The Complete Cybersecurity Educator

Editable Companion Resources

Dr. Jason Edwards

Companion Use and Permissions

These resources accompany *The Complete Cybersecurity Educator*. The original purchaser may edit, print, and reproduce the identified classroom and program resources for use with that purchaser's own students, colleagues, or program participants. The resources may not be resold, posted publicly, or incorporated into another commercial product without written permission.

All cybersecurity activities require lawful authorization, appropriate supervision, safe environments, privacy protection, accessibility, and a documented recovery path. Replace fictional names and scenarios only with other fictional or properly authorized material. Never place real passwords, recovery codes, regulated records, employer data, or student secrets into a classroom handout or public portfolio.

This companion is intentionally editable. Add local policies, contacts, accessibility support, version information, and source dates before use.

Final release status: The companion text and workbook were developmentally reviewed and verified on September 15, 2026. Volatile laws, certifications, programs, tools, prices, and platform rules still require local revalidation before deployment.

Resource Index

Resource group	Included resources	Primary book connection
Lesson plans	Twelve complete K-12 lessons across four grade bands	Chapters 7-9 and 13-14; Appendix C
Student worksheets	Privacy, message analysis, risk, timeline, source evaluation, and career-evidence forms	Chapters 4, 8, 14, 20-24
Lab runbooks	Message triage, account recovery, log triage, configuration review, and tabletop templates	Chapter 10; Appendix F and I
Assessment tools	Blueprints and rubrics for labs, cases, teamwork, ethics, presentations, and capstones	Chapters 19-23; Appendix G
Mentoring and work-based learning	Mentoring agreement, meeting record, internship plan, check-in, and portfolio review	Chapters 24-26; Appendix K
Partnership and funding	Outreach brief, partner review, grant concept, and sustainability plan	Chapters 26-27; Appendix K
Remote instruction	Home-office and remote-course readiness checklists	Chapter 11
Curriculum maintenance	Inventory, change request, release record, backlog, risk register, and handoff test	Chapter 30 and companion workbook

Resource group	Included resources	Primary book connection
Question banks	Complete 350-item legacy source bank with final editorial dispositions, thirty-five resolved issue items, and the sixty revised print questions	Appendix L and companion workbook

Standard Editable Lesson-Plan Template

Title: Grade band: Time: Course or unit: Version and review date:

Learning Outcome

The learner will be able to...

Evidence of Learning

The learner will produce or demonstrate...

Materials and Access

- Required materials:
- Approved devices, applications, or accounts:
- No-device alternative:
- Accessibility supports:

Safety, Privacy, and Authorization

- Authorized environment and actions:
- Prohibited actions:
- Data restrictions:
- Safeguarding or reporting path:
- Stop conditions:

Preparation

1. 2. 3.

Launch

Guided Learning

Learner Activity

Debrief

Assessment

Differentiation and Extension

Family or Community Extension

Instructor Reflection

- What evidence showed learning?
- Where did learners struggle?
- What should change before the next delivery?

Lesson Set 1: K-3

Lesson 1.1 - Safe Choice Traffic Light

Time: 30 minutes **Outcome:** Learners will classify fictional online situations as **stop**, **slow down and ask**, or **safe to continue with permission**.

Materials

- Red, yellow, and green cards
- Six fictional scenario cards
- “My Safe Choice” worksheet
- Picture symbols or objects for nonreaders

Safety and Privacy

Do not ask learners to describe real incidents publicly. Use fictional names and services. Follow school safeguarding procedures if a learner shares a concern.

Preparation

Create scenarios such as:

- A familiar teacher opens an approved class website.
- A pop-up says the learner won a prize and asks for a home address.
- A game asks to turn on a camera.
- A classmate sends a kind message.
- An unknown person asks the learner to keep a conversation secret.
- A device asks whether to install an update while the learner is in class.

Launch

Show a traffic light and ask how it helps people make safe decisions. Explain:

- **Red - Stop:** Do not click, reply, download, or share.
- **Yellow - Slow down and ask:** Find a trusted adult before continuing.
- **Green - Continue as directed:** The activity is expected, approved, and appropriate.

Guided Learning

Model two scenarios. Think aloud about who is asking, what action is requested, what information could be exposed, and which adult is responsible for the activity.

Learner Activity

Read or show one scenario at a time. Learners hold up a card and explain one reason. Accept more than one defensible answer when the learner identifies missing information and chooses to ask.

Evidence and Assessment

Each learner completes three final scenarios. Mastery is demonstrated when the learner:

- Uses the stop-or-ask routine rather than acting impulsively

- Identifies an appropriate trusted adult
- Can explain one risk or uncertainty in age-appropriate language

Debrief

- Why can asking be a strong choice?
- What should happen after an accidental click?
- Why should adults avoid making learners afraid to report mistakes?

