Appendix A: Quick-Start Implementation Plans

This appendix converts the book's larger system into practical entry points. It is intended for educators who need to begin responsibly without waiting for a perfect course, perfect lab, or complete program redesign.

A First-Week Plan for a New Cybersecurity Educator

The first week should establish boundaries, outcomes, learner expectations, and a repeatable teaching rhythm. It should not be dominated by tool installation or an attempt to prove technical expertise.

Before the First Meeting

Action	Minimum evidence of completion
Confirm authorization and institutional boundaries	Written approval, acceptable-use requirements, escalation contacts, and prohibited activities are known
Identify the learners	Expected age, prior experience, device access, accessibility needs, language needs, and course purpose are documented
Select three to five outcomes	Outcomes describe what learners will be able to recognize, explain, decide, configure, analyze, or communicate
Verify the delivery environment	Classroom, learning platform, accounts, lab access, reset procedure, and backup activity have been tested
Prepare a low-risk diagnostic	Short survey, concept sort, scenario discussion, or skills inventory that does not require prior technical experience

Action	Minimum evidence of completion
Establish communication channels	Learners know where announcements, help requests, office hours, and urgent safety concerns belong
Prepare the first practical activity	The activity has a learning objective, instructions, evidence requirement, debrief, and stop condition

Days 1 and 2: Establish the Learning Contract

1. Explain the purpose of the course in terms of learner capability, not topic coverage.
2. Distinguish lawful, authorized practice from experimentation on systems that are not part of the course.
3. Introduce the classroom norms: curiosity, evidence, respectful disagreement, protection of sensitive information, and prompt reporting of mistakes.
4. Conduct the diagnostic without grading it as a high-stakes assessment.
5. Give learners a short success experience, such as identifying suspicious message cues, mapping an account-recovery process, or explaining the confidentiality, integrity, and availability consequences of a familiar incident.
6. Close with a debrief that models how the course will connect action, evidence, and reflection.

Days 3 through 5: Establish the Course Rhythm

Use a simple recurring pattern:

- **Prepare:** A short reading, video, demonstration, or vocabulary activity.
- **Explain:** A focused lesson on one durable concept.
- **Practice:** A controlled activity that produces observable evidence.
- **Debrief:** Discussion of decisions, errors, assumptions, and alternatives.
- **Check:** A low-stakes assessment or exit ticket.
- **Improve:** One change the learner or instructor will make next time.

At the end of the first week, confirm that every learner can answer four questions:

1. What are we learning to do?
2. What activities are authorized?
3. How will my work be evaluated?
4. Where do I go for help?

A First-Semester Plan for a New Course

The following fifteen-week model can be compressed, expanded, or adapted for secondary, undergraduate, or professional programs. It assumes that practical work is introduced gradually and that ethics, communication, and reflection are integrated rather than isolated.

Week	Primary focus	Representative evidence
1	Course purpose, authorization, learner diagnostic, and safety	Signed learning agreement, diagnostic results, first reflection
2	Confidentiality, integrity, availability, risk, and resilience	Scenario classification and short explanation
3	Identity, authentication, authorization, and account recovery	Identity-lifecycle map or account-protection plan
4	Networks, systems, applications, cloud, and data	Annotated architecture or data-flow diagram
5	Social engineering and human-centered security	Suspicious-message analysis and reporting decision
6	Vulnerabilities, configuration, updates, and secure defaults	Configuration review or control-selection exercise

Week	Primary focus	Representative evidence
7	Cryptography, privacy, and data protection	Explain-and-apply activity using a safe demonstration
8	Mid-course synthesis and feedback	Scenario assessment, learner conference, course adjustment
9	Detection, logging, and evidence	Log-triage worksheet or event timeline
10	Incident response, recovery, and communication	Tabletop response plan and stakeholder update
11	Governance, policy, standards, and professional judgment	Policy critique or governance briefing
12	Secure design, software, and supply-chain thinking	Threat model or secure-design review
13	Career pathways, teamwork, and professional communication	Portfolio artifact and role exploration
14	Integrative project or capstone	Draft deliverable, peer review, revision record
15	Demonstration, reflection, and next-step planning	Final product, presentation, self-assessment, learning plan

First-Semester Control Points

- Review learner access and participation after Week 2.
- Test every lab from a clean environment before release.
- Review grade distribution and assessment validity by mid-course.
- Check whether learners are producing evidence of reasoning, not only correct answers.
- Retire or revise one activity that consumes time without supporting an outcome.
- Archive the final course release with changes, known issues, and recommendations for the next delivery.

Program-Review Checklist

Use this checklist at the end of a course, annually for a program, or before a major revision.

Purpose and Outcomes

- [ ] The intended learner population is current and accurately described.
- [ ] Program and course outcomes are measurable.
- [ ] Outcomes include technical performance, ethical judgment, communication, and adaptability where appropriate.
- [ ] Every required activity and assessment supports at least one outcome.
- [ ] Material that does not support an outcome has been revised, moved, or retired.

Curriculum and Instruction

- [ ] Enduring concepts are separated from volatile tools, incidents, laws, and certification mappings.
- [ ] Progression from foundational to advanced performance is visible.
- [ ] Learners receive enough guided practice before high-stakes evaluation.

