Grand Valley State University
Confidentiality Agreement & Security Policy

Instructions to Sign and Upload:

Option #1: Print, Sign, and Upload
Print this document, sign the last page, then scan the signed document and upload to the Slate Access Request Form in TDX.

Option #2: Sign Electronically and Upload
Download this file and save the file to your computer. Open with Adobe Acrobat. (You can download a free version of Adobe Acrobat at https://get.adobe.com/reader/.)
On the last page, type your name and the date, then click the signature field to generate your electronic signature. Save the file and upload it to the Slate Access Request form in TDX.

Grand Valley State University
Confidentiality Agreement & Security Policy

Grand Valley State University regards security and confidentiality of data and information to be of utmost importance. As such, individuals employed by the University must follow the procedures outlines below:

Confidentiality of Data

Each individual granted access to data and information holds a position of trust and must preserve the security and confidentially of the information they use. Individuals are required to abide by all applicable Federal and State guidelines and University policies regarding confidentially of data including, but not limited to, the Family Education Rights and Privacy Act (FERPA). FERPA protects student information and may not be released without proper authorization. Requests for information/documentation should be referred to the Registrar's Office or the Office of University Counsel.

Individuals with authorized access to Grand Valley University's computer resources, information system, records, or files are given access to use the University's data or files solely for the business of the University. Specifically, individuals should:

1. Access data solely in order to perform their job responsibilities.

2. Not seek personal benefit or permit others to benefit personally from a data that has come to them through their work assignments.

3. Not release University data other than what is required in completion of job responsibilities.

4. Not exhibit or divulge the content of any record, file or information system to any person except as it is related to the completion of their job responsibilities.

Additionally, individuals are not permitted to operate or request others to operate any University data equipment for personal business, to make unauthorized copies of University software or related documentation, or use such equipment for any reason not specifically required by the individuals.

It is the individual's responsibility to report immediately to their supervisor any violation of this policy or any other action, which violates confidentiality of data.

Security Measures and Procedures

Some individuals employed by the University are supplied with a network account to access the data necessary for the completion of their job responsibilities. Users of the University information system are required to follow the procedures outlined below:

1. All transactions, processed by a user ID and password, are the responsibility of the person to whom the user ID was assigned. The user's ID and password must remain confidential and must not be shared with anyone.

2. Access to data may be requested by faculty/staff member and/or the direct supervisor for specific job requirements. The request must be submitted to the data owner for approval. For instance, if an employee (faculty, staff or student) needs access to Banner Student Data to perform their job, the request must be sent to the Registrar's Office for approval and access.

   You are prohibited from viewing or accessing additional information (in any format). Any access obtained without written authorization is considered unauthorized access.

3. Staff shall log off all application and the workstation upon finishing the specific job requirements

4. Passwords should be changed periodically and if there is reason to believe they have been compromised or revealed inadvertently.

5. Upon termination or transfer of an individual, Information Technology will immediately remove access to GVSU data. The GVSU email account remains active for a period of up to 30 days.

Confidentiality Agreement and Security Policy

I understand that my access to University data and information is for the sole purpose of carrying out my job responsibilities. Breach of confidentiality, including aiding, abetting, or acting in conspiracy with any other person to violate any part of this policy, may result in sanctions, civil or criminal prosecution and penalties, loss of employment and/or University disciplinary action, and could lead to dismissal, suspension, or revocation of all access privileges. I understand that misuse of university data and information and any violation of this policy or the FERPA policy are grounds for disciplinary action, up to and including, dismissal.

I have read the above and agree to comply with Grand Valley State University's Confidentiality Agreement and Security Policy, and any updates or revisions published or posted.

Name (please print):_____

Signature:_____

Date:_____