Family Extension

Families select a phrase the child can use when asking for help, such as “Something unexpected happened on the screen. Can you help me check it?”

My Safe Choice Worksheet

Situation	Stop	Ask	Continue with permission	Why?

Lesson 1.2 - The Secret Is Not the Password

Time: 30 minutes **Outcome:** Learners will explain that passwords and recovery codes protect access and should be handled with trusted adult guidance.

Materials

- Paper treasure-box picture
- Example cards labeled “password,” “recovery code,” “favorite animal,” “drawing,” and “nickname”
- Fictional account cards

Safety and Privacy

Do not ask learners to create, write, or say a real password. All examples must be invented and should never resemble school or family credentials.

Launch

Show the paper treasure box. Explain that an account secret is more like a key than a personal secret about feelings or safety. Children should always tell a trusted adult about something that makes them uncomfortable, even if someone says it is a secret.

Guided Learning

Explain:

- Passwords and recovery codes control access.
- They are not shared with friends or strangers.
- A parent, guardian, or responsible school adult may help manage a child's account.
- A person who pressures a child to hide an online interaction from trusted adults is creating an unsafe situation.

Learner Activity

Learners sort cards into:

- **Account key - protect with adult help**
- **Okay to share in the class activity**
- **Ask before sharing**

Discuss why context matters. A pet's name may seem harmless but could be used as an account-recovery answer.

Evidence and Assessment

Learners complete the sentence: “An account key should be protected because...” and identify one trusted adult who can help after an account problem.

Debrief

- What is the difference between a password and a secret about being hurt or afraid?
- Why should a child tell an adult after a password is exposed?
- How can adults help without blaming the child?

Family Extension

Families review who manages the child's accounts and how the child should report an unexpected sign-in prompt. No credentials are recorded on the worksheet.

Lesson 1.3 - Kindness, Evidence, and Help

Time: 35 minutes **Outcome:** Learners will choose a safe response to harmful online behavior without retaliating or spreading the content.

Materials

- Fictional chat cards
- “Help, Do Not Spread” poster
- Role cards: learner, trusted adult, bystander, and helper

Safety and Privacy

Keep examples mild and fictional. Do not ask learners to act out abusive language. Follow safeguarding procedures for any real disclosure.

Launch

Ask whether showing an unkind note to everyone makes the problem smaller or larger. Introduce three goals: protect the person, preserve only what is needed for help, and avoid spreading harm.

Guided Learning

Model the response:

1. Do not reply in anger.
2. Do not repost the harmful content.

3. Save or show appropriate evidence if a trusted adult requests it.
4. Block or mute through approved tools when appropriate.
5. Tell a trusted adult or use the school's reporting process.
6. Support the affected person with kindness.

Activity

Small groups receive a fictional situation and role cards. They create a two-minute safe-response demonstration using respectful language. Rotate roles.

Evidence and Assessment

Learners are successful when their response avoids retaliation, identifies a help path, and protects the affected person from additional exposure.

Debrief

- Why can reposting make harm worse?
- What evidence might a trusted adult need?
- How can a bystander help?
- Why should reporting be easy and free from shame?

Lesson Set 2: Grades 4-6

Lesson 2.1 - The Privacy Puzzle

Time: 45 minutes **Outcome:** Learners will explain how several ordinary details can combine to reveal identity, location, routine, or account-recovery information.

Materials

- Fictional profile cards
- Detail cards
- Privacy puzzle worksheet
- Highlighters

Safety and Privacy

Use only fictional details. Learners must not record real addresses, schedules, account names, passwords, recovery answers, or live locations.

Launch

Show three cards: a school mascot, a sports schedule, and a photo with a street sign. Ask what a stranger could infer when the details are combined.

Guided Learning

Define four questions:

- Who can see the information?
- Why is it being shared?
- What could be learned when it is combined with other information?
- Is there a safer way to meet the same purpose?

Activity

Teams receive a fictional profile and ten detail cards. They build two versions:

- A risky version that exposes unnecessary detail
- A safer version that still communicates the person's interests or achievement

Teams explain which details were removed, generalized, delayed, or shared only with permission.

Evidence and Assessment

Each learner identifies one detail that changes classification when context changes and one way to reduce exposure without eliminating all participation.

Debrief

- Why is privacy not the same as hiding everything?
- What information should never be used in a classroom example?
- Why do privacy settings not guarantee that content stays private?

Privacy Puzzle Worksheet

Detail	Intended audience	What could be inferred?	Safer alternative

Lesson 2.2 - Phishing Detective Case File

Time: 50 minutes **Outcome:** Learners will analyze fictional messages using context, identity, action, pressure, destination, and data.

Materials

- Four nonclickable fictional messages
- Case-file worksheet
- Approved reporting-flow card

Safety and Privacy

Do not send deceptive messages through real accounts. Use invented organizations and links. Learners must not interact with any destination.

Launch

Display a well-written fictional message with correct spelling and branding but an unexpected request. Ask why appearance alone is weak evidence.

Guided Learning

Teach the **CIAPDD** check:

- **Context:** Was the request expected?
- **Identity:** Can the sender be verified independently?
- **Action:** What does the message want?
- **Pressure:** What emotion or urgency is used?
- **Destination:** Where would the action lead?
- **Data:** What information, money, access, or approval is at risk?

Activity

Pairs analyze four messages. One should be legitimate, one deceptive, one ambiguous, and one sent from a compromised fictional account. Learners must record uncertainty rather than force every message into “safe” or “scam.”

Evidence and Assessment

A complete case file must include the safest verification method and reporting path. Grade evidence quality rather than the number of suspicious cues highlighted.

Debrief

- Which cue was easy to fake?
- How can a compromised real account change the analysis?

- What should happen after credentials are exposed?

Lesson 2.3 - Device Care and Recovery Plan

Time: 45 minutes **Outcome:** Learners will create a practical device-care plan covering updates, screen lock, approved applications, backups, account recovery, and reporting.

Materials

- Fictional device profile
- Device-care checklist
- Recovery sequence cards

Safety and Privacy

Do not inspect learner devices or ask for real settings, accounts, or recovery information. Use a fictional device profile.

Activity

Learners review a fictional device with these conditions:

- Updates postponed for several weeks
- No screen lock
- Photos stored only on the device
- An unfamiliar application requesting broad permissions
- A lost recovery code
- A recent unexpected sign-in alert

Learners create a prioritized plan. They must identify which steps need adult or institutional support and which evidence should be preserved.

Assessment

Score prioritization, explanation, recovery thinking, and recognition that one control does not solve every problem.

Debrief

- Why is a backup different from synchronization?
- Why should recovery be planned before a device is lost?
- Which actions could destroy useful evidence?

Lesson Set 3: Grades 7-8

Lesson 3.1 - Identity Lifecycle Map

Time: 55 minutes **Outcome:** Learners will map proofing, provisioning, authentication, authorization, review, change, recovery, and deprovisioning for a fictional account.

Materials

- Identity lifecycle cards
- Fictional school-club account scenario
- Mapping worksheet

Safety and Privacy

Use a fictional account and invented roles. Do not review real school directory information or account settings.

Activity

Teams arrange lifecycle cards for a new student club member. The scenario then changes: the learner becomes treasurer, loses a device, and later leaves the club. Teams update access and identify risks at each transition.

Evidence

An annotated lifecycle map showing who approves access, how authentication is protected, how access is reviewed, and how sessions and credentials are removed.

Debrief

- Why can an unused account remain dangerous?
- How can recovery become an alternate attack path?
- What evidence should exist after access changes?

Lesson 3.2 - Social Engineering Verification Drill

Time: 50 minutes **Outcome:** Learners will respond to pressure-based requests using independent verification and documented reporting.

Materials

- Role cards
- Request cards
- Verification-plan worksheet

Safety and Privacy

Do not target real students with surprise deception. All requests are announced classroom simulations.

Activity

Learners rotate through roles: requester, recipient, verifier, and observer. Request cards include authority, urgency, curiosity, fear, and reward. The recipient must avoid using contact details contained in the request and select a separately trusted verification channel.

Evidence

The observer records pressure technique, recipient action, verification path, and one improvement.

Debrief

- Which pressure technique was hardest to resist?
- Why can helpfulness create risk?
- How should organizations design reporting so people do not feel blamed?

Lesson 3.3 - Secure Configuration Review

Time: 60 minutes **Outcome:** Learners will identify and prioritize security weaknesses in a sanitized configuration excerpt.

Materials

- Fictional configuration sheet
- Risk-ranking cards
- Recommendation template

Safety and Privacy

No live system access is required. The configuration is invented and contains no operational target information.

Activity

The fictional configuration includes:

- Shared administrator account
- Unused account still active
- Logging disabled for account changes
- Overly broad access rule
- Unprotected backup share
- Missing owner and review date

Teams identify evidence, risk, recommendation, operational consequence, test, and rollback for each issue.

Assessment

Use accuracy, prioritization, consideration of operational impact, and verification plan.

Debrief

- Why can a technically stronger setting still create operational risk?

- What should happen before a configuration is changed?
- Which finding should be addressed first, and what evidence supports that decision?

Lesson Set 4: Grades 9-12

Lesson 4.1 - Incident Timeline and Competing Hypotheses

Time: 70 minutes **Outcome:** Learners will build an evidence-based timeline and maintain at least two plausible explanations until evidence distinguishes them.

Materials

- Sanitized fictional log set
- Timeline worksheet
- Hypothesis table
- Briefing template

Safety and Privacy

All data are invented. No malware, live target, real account, or personal information is included.

Activity

Learners normalize timestamps, identify relevant events, label statements as fact/inference/unknown, and create two hypotheses. The instructor then provides an additional log entry that supports one hypothesis but does not prove attribution.

Evidence

Timeline, hypothesis table, next-evidence request, and one-minute briefing.

Debrief

- Which early conclusion was tempting but unsupported?
- How did missing logs affect confidence?
- What action could be justified before attribution was known?

Lesson 4.2 - Threat Model a Student Service

Time: Two 55-minute sessions **Outcome:** Learners will identify assets, users, trust boundaries, misuse cases, and safeguards for a fictional student service.

Materials

- Fictional service description
- Data-flow template
- Threat-model worksheet

Safety and Privacy

The service is conceptual. Learners do not test a real application or use real student data.

Activity

Teams design a fictional service for scheduling tutoring appointments. They identify:

- Users and administrators
- Data collected and purpose
- External services
- Trust boundaries
- Misuse cases
- Identity and access requirements
- Privacy and retention decisions
- Logging, recovery, and abuse-reporting needs

Evidence

Data-flow diagram, prioritized threats, design decisions, and residual risk.

Debrief

- Which risk was created by a convenience feature?
- What data could be removed entirely?
- How should the service recover after account compromise?

Lesson 4.3 - Executive Security Briefing

Time: 70 minutes **Outcome:** Learners will translate technical evidence into a concise decision briefing for a nontechnical audience.

Materials

- Fictional incident packet
- Executive briefing template
- Communication rubric

Activity

Teams receive technical findings, business context, user impact, and incomplete evidence. They prepare a three-minute briefing containing:

- Confirmed facts
- Current impact
- Actions completed
- Decision requested
- Options and tradeoffs
- Uncertainty and next evidence
- Next update time

A second team plays the executive audience and asks questions about mission, cost, legal concern, user impact, and recovery.

Evidence

Briefing, question responses, and revision after feedback.

Debrief

- What technical detail was important but did not belong in the opening?
- What consequence needed clearer explanation?
- How can uncertainty be communicated without appearing unprepared?

Student and Learner Worksheets

Worksheet 1 - Information Classification

Scenario or activity: Audience and purpose:

Information item	Public	Personal - ask first	Sensitive/ private	Why?	Safer alternative

Reflection:

- Which item changed classification because of context?
- What could be inferred by combining two or more items?
- What information was not necessary for the purpose?

Worksheet 2 - Suspicious Message Evidence Record

Evidence question	Observation
What is the message asking the recipient to do?	
Was the request expected?	
What identity is claimed?	
What pressure, authority, fear, curiosity, or reward is used?	
What information, money, access, or approval could be exposed?	
What destination or attachment is involved?	
How can the request be verified independently?	
What is the reporting path?	
What facts remain unknown?	

Decision: Reasoning: Action after an accidental click or disclosure:

Worksheet 3 - Risk Relationship Map

Objective or mission: Asset or service:

Threat or harmful condition	Vulnerability or exposure	Existing control	Likelihood evidence	Impact evidence	Proposed action	Residual risk

Avoid false precision. Explain the evidence and uncertainty behind any rating.

Worksheet 4 - Incident Timeline and Hypothesis Table

Timeline

Time	Source	Observed event	Fact, inference, or unknown	Reliability or limitation

Competing Hypotheses

Hypothesis	Supporting evidence	Contradicting evidence	Evidence needed next	Confidence and reason

Status Update

- Confirmed:
- Not confirmed:
- Actions completed:
- Decision requested:
- User or mission impact:
- Next update:

Worksheet 5 - Source and Claim Evaluation

Claim	Source	Original or interpreted source?	Date/ version	Evidence provided	Limitations	Use, qualify, or reject?

Questions:

- Is the source authoritative for this specific claim?
- Is the source current enough for the decision?
- Does the claim exceed the evidence?
- Is a commercial, political, or institutional interest relevant?
- Can the information be corroborated?
- What would change the conclusion?

Worksheet 6 - Career Evidence Inventory

Target role or capability	Evidence already available	Gap	Next project or learning action	Reviewer	Completion date

For each portfolio artifact, document:

- Problem and audience
- Authorization and boundaries

- Method
- Evidence
- Result
- Limitation
- Communication product
- Reflection and next improvement
- Confidentiality review before publication

Editable Lab Runbooks

Runbook 1 - Suspicious Message Triage

Lab ID: MSG-TRIAGE-01 **Outcome:** Analyze fictional messages and select safe verification and reporting actions. **Environment:** Printed or offline digital evidence set; no live links. **Time:** 30-60 minutes.

Authorization and Boundaries

- Only instructor-supplied fictional messages may be analyzed.
- Learners do not click, reply, download, call, scan, or enter information.
- No real person or organization is impersonated.
- If a real suspicious message is discovered, stop the exercise and use the institution's reporting process.

Instructor Preparation

1. Create or review three to six messages.
2. Confirm every link and contact is inert or fictional.
3. Include at least one legitimate but unusual message and one ambiguous message.
4. Print or distribute the evidence record.
5. Verify the reporting flow used in the course.

Expected Learner Evidence

- Context, identity, action, pressure, destination, and data analysis
- Independent verification method
- Reporting decision
- Response after accidental exposure
- Statement of unresolved uncertainty

Reset

Collect or delete learner copies if required, remove annotations containing personal information, restore the clean evidence set, and record confusing cues for revision.

Common Failure Modes

- Treating spelling errors as the primary indicator
- Assuming familiar branding proves identity

- Using contact information contained in the suspicious message
- Declaring a message malicious without sufficient evidence
- Failing to describe action after credentials are exposed

Runbook 2 - Identity and Account Recovery Design

Lab ID: IAM-RECOVERY-01 **Outcome:** Evaluate identity lifecycle and recovery controls for a fictional service. **Environment:** Diagram and scenario; optional approved test tenant. **Time:** 45-75 minutes.

Scenario Elements

- Account proofing
- Provisioning and role assignment
- Password or passkey enrollment
- Multifactor or phishing-resistant authentication
- Registered device
- Recovery code
- Help-desk or support recovery
- Session revocation
- Access review
- Deprovisioning

Learner Tasks

1. Map the normal identity lifecycle.
2. Map two recovery paths.
3. Identify abuse cases for support, device loss, and recovery codes.
4. Recommend proofing, notification, rate limiting, logging, review, and session controls.
5. Address accessibility and continuity.
6. Explain residual risk.

Instructor Verification

- No real account information is used.
- Recovery does not depend on one unverified channel.
- Learners distinguish authentication from authorization.
- Deprovisioning and active-session revocation are included.

Evidence

Lifecycle diagram, misuse-case table, control recommendations, and two-minute design briefing.

Runbook 3 - Sanitized Log Triage

Lab ID: LOG-TRIAGE-01 **Outcome:** Build a timeline, identify relevant evidence, and maintain competing hypotheses. **Environment:** Offline text or spreadsheet data set. **Time:** 60-90 minutes.

Data Design

Include a small set of:

- Authentication events
- Administrative changes
- File or service access
- Endpoint or application alert
- Benign background events
- Missing fields or time-zone differences

Do not include real user data, public IP attribution claims, active malware, or operational secrets.

Learner Tasks

1. Identify the data source and limitations.
2. Normalize time and sort events.
3. Mark events as relevant, background, or uncertain.
4. Build two hypotheses.
5. Identify evidence needed next.
6. Recommend proportionate containment that protects evidence and operations.
7. Produce a status update.

Scoring Evidence

- Timeline accuracy
- Fact/inference distinction
- Quality of competing hypotheses
- Proportionality of actions
- Communication of uncertainty

Reset and Revision

Restore the clean data set. Review whether any clue made the intended answer obvious. Add alternative explanations if the activity rewarded guessing or premature attribution.

Runbook 4 - Configuration Review and Change Plan

Lab ID: CONFIG-REVIEW-01 **Outcome:** Identify weaknesses in an approved configuration and propose testable, reversible changes. **Environment:** Invented text configuration or isolated lab. **Time:** 60-90 minutes.

Required Finding Fields

Finding ID	Evidence	Risk relationship	Recommendation	Operational consequence	Test	Rollback	Priority

Instructor Preparation

Create six to ten findings across identity, logging, network rules, updates, backups, ownership, and recovery. Include at least one setting that appears weak but is justified by a documented dependency so learners must ask questions rather than mechanically harden everything.

Stop Conditions

Stop if the environment reaches an unapproved network, uses real credentials, or affects a service outside the exercise. Preserve evidence and notify the lab owner.

Debrief

- Which recommendation reduced risk but created the largest operational consequence?
- Which change required sequencing or a compensating control?
- How would the team verify success and detect regression?

Runbook 5 - Incident Decision Tabletop

Lab ID: TABLETOP-IR-01 **Outcome:** Coordinate technical, operational, privacy, legal, and communication decisions during a fictional incident. **Environment:** Scenario packet and role cards. **Time:** 60-120 minutes.

Roles

- Incident coordinator
- Security analyst
- IT or service owner
- Privacy or records lead
- Legal or compliance advisor
- Communications lead
- Executive sponsor
- User or community representative

Scenario Design

The starting packet should include:

- Mission and critical services
- Known and unknown facts
- Initial technical indicators
- Affected users or data categories
- Recovery dependencies
- Contact and authority structure

Injects may include new evidence, a service outage, media inquiry, unavailable backup, third-party notification, or accessibility concern.

Decision Log

Time	New information	Decision	Reason	Dissent or unresolved issue	Owner	Next review

Evaluation

Assess prioritization, evidence, coordination, communication, protection of people and mission, recovery thinking, and documentation. Do not score one predetermined response as the only acceptable answer when multiple defensible options exist.

Editable Assessment Tools

Assessment Blueprint Template

Outcome	Importance	Evidence required	Method	Difficulty or independence	Weight	Accommodation review	Item or task owner

Practical Performance Rubric

Criterion	4 - Independent and defensible	3 - Competent	2 - Developing	1 - Limited	Score/notes
Authorization and safety	Confirms and follows scope, data, stop, and reporting controls	Follows controls with minor prompting	Misses or misunderstands a control	Disregards essential controls	
Method	Uses a logical, repeatable process and adapts to evidence	Uses an appropriate process	Process is incomplete or heavily prompted	No coherent process	
Technical result	Accurate, verified, and appropriate to the task	Correct with minor errors	Partial or weakly verified	Incorrect or absent	
Evidence	Relevant, protected, labeled, and sufficient	Sufficient with minor omissions	Incomplete or excessive	Unreliable or absent	
Troubleshooting	Tests hypotheses and recovers safely	Resolves ordinary issues	Uses unstructured changes	Cannot recover or explain actions	
Communication	Explains decision, consequence, limitation, and next action	Communicates major reasoning	Mostly descriptive or jargon-heavy	Unclear or misleading	
Reflection	Identifies specific improvement and transferable lesson	Identifies useful lesson	General reflection	No meaningful reflection	

Ethical Reasoning Rubric

Criterion	4	3	2	1	Notes
Stakeholders and impact	Identifies affected groups, unequal impact, and duties	Identifies major stakeholders	Omits important perspectives	Focuses on self or one party only	
Facts and uncertainty	Separates evidence, inference, and missing information	Notes most uncertainty	Mixes fact and assumption	Makes unsupported claims	
Authority and obligations	Integrates permission, policy, law, ethics, and professional duty	Uses relevant rules	Names rules without application	Ignores boundaries	
Alternatives and safeguards	Compares feasible options and mitigations	Offers more than one option	Alternatives are weak	Presents no real alternative	
Justification	Clear decision, reasoning, limitations, and review conditions	Defensible reasoning	Partial or inconsistent reasoning	Opinion without support	

Presentation and Briefing Rubric

Criterion	4	3	2	1	Notes
Audience alignment	Prioritizes consequences and actions for the audience	Generally audience-aware	Excessive or missing detail	Unusable for the audience	
Accuracy	Claims match evidence and uncertainty	Minor inaccuracies	Several unsupported claims	Misleading or materially wrong	
Structure	Clear purpose, status, options, recommendation, and next update	Understandable structure	Important elements are hard to find	Disorganized	
Visual or written support	Simple, legible, and directly supports decisions	Mostly useful	Cluttered or incomplete	Distracting or inaccessible	

Criterion	4	3	2	1	Notes
Questions	Responds directly, identifies unknowns, and records follow-up	Responds adequately	Avoids or overstates	Cannot answer or speculates	

Capstone Review Form

Proposal Gate

- [ ] Problem and audience are defined.
- [ ] Outcomes and success criteria are measurable.
- [ ] Authorization, data, ethics, privacy, safety, and intellectual property are approved.
- [ ] Scope is feasible.
- [ ] Methods and sources are appropriate.
- [ ] Milestones, reviewers, and fallback are identified.

Midpoint Gate

- [ ] Evidence supports continued work.
- [ ] Scope and risk remain controlled.
- [ ] Limitations and unexpected findings are documented.
- [ ] Sponsor input has not replaced academic judgment.
- [ ] Accessibility and transfer requirements are being met.
- [ ] A recovery or rollback path exists for technical work.

Final Gate

- [ ] Deliverables meet the stated outcome.
- [ ] Findings and claims are supported.
- [ ] Limitations and residual risk are explicit.
- [ ] Sensitive information has been removed or protected.
- [ ] The product can be reproduced, transferred, maintained, or responsibly archived.
- [ ] The learner can defend the work and identify the next improvement.

