BYU

Church Educational System
Security Operations Center

Data Access and Investigative Request Procedures

Effective Date: 1 Nov 2021
Last Updated: 23 April 2026

Document Custodian: John Payne
Chief Information Security Officer
801-422-9099
John_Payne@byu.edu

RELATED POLICIES: Appropriate Use of IT Resources Policy
Data Use, Privacy, and Security Policy

INTRODUCTION

The Office of IT (BYU OIT) and the CES Security Operations Center (CES SOC) periodically receive requests to provide access to data in institutional accounts of individuals or perform investigations that are unrelated to cybersecurity threats or the day-to-day operation of BYU OIT systems. These requests take a variety of forms, including:

- Campus units seeking access to data after an individual is no longer employed by the University
- Requests for information about an individual's activities, for example whether an individual sent a particular email to a specific group or which websites an individual has visited
- Family members wanting access to institutional accounts (email, Box, etc.) of an individual

Limited capacity exists to address these requests and there may be privacy or legal issues associated with how, when, or why this data is shared. This document outlines how to make data access requests and addresses the most typical use cases and some of the challenges fulfilling these requests. This procedure also establishes a consistent framework for responding to data access and investigative requests, while safeguarding the privacy and rights of individuals and minimizing institutional risk.

Note: This procedure is targeted at ad-hoc requests for data, not ongoing data needs associated with business processes. Ongoing data needs should follow the university data sharing agreement process (see https://edm.byu.edu/services).

REQUEST ELIGIBILITY AND AUTHORIZATION

Data requests will be honored from campus units with a need to know. A campus unit has a 'need to know' when the data is necessary for the campus unit or its employees to be able to perform their function, duties, or decision-making responsibilities, but not when the data is merely interesting or convenient. Requests from individuals, those not associated with the university, and law enforcement will only be honored at the direction of the Office of General Counsel (BYU OGC).

PROCEDURE

For information request types as described below:

1. The requestor should email their request to:
   John Payne - John_Payne@byu.edu (BYU Chief Information Security Officer)
   Madelyn Blanchard - Madelyn_Blanchard@byu.edu (University Counsel)
2. The email request should include the scope of the problem (including business need, if applicable), desired objectives, and the date(s) for which data is desired (if applicable)

If the primary contacts are not available to assist with this type of data request, please contact one of the following:

- Scott Hunt - Scott.Hunt@byu.edu (Assistant VP Information Technology)
- Michelle Bennett - Michelle.Bennett@byu.edu (Assistant VP Information Technology)

Requestors should be aware that data or answers may not be able to be provided in every case.

EXAMPLE INFORMATION REQUEST TYPES

These are provided as the most common type of information requests that are made, where procedures for getting the data are well known. Individuals or units with requests that don't fit within one of these common cases are still welcome to reach out with their request.

Microsoft Teams & Email

Litigation Hold

Litigation holds on Teams and Exchange accounts are performed only by BYU OGC and at its direction. This type of hold should not be initiated or managed independently. End users are not normally notified when accounts are placed on litigation hold. All decisions regarding scope, duration, and release of holds are managed in accordance with legal requirements and at the direction of BYU OGC.

Mailbox Search

Search & Destroy: Search and destroy activities are conducted by the CES SOC to identify and remediate known malicious messages that pose a risk to the campus community. These activities are performed only after consultation with the Chief Information Security Officer and are limited in scope to identifying and removing specific malicious content. This process does not involve exposing general mailbox contents to a security analyst.

Search and Destroy actions are not performed for all malicious messages and are not used for non-malicious or investigative purposes.

Litigation search: Litigation searches are conducted only at the direction of BYU OGC and in accordance with applicable legal processes and requirements. Litigation-related searches will not be performed without explicit authorization. The scope and methodology of such searches are determined by BYU OGC and results are handled in accordance with legal requirements, including any designation of privilege or confidentiality.