- [ ] Activities include debriefing and reflection.
- [ ] Content is accessible and usable across the delivery modes actually offered.

Labs and Technology

- [ ] Authorization, isolation, stop conditions, data handling, reset, and recovery are documented.
- [ ] Labs have been tested from a clean learner environment.
- [ ] Required hardware, bandwidth, accounts, and licenses are realistic.
- [ ] A lower-technology alternative exists for essential outcomes when practical.
- [ ] Unsupported or unsafe tools and images have been retired.

Assessment

- [ ] The assessment system includes diagnostic, formative, and summative evidence.
- [ ] Knowledge questions are balanced with performance, analysis, and communication tasks.
- [ ] Rubrics measure the intended capability rather than presentation polish alone.
- [ ] Accommodations preserve the outcome while removing unnecessary barriers.
- [ ] Item performance, grading consistency, and learner feedback are reviewed.

Sustainability and Improvement

- [ ] Each course and major resource has an owner and backup owner.
- [ ] Sources, versions, review dates, dependencies, and open issues are recorded.
- [ ] Partner, advisory, and employer input informs but does not control academic judgment.
- [ ] Faculty workload and support requirements are visible.
- [ ] The next review and release decision are scheduled.

Role-Specific Reading Paths

Quick-Start Principle: Begin with one coherent, safe, assessable learning experience. Expand only after the first experience works for learners and can be repeated by another qualified educator.

Reader	Begin with	Then use	Immediate product
New K-6 educator	Chapters 1, 3, 4, 7, and 13	Appendices B and C	One age-appropriate lesson and family extension
Grades 7-12 educator	Chapters 3, 7-10, and 14	Appendices B, C, H, and I	One safe project or challenge with a debrief
Undergraduate faculty member	Chapters 5-10, 15, and 19-23	Appendices D-G and J	Course map, lab plan, and assessment blueprint
Graduate faculty member	Chapters 6, 8, 10, 16, and 28-30	Appendices D, E, J, and K	Research or capstone sequence with review gates
Adjunct instructor	Chapters 1, 6, 10-12, and 27	Appendices A, E, F, and K	Delivery checklist and supported teaching plan
Certification or bootcamp instructor	Chapters 7, 11, 18, and 19-23	Appendices E-G, I, and L	Balanced exam-and-performance assessment plan
Program director	Chapters 5, 6, 23, and 26-30	Appendices A, D, F, G, and K	Program inventory, update backlog, and release plan
Practitioner becoming an educator	Chapters 1-4 and 7-8	Appendices A, B, C, and G	Learner profile, lesson plan, and feedback method

Appendix B: Grade-Band Competency Maps and Cybersecurity Glossaries

Competency maps describe observable learner capability. They are not age-based ceilings. A learner may enter above or below the expected range, and instruction should be adjusted without removing essential safety or ethical boundaries.

K-3 Competency Map

Competency	Learner can…	Acceptable evidence	Boundary for instruction
Trusted help	Identify a trusted adult and ask for help when something online feels confusing, scary, or secretive	Names a help path in a scenario	Do not require disclosure of personal experiences in public discussion
Personal information	Sort examples into information that may be shared, information that requires permission, and information that should remain private	Card sort or verbal explanation	Avoid teaching that one visible website signal guarantees safety
Account secrets	Explain that passwords and recovery codes protect access and should be handled with adult guidance	Story response or classroom routine	Do not have children create or reveal real passwords in class

Competency	Learner can…	Acceptable evidence	Boundary for instruction
Pause before action	Stop before clicking, downloading, replying, or scanning an unfamiliar code	Demonstrates a pause-ask-tell routine	Use fictional messages and offline examples
Kind digital behavior	Recognize respectful and harmful online behavior	Chooses and explains a kind response	Follow school safeguarding procedures for disclosures
Device care	Log out, lock, or return a shared device as directed	Demonstration with a practice account or paper model	Do not collect real credentials

Grades 4-6 Competency Map

Competency	Learner can…	Acceptable evidence	Boundary for instruction
Information classification	Distinguish public, personal, sensitive, and account-recovery information	Annotated scenario or classification chart	Emphasize context; a detail can become sensitive when combined with other details
Strong authentication habits	Explain uniqueness, length, password managers, and additional verification	Designs a fictional account-protection plan	Avoid rewarding disclosure of memorable real passphrases
Suspicious-message recognition	Identify urgency, unusual requests, mismatched context, unsafe attachments, and verification needs	Message-analysis worksheet	Do not send deceptive messages to learners without approval and safeguards

Competency	Learner can...	Acceptable evidence	Boundary for instruction
Digital footprint	Explain how posts, images, searches, and account activity can persist or be copied	Profile review or reflection	Avoid fear-based claims that every action is permanent or public
Updates and backups	Explain why devices and data need updates, secure settings, and recoverable copies	Home or school device-care checklist	Follow institutional ownership and support rules
Reporting and recovery	Use the correct reporting path after a mistake or suspected compromise	Scenario response sequence	Reward early reporting; do not shame errors
Source judgment	Compare claims, sources, dates, and evidence before sharing	Fact-checking activity	Do not treat popularity or appearance as proof of credibility

