VIRGINIA COMMONWEALTH UNIVERSITY

VCU

Policy on data access and privacy

Policy Type: Local
Responsible Office: Office of Development and Alumni Relations
Initial Policy Approved: 12/2012

Policy Statement and Purpose

Confidential information is collected and maintained by the Office of Development and Alumni Relations for the purpose of furthering the fundraising, engagement, and membership operations of the university. Therefore, any confidential information is released for those purposes only. Legal documents, however, will be released only with the permission of the donor.

Confidential information will not be released to groups or individuals for any uses other than indicated on the request, including unapproved vendor use, political mailings or locating old friends. Therefore, addresses, email addresses or telephone numbers are not released to third parties without authorization from the associate vice president of Advancement Services.

These protocols will protect our members and donors and guide our staff by providing general principles and practices related to all aspects of confidentiality. Because the protocol is not intended to give every detail, operational areas might need to develop specific guidelines that address their unique circumstances.

Access to confidential information is given only to those university employees and other groups including, but not limited to, volunteers, vendors, partners and students who are authorized to view it by the AVP of Advancement Operations. Those who receive authorization must sign a DAR Confidentiality Agreement. Signing of the DAR Confidentiality Agreement does not guarantee access to DAR systems, including the university's alumni and donor database of record, Millennium. Access to Millennium must be granted in a manner that best utilizes the limited number of software licenses available.

The associate vice president of Advancement Operations makes final decisions regarding the allocation of access to Advancement Services systems.

Table of Contents

Who Should Know this Policy?

All university employees engaged in activities related to development and alumni relations are responsible for knowing this policy and familiarizing themselves with its contents and provisions.

Definitions

DAR employee

Someone who is employed by Virginia Commonwealth University and reports directly or indirectly to the vice president of Development and Alumni Relations.

VCU employee

Someone who is employed by Virginia Commonwealth University.

Volunteer

Someone who is not employed by Virginia Commonwealth University but works in an official capacity with the university and acts on its behalf.

Confidential information

This information is described by, but not limited to, the following general classes:

- Name, address, email address, telephone number or other contact information or social security number.
- Information about alumni, members, prospects, donors and other constituents gathered to aid in determining appropriateness of solicitation and level of membership or gift request; specific data in prospect lists that would identity prospects to be solicited; dollar amounts to be requested; and name of solicitor.
- Portions of solicitation letters and proposals that identity the prospect being solicited and the dollar amount requested. Letters, pledge cards, copies of checks or other responses received from members or donors regarding memberships or prospective gifts in response to solicitations.
- Portions of receipts, thank you letters or other membership or gift acknowledgment communications that would identify the name of the member or donor and the specific amount of the gift, pledge or pledge payment.
- Donors' or prospects' financial or estate planning information or portions of memoranda, letters, interview notes or other documents about any donor's or prospect's financial circumstances.
- Data detailing dates of memberships, gifts, event registrations, payment schedule of gifts, form of gifts or specific gift amounts made by donors.

Advancement Services

Advancement Services is managed by the assistant vice president for Advancement Services and oversees the following service functions for the Office of Development and Alumni Relations and the university: Advancement Information Technology and Online Services, Gifts and Records Management, Prospect Research and Campaign Data Analysis and DAR Finance and Administration

This department is responsible for managing application development and data integrity in Millennium and other systems, providing application training to users and ensuring security for information in the D&AR databases, in accordance with university IT policy. It is also responsible for gift processing; managing the development and production of reports, including fundraising analysis, data files for solicitations or project and alumni statistics; technical management of the division's Web space for both internal and external users; and management of the division's budgeting, expenditures and human resource functions.

Advancement Services' records
Advancement Services' records include all written papers, letters, documents, photographs, tapes, microfiche, microfilm, photocopies, sound recordings, maps and other documentary materials or information in any medium regardless of physical form or characteristics, including data processing devices and computers, relating to development and alumni relations.

Advancement Services' systems
All systems managed by Advancement Services, including, but not limited to, Millennium, Development and Alumni Relations intranet and Internet sites, online reporting center, online giving and payments, online event registrations and event registrations, e-communications and the alumni website and alumni portal.

Advancement Services' sensitive systems
All systems managed by Advancement Services that contain any confidential information. These include, but are not limited to, Millennium, the online reporting center and the event registration system.

