Procedures for obtaining access to user data

Objective

In accordance with the Information Security and Acceptable Use Policy, server and application administrators may be called upon to provide information to support authorized investigations. This procedure document outlines types of investigations and the appropriate authority to sign off on each.

Responsibilities

Purpose	User(s) involved	Authorized requestor	Authorized approver	Additional requirements
Legal issues (Litigation hold, etc.)	Any	UTD Attorney or UT System OGC	None needed	Document chain of custody
Criminal investigation	Any	UTD Police	UTD Attorney	Document chain of custody
HR investigation	Current or former faculty, staff, or student workers	HR	Associate VP, HR	None needed
Compliance investigation	Current or former faculty, staff, or student workers	Office of Institutional Compliance	Assistant VP, Office of Institutional Equity and Compliance	None needed
Internal Audit	Any	Internal Audit	Executive Director, IA	None needed
Academic investigation	Current or former student	Office of Community Standards and Conduct	Dean of Students	None needed
Continuity of business	Former faculty or staff	User's Dept. Head	None / University Attorney[1]	None needed
Continuity of business	Current faculty or staff	User's Dept. Head	Associate VP, HR	If account is active, user must be unavailable.
Open Records Request	Any	Office of Administration	None needed	None needed

[1] University Attorney should be consulted in cases that are unusual or not objectively reasonable.

Process

1. Requestor submits request to ISO.
2. ISO verifies the request is within the scenarios defined above, with appropriate authority and approval. If the user assigned responsibility for an electronic resource has an active user account, the requestor must justify in writing why the user is not available to provide access to the electronic resource directly – for example, a user may be on leave and / or repeated contact attempts to reach the user may have failed. If there is a concern that delay due to waiting for approvals would compromise the ability to collect the data (e.g., logfiles aging off the system), then ISO may act on the request, in order to preserve data that would otherwise be lost, but must wait for approval before releasing it.
3. ISO creates JIRA ticket, which includes:
    - The purpose of the request, including as much detail as possible to demonstrate the need for the requested data.
    - The individual(s) requesting access, the data requested, and the individual(s) who will receive access, including NetIDs and file paths as necessary.
    - Approval by Authorized requestor - an attached e-mail is sufficient.
4. Office of Information Technology (OIT) System Administrators secure the data, if available, and document status in the JIRA ticket.
5. OIT System Administrators provide data to ISO
6. ISO conducts any additional validation or filtering, and provides data to the individual designated in the request. This must be done in a secure manner, such as via a temporary box.com share or via an encrypted external drive. ISO verifies the requestor is able to access the data and that the collection appears to be complete.
7. ISO closes the JIRA ticket.

Exemptions

In the event that compliance with this procedure cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.