Grades 7-8 Competency Map

Competency	Learner can...	Acceptable evidence	Boundary for instruction
Identity and access	Explain authentication, authorization, least privilege, account recovery, and multi-factor authentication	Identity-lifecycle diagram	Use school-approved test accounts only
Threat reasoning	Distinguish threat, vulnerability, likelihood, impact, and control	Risk scenario analysis	Keep examples age-appropriate and non-operational

Competency	Learner can…	Acceptable evidence	Boundary for instruction
Network and data flow	Trace how a message or request moves among device, network, service, and user	Annotated diagram	Do not capture or inspect traffic without authorization
Social engineering	Analyze how trust, urgency, authority, fear, and reward can influence decisions	Role-play or message analysis	Debrief emotional manipulation carefully
Ethical boundaries	Explain why permission and scope matter even when a technique is technically possible	Written decision or discussion	Never assign testing against public or live targets
Evidence and communication	Record observations, distinguish facts from assumptions, and communicate a concern clearly	Short incident note	Protect student and institutional information
Secure configuration	Identify simple security improvements in an approved sample configuration	Configuration review	Use sanitized examples and reversible settings

Grades 9-12 Competency Map

Competency	Learner can…	Acceptable evidence	Boundary for instruction
Risk analysis	Prioritize risks using assets, threats, vulnerabilities, controls, likelihood, and impact	Risk register or briefing	Avoid false precision when evidence is limited
Systems and networks	Interpret basic architecture, trust relationships, logs, and common defensive controls	Diagram, log analysis, or safe lab	Use isolated environments and documented reset procedures
Incident response	Organize detection, analysis, containment, recovery, communication, and lessons learned	Tabletop plan or after-action report	Do not simulate real emergencies without coordination
Secure design	Identify misuse cases, trust boundaries, defaults, dependencies, and recovery needs	Threat model or design review	Keep offensive detail proportional to the outcome
Privacy and ethics	Analyze stakeholder interests, consent, data minimization, monitoring, and disclosure	Structured dilemma analysis	Distinguish legal requirements from ethical judgment

Competency	Learner can…	Acceptable evidence	Boundary for instruction
Professional practice	Work in roles, document decisions, manage evidence, and present to technical and nontechnical audiences	Team project and presentation	Evaluate contribution as well as final product
Career exploration	Connect interests and evidence of skill to multiple cybersecurity roles	Portfolio and pathway plan	Avoid implying that one certification or job title fits everyone

Postsecondary and Professional Competency Map

Competency domain	Learner can…	Representative evidence
Governance and risk	Translate mission, assets, obligations, and risk appetite into prioritized security decisions	Risk treatment plan, governance memo, or control justification
Identity-centered security	Design or evaluate identity lifecycle, authentication, authorization, privileged access, and review processes	Architecture review or identity-control assessment
Architecture and engineering	Analyze trust boundaries, dependencies, attack paths, resilience, and recovery	Architecture diagram, threat model, or design decision record

Competency domain	Learner can…	Representative evidence
Security operations	Interpret evidence, investigate events, coordinate response, and preserve lessons learned	Incident analysis, timeline, briefing, and after-action report
Secure software and supply chain	Evaluate development practices, components, provenance, vulnerabilities, and release controls	Secure-design review, SBOM analysis, or pipeline assessment
Cloud, data, and privacy	Apply shared-responsibility, configuration, data lifecycle, privacy, and monitoring principles	Cloud-control review or privacy impact analysis
Research and innovation	Formulate a defensible question, select methods, evaluate evidence, and communicate limitations	Research proposal, experiment, thesis, or applied capstone
Leadership and communication	Adapt security information for learners, peers, executives, partners, and affected communities	Briefing, policy, teaching artifact, or stakeholder plan

Core Cybersecurity Glossary

The definitions below are designed for teaching. Educators should adapt the wording to learner age while preserving the underlying idea.

Term	Learner-friendly meaning	Educator note
Asset	Something people or organizations value and need to protect	Assets include people, services, data, reputation, equipment, and time
Authentication	The process of showing that an identity claim is credible	A password, security key, device, or biometric may be part of authentication
Authorization	The decision about what an authenticated identity is allowed to do	Authentication and authorization answer different questions
Availability	Information and services are accessible when authorized users need them	Availability includes resilience, capacity, recovery, and protection from disruption
Backup	A recoverable copy kept so information can be restored after loss or damage	A backup is useful only if it can be restored and is protected from the same failure
Cloud service	Computing capability delivered through remotely operated infrastructure or software	Teach shared responsibility rather than treating the cloud as automatically secure or insecure
Confidentiality	Information is disclosed only to authorized people, processes, or systems	Confidentiality can be affected by oversharing, weak access control, or interception
Control	A safeguard or practice used to change risk	Controls may be preventive, detective, responsive, corrective, physical, technical, or administrative

Term	Learner-friendly meaning	Educator note
Credential	Information or an object used to support identity or access	Passwords, keys, tokens, certificates, and recovery codes are credentials
Cyberbullying	Repeated or harmful behavior carried out through digital communication	Follow safeguarding and reporting requirements rather than handling serious cases only as classroom conflict
Cybersecurity	The work of managing risks to systems, services, data, and people in digital environments	Cybersecurity is broader than hacking and includes governance, design, operations, recovery, and human behavior
Data	Recorded information that can be stored, processed, transmitted, or analyzed	Data sensitivity depends on content, context, combination, and use
Digital footprint	Information produced or collected through a person's digital activity	A footprint may be visible, inferred, copied, retained, or used in ways the person did not expect
Encryption	A cryptographic process that transforms readable data so it cannot be understood without authorized access to a key	Encryption protects data but does not by itself prove that a source is trustworthy
Firewall	A control that permits, blocks, or monitors network traffic according to rules	A firewall is one layer, not a complete security strategy
Hash	A one-way mathematical result used to represent data and detect change	Hashing is not the same as encryption because it is not intended to be reversed

Term	Learner-friendly meaning	Educator note
Identity	A representation of a person, device, service, or other entity in a system	Identity lifecycle includes proofing, provisioning, use, review, change, and deprovisioning
Incident	An event or set of events that threatens or violates security objectives	Not every unusual event is an incident; analysis determines significance
Integrity	Information and systems remain accurate, complete, and protected from unauthorized change	Integrity includes trustworthy processes and records, not only file checks
Least privilege	Giving only the access needed for an authorized purpose and duration	Least privilege should be reviewed as roles and needs change
Log	A record of system, application, network, or user activity	Logs require context, time accuracy, protection, retention, and interpretation
Malware	Software or code intended to damage, disrupt, spy, extort, or gain unauthorized control	Avoid describing every unwanted program as a virus
Multi-factor authentication	Authentication that uses factors from more than one category	Two passwords are two steps but not two different factors
Network	Connected devices and services that exchange information	A network includes protocols, paths, trust relationships, and management decisions

Term	Learner-friendly meaning	Educator note
Passkey	A phishing-resistant credential that uses public-key cryptography and is unlocked through an approved device or authenticator	Explain that recovery, device security, and service support still matter
Password manager	A tool that generates, stores, and fills unique credentials securely	The manager itself requires strong protection and a recovery plan
Phishing	Deceptive communication intended to influence a person to reveal information, approve an action, open content, or visit a destination	Verification should use a separate trusted channel, not the contact information in the suspicious message
Privacy	Appropriate control and protection of information about people and its collection, use, sharing, retention, and deletion	Privacy is related to but not identical with secrecy or security
Recovery	Restoring acceptable operations, information, access, or service after disruption	Recovery objectives, dependencies, backups, communication, and testing all matter
Resilience	The ability to prepare for, withstand, respond to, and recover from disruption	Resilience accepts that prevention can fail and designs for continued mission performance
Risk	The effect of uncertainty on objectives, often considered through likelihood and consequence	Risk is not simply a threat or vulnerability and cannot always be reduced to one number

Term	Learner-friendly meaning	Educator note
Social engineering	Influencing people to take actions that benefit an attacker or violate expected safeguards	It exploits context and human behavior, not intelligence or character defects
Threat	A circumstance or actor that could cause harm	A threat needs a relevant path or condition to create risk
Threat model	A structured way to identify what could go wrong, why it matters, and how design can reduce the risk	Threat modeling should occur before and during design, not only after deployment
Update or patch	A change intended to fix defects, improve security, or maintain support	Updates require inventory, testing, deployment, verification, and exception handling
Vulnerability	A weakness or condition that could be used or triggered to cause harm	A vulnerability may be technical, procedural, physical, or human-centered
Zero trust	A security approach that continually evaluates access based on identity, context, policy, and least privilege rather than assuming trust from network location	Zero trust is an architecture and operating model, not a single product

Using the Maps and Glossary

- Select the competency statement that matches the intended learner performance.
- Choose evidence that can be observed without requiring real credentials or unsafe activity.
- Use glossary terms in context rather than teaching isolated definitions.

- Revisit terms as learner capability grows; the definition can become more precise without contradicting the earlier meaning.
- Record accommodations and alternative evidence formats before the assessment begins.
- Review volatile examples, tools, and policies each term even when the underlying competency remains stable.

Appendix C: K-12 Lesson Plans and Student Handouts

The four representative lessons below demonstrate the standardized format used in the companion resource package. Each numbered lesson is one complete activity. The labels beneath it - such as Materials, Safety and Privacy, Activity, Assessment, Debrief, Family Extension, and Student Handout - are components of that lesson unless otherwise noted. Student handouts begin on a fresh page so they can be copied or printed separately.

The structure repeats intentionally so an educator can scan each lesson in the same order: preparation and boundaries, delivery, evidence of learning, debrief, and extension.

Field	**Required information**
Title and learner band	Clear title and grade range
Time	Total time plus optional extension
Learning outcome	Observable learner performance
Materials	Approved materials, devices, accounts, and alternatives
Safety and privacy	Authorization, data restrictions, stop conditions, and safeguarding notes
Preparation	Instructor testing and setup
Launch	Short context-setting prompt or scenario
Guided learning	Focused explanation and modeling
Learner activity	Steps, roles, time, and evidence
Debrief	Questions that connect action to principle
Assessment	What will be collected or observed and how it will be judged

Field	Required information
Differentiation	Supports, alternatives, and advanced extension
Family or community extension	Optional application outside the classroom without requiring disclosure of private information

Lesson C.1 - Pause, Ask, Tell

Learner band: K-3 **Time:** 25 minutes **Outcome:** Given fictional online situations, learners will demonstrate a three-step response: pause, ask a trusted adult, and tell what happened.

Materials

- Four fictional scenario cards
- Three large signs: **Pause**, **Ask**, and **Tell**
- Exit card with one simple scenario
- Optional picture symbols for learners who benefit from visual support

Safety and Privacy

Do not ask children to describe personal online incidents in front of the class. If a learner discloses a concern, follow school safeguarding and reporting procedures. The scenarios should use fictional names, services, and messages.

Preparation

Place the three signs in different areas of the room. Prepare scenarios such as:

1. A game asks for a real name and home address.
2. A message says a prize will disappear unless the learner clicks immediately.
3. A classmate sends an unkind message in a shared game.
4. A tablet displays a download request the learner does not understand.

Launch

Ask: “What do we do when a sign, message, or person online asks us to do something and we are not sure?” Explain that being safe does not require knowing every answer. Safe people pause, ask, and tell.

Guided Learning

Model the routine:

- **Pause:** Stop touching the device or replying.
- **Ask:** Find the trusted adult responsible for the activity.
- **Tell:** Explain what appeared and what action was or was not taken.

Emphasize that mistakes should be reported quickly and honestly. Learners are not in trouble for asking for help.

Activity

Read one scenario at a time. Learners move to the first sign and say or demonstrate the action. Continue to the second and third sign. After each scenario, ask one learner to explain why the routine helps.

For a seated alternative, learners can hold up three cards in sequence. For a language-support alternative, use icons and allow pointing.

Assessment

Provide a final fictional scenario. The learner earns evidence of mastery by placing or naming all three steps in order and identifying an appropriate trusted adult.

Debrief

- Why is pausing useful?
- Why should the learner use a different, trusted way to ask for help?
- What should happen after an accidental click?
- How can adults make it easier for children to report mistakes?

Family Extension

Send home a one-page “Who Can Help?” activity. The family identifies two or three trusted adults and the words the child can use when asking for help. No account names, passwords, or private incidents are recorded.

Student Handout: My Safe Response

When I am unsure online, I will:

1. **Pause.** I stop clicking, typing, downloading, or replying.
2. **Ask.** I find a trusted adult.
3. **Tell.** I explain what I saw and what I did.

Trusted adults I can ask: _____ and _____

Lesson C.2 - Private, Personal, or Public?

Learner band: Grades 4-6 **Time:** 40 minutes **Outcome:** Learners will classify information by context and explain why combining several ordinary details can create a privacy risk.

Materials

- Information cards
- Three category sheets: **Public**, **Personal - Ask First**, and **Private or Sensitive**
- Fictional profile worksheet
- Colored pencils or annotation tools

Safety and Privacy

Use fictional information only. Do not ask learners to list their real address, birthday, school schedule, recovery questions, account names, or family details.

Launch

Display three facts about a fictional person: favorite sport, school mascot, and the time that person walks home. Ask whether each fact is always safe to share. Introduce the idea that privacy depends on audience, purpose, combination, and permanence.

Guided Learning

Discuss examples:

- A favorite book may be public in one context.
- A full name and school may require permission.
- A home address, recovery code, live location, or password should remain private.
- Several harmless-looking details can be combined to answer security questions or identify routines.

Clarify that privacy settings reduce exposure but do not guarantee that content cannot be copied or shared.

Activity

In groups, learners sort fictional cards. Cards should include:

- Favorite food
- First name only
- Full legal name
- Home address
- A photo showing a school badge
- A password-reset code
- A drawing
- Live location
- A team schedule
- A pet's name used as a recovery answer

After sorting, give each group a fictional profile. Learners highlight information that should be removed, generalized, delayed, or shared only with permission. They then write two recommendations.

Assessment

Each learner completes three statements:

1. One piece of information that is usually public is _____ because _____.
2. One piece of information that requires permission is _____ because _____.
3. Several details can become risky when _____.

Debrief

- Why can context change a classification?
- What is the difference between privacy and secrecy?
- How can a person share an achievement without revealing a location or schedule?
- What should someone do after oversharing?

Differentiation

Provide fewer cards and picture cues for learners who need reduced reading load. Advanced learners can redesign the profile to preserve the person's purpose while reducing exposure.

Family Extension

Invite families to review one device or service together using its official privacy and account settings. The learner records only the categories reviewed, not the family's actual settings or account information.

Student Handout: Information Check

Before sharing, ask:

- Who can see this?
- Why do they need it?
- Could it reveal where I am or when I will be there?
- Could it help someone guess an account-recovery answer?
- Would I be comfortable if it were copied?
- Is there a safer way to share the same message?

Lesson C.3 - Phishing Evidence Lab

Learner band: Grades 7-8 **Time:** 50 minutes **Outcome:** Learners will analyze fictional messages, identify evidence of manipulation or inconsistency, and choose a safe verification and reporting action.

