Account or Data Access Policy [1]

Version 1.1

Authority

Duke University Chief Information Officer
Duke University Chief Information Security Officer

Scope

When a Duke employee or student leaves the University, their account information (such as email electronic files, voice mail, and other data) will not be made available to a third party except in rare cases as defined in the Duke Acceptable Use Policy.

Some typical requests include:

**Access by a department to a former employee?s email or files**

If a Duke faculty or staff member has left the University and their department believes that there is a critical need to directly access the former employee’s account(s) (email account, file space, and other data), a request from the departmental chair or director can be submitted to the University IT Security Office for consideration. Granting such a request requires the approval of the University's President, Executive Vice President, and the Office of Counsel. In general, direct access to the account is not provided, and an away message can be put on the person’s email account until the account expires to direct people to an alternate email address or contact person.

**Access by a departed faculty, staff or student to their accounts**

If a former employee or student wishes to access their own central Duke mail, approval must be obtained from the CIO; if a former employee or student wishes to access their own local departmental email account, approval must be obtained from that department's Dean.

**Access to files or emails of a deceased faculty, staff or student’s files by the Estate**
In the case of a University community member who is deceased, direct access to the e-mail account or file space is not usually provided; however, we can place an away message on the individual’s email account to direct people to an alternate contact, or set up the email to be forwarded to another account for a short period of time with the approval of the departmental chair and/or director. Contents of the email account and computer files may also be retrieved and provided to the executor of the estate through arrangement with the University IT Security Office.

To request the release of the email or computer files, we ask the executor to provide the following:

1. Your full name and contact information, including a verifiable email address.
2. A copy of the death certificate of the deceased.
3. A copy of the document that identifies you as the Executor or Administrator of the estate or that gives you Power of Attorney to retrieve the files and emails.
4. If you are the parent of the individual, please send us a copy of the Birth Certificate if the Duke account owner was under the age of 18. In this case, Power of Attorney or executor/administrator documentation is not required.

This information can be sent via fax or postal mail. You may also contact the University IT Security Office at security@duke.edu for assistance or more information.

Requests for the emails and files should be made expeditiously to avoid possible deletion from Duke systems. Once a request is made, the IT Security Office will coordinate placing the away message and archiving of the files until the above documentation and approvals have been completed. While we make every effort to process requests in a timely fashion, it may take up to 30 days to complete a request, depending on the availability of the documents and facilitating delivery of the files.

Access by a faculty, staff or student to files that have accidentally been deleted
Duke users who are actively affiliated with the university and need to restore their own accidentally deleted data can open a service ticket with OIT to request the restoration.

Document Type: Policy
Topic: Data Security
Applicable To: Duke University
Source URL: https://security.duke.edu/policies/account-or-data-access-policy

Links
[1] https://security.duke.edu/policies/account-or-data-access-policy
[2] mailto:security@duke.edu