# FERPA Compliance Policy for Individual Evaluations in Cybersecurity Team Projects

## Effective Date

Spring 2025

## Prepared by

Ran Hinrichs

## Applicable To

Faculty, Evaluators, and Program Coordinators overseeing professional evaluations in the University of Washington Spring Cybersecurity Framework Project

## Purpose

This policy outlines procedures to ensure that the evaluation process for cybersecurity team projects complies with the Family Educational Rights and Privacy Act (FERPA), safeguarding student privacy and the confidentiality of education records.

## Scope

This policy applies to all evaluation documents, digital tools, and workflows associated with the individual assessment of team members participating in University of Washington’s Spring 2025 cybersecurity project courses.

## Policy Statements

## 1. Confidential Record Keeping

Individual evaluations are created and stored in non-public, secure digital formats (e.g., .docx files). Files are labeled with student names only for internal organizational purposes and are not shared in bulk or group formats.

## 2. Legitimate Educational Interest

All evaluations are conducted by instructors or evaluators who have a legitimate educational interest under FERPA, specifically those responsible for assessing course performance and learning outcomes.

## 3. Secure Distribution

Evaluations are distributed exclusively via institutionally approved platforms (e.g., Canvas, encrypted university email, secure LMS folders) that enforce authentication and access control. Under no circumstances will evaluations be shared via public links, open folders, or external tools without role-based access.

## 4. No Public Disclosure of Educational Records

Student evaluations are not posted in shared repositories (e.g., GitHub, Google Drive, OneDrive) without access restriction. Student names, evaluation summaries, and role performance feedback will never be publicly disclosed without explicit written consent.

## 5. Use of AI and Data Protection

AI-generated content is used in support of educational evaluation, not for decision automation. No personally identifiable student information is retained by any AI service. All AI interaction is conducted on platforms approved or safeguarded by the evaluator’s data privacy standards.

## 6. Audit and Retention

Evaluation records are retained in accordance with university academic record-keeping policies and may be archived or deleted in line with departmental guidance.

## 7. Incident Reporting

Any suspected FERPA violation or unauthorized disclosure of educational records must be reported immediately to the university’s FERPA compliance officer or registrar’s office.

## Review and Amendments

This policy will be reviewed at the end of each academic term and may be updated in response to changes in university guidance, FERPA interpretations, or digital evaluation practices.

## Approval

This policy is issued by the evaluator in compliance with university FERPA standards and ethical evaluation practices.