Mailbox search for business data: E-mail searches for business-related data may be performed when there is a clear and documented business need. Requests must define a specific scope and demonstrate that the information cannot reasonably be obtained through other means. Searches will be narrowly scoped to minimize exposure to unrelated or personal content.

Results may be provided in a summarized or filtered format. Broad or unrestricted searches will generally not be approved.

Mailbox search for personal data: Requests for personal data contained within institutional mailboxes are highly restricted due to privacy considerations. Searches will generally not be performed for personal content unless directed by BYU OGC or required by law. Any approved requests will include additional safeguards and oversight. Results may be limited or denied.

Note: The university does not maintain email accounts for individuals who are no longer affiliated with the University. Once the email account has been deleted, the contents of the mailbox are irretrievable.

Mailbox Delegation

Mailbox Delegation is the process of giving one person access to another's email mailbox. This request typically comes in two forms:

1. Campus units seeking access to business-related information from the mailbox of an individual who has recently left university employment.
2. Requests from family members or other third parties seeking access to the mailbox of an individual who is deceased or otherwise unable to access their email.

University email accounts may contain both institutional data and incidental personal content. Accordingly, mailbox access must be carefully controlled to ensure appropriate use of institutional data and to minimize unnecessary exposure to unrelated content.

Requests from family members, those not affiliated with the university, and law enforcement will be considered and responded to only at the direction of BYU OGC or as required by law.

When access is granted:

- It must be **time bound**
- It should **involve oversight** by more than one authorized individual.

Mailbox delegation for campus units that need information from a mailbox of someone who has recently departed university employment should be performed very rarely. Campus units are encouraged to use shared mailboxes for business purposes to avoid the need for delegation.

Chat History

Chat history request (e.g. Microsoft Teams messages) follow similar guidelines to email data requests. Access to chat content requires a clearly defined business need and must be limited in scope. Chat data may be incomplete or unavailable depending on retention policies and system limitations. Requests involving sensitive investigations, personnel matters, or those with potential legal implications must be reviewed by OGC prior to any action.

End Users are not notified when chat data is accessed as part of an approved request.

Microsoft OneDrive & Box

Folder Search

Searches of files stored in OneDrive or Box may be performed when there is a legitimate business need and a clearly defined scope. Requests must include sufficient detail to identify relevant files or folders. Searches will be conducted in a manner that minimizes exposure to unrelated or personal content. Broad or exploratory searches without a defined objective will not be approved.

Folder Access

Granting access to another individual's OneDrive or Box content is strongly discouraged and will only be approved in limited circumstances.

When access is granted:

- It must be **time bound**
- It must be limited to **specific folders** or **data sets**
- It should **involve oversight** by more than one authorized individual.

Whenever possible, campus units should use shared storage solutions, folders, and service accounts rather than individual accounts and folders for business-critical data.

Other

Drive Forensics

Drive forensics involves the detailed examination of endpoint devices or storage media. These activities are typically performed only in response to security incidents or formal investigations.

Because these activities are resource- intensive, the CES SOC is not staffed to support routine or ad hoc disk inspections. Requests for forensic analysis may be referred to a third party at a cost to the university. For these reasons, forensic analysis will not be performed for general information-gathering purposes.

Requests for forensic analysis must be approved by the Chief Information Security Officer and if the matter involves a legal or policy matter, BYU OGC.

User Campus Activity Tracking

Requests to track or reconstruct a user's activity across campus (e.g., logins, network usage, location data) are highly sensitive and subject to strict controls. Such requests must demonstrate a compelling business or investigative need and will require approval from the BYU CIO and BYU OGC. Availability and accuracy of data may vary depending on system logging practices and retention policies.

BYU OIT and the CES SOC do not provide continuous monitoring of individuals and will not support requests that resemble surveillance without appropriate authorization.

Browser History

Browser history is not centrally stored or accessible by BYU OIT or the CES SOC. The only browser activity that is exposed is related to browsing of malicious sites or content, flagged and alerted from automated security tools.

All requests are subject to availability of data, system limitations, and applicable legal and university policy constraints.