Materials

- Four instructor-created fictional messages
- Evidence worksheet
- Highlighters
- Approved reporting-flow diagram

Safety and Privacy

Messages must be fictional and must not imitate a real emergency involving a student. Do not send deceptive messages through real school accounts. Do not ask learners to click links, open attachments, call numbers, or reply.

Launch

Present a message that appears polished but asks the recipient to approve an urgent account change. Ask: “What evidence would you need before acting?” Explain that spelling and visual quality are weak indicators because deceptive messages may look professional.

Guided Learning

Introduce the evidence categories:

- **Context:** Was the request expected?
- **Identity:** Does the claimed sender match a trusted, independently known channel?
- **Action:** What does the message want the recipient to do?
- **Pressure:** Does it create urgency, fear, authority, curiosity, or reward?

- **Destination:** Can the destination be verified without using the message itself?
- **Data:** Does it request credentials, codes, money, files, or sensitive information?

Explain that encrypted transport or a familiar-looking site does not prove that the sender or request is legitimate.

Activity

Teams review four messages and record:

1. Claimed sender and purpose
2. Evidence supporting or contradicting the claim
3. The safest next action
4. The correct reporting path
5. One fact that remains unknown

One message should be legitimate but unusual, one obviously deceptive, one ambiguous, and one compromised-account scenario. This prevents learners from assuming every unexpected message is malicious.

Assessment

Learners individually analyze a fifth message and write a three-sentence response:

- The most important evidence is…
- I would verify by…
- I would report or respond by…

Score accuracy of evidence, separation of fact from assumption, and safety of the proposed action.

Debrief

- Which cue was most persuasive but least reliable?
- Why is independent verification important?
- What should a learner do after entering credentials into a suspicious site?
- How can organizations make reporting easier?

Differentiation

Provide an evidence checklist and pre-highlighted message sections for learners who need support. Advanced learners can compare two messages and explain which uncertainty would change their decision.

Student Handout: Message Evidence Record

Question	Notes
What is the message asking me to do?	
Was I expecting this request?	
What pressure or emotion does it use?	
What identity evidence can I verify independently?	
What information, money, approval, or access could be exposed?	
What is the safest verification method?	
Where should I report it?	

Lesson C.4 - Incident Briefing and Decision Tabletop

Learner band: Grades 9-12 **Time:** 75 minutes plus optional extension **Outcome:** Learners will analyze a fictional incident, distinguish confirmed facts from assumptions, recommend immediate priorities, and deliver a concise stakeholder briefing.

Materials

- Fictional incident packet
- Timeline cards
- Role cards
- Decision log and briefing template
- Rubric from Appendix G

Safety and Privacy

The scenario must use invented organizations, accounts, people, logs, and data. It must not include deployable malware, real credentials, live targets, or instructions for exploitation. Clarify that the exercise is a decision and communication simulation, not an offensive lab.

Scenario

A fictional community organization reports that several staff accounts generated unusual sign-ins. One employee opened an attachment before the alert. A shared file repository contains unfamiliar file changes, and the public website remains available. The team has incomplete logs and must decide what to protect, verify, communicate, and preserve first.

Roles

- Incident coordinator
- Security analyst
- IT operations lead
- Privacy or records lead
- Communications lead
- Executive decision-maker

Activity Sequence

1. **Initial review - 10 minutes:** Teams sort the packet into confirmed facts, plausible interpretations, and missing information.
2. **Priority decision - 15 minutes:** Teams identify critical services, people, data, and evidence. They select immediate actions and record tradeoffs.
3. **Inject - 10 minutes:** The instructor adds one new fact, such as a confirmed external login, an unavailable backup, or a media inquiry.
4. **Response update - 15 minutes:** Teams revise containment, recovery, evidence, and communication priorities.

5. **Briefing - 15 minutes:** Each team gives a three-minute briefing and answers two stakeholder questions.
6. **Debrief - 10 minutes:** Compare reasoning rather than declaring one perfect response.

Decision Log

Time	
Confirmed fact	
Decision	
Reason	
Owner	
Follow-up evidence needed	

Briefing Template

- What is known
- What is not yet known
- Services or data at risk
- Actions completed
- Actions requested
- User or stakeholder impact
- Next update time

Assessment

Evaluate:

- Accuracy and distinction between fact and assumption
- Protection of people, mission, data, and evidence
- Proportionality of actions
- Attention to recovery and continuity
- Clear technical and nontechnical communication
- Quality of decision documentation

Extension

Learners produce a one-page after-action report identifying one successful practice, one avoidable weakness, one unanswered question, and one improvement to the organization's preparation.

Family or Community Extension

Learners create a nontechnical “What to Do After an Account Alert” guide for a fictional household or community group. The guide must encourage prompt reporting, use of trusted channels, credential changes through official recovery methods, review of active sessions, and protection of evidence without blaming the affected person.

Appendix D: Undergraduate, Graduate, and Professional Program Maps

The maps below are examples of progression, not accreditation or certification prescriptions. Programs should map their own mission, learners, resources, legal context, and institutional requirements before adopting a sequence. Each map separates enduring capability from provider-specific tools or credentials.

