workstation component. The need for an exception will be validated by Device Management and Technology Support and approved by the Information Security Office. If an exception is required, the Information Security Office and Device Management team must work with the department to develop a plan to provide compensating controls for the workstation that meet the minimum technical, administrative and physical security requirements to protect against unauthorized access, loss or theft.
    b. Individuals that require exceptions to the minimum security standards and configurations for a workstation can provide the business justification to the Information Security Office for review and approval of the exception for the specific control or requirement. If approved, the individual is responsible to:

        i. Incorporate the University's baseline security controls, safeguards, and configurations into their workstation builds.
        ii. Maintain an accurate and current inventory of all their workstations.
        iii. All exceptions, including extending the end-of-life policy are not valid for more than one year and the workstation will have to be replaced or updated to comply with the requirements of this policy.

VI. POLICY COMPLIANCE

Violations of this policy may subject the violator to disciplinary actions up to or including termination of employment or dismissal from school, subject to applicable collective bargaining agreements and may subject the violator to penalties stipulated in applicable state and federal statutes. Students who fail to adhere to this Policy or the Procedures and Standards will be referred to the Office of Student Affairs and may be expelled. Contractors and vendors who fail to adhere to this Policy and the Procedures and Standards may face termination of their business relationships with the University. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization per the Acceptable Use Policy.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer