# UW Professional Evaluation Summary (Post-Reset Reboot Protocol)

## Purpose:

This document defines the streamlined process for evaluating professionals participating in the University of Washington Spring 2025 Cybersecurity Framework project. These individuals are not students and should not be evaluated through academic development frameworks or Co-Op eligibility models. Evaluations are based on professional role execution and NICE Work Role expectations.

## 1. Evaluation Model

- Target Group: Practicing cybersecurity professionals.  
- Role Assignment: Based on NICE Framework Work Roles assigned per team.  
- Evaluation Basis:  
 - Performance in team deliverables (e.g., NIST CSF 2.0, Threat Model, SOW, FCI, Supply Chain)  
 - Alignment of deliverable contributions with the responsibilities of the assigned role  
 - Use of AI in content development (based on AiBQ – AI Behavior Quotient model)

## 2. Individual Evaluation Format (Per Team Member)

Each individual's evaluation will include:  
- Assigned Role: NICE Framework Role Name and ID  
- Contribution Summary: A short narrative (1–2 paragraphs) evaluating the alignment of their observed contributions with role expectations  
- AI Behavior Quotient (AiBQ):  
 - Classification: AI-Augmented / AI-Interrogated / AI-Transformed  
 - Brief comment on AI interaction style (e.g., Did the individual revise, localize, or synthesize AI-generated content?)  
- No Co-Op, learning trajectory, or Year 1–3 pathway information will be included

## 3. Team Evaluation Format

- Team Function Summary: Overview of group effectiveness based on how well individual roles contributed to deliverable completion  
- Role Integration: Did assigned responsibilities (e.g., IR Planning, Policy Drafting, Threat Modeling) align across members?  
- Collaboration & Communication: Evidence of technical handoffs, referencing, or shared workflows  
- AI Integration Summary: Composite team score based on observed use of AI tools and engagement quality

## 4. Data Sets Required for Execution

To generate individual and team evaluations, the following files must be uploaded:  
- Student Profiles Folder (e.g., "UW Students Profiles.zip") containing:  
 - CyberGEN.IQ report or analysis for each member  
 - Role assignment evidence (from Formation document or file structure)  
 - Key artifacts authored or contributed to by each individual (e.g., Threat Model doc, IRP, SOW)  
- Team Formation Document (e.g., "UW\_CSF\_Team\_Formations\_Final.docx") containing:  
 - Team names and roles assigned to each member  
- Team Deliverables Folder (e.g., "UW Q2.zip") containing:  
 - Finalized versions of: NIST CSF 2.0 Outline, Statement of Work, Threat Model, Supply Chain Paper, FCI Assessment  
Optional: Cincinnati Example (if re-calibration to prior format is needed)

## 5. Reboot Keywords for Reactivation (Post-Reset)

When re-uploading, simply state: “Let’s resume UW Q2 Evaluations.”  
This will trigger:  
- Activation of this document  
- Re-application of the professional rubric model (short format, no Co-Op framing)  
- AiBQ analysis and NICE Role alignment as core structure

## Prepared by:

ChatGPT on behalf of Ran Hinrichs  
Date: Spring 2025