Data Access and Compliance for EMPLOYEES

The Alumni Association of the University of Michigan expects that individuals with access to alumni data understand their responsibility with respect to use, interpretation, and distribution of that data as well as the consequences for misuse of data. There are several important university, state, and federal policies which affect the use of alumni information, which requires all users of alumni data to understand and follow the policies in this statement.

As these standard policies state, users of alumni data need to be aware that name, address, and other information on individuals (whether appearing singly or as part of labels or lists) may not be released in any format or for any reason except in the case where the information is being used specifically to support an alumni relations function. Release of this information for any other purpose is strictly prohibited and can result in termination of access.

Use and Release of Alumni Information

This policy relates to all information about alumni of the University of Michigan. The University of Michigan owns this information and the Alumni Association and the Office of Development are responsible for its use and release. This policy regarding use and release of alumni information is issued by the Alumni Association of the University of Michigan (AAUM) and is applicable to all affiliated organizations of the AAUM. It is intended to allow agents of affiliated organizations to use information about U-M alumni while insuring that alumni privacy is protected to the fullest extent required by law. The information must not be given, sold, traded, exchanged, etc., to people or institutions not affiliated with the AAUM or without an explicit written permission from AAUM.

ALUMNI RELATED INFORMATION

A. GENERAL STATEMENT. Alumni information will not be released except as permitted under this policy or as required by law.

B. DEFINITION OF ALUMNI INFORMATION. Alumni information is defined as the name, any addresses, telephone numbers or any other information pertaining to an alumnus/alumna of the University of Michigan, which is gathered after the individual is no longer enrolled as a student.

C. AAUM ASSOCIATED ORGANIZATION. An associated organization is defined as an organization that acts on behalf of the AAUM by furthering the alumni relations effort of the University of Michigan.

D. INDIVIDUAL AGENTS. Each associated organization may appoint one individual agent who may receive access to alumni data.

- The Individual Agent (IA) agrees to only use alumni information in accordance with University and AAUM policies.
- The Individual Agent will receive all training documents before he/she receives access to the data.
- Upon completion of training, the IA will be assigned a password and uniqname, which will give him/her online access to the data source.
- Individual agents will not release their password and uniqname to others.

E. ACCESS AND USE OF ALUMNI INFORMATION BY AAUM AFFILIATED ORGANIZATIONS. Alumni information may be released to AAUM associated organizations, not under Regental control, only if the organization certifies by signing this agreement that:

- It will use the information only in an activity that will directly serve a function of the University. The AAUM will have the final authority to determine if an activity will directly serve a function of the University.
- It will not use the information for any other purpose.
- It shall not release or disclose the information to any third party. It shall not release the information to a person affiliated with the organization unless that person has a need to know and that person agrees to maintain the confidentiality of the information pursuant to these guidelines.
- The organization agrees to return or destroy all copies and/or versions of the alumni information in whatever form maintained once the activity is completed.

F. ALUMNI DIRECTORIES. Associated organizations may publish alumni directories using alumni information.

- All directories will include only those alumni who have given permission to release such information.
- Associated organizations will gather permission prior to producing an alumni directory.

G. RELEASE OF ALUMNI INFORMATION UNDER OTHER CIRCUMSTANCES. All requests for information in these circumstances should be directed to the AAUM.

- Law Enforcement Agencies
- Subpoena or Court Order
- All other requests

H. NONCOMPLIANCE. Failure to comply with this policy will result in denial of future access to alumni information for the individual and possibly the affiliated organization.

I. ACCESS. Designated representatives of the recognized affiliated organizations receiving password-protected access to alumni data will have the ability to access their organization's related alumni records on the database.

Please refer to the University of Michigan's SPG 602.05 Use and Release of Donor and Alumni Information (http://spg.umich.edu/policy/602.05), which is the overall guiding policy related to how and under what circumstances alumni information can be released while protecting individuals' privacy.

Enterprise Systems Access

The University of Michigan Information and Technology Services

Prior to obtaining access to U-M enterprise systems, AAUM staff is required to complete the online training: Access and Compliance: Handling Institutional Sensitive Data module and agree to the Institutional Data Access and Compliance Agreement, which are described at https://safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data.

The above agreement is accessible on Wolverine Access and is signed electronically.

Use of multi-factor authentication

Prior to obtaining access to institutional data, AAUM staff must adopt the use of the current multi-factor authentication solution provided by ITS and utilize such system to access alumni data. More information on the university's multi-factor authentication system, and the process of adopting it can be found here:

http://its.umich.edu/accounts-access/uniqnames-passwords/two-factor-authentication

Accessing Institutional data on personal devices

In accordance to University of Michigan's SPG 601.33, the following policy applies to the Alumni Association of the University of Michigan staff and volunteers

SPG 601.33 reference: Security of personally owned devices that access sensitive institutional data http://spg.umich.edu/policy/601.33

Staff and affiliates of the Alumni Association of the University of Michigan (AAUM) are prohibited from accessing and/or storing sensitive institutional data on personally owned devices without prior written authorization from the Vice President & CFO, or a delegated executive authority.

Implementation

If written authorization is granted for accessing institutional data from personal device, users must review the following information and follow directions described within to secure personal devices - prior to accessing data:

- Instructions for Securing Your Devices and Data: https://www.safecomputing.umich.edu/protect-yourself/secure-your-devices

Individual responsibility

Members and affiliates of the university community using their personal devices to work with sensitive institutional data are required to:

- Properly secure and manage their devices (as described above)
- Return or delete the data upon university request or when they are no longer authorized for access
- Report within 24 hours any type of compromise of their devices (loss, theft, unauthorized access, etc.) at 734-764-HELP or 4help@umich.edu
- Allow the inspection of their devices by the university in the course of an incident investigation
- Respond to requests for information if relevant (e.g. FOIA requests)

Violation of this policy may result in termination of data access and consideration of dismissal.

Staff members must declare personally owned devices that they are accessing sensitive institutional data on here: Declaration of Access to AAUM Data from a Personally Owned Device

Data Storage Policy

This policy provides guidance regarding the digital storage and management of university data, including both sensitive data (as defined by the university), AAUM departmental data, and other business-related digital content. This policy outlines the appropriate resources and storage systems available to house such data, and the rules related to each storage type. AAUM staff, volunteers, and vendors/partners accessing and/or storing university sensitive data must also sign the Data Access & Compliance policy (available from HR), and follow additional University of Michigan policies as noted therein.

This policy promotes responsible data storage practices, but also allows reasonable flexibility to provide a computing environment conducive to AAUM's business needs.

The University of Michigan's ITS department provides U-M units with storage options intended to appropriately manage different data types. Below is an outline of the most common storage facilities, and a guideline of how each should be used in order to keep business data accessible and at the same time remain safe, secure, and regularly backed up.

Storage options from ITS include: MiStorage, U-M Google Drive, and U-M Dropbox. It is strongly discouraged to save any business data locally on your computer's hard drive, thumb drives, or any other "personal" storage devices. Local storage on AAUM-provided equipment is not backed-up, and data residing on the device's local storage is at risk. Storage of institutional data on any personal device or personal online account (i.e. thumb drive, Dropbox, OneDrive, external drive, etc.) is strictly prohibited.

Using Dropbox Team Folders or Google Shared Drives for business data offers flexibility, granular access management, and shall be the first choice for creating work-related documents. Personal data (e.g. W-2 forms, employee valuations, or other financial documents) shall be stored in a "personal and private" folder in Dropbox and Google Drive.

Below is a summary of use-cases for each of the U-M provided data storage options:

Dropbox Team Folders – are to be used for business file storage and long-term storage and reference by the entire team/organization. This is where most of our business data should permanently reside. Dropbox offers data sharing and remote access, revision control, and full backups.

Google Shared Drives – are the best choice for real-time collaboration. Once documents are finalized, they should be moved to Dropbox for permanent storage and access.

Server Storage – is to be used for special needs where cloud storage cannot support the required business function or process. Examples include filesystem-based inter-linked files and other unique file types.

Local or removable storage (e.g., HDD, SSD, USB, SD cards) are not recommended for data storage, with the exception of temporary, transient, personal, or non-critical data which also exists elsewhere.

Google Drive and Dropbox include standalone apps that sync data between the cloud and local storage. Recently accessed files are available even when offline. Google Drive and Dropbox also include apps for Android, iOS, and iPadOS. Find a comparison chart and a summary of the various storage options available from ITS here.

AAUM's Tech Team manages, tracks, and maintains all technology resources and services on a regular basis. Employees are prohibited from storing any non-personal data within resources other than outlined above unless explicit permission is provided by the Vice President & CFO. Employees are responsible for reporting any data breach, loss, or other security incidents to the Director of Information Technology.