D.1 Undergraduate Program Map

A bachelor's-level sequence should establish broad foundations, repeated practical experience, increasing independence, and a culminating demonstration of integrated capability.

Stage	Primary outcomes	Representative courses or modules	Evidence and progression gate
Entry foundation	Digital systems, programming or scripting, networking, data, professional communication, and ethical boundaries	Computing foundations; networking; operating systems; programming; introduction to cybersecurity	Learner can explain basic system and network behavior, use approved tools, document work, and follow authorization rules
Cybersecurity core	Risk, identity, architecture, secure configuration, cryptography, security operations, incident response, and governance	Security principles; network defense; identity and access; secure systems; risk and governance; incident response	Learner can analyze a bounded scenario, configure or evaluate controls, and communicate evidence

Stage	Primary outcomes	Representative courses or modules	Evidence and progression gate
Applied depth	Specialization in one or more areas with greater ambiguity and independent work	Cloud security; digital forensics; secure software; threat analysis; privacy; operational technology; penetration testing in controlled environments	Learner produces a portfolio artifact that demonstrates method, evidence, limitations, and professional communication
Integration	Cross-disciplinary decision-making, teamwork, career preparation, and sustained project work	Internship or work-based learning; research methods; capstone; seminar	Learner completes a capstone or practicum with sponsor, scope, safety, assessment, and reflection gates

Undergraduate Design Rules

- Require writing, speaking, teamwork, ethics, and evidence management throughout the sequence.
- Introduce labs early, but increase independence only after learners demonstrate safe practice.
- Use certification objectives as one input, not the architecture of the degree.
- Ensure electives add real depth rather than repeating the core with new tool names.
- Preserve multiple career paths: operations, engineering, governance, privacy, research, education, and leadership.

D.2 Graduate Program Map

Graduate education should move beyond broader coverage toward synthesis, research, leadership, design, and defensible judgment under uncertainty.

Stage	Primary outcomes	Representative learning experiences	Evidence and progression gate
Advanced foundation	Evaluate security models, architectures, evidence, risk assumptions, and research quality	Advanced security architecture; risk analysis; research methods; policy and governance	Learner critiques existing approaches and defines a defensible problem statement
Specialization	Develop depth in a technically or organizationally significant area	Advanced cryptography; AI security; cloud and platform security; privacy engineering; secure software; cyber-physical security	Learner conducts advanced analysis, experiment, design, or evaluation with explicit limitations
Leadership and integration	Make decisions across technical, legal, operational, financial, and human constraints	Security leadership; enterprise resilience; policy; interdisciplinary seminars; consulting practicum	Learner produces an executive-quality recommendation supported by technical evidence
Thesis or capstone	Create, evaluate, or apply knowledge to a substantial problem	Thesis, applied research, design project, or sponsored capstone	Proposal approval, ethics and safety review, milestone evidence, final defense, reproducibility or transfer package

Graduate Design Rules

- Distinguish advanced depth from simply assigning more pages or harder tools.
- Teach research integrity, source quality, reproducibility, and uncertainty.
- Require students to defend assumptions and alternative interpretations.
- Use practitioner problems without allowing a sponsor's preferred answer to determine the academic result.
- Preserve an archive sufficient for another researcher or practitioner to understand and continue the work.

D.3 Adult Career-Change Pathway

Career changers benefit from a transparent route that recognizes prior experience, protects limited time, and produces evidence of capability early.

Phase	Purpose	Learning focus	Deliverable
Orientation	Translate existing experience into cybersecurity relevance	Role families, baseline concepts, learning plan, realistic time and cost	Skills inventory and twelve-month pathway
Foundation	Establish systems, networking, identity, risk, and safe practice	Short modules, guided labs, vocabulary, troubleshooting	Two small portfolio artifacts and a reflection

Phase	Purpose	Learning focus	Deliverable
Applied concentration	Build depth aligned to a target role or domain	Operations, governance, cloud, secure software, privacy, or another defined pathway	Role-relevant project with rubric and mentor feedback
Transition	Prepare for selection and early performance	Resume evidence, interview explanation, professional communication, network building	Portfolio, targeted application package, and continuing-learning plan

Career-Change Design Rules

- Do not require learners to discard prior expertise in operations, military service, finance, healthcare, education, law, communication, or project management.
- Use evening, hybrid, asynchronous, and pause-and-resume structures without lowering outcomes.
- Avoid promising employment based only on course completion or one credential.
- Design practical work that can be completed on realistic equipment and documented without exposing employer or personal data.

D.4 Certification and Intensive Pathway

Short-term programs should prepare learners for both the assessment and the work represented by the assessment.