Related Documents

- State Government Data Collection and Dissemination Practices Act, § 2.2-3800
- State Policy 6.05, Personnel Records Disclosure
- State Policy 6.10, Personnel Records Management
- VCU Computer and Network Resources Use Policy
- VCU Information Security Policy (http://ts.vcu.edu/askit/3408.html)
- VCU Technology Services Security Standard for Encryption (http://ts.vcu.edu/askit/mc-docs/VCUSecurityStandardforEncryption.pdf)
- VCU Web Privacy Statement
- Virginia Freedom of Information Act
- Virginia Privacy Protection Act
- VCU HR Maintenance and Release of Employment and Personal Information Policy
- Policy on Data Integrity Policy
- Policy on Use of University Data and Outside Applications
- Policy on Advancement Services' Request for Services
- Disciplinary Policy
- Policy on Gift Processing

Contacts

The Office of Development and Alumni Relations officially interprets this policy. The Office of Development and Alumni Relations is responsible for obtaining approval for any revisions as required by the policy Creating and Maintaining Policies and Procedures through the appropriate governance structures. Direct policy questions to the Advancement Services' IT manager or the AVP of Advancement Operations.

Procedures

Data collection
Advancement Services collects alumni, donor and constituent data that is needed for valid business purposes or to comply with law. Any such data is obtained only by lawful and fair means. All data is used only for the authorized purpose or in support of university business purposes. DAR strives to maintain the accuracy of the personal data held and establishes mechanisms allowing alumni to review and update or correct their personal information.

Requests for confidential data by DAR employees
Report requests must be submitted through the Advancement Services online Help Desk system. The DAR employee receiving the data is responsible for maintaining the confidentiality of the data. Information in the

reports must not be shared with individuals who do not have explicit approval to see the data. Not all DAR employees will have the same level of access.

Sharing confidential data with other VCU employees
DAR employees are responsible for maintaining the confidentiality of data to which they have access. Confidential data must not be shared between divisions. Confidential information received in a VCU email account should not be forwarded to other individuals who do not have explicit approval to access that information. If confidential data needs to be distributed to individuals across divisions, it should be coordinated with Advancement Services to ensure that only authorized individuals have access to the information. Not all VCU employees have the same level of access.

Requests for confidential data by vendors
Refer to the Development and Alumni Relations policy, Use of University Data and Outside Applications.

Requests for confidential data by volunteers
Volunteers must sign the DAR Confidentiality Agreement, which must be approved by the AVP of Advancement Services before any information can be released to the individual. Nonetheless, the DAR employee is ultimately responsible for the release of the confidential information. All DAR Confidentiality Agreements are kept on file by Advancement Services. Sharing of this data to other volunteers or individuals is prohibited. Report requests that are intended for distribution to volunteers must be clearly identified when the request is submitted. Requests should be made only for the information necessary for volunteers to perform their duties.
If the data file is being used for registration check-in or name tags, then all volunteers handling the information must sign the DAR Confidentiality Agreement. Volunteers must not send mass communications by direct mail or email using this list.
Volunteers are required to delete or destroy all data after the agreed upon period of time.

Credit card data
Alumni, donor or other constituents' credit card numbers must never be saved or stored in any format (paper or electronic). Documents with un-redacted credit card numbers should never be transferred between departments by any means. For processing credit card transactions, refer to the Development and Alumni Relations Policy on Gift Processing**.**

Requests for system access
1. All employees must apply for a license to access the Millennium database and to access other Advancement Services systems' through the Advancement Services Help Desk system.
    a. If access to sensitive systems is being requested, a copy of a signed DAR Confidentiality Agreement must be attached to the access request form.
2. Millennium access
    a. Each dean's office receives a license to access the Millennium database.
    b. Development and Alumni Relations personnel receive a license to access the Millennium database.
    c. Employees of university-affiliated foundations are considered for a license to access the Millennium database, and licenses are granted based on need and availability.
    d. Unit-level employees who are not considered DAR employees are considered for a license to access the Millennium database based on need, availability and recommendation by the unit's director of development.
    e. Requests for access and for the allocation of a Millennium license are directed to Gifts and Records Management for processing and assigning to the appropriate role-based user group.
    f. Requests for Millennium access based on need are directed to the assistant vice president for Advancement Services for approval.
    g. If a user does not access the Millennium system for 60 days, the user is contacted by Advancement Services to verify the need for the license. If no response to a request for

verification of need is received within 30 days, access is removed and reapplication, requiring approval by the assistant vice president for Advancement Services, is necessary.

h. Millennium passwords must be at least eight characters long and must include a capital letter, a number and a symbol. The number cannot be the first or last character in the password.

