Responsible Use of University Computing Resources Policy Document

Computing Account Management

1.0 Purpose

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to Montclair State University information resources. An account, at minimum, consists of a user ID and a password. Supplying account information will usually grant access to some set of services and resources. This policy establishes guidelines for issuing and managing accounts.

2.0 Scope

This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices; information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally by the Information Technology Division.

3.0 Policy

Server Owners and Application Administrators are responsible for ensuring that all accounts at the OS level or within a particular application are created according to the following procedures:

3.1 Account Provisioning and Access Control Standards

Accounts that access electronic computing and information resources require prudent oversight. The following security precautions should be part of account management:

- All accounts must have a password that adheres to the practices outlined in the Password Management Policy document.
- Any account that is not used for interactive login or authentication must be "locked" or "disabled" according to the definition of those terms for the particular OS in question.
- Prior to creating a user account, that user's affiliation with the University must be verified by the sponsoring unit or division (i.e., Human Resources, Registrar).
- Users must attend all appropriate application or data handling training courses prior to their account being activated.

- Accounts for individuals not affiliated with the University must have prior approval from IT.
- There may be only one user associated with an account. Users may NOT share an account.
- Accounts should not be granted any more privileges than those that are necessary for the functions the user will be performing. When establishing accounts, standard security principles of "least required access" to perform a function must always be used, where administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will suffice.
- Directory and file permissions should be set correctly to prevent users from listing directory contents or reading, modifying, or deleting files that they are not authorized to access.
- Account setup and modification shall require the signature of the account requestor, the requestor's immediate supervisor, the data owner and the Office of Information Technology.
- The organization responsible for a resource shall issue a unique account to each individual authorized to access that networked computing and information resource. It is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.
- The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access (e.g., user accounts used for email do not require an identity validation process as thorough as for those user accounts that can be used to post information to public web pages or modify department budgets).
- Passwords for new accounts should NOT be emailed to remote users unless the email is encrypted.
- The date when the account was issued and its expected expiration date (if applicable) should be recorded in an audit log.
- All managers of accounts with privileged access to MSU data must sign a Confidentiality Agreement that is kept in the department file under the care of a Human Resources representative or liaison.

3.2 Managing Accounts

- All accounts shall be reviewed at least annually by the data owner to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. IT Security may also conduct periodic reviews for any system connected to the MSU network.
- All guest accounts (for those who are not official members of the University community) with access to computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.
- For access to sensitive information managed by a department, account management should comply with the standards outlined above. In addition, naming conventions must not cause contention with centrally managed MSU NetIDs. Should the potential for contention arise, the account will not be created until a mutually satisfactory arrangement is reached.
- The identity of users must be authenticated before providing them with ID and password details. In addition, it is required that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.
- Account management should allow for lock-outs after a set number of failed attempts (ten is the recommended number). Access should then be locked for a minimum of one hour, unless a local system administrator intercedes. Lock-outs should be logged unless the log information includes password information.

4.0 Enforcement

Any member of our community found in violation this policy is subject to disciplinary proceedings including suspension of system privileges, expulsion from school, termination of employment and/or legal action as may be appropriate and in accordance with the administrative handbooks and codes of conduct applicable to the individual’s role at the University.

5.0 Related Policies and Links

Responsible Use of University Computing Resources

Password Management Policy