

## Statement of Responsibility and Rules of Conduct

All UVU employees and authorized system users are responsible for the security and confidentiality of institutional data, records, and reports. Individuals who have access to confidential data (see GRAMA and/or FERPA officer for definition of confidential data) are responsible for maintaining the security and confidentiality of such data as a condition of their employment. The unauthorized use of, or access to, confidential data is strictly prohibited and will subject the individual to disciplinary action up to and including termination and up to and including prosecution to the fullest extent permitted by law.

The system access rules of conduct and user responsibilities include, but are not limited to:

- System users shall not personally benefit or allow others to benefit from knowledge or information gained by virtue of their work assignments or system access privileges.
- System users shall not exhibit or divulge the contents of any record or report containing confidential data to any person, except in the execution of assigned duties and responsibilities.
- System users shall not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.
- System users shall not knowingly expunge or cause to be expunged data from any record or report, except as is a normal part of their duties. Due caution will be exercised in the storage and disposal of documents and reports containing confidential data, including those stored electronically.
- System users shall not publish or cause to be published any reports, records or other information without proper authorization.
- System users shall comply with information security procedures and rules of conduct as promulgated by the University.
- System users shall not share passwords with office workers or anyone else. Passwords that are written down, stored electronically or imbedded within automatic log in procedures must be physically secured, e.g., encrypted, password protected, or physically locked.
- System users are responsible for the proper use of their account, including not allowing others to use their account and insuring that while logged into the account only he/she has access to the account by using means such as password protected screen savers. The system footprints user activity and you will be held responsible for anything done under your login name.
- No person shall aid, abet or act in concert with another to violate any part of these rules.
- System users agree to read, understand and abide by the Appropriate Use of Computing Facilities Policy #441, found at <https://uvu.edu/policies/officialpolicy/policies/show/policyid/86>

Violation of these rules of conduct may subject an individual to loss of information access privileges, to reprimand, suspension, or dismissal in such manner as is consistent with University policies, and to prosecution under federal and state computer and information security laws.

I have **READ** and fully **UNDERSTAND** the Statement of Responsibility and Rules of Conduct printed on this form. I understand that violation of such may result in disciplinary action up to and including the termination of my employment and may also include prosecution under federal and state law.

User signature \_\_\_\_\_

Date: \_\_\_\_\_