**Cloud Storage and Application Policy**

|  |  |  |  |
| --- | --- | --- | --- |
| Date Approved: |  | Revision: |  |

I. PURPOSE

Cloud storage and applications are valuable resources allowing University employees to store large amounts of information and perform collaborative tasks more effectively.  There are, however, risks that must be mitigated in order to properly secure the data that is placed into and processed in the cloud.  The purpose of this Policy is to provide the framework within which Weber State University employees will be expected to operate for storage and processing of Data in cloud environments.

II. SCOPE

This Policy and any of its supporting documents apply to all Weber State University faculty, staff, and anyone doing business with the university that has access to University data.  Information that is not sensitive and is deemed to be the owned by an individual (e.g. lecture notes, videos, PowerPoint slides for classroom teaching) is not covered under this policy.

III. DEFINITIONS

*Cloud Application* - A computer program that does not reside entirely on a desktop or laptop computer which may access University data stored either in cloud storage, directly from a user’s computer storage, or from other University physical storage mediums and where the processing of the data is performed on non-premise computer systems.  The most common applications that fit this definition are any of the ones provided through the Google and Box application store.

*Cloud Storage* – A model of networked online storage where data is stored in virtualized storage pools generally hosted by third parties and in locations not owned by the University

*Data* – Information contained in either University computer systems, cloud storage, or in physical copy that is utilized for the purposes of administering University business or learning.

*Sensitive Information* – Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Weber State University interests, the conduct of University programs or the privacy to which individuals are entitled.  Examples of such data would include the data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the University as requiring protective measures.

*ISO* - Information Security Office

*User* - All persons and/or organizations that have access to University data.

IV. REFERENCES

PPM 10-1, Information Security Policy

PPM 10-2, Acceptable Use Policy

20 U.S.C. § 1232g; 34 CFR Part 99 (FERPA)

15 U.S.C. § 6801 (GLBA)

Utah Code Title 63G Chapter 2 (GRAMA)

42 U.S.C § 1320d-6 (HIPAA)

V. POLICY

All Users who utilize cloud services for storage and/or processing of University data must utilize only University approved and contracted cloud services for such activities.  Anyone wishing to utilize services for any reason outside of the University approved solution, must submit a copy of the contract for such services to University Legal Counsel and to the Information Security Office for review prior to purchase.  Users must also review rights and permissions requested by an application prior to installation to ensure they do not put University data or systems at risk of being compromised.  If the user is unsure of the risk of the rights or permissions requested, they must contact the ISO for further guidance.  Additionally, cloud services users are required to comply with any additional requirements for the storage or processing of University data prescribed in PPM 10-1, Information Security Policy, and PPM 10-2, Acceptable Use Policy.

VI. Exceptions

University employees who are unable to comply with this policy must file an exception.  Exceptions to this policy must be approved by the ISO based on academic or business need and reviewed by the ISTF.  The ISO will review exceptions annually for continued application and notify the exception holder of any concerns.