Title:	Reporting Security Guidelines

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	12/14/2020		
Related Policies or Procedures:	EWU 203-01: Information Security EWU 401-06: Protected Health Information (PHI) Password Complexity and Expiration Requirements		

History

Revision Number:	Change:	Date:
1.0	Initial version	12/14/2020

A. Purpose

This procedure details the security requirements for university employees, including student employees, with access to institutional reporting systems and databases.

B. Definitions

FERPA - The Family Education Rights and Privacy Act (FERPA) of 1974

Data Custodian – Individuals officially designated by the President whose position is accountable for the oversight and general operation of data systems that serve the university community.

C. Procedure

The following rules apply to all university employees with reporting access:

1. All employees of Eastern Washington University (administrative, academic, staff and students) are required to abide by the policies governing review and release of student education records. FERPA mandates that information contained in a student's education record must be kept confidential and outlines the procedures for review, release and access of such information. A complete policy statement on the Eastern implementation of FERPA guidelines can be found at https://inside.ewu.edu/records-and-registration/ferpa/
2. Account sharing is strictly prohibited by university policy and procedure. Employees shall use their own username. Each employee given a username is held responsible for any data retrieved using that username. Passwords are to be kept confidential and are not to be shared or given to anyone, including supervisors, co-workers, student employees, or friends. It is the responsibility of each employee to keep his/her password confidential and to change passwords whenever he/she feels someone else may have obtained access to it.

Approval for access to institutional data will be granted to those individuals who have been determined to have a

legitimate educational interest in the data by the appropriate data custodian(s). Individuals who have been granted access to student data must understand and accept the responsibility of working with confidential student records. In part, the policy states that officials of the University may be given access to student education records on a "need-to know" basis and that such access must be limited to job-related, legitimate educational interests. The information contained in a student's education record shall not be released to a third party without written consent of the student. Such requests for information should be referred to the Records and Registration office.

Examples of inappropriate use of student records are:

1. Releasing confidential (non-directory) information to another student, university employee, parent, or anyone not having legitimate educational interest, without the student's written consent.
2. Leaving reports or computer screens containing confidential student information logged on or in view of others, who do not have legitimate educational interest in the data.
3. Giving your personal password to anyone for any reason.
4. Discussing the information contained in the student record outside of the University or while on the job with individuals who do not have a legitimate educational interest in the information (need-to-know.)

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.