Mentoring and Work-Based Learning Forms

Mentoring Agreement

Mentor: Learner: Start date: Planned end or review date: Meeting frequency:

Purpose

Learner Goals

1. 2. 3.

Mentor Commitments

- Provide candid, respectful feedback.
- Help the learner identify evidence, options, and next actions.
- Share perspective and connections without taking ownership of the learner's work.
- Protect appropriate confidentiality and explain its limits.
- Maintain professional boundaries and disclose conflicts of interest.

Learner Commitments

- Prepare for meetings and complete agreed actions.
- Ask questions and disclose obstacles early.
- Own decisions, work products, and follow-through.
- Protect confidential information and use only authorized resources.
- Give feedback on the mentoring relationship.

Communication and Boundaries

Decision	Agreement
Channels	
Typical response time	
Rescheduling	
Topics outside the mentor's role	
Employment or recommendation expectations	
Confidentiality and reporting obligations	
How either person may end the relationship	

Signatures or acknowledgement: _____

Mentoring Meeting Record

Date: Primary goal: Evidence reviewed:

Discussion	Notes
Progress since last meeting	

Discussion	Notes
Current obstacle	
Options considered	
Agreed next action	
Support or connection requested	
Risk, boundary, or confidentiality issue	
Follow-up date	

Internship Learning Plan

Student: Academic program: Host organization: Supervisor: Faculty contact: Dates and expected hours:

Role Purpose

Learning Outcomes

1. 2. 3.

Authorized Work

Prohibited or Restricted Work

Systems, Data, and Access

Element	Approved scope and control
Accounts and privileges	
Data and confidentiality	
Tools and systems	
Remote access	
Evidence and screenshots	
Portfolio use	
Incident or concern reporting	

Deliverables and Evaluation

Deliverable	Due date	Reviewer	Evidence of learning

Check-In Schedule

Date	Student focus	Supervisor focus	Faculty focus

Internship Check-In Form

- What work was completed?
- Which learning outcome did it support?
- What new concept, tool, or professional behavior was required?
- What information may not be shared outside the host?
- What obstacle or concern needs attention?
- Are workload, supervision, accessibility, and authorization still appropriate?
- What is the next milestone?

Portfolio Confidentiality Review

Before publishing or sharing an artifact, confirm:

- [ ] The organization, client, and affected people have authorized the intended use.
- [ ] Real credentials, keys, tokens, addresses, names, and internal identifiers are removed.
- [ ] Screenshots do not reveal hidden tabs, browser history, notifications, file paths, or metadata.
- [ ] Data are fictional, public, or properly sanitized.
- [ ] The artifact does not reveal security weaknesses that remain exploitable.
- [ ] Proprietary code, documents, diagrams, and contracts are excluded or approved.
- [ ] The description accurately states the learner's own contribution.
- [ ] The artifact explains method and learning without overstating organizational results.

Partnership and Funding Forms

One-Page Partnership Brief

Proposed partner: Institutional owner: Learner population: Pilot period:

Shared Need or Opportunity

Proposed Learner Experience

Value to Learners

Value to the Partner

Contributions

Party	People	Time	Equipment or access	Funding	Data or content	Other
Institution						
Partner						

Controls and Boundaries

- Student supervision and safeguarding:
- Systems and data access:
- Confidentiality and intellectual property:
- Accessibility:
- Academic independence:
- Communications and issue escalation:
- Evaluation:
- Exit or termination:

Pilot Success Evidence

Partner Review Form

Area	Evidence	Finding	Action
Learner value			
Partner value			
Safety and privacy			
Access and inclusion			
Workload and cost			
Academic independence			
Communication			
Sustainability			

Decision: Continue / Revise / Pause / End Owner and next review:

Grant Concept Form

Working title: Funding opportunity: Deadline: Project owner:

Problem and Evidence

Population and Barriers

Intended Outcomes

Outcome	Baseline	Target	Evidence source	Collection burden

Activities and Milestones

Activity	Owner	Start	Finish	Dependency	Deliverable

Budget Narrative

Category	Amount	Justification	Recurring after grant?
Personnel			
Equipment			
Software or cloud			
Training			
Accessibility			
Evaluation			
Partner or participant support			
Other			

Safety, Privacy, Ethics, and Accessibility

Sustainability and Handoff

Risks and Fallbacks

Risk	Likelihood	Consequence	Mitigation	Fallback	Owner

Remote and Hybrid Teaching Readiness

Instructor Home-Office and Delivery Checklist

Space and Privacy

- [ ] A stable workspace reduces interruptions and protects confidential conversations.
- [ ] Camera background and screen-sharing areas do not expose personal or institutional information.
- [ ] Headset or microphone supports clear communication without broadcasting private conversations.
- [ ] Lighting allows learners to see demonstrations when video is needed.
- [ ] Sensitive papers, whiteboards, notifications, and smart speakers are controlled.

Connectivity and Continuity

- [ ] Primary internet connection supports the expected class and lab load.
- [ ] A backup connection or communication plan exists.
- [ ] Power-loss and device-failure procedures are known.
- [ ] Course files and instructor notes are backed up and available from an approved alternate device.
- [ ] Learners know where to find updates if the live session fails.

Systems and Accounts

- [ ] Teaching device is supported, updated, encrypted where required, and protected by approved authentication.
- [ ] Separate profiles or devices are used when needed to protect personal and institutional data.
- [ ] Classroom, lab, conferencing, and storage accounts use appropriate access controls.
- [ ] Recordings, transcripts, chat logs, and attendance data follow institutional policy.
- [ ] Screen-sharing is tested to prevent exposure of email, messages, passwords, or unrelated windows.

Accessibility and Participation

- [ ] Captions, transcripts, keyboard access, readable documents, and alternative formats are available.
- [ ] Learners can participate without mandatory camera use when it is not essential to the outcome.
- [ ] Asynchronous alternatives exist for predictable access barriers.
- [ ] Time-zone, work, family, and disability needs are considered in participation rules.
- [ ] Technical support and response expectations are published.

Remote Course Session Plan

Segment	Time	Instructor action	Learner action	Evidence	Backup if technology fails
Opening and check-in					
Focused explanation					
Guided demonstration					
Small-group or individual practice					
Debrief					
Knowledge check and next step					

Remote Lab Readiness Gate

- [ ] The environment has been tested from a learner account and ordinary connection.
- [ ] Required downloads, browser settings, ports, and authentication are documented.
- [ ] Learners can recover from common access failures.
- [ ] The instructor can observe enough evidence without intrusive monitoring.
- [ ] The lab has a low-bandwidth or offline alternative.
- [ ] Reset, cost controls, expiration, and account removal are automated or assigned.
- [ ] Support does not require learners to share passwords or grant uncontrolled device access.

Curriculum Maintenance Forms

Curriculum Element Inventory

Element ID	Course/ module	Outcome	Audience	Owner	Source	Version	Volatility	Dependency	Accessibility	Safety/ privacy	Last review	Next review	Status

Suggested volatility values:

- **Enduring:** Durable principle reviewed mainly for pedagogy and clarity
- **Periodic:** Framework, model, or practice reviewed at planned intervals
- **Volatile:** Tool, law, threat, incident, certification, or live resource likely to change quickly
- **Local:** Institution-specific procedure, contact, policy, or technology
- **Experimental:** Pilot content requiring evidence before permanent adoption

Curriculum Change Request

Request ID: Requestor: Date: Affected element:

Problem or Opportunity

Evidence or Source

Risk of No Action

Proposed Change

Impact Review

Area	Impact and required action
Outcomes	
Instruction	
Labs and tools	
Assessment and answer keys	
Accessibility	
Safety and privacy	
Sources and citations	
Faculty workload and support	
Learner communication	
Partners or accreditation	

Acceptance Criteria

Test Plan

Rollback Plan

Disposition: Reject / Clarify / Backlog / Hotfix / Minor release / Major release / Pilot

Release Record

Release: Date: Owner: Approver: Previous release:

Changes

Source and Version Verification

Tests Completed

- [ ] Content and citation review
- [ ] Lab clean-deployment and reset test
- [ ] Assessment and answer-key test
- [ ] Accessibility review
- [ ] Safety and privacy review
- [ ] Link and resource check
- [ ] Visual and publication QA
- [ ] Handoff or second-person verification

Known Limitations

Learner and Instructor Communication

Archive and Rollback Location

Next Review

Update Backlog

ID	Request	Evidence	Impact if deferred	Effort	Priority	Target release	Owner	Status

Curriculum Risk Register

Risk ID	Curriculum risk	Cause	Affected outcome or learner	Likelihood	Consequence	Existing control	Planned action	Residual risk	Owner	Review date

Handoff Test

Ask a qualified colleague who did not build the current release to:

1. Locate the controlling course files.
2. Identify the current version, known issues, and next review.
3. Find the authoritative source for one volatile claim.
4. Deploy and reset one lab from the runbook.
5. Administer and score one assessment using the current rubric or key.
6. Locate student support, accessibility, safety, and escalation procedures.
7. Identify one dependency that could prevent delivery.
8. Record every point where undocumented knowledge was required.

Handoff Findings

Task	Pass/Fail	Undocumented dependency or confusion	Required correction	Owner

Companion Resource Revision Log

Resource	Version	Date	Change	Source or reason	Reviewer	Next review

Sharing and reuse

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

Educators Hub: https://educate.baremetalcyber.com/