**FERPA-Compliance**

Like many other government regulations, there’s no formal compliance auditing or certification process. It’s left to the schools and universities to ensure that their IT systems and practices are FERPA-compliant. The Department of Education has established the [Privacy Technical Assistance Center (PTAC)](https://www.ed.gov/open/plan/privacy-technical-assistance-center) with online documentation, webinars, and videos to help schools get familiar with FERPA and inform education IT professionals on security best practices and FERPA compliance

**Policy and governance:** Develop a comprehensive data governance plan that outlines organizational policies and standards regarding data security and individual privacy protection.

**Personnel security:** Create an Acceptable Use Policy that outlines appropriate and inappropriate uses of Internet, Intranet, and Extranet systems.

**Physical security:** Make computing resources physically unavailable to unauthorized users. This includes securing access to any areas where sensitive data are stored and processed, such as buildings and server rooms.

**Network mapping:** Network mapping provides critical understanding of the enterprise (servers, routers, etc.) and its connections.

**Inventory of assets:** The inventory should include both authorized and unauthorized devices used in your computing environment. Usually checked by an automated system monitoring device.

**Authentication:** The ways in which someone may be authenticated fall into three categories: something you know, something you have, or something you are. Two-factor authentication (TFA) combines two of these elements and is more costly, but provides more security.

**Provide a layered defense:** Employ a “Defense in Depth” architecture that uses a wide spectrum of tools arrayed in a complementary fashion.

**Secure configurations:** It is a best practice not to put any hardware or software onto your network until it has been security tested and configured to optimize its security.

**Access control:** Securing data access includes requiring strong passwords and multiple levels of user authentication, setting limits on the length of data access, limiting logical access to sensitive data and resources, and limiting administrative privileges.

**Firewalls and Intrusion Detection/Prevention Systems (IDPS):** A firewall is a device designed to permit or deny network transmissions based upon a set of rules.

**Automated vulnerability scanning:** When new vulnerabilities (to hardware, operating systems, applications, and other network devices) are discovered, hackers immediately scan networks for these vulnerabilities.

**Patch management:** Patch management is the process of using a strategy and plan for the testing and roll out of software updates and patches on a regular basis.

**Shut down unnecessary services:** Each port, protocol, or service is a potential avenue for ingress into your enterprise.

**Mobile devices:** When sensitive data are stored on servers or on mobile devices, such as laptops or smartphones, the data should be encrypted.

**Emailing confidential data:** Consider the sensitivity level of the data to be sent over the email.

**Incident handling:** When an incident does occur it is critical to have a process in place to both contain and fix the problem.

**Audit and compliance monitoring:** Audits are used to provide an independent assessment of your data protection capabilities and procedures.

Source: <https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Security%20Checklist_0.pdf>

Weber State Currently Insists these 3 Rules must be followed to comply with FERPA:

1. Electrically stored must be encrypted, physical security must be around

2. Ensure the students are trained with FERPA certificates

3. Does it make sense for the individual to have FERPA. (Need to know)

If data is kept internal WSU is in charge of data, once third-party apps are involved it will need to be looked into individual

Weber State University Important Contact information

* Jonathan Karras - jonathankarras@weber.edu x7529 - Network including firewall.
* Mark Buxton - markbuxton@weber.edu x - Servers
* Florian Stellet - florianstellet@weber.edu x - Security (FERPA Specialist)
* Peter Waite - pwaite@weber.edu x8597 - Director of Application Development Services
* Shelly Belflower - sbelflower@weber.edu x8610 - Director of Academic Technology (classroom tech)