



## Information Technology Employee Confidentiality Agreement

In accordance with the trust placed in us by Utah State University and expected by our users, Information Technology (IT) employees are responsible for: 1) maintaining the confidentiality and privacy of the data under our administrative control with the diligent application of the best technology available and 2) providing access only to those who have rights to this information.

These confidential data must not be divulged to any individual or entity without approval via policy, regulation, statute or other lawful direction of the appropriate authorities. Employees are encouraged to seek clarification of the authority of any requests for release of confidential or private information.

Employees will refrain from using their administrative rights to access and review confidential data except as required to carry out their job responsibilities. Such information seen in the course of duties will be kept confidential during and after the term of employment.

Failure to comply with these requirements will result in disciplinary action up to and including dismissal, as well as any civil and criminal penalties that may apply.

Examples of confidential or private data may include, but are not limited to, student academic records, disciplinary action records, health records, financial records, private communications, personal data storage, unpublished research data and notes, network transaction contents, authorization codes for access to personal information, course content and materials, assessment and homework assignments, answer sheets, etc. Specific federal and state laws and regulations itemizing confidential/private data include: Health Insurance Portability and Accountability Act of 1996 ([HIPAA](#)); Family Educational Rights and Privacy Act ([FERPA](#)) (20 U.S.C. § 1232g; 34 CFR Part 99); Utah Government Records Access Management Act ([GRAMA](#)); FTC's "[Red Flag Rules](#)" under the Fair and Accurate Credit Transactions Act; [Sarbanes-Oxley Act](#) of 2002, etc.

If at any time information in the care of IT is thought to be compromised, either your team coordinator, the Office of the VP for IT, or the Office of General Counsel should be notified immediately.

I have read the above agreement and understand these conditions of my employment.

\_\_\_\_\_  
(Employee A-Number)

\_\_\_\_\_  
(Employee Name)

\_\_\_\_\_  
(USU Title)

\_\_\_\_\_  
(Employee Signature)

\_\_\_\_/\_\_\_\_/\_\_\_\_  
(date) mm/ dd / yyyy