Segment	Exam-readiness function	Capability-readiness function	Evidence
Baseline diagnostic	Identifies domain gaps and question-format familiarity	Identifies missing prerequisite knowledge and practical barriers	Individual learning plan
Concept modules	Covers objectives and vocabulary	Connects concepts to decisions, systems, and consequences	Retrieval practice plus brief scenario explanations
Guided performance	Reinforces command and tool familiarity	Builds safe, repeatable procedures and troubleshooting habits	Lab evidence and instructor observation
Scenario integration	Practices performance-based and scenario questions	Requires prioritization, communication, and tradeoff analysis	Timed scenario plus debrief
Readiness review	Uses practice results to target remaining gaps	Confirms ability to explain and demonstrate key skills	Exam decision, portfolio artifact, and next-step plan

Intensive-Program Design Rules

- State prerequisites honestly and provide bridge material.
- Use frequent low-stakes checks rather than one late discovery of failure.
- Schedule recovery time and prevent unsustainable workload.
- Separate memorization aids from professional decision-making.
- Track completion, learning evidence, certification attempts, persistence, and employment outcomes without misrepresenting causation.

D.5 Program Mapping Worksheet

Program element	Current state	Desired learner capability	Evidence	Owner	Next review
Audience and entry assumptions					
Required outcomes					
Course or module sequence					
Practical environments					
Assessment system					
Accessibility and learner support					

Program element	Current state	Desired learner capability	Evidence	Owner	Next review
Career and work-based learning					
Faculty capability and workload					
Sources and version control					

Appendix E: Sample Course Outlines and Syllabus Models

These outlines show how outcomes, activities, evidence, and updateable modules can fit together. They are deliberately product-neutral. Named tools should be selected only after the learning outcome, safety boundary, accessibility requirement, and operational support are known.

E.1 Undergraduate Course Outline: Foundations of Cybersecurity Practice

Length: Fifteen weeks **Recommended prerequisites:** Basic computing and networking literacy **Course purpose:** Develop durable cybersecurity concepts, safe practical habits, analytical reasoning, and professional communication.

Course Outcomes

By the end of the course, learners will be able to:

1. Explain core security objectives, risk relationships, identity concepts, and defensive principles.
2. Analyze common attack paths and recommend proportionate safeguards.
3. Perform approved configuration, log-analysis, and incident-response tasks in a controlled environment.
4. Distinguish facts, assumptions, evidence, and uncertainty.
5. Communicate findings to technical and nontechnical audiences.
6. Apply legal, ethical, privacy, and authorization boundaries to coursework.

Weekly Sequence

Week	Theme	Guided practice	Evidence
1	Mission, ethics, authorization, and learning environment	Scenario sorting and lab orientation	Learning agreement and diagnostic
2	Confidentiality, integrity, availability, assets, threats, and risk	Risk relationship map	Short analysis
3	Identity, authentication, authorization, and account lifecycle	Identity-lifecycle activity	Access-control explanation
4	Networks and trust boundaries	Packet-flow or architecture mapping using approved data	Annotated diagram
5	Systems, configuration, updates, and secure defaults	Configuration review	Findings and remediation plan
6	Social engineering and verification	Message-evidence lab	Reporting decision
7	Cryptography and data protection	Safe encryption demonstration and key-management discussion	Concept application
8	Mid-course integration	Scenario assessment and learner conference	Revised learning plan
9	Logging, monitoring, and detection	Log triage	Event timeline
10	Incident response and recovery	Tabletop exercise	Response brief

Week	Theme	Guided practice	Evidence
11	Cloud and shared responsibility	Responsibility and configuration analysis	Control map
12	Secure software and dependency risk	Threat model or secure-design review	Design decision record
13	Governance, policy, and professional judgment	Policy critique	Governance memo
14	Career evidence and capstone workshop	Peer review	Portfolio draft
15	Integrated demonstration and reflection	Presentation and debrief	Final project and reflection

Assessment Model

- Diagnostic and participation evidence: 5%
- Low-stakes knowledge checks: 15%
- Practical exercises and documentation: 30%
- Scenario analyses and communication: 20%
- Integrated final project: 25%
- Professional reflection and portfolio organization: 5%

No single timed exam should be the sole evidence of course mastery.

E.2 Graduate Course Outline: Security Architecture, Evidence, and Research

Length: Twelve to fifteen weeks **Recommended prerequisites:** Prior coursework or professional experience in cybersecurity and systems **Course purpose:** Evaluate security architectures and claims through rigorous evidence, research, design, and stakeholder analysis.

Course Outcomes

Learners will be able to:

1. Evaluate architectures, trust assumptions, identity models, dependencies, and resilience strategies.
2. Formulate researchable or designable security problems.
3. Assess source quality, methods, limitations, and reproducibility.
4. Develop and defend an architecture, experiment, policy, or applied solution.
5. Communicate uncertainty and tradeoffs to expert and executive audiences.
6. Maintain ethical, privacy, legal, and safety controls throughout the work.

Module Sequence

Module	Focus	Core product
1	Architecture as a set of trust and risk decisions	Architecture critique
2	Threat modeling and misuse cases	Threat model with assumptions
3	Identity-centered and zero-trust design	Identity and policy decision record
4	Cloud, platform, and supply-chain dependencies	Dependency and responsibility analysis
5	Resilience, incident response, and recovery architecture	Resilience design and test plan
6	Research design, evidence, and reproducibility	Proposal and source review
7	Privacy, governance, and stakeholder conflict	Structured dilemma or impact analysis

Module	Focus	Core product
8	Emerging topic evaluation	Evidence maturity and adoