CONFIDENTIALITY, DATA & SECURITY POLICY

PC 11.7

POLICY STATEMENT

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 outlined below.

PROCEDURES

Confidentiality of Data

Each individual granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information they use. Individuals are required to abide by all applicable Federal and State guidelines and University policies regarding confidentiality 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/documents should be referred to the Registrar's Office or the Legal, Compliance & Risk Management Division.

Individuals with authorized access to GVSU 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:

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

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

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

d. 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 individual's job description.

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 systems are required to follow the procedures outlined below:

1. Storage of student or employee confidential data on local storage media (Laptops, Desktops, CDs, Thumb drives, etc) without proper data encryption is strictly prohibited. Please contact Information Technology to discuss secure options if confidential data must be transported outside of the secure network.
2. 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.
3. Passwords should be changed periodically or if there is reason to believe they have been compromised or revealed inadvertently.
4. Upon termination or transfer of an individual, Information Technology will immediately remove access to GVSU data. The email account may stay active for a period of up to 30 days unless a shorter or longer active period is requested by an executive officer.
5. GVSU Owned Computers are for the sole use of the Faculty or Staff Member. Family Members and Friends should not be allowed to use the device.

Access to University data and information is for the sole purpose of carrying out job responsibilities. Breach of confidentiality, including aiding, abetting, or acting in conspiracy with any other person to violate any part of this policy or FERPA 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.

GVSU Security Framework References

- NIST ID.GV-1; PR.AT-1; PR.AT-3; PR-AT-4; PR-AT-5