



DRAFT

Policy Number (###)  
University-wide Policy



### Email Alias Policy

Effective Date:	Month, ##, 2007
Date(s) Reviewed:	
Date (s) Revised:	

**PURPOSE:**

Confidentiality, Integrity, and Availability are extremely important requirements regarding electronic messaging at the University of Miami. Assigning everyone a permanent internal email address establishes a reliable framework for secure communication. To uphold these principles, the Email Alias Policy establishes requirements for selecting and configuring an email alias for any mail system associated with the University.

**SCOPE:**

This policy applies to all University employees, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties utilizing University resources.

**DEFINITIONS:**

**Email:** Is an abbreviation used for electronic mail, which is a store and forward method of composing, sending, storing and receiving messages over electronic communication systems.

**Preferred email address:** A preferred email address identifies a location where email messages can be delivered and is automatically created when a user receives a mailbox on any server throughout the University of Miami (i.e. sebastian@exchange.ir.miami.edu). The preferred email address is automatically generated for the user without client input and will never change.

**Email Alias:** An email alias is an additional email address configured for a mailbox via user input. For example, whether email is addressed to the preferred email address sebastian@exchange.ir.miami.edu (that was automatically generated) or to the email alias Sebastian44@miami.edu (that was selected by the user), it will be delivered to the same mailbox. The email alias can be changed if the user has a legal name change or to resolve abuse or SPAM issues.

**Internal University of Miami email server:** A system owned, configured and maintained by the University that provides users with electronic email services.

## **POLICY:**

The University of Miami allows a user to have one preferred email address and one email alias. The requirements for establishing an email alias are as follows:

- The alias must be unique, therefore users will be asked for alternatives if the alias is already taken by another user on the system.
- The alias can contain alphanumeric characters, and periods (no underscores, dashes or special characters).
- Aliases must be based on the individual's actual name. For example, if a user's name is John P. Smith he may request an alias of Johnny, but he may not request nicknames such as *strongman*, or *gocars*.
- The alias cannot be offensive, derogatory, contain profanity, ethnic slurs or any verbiage that would be considered inappropriate.
- The alias cannot be requested for the purpose of impersonating another user and must not contain department names and/or titles. For instance, if someone's name is John P. Smith, and he requests the alias *UniversityPresident*, the request will be denied.
- All email aliases will point to internal University of Miami email servers. Aliases are not allowed to reference external mail providers (i.e. Hotmail, Yahoo, BellSouth, etc.).

## **ENFORCEMENT:**

End User Support:

- Responsible for configuring an email alias and will escalate to Human Resources in the event a request poses a concern.

Human Resources:

- Responsible for reviewing any email alias requests that are escalated to them from the End User Support group.

Chief Security Officer (CSO):

- Responsible for monitoring the enforcement of the policy.

## **SANCTIONS:**

Violations of the policy will be addressed by the individual's respective disciplinary policies and procedures. All known and/or suspected violations must be reported to the applicable Network/Systems Administrator or their management. The Information Security Department must be notified of any reports within 24 hours of the claim at [security@miami.edu](mailto:security@miami.edu). The appropriate University administrative office will investigate all allegations of policy violation with the assistance of the Department of Information Technology, General Counsel, and the Department of Human Resources.

Any faculty/staff found to have violated this policy may be subject to disciplinary action, up to and including suspension and/or termination of employment.