The University of Mississippi
IT Accounts

Summary/Purpose: This policy defines the means by which accounts are allocated and administered on University of Mississippi (UM) Office of Information Technology (IT) computer/networking facilities.

ACCOUNT ALLOCATION

The following individuals/groups are eligible for accounts on IT managed systems:

- UM students, faculty, and staff.

- Students, faculty, and staff at the Mississippi Institutions of Higher Learning (IHLs) who require access to Mississippi Center for Supercomputing Research (MCSR) high performance computing facilities.

- University offices or groups needing an account for email correspondence with their clients.

    - *In this case, the account is authorized by the department head or group leader, and a permanent faculty/staff member must assume responsibility for the account. Student organizations are not eligible for group accounts; however, they may request an email alias on the campus email system.*

- Employees who work for agencies that are under contract or have an official relationship with the University to perform a particular service.

- Volunteers, campus ministers and others who function in roles that are integral to campus life.

- Emeritus personnel and also faculty/staff who retire with twenty-five years of service to the University.

- Individuals who are participating in special programs with the University, e.g., PACE.

- Local school teachers and students, providing (1) IT resources are used to enhance teaching/learning and (2) usage does not adversely affect the service that is provided to other users.

- Parents who are authorized to receive WebIDs by their student children.

- Individuals who are authorized to receive UM WIFI access by an active UM employee.

- Other individuals as approved by the Chief Information Officer (CIO).

Some systems may be designated for certain purposes and therefore may be limited to certain individuals. For example, only those individuals who require access to high performance computational facilities/programming environments will be given access to MCSR systems.

Each individual is allowed **one** account per system with the exception of parents who receive parent WebIDs and individuals who receive only UM WIFI accounts. Parent WebIDs are allocated in a one-to-one relationship with the student.

MCSR research accounts are also an exception to this standard in that they may be assigned on a per project basis. Individuals requiring more than one account on a system should submit a written request to the CIO explaining why the additional account is needed.

ACCOUNT INITIATION

Account names are automatically assigned to all incoming UM freshman/transfer students. The relevant accounts, (e.g., email, WebID, and Blackboard, are created when the student is admitted).

Other or "special" accounts are created in response to an individual's application for an account through the IT account application interface or through MCSR's on-line application for research accounts. Individuals applying for accounts will be asked to provide appropriate identification showing that they are eligible for an account as described above. These accounts are *approved* by the IT accounts administrator prior to being created. Normally, accounts are created within two working days of being requested and approved.

ACCOUNT NAMES

Individuals who have accounts on more than one IT machine will be assigned the same *username* across all machines. An exception to this is the case of parent WebIDs, which are assigned in a one-to-one relationship with the student.

IT staff will change an account name at no charge under the following circumstances:

- An individual's official name changes, e.g., as the result of marriage.

- The account name that was automatically assigned is unacceptable to the individual, and the individual notifies the OIT of this **within one month** of the account's creation.

- An individual is a victim of email harassment.

IT staff will change an account name in other circumstances; however, there will be a fee of $15 per account name change.

ACCOUNT TERMINATION

Accounts belonging to the following individuals are subject to being terminated:

- Students who are no longer enrolled in classes at UM or one of the MS IHLs.

- Faculty/staff members who are no longer employed by UM or one of the MS IHLs.

- "No shows" -- UM students who were automatically assigned an account but who do not enroll in classes.

- Individuals who are no longer affiliated with the University -- for example, a volunteer who retires or a participant in a special program that has ended.

- Individuals who fail to access an account for six months or longer.

Other or "special" accounts are subject to an annual review which should be performed by the individual designated as the owner of the account upon receiving a review notice. The owner may extend the account for another year, delete the special account, or modify the special account configuration. If no action is taken within thirty days of the review notice, IT will assume the special account is no longer required and the account will be restricted.

In addition, violations of the IT Appropriate Use Policy may result in the permanent or temporary loss of account privileges. Accounts which cause a security vulnerability, such as those having a password that can be easily broken, may be restricted until the account owner takes action to correct the problem. Lastly, accounts belonging to employees or students who are terminated for disciplinary reasons may be restricted immediately.

Individuals are given a minimum of one month following their separation from the University (or one of the MS IHLs) before their accounts are restricted; this is to provide ample time to relocate to another system/service provider. Accounts are restricted for a minimum of three months prior to being deleted. Forwarding of emails via the UM Gmail or UM Mail interfaces will no longer be valid if accounts are restricted. The University reserves the right to restrict accounts immediately in the event of employment termination for disciplinary reasons.

OTHER

Files and directories on IT/MCSR systems are archived to tape on a periodic basis. For most systems, full backups are performed weekly, and incremental backups are performed nightly. When there are no user backups available, individuals that mistakenly delete files can request to have the data restored from IT/MCSR tape backups. Further, requests for recovery services related to an e-discovery need must be approved by the Security Coordinator or the Chief Information Officer. The fee for having

files restored from a tape backup is $25 per hour.   Depending on the time the email or files were removed and the time of the last backup, the data may or may not be available.

UM Box accounts and UM Gmail accounts are not hosted on IT/MCSR systems and are not eligible for file recovery services from UM IT.

IT may impose various user limits on certain systems (such as disk quotas) in order to allocate finite system resources in an equitable manner.

Individuals who forget or misplace a password will be asked to provide appropriate identification in order to have the password reset. For UM students, this means visiting the IT Helpdesk and showing a valid UM student ID. In cases where a visit is not possible, an individual may be allowed to FAX a copy of his or her ID as validation. Alternatively, individuals may request to have the password reset and sent as a text message to the cell number on record.