Access and Compliance Statement
Alumni Association of the University of Michigan

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 that affect 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.

   1. The Individual Agent (IA) agrees to only use alumni information in accordance with University and AAUM policies.
   2. The Individual Agent will receive all training documents before he/she receives access to the data.
   3. Upon completion of training, the IA will be assigned a password and uniqname, which will give him/her on-line access to the data source.
   4. 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:
1. 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.

2. It will not use the information for any other purpose.

3. 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.

4. 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.
   1. All directories will include only those alumni who have given permission to release such information.
   2. 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.
   1. Law Enforcement Agencies
   2. Subpoena or Court Order
   3. 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 http://www.mais.umich.edu/access.

The above agreement is accessible on Wolverine Access and is signed electronically.
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 Executive Director of Business Operations, 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:

• Review the following informational tutorial:
  http://safecomputing.umich.edu/protect-personal/devices/

• Instructions for Securing Your Devices and Data:
  http://safecomputing.umich.edu/protect-personal/instructions.php

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 dismissal
Certification of intent to comply with policy regarding access and use of alumni data

By signing this form, I certify that:

1. I have received, reviewed, and understand the Alumni Association of the University of Michigan’s Policy Regarding Access and Use of Alumni Data and that I agree to abide by the policies referenced therein, as well as applicable state and federal laws, relating to the proper use of institutional data.
2. I will be a responsible user of institutional data and will only access institutional data to carry out university business appropriate to my role.
3. I will do my part to help ensure compliance with all relevant laws, regulations, and policies regarding sensitive institutional data.
4. I will follow the provisions of Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan (SPG 601.07).
5. I will make every reasonable effort to maintain the privacy and integrity of institutional data.
6. I will appropriately secure sensitive institutional data obtained from any institutional data source, whatever the format.
7. Prior to sharing institutional data with others, I will ensure that recipients are authorized to access the data. I will not disclose sensitive institutional data to any unauthorized person.
8. I will log off data systems when not using them.
9. I will keep my passwords secure and not share them with anyone.
10. I will dispose of sensitive institutional data, in whatever format, in an appropriate manner.
11. I will report to the ITS Service Center any inappropriate use, disclosure, or breach of sensitive institutional data of which I become aware. I will also report if I think my account or password has been compromised.
12. I understand that misuse of institutional data will subject me to disciplinary action as described in Discipline (SPG 201.12).

Name: ________________________________________________________________

Signature:____________________________________________________________

Unit:_____________________ Unit Position Held:___________________________

Address:________________________________________________________________

_______________________________________________________________________

Daytime Phone: _____________________ Email address: _____________________