Employer-Sponsored Project Brief

Faculty, program leaders, employer partners, and students | Project Brief

Project title: _____ **Employer / sponsor:** _____

Course / program: _____ **Faculty lead:** _____

Sponsor contact: _____ **Project period:** _____

Use this brief before students begin an employer-sponsored cybersecurity project. The goal is to create a bounded learning experience with explicit authorization, sanitized or appropriately controlled information, realistic deliverables, and a clear approval path. Do not use a student project to perform unauthorized testing, expose live credentials, disclose regulated or proprietary data, or place students in a production environment without the institution and sponsor deliberately approving the risk and supervision model.

1. Learning and Business Context

Prompt	Project record
Business / mission context	
Student learning outcomes	
Why this project is suitable for students	
What success will look like for the sponsor	
What success will look like for the course / program	

2. Scope and Boundaries

In scope	Out of scope / prohibited
Systems, artifacts, data sets, or environments explicitly approved for the project.	Any system, account, network, device, tenant, or data not explicitly authorized in writing.
Approved analysis, design, documentation, automation, simulation, policy, awareness, or defensive validation tasks.	Unapproved scanning, exploitation, credential use, persistence, social engineering, destructive testing, or bypass of controls.
Sanitized or synthetic information supplied for learning when production data is unnecessary.	Live secrets, personal data, regulated data, proprietary source, customer data, or sensitive incident material unless a specific approved handling process exists.
Deliverables listed in this brief.	Operational changes to sponsor systems unless separately authorized, supervised, tested, and approved.

3. Deliverables and Acceptance

Deliverable	Audience	Required evidence / contents	Acceptance owner	Due
Project plan				
Midpoint evidence / prototype				

Deliverable	Audience	Required evidence / contents	Acceptance owner	Due
Technical or analytical deliverable				
Executive / stakeholder summary				
Handoff / reproducibility notes				

4. Milestones and Decision Gates

Gate	Date / window	Student output	Sponsor / faculty decision
Kickoff and scope confirmation			Proceed / revise
Data / environment readiness			Approved for student use / substitute materials
Midpoint review			Continue / redirect / reduce scope
Draft review			Approve revisions / request changes
Final acceptance			Accepted / accepted with notes / returned for correction

5. Data, Privacy, Security, and Authorization

[ ] The sponsor identifies who owns the project data, artifacts, and final deliverables.

[ ] The project uses synthetic or sanitized data unless real data is genuinely necessary and approved under institutional and sponsor requirements.

[ ] Students are told exactly what information may not be copied into personal storage, public repositories, AI tools, screenshots, presentations, resumes, or portfolios.

[ ] Credentials, API keys, tokens, recovery codes, private keys, secrets, and sensitive configuration values are never embedded in student deliverables or public repositories.

[ ] Any security testing has written authorization that identifies the environment, technique boundaries, time window, sponsor contact, stop conditions, and escalation path.

[ ] The project environment is separated from unrelated production systems when practical, and reset / recovery responsibility is known.

[ ] Sponsor and institution contacts know how to report accidental exposure, suspicious activity, scope questions, or a need to stop work.

6. Student-Safe Handling Expectations

Area	Expectation
Repositories and files	Use only approved storage and access controls. Do not make sponsor material public by default.
Screenshots and recordings	Capture only what is necessary; remove identities, secrets, internal addresses, customer data, and other restricted details.
AI-assisted work	Follow course and sponsor rules. Do not submit sponsor-confidential or sensitive material to an external AI service unless specifically approved.

Area	Expectation
Communication	Use approved channels and include the faculty lead on scope, risk, or access changes.
Portfolio use	Students may publish only the sanitized artifacts and descriptions the sponsor and faculty have approved for public use.
End of project	Return or delete sponsor information as required and revoke project access that is no longer needed.

7. Contacts, Escalation, and Change Control

Role / trigger	Primary contact	Backup / escalation	Expected response
Scope clarification			
Access or environment issue			
Privacy / data concern			
Security event / stop-work trigger			
Deliverable approval			

[ ] Any change to scope, data, access, testing method, deliverable, or deadline is recorded before students act on it.

[ ] Faculty retains authority to stop or redesign the learning activity when the sponsor request conflicts with course outcomes, student safety, institutional policy, law, or authorization boundaries.

[ ] Students know that “the sponsor asked” is not a substitute for documented authorization when access or security testing is involved.

8. Final Approval and Handoff

Approval / record	Name / date / notes
Sponsor scope approval	
Faculty academic approval	
Environment / data cleared for student use	
Final deliverables accepted	
Public / portfolio artifacts approved	
Access closed and data handled per agreement	

Source and use

Bare Metal Cyber Educators Hub, Dr. Jason Edwards. Industry & Workforce Partnership Toolkit - Employer-Sponsored Project Brief.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Keep the Bare Metal Cyber Educators Hub URL below intact. Use fictional, sanitized, or appropriately authorized data where applicable and follow institutional and sponsor policy.

Read online: https://educate.baremetalcyber.com/resources/employer-sponsored-project-brief/