OFFICE OF INFORMATION TECHNOLOGY – INTERNAL POLICY

Granting and/or Restricting Access to Information Technology Resources

RESPONSIBLE ADMINISTRATOR: VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(s): OFFICE OF THE VICE PROVOST FOR INFORMATION TECHNOLOGY
ORIGINALLY ISSUED: OCTOBER 20, 2017

APPROVALS:

APPROVED BY:

OIT Steering Committee 10/20/2017
Date

[Signature]
Lori L. Temple
Vice Provost for Information Technology 01/26/18
Date

REVISION DATE: JANUARY 26, 2018

STATEMENT OF PURPOSE

The Office of Information Technology (OIT) is, on occasion, asked to grant or restrict access to an account by someone other than the account holder.

The purpose of this policy is to:

- Delineate the circumstances under which OIT is authorized to grant or restrict account access
- Ensure decisions to grant or restrict account access are made at the appropriate level
- Protect information technology resources from unauthorized access
- Comply with university, system, state, and federal investigations
- Provide business continuity at the time an individual separates from the university

ENTITIES AFFECTED BY THIS POLICY

OIT staff and student employees, UNLV employees seeking access to accounts other than their own, approving authorities.

WHO SHOULD READ THIS POLICY
OIT staff and student employees, UNLV employees seeking access to accounts other than their own, approving authorities.

**Policy**

OIT will only grant and/or restrict access to information technology resources with consent of the *account holder* or upon authorization from the appropriate *approving authority*.

In the event the *approving authority* is not clear, General Counsel will determine the appropriate *approving authority*.

Refer to the Office of Information Technology internal policies and procedures web page on InsideOIT at [https://www.it.unlv.edu/oit/inside/policies-procedures](https://www.it.unlv.edu/oit/inside/policies-procedures) for additional information.

**Related Documents**

Not Applicable

**Contacts**

Refer to the Office of Information Technology internal policies and procedures web page on InsideOIT at [https://www.it.unlv.edu/oit/inside/policies-procedures](https://www.it.unlv.edu/oit/inside/policies-procedures) for a list of individuals who can answer questions about the policy.

**Definitions**

*Account Holder* - A current student, employee, or individual granted a guest account. Individuals who have separated from the institution are no longer considered account holders.

*Approving Authority* - The appropriate cabinet-level administrator for the account holder; any member of the Office of General Counsel; senior leader in the Office of Human Resources; or senior leader in the Office of Student Conduct. In cases where the expedited procedure applies, the approval authority is the former account holder’s supervisor.
SECTION 1: Expedited Procedures for Account Access

**Expedited Procedure for Former Account Holder Access within Seven Days of Separation**

Within seven days of an account holder’s separation date from the university, access may be granted to personal files on university IT resources with the approval of the individual’s supervisor. Access will be granted for no longer than 24 hours.

Expedited requests will be handled by the IT Help Desk.

Beginning with the eighth day of separation from the university, former account holders must follow the procedures outlined in Section 2.

SECTION 2: Full Procedures for Account Access

**Types of Requests**

The following are examples of common actions and the information technology resources on which they are performed. Please note that this list may not be all-inclusive as the specific situation dictates the actions that must be performed.

**Actions:**
- Authorize Access to
- Reinstall Access to
- Provide an archive of
- Deactivate
- Capture
- Research / Investigate

**IT Resources:**
- Email Account
- Email Correspondence
- Hard Drive
- File Services
- System Logs
- Network Logs
- User Accounts
- User Files
Procedure for Making Requests

The requestor sends a written description of the action desired with a short description of the reason for the action to the approving authority for authorization.

The approving authority sends authorization for the action to the Vice Provost for Information Technology via email.

OIT Approval

The highest ranking security position within OIT prepares an authorizing memo to the OIT employee who will perform the action. The employee is informed that confidentiality must be maintained and only the people needed to complete the task should be informed of the action.

The authorizing memo must be signed by two of the following:
- Vice Provost for Information Technology
- Associate Vice Provost for Information Technology
- Highest ranking security position within OIT
MEMORANDUM of RECORD

TO: Chris Doe, Senior Systems Administrator
FROM: [Current VPIT], Vice Provost for Information Technology
DATE: Friday, August 11, 2017
SUBJECT: Authorization to Authorize Access to File Services

The Office of Information Technology has received a request from The Executive Vice President and Provost, Diane Chase to authorize access to the file services assigned to Joe Employee for the purpose of business continuity.

Additional Instructions:
Please grant access to Jane Doe to the Window File Services storage belonging to Joe Employee.

Contact the user and ensure that she can access the necessary files.

As always, you should maintain confidentiality in this matter, informing only those people who need to know to complete the task.

Must be authorized by two of the following:

UNLV Vice Provost for Information Technology: _____________________________

UNLV Associate Vice Provost for Information Technology: ______________________

UNLV Information Security Officer or designee: _______________________________