3. Units must immediately notify Gifts and Records Management, through the Advancement Services Help Desk system, when a user from their area is no longer employed, so access can be terminated.
4. Users with applicable access must comply with data entry and update standards for constituent records maintained in Millennium. Users are contacted by Advancement Services with proper use recommendations for instances of noncompliance.
5. Continued noncompliance could result in a loss of access. In this instance, access restoration requires the approval of the assistant vice president for Advancement Services.
6. Breech of the DAR Confidentiality Agreement could result in loss of license to access the Millennium database and other Advancement Services' systems. Employees are referred to appropriate authorities for any violation of VCU policies or state or federal law.

Forms

See the Advancement Services' Online Request forms at http://staff.oda.vcu.edu/HelpDesk.

Revision History

This policy supersedes the following BOV policy approved in 5/2009:

- 9.1.1 Advancement Information Technology Data Privacy

FAQs

Q: Can sensitive information be saved on a computer hard drive?

A: No. The storing of confidential data on VCU computers and other removable devices is prohibited. The loss or theft of the computer could result in a confidential data breech. All confidential data must be stored on secure network storage systems (Shared/network drive).

If a computer was to be lost or stolen, and if confidential data was stored on the device, then all potential individuals whose data was compromised, must be notified. If the file was stored on a network drive, then notification would not be necessary because the files were not on the computer.

Storing of confidential data on unencrypted portable devices, including but not limited to, iPads and other tablets, cell phones, CDs, DVDs, USB/ flash drives, or external hard drives, is prohibited.

Q: What additional precautions should be taken for VCU-owned laptop computers?

A: Laptop users must follow the general rules for accessing sensitive data, stated above. Additionally, all laptops should have VCU Technology Services-supported hard drive encryption. This is to ensure the protection of data if the laptop is lost or stolen.

Q: Can sensitive information be accessed from my mobile device?

A: Yes. All mobile devices used to access sensitive data must have encryption enabled on them. Encryption is enabled by setting a password for iPhone, iPad and Android devices.

Q: How are sensitive data and systems accessed from off-campus?

A: Confidential information can be accessed from off-campus by logging into the VCU WebVPN client (webvpn.vcu.edu) from a VCU-provided laptop or using a Remote Desktop Connection to access a VCU computer from an off-campus personal computer.

Q: Can sensitive information be sent via email?

A: No. Emailing confidential information to a non-vcu.edu, personal email address is prohibited.

Using VCU FileDrop or other “file upload and send” services is prohibited as this is not a secure method of transferring files. ZixMail, provided by Technology Services, must be used for emailing confidential data (http://ts.vcu.edu/askit/2152.html).

Q: Can sensitive information be accessed from my personal laptop or computer?
A: No. All personal devices used to access sensitive data must use a Remote Desktop Connection to access your VCU computer.

Q: Can sensitive information be accessed from my personal email or other online account?
A: No. Sensitive information should not be sent to personal email or other personal online accounts such as Dropbox, Google Drive, Box, etc. A VCU provided account must be used to access and store this information.

Q: How can sensitive data be safeguarded?
A: Electronic data

- An individual with a legitimate need for access to any of the databases must obtain the proper authorization by filling out an Advancement Services' request form.
- Access accounts and passwords must not be loaned, shared or transferred to others.
- When employment is terminated or when job duties change so an individual no longer needs access, the supervisor must notify Advancement Services immediately.
- Users must log off when they will be away from their computer terminal for a break or any other extended period.
- Electronic mail, other than a @vcu.edu account, is not a secure communication medium and must not be used. Special approval is required to transfer files to and to communicate regarding sensitive information with non-VCU employees.
- VCU FileDrop, YouSendIt.com and other file transfer methods are not secure communication mediums and must not be used.
- Secure File Transfer Protocol (SFTP) and emailing between two @vcu.edu email accounts are the approved methods for transferring confidential data. Please contact Advancement Services if assistance is needed.
- Screen prints and paper downloads must be handled as hard copy.

Hard copy data

- Hard copies containing confidential information must be marked as confidential and the property of that entity.
- Confidential documents must be kept under lock, when possible. Only the source of a confidential document is authorized to share it. Therefore, never share an open copy or a blind copy without the permission of the originator.
- Because of the sensitive nature of the information they contain, biographical and financial reports and other confidential material must not be transmitted by facsimile.
- When confidential information is mailed or sent through intra-office channels, always place it in a sealed envelope and clearly mark it "Confidential."
- Dispose of all confidential documents by shredding when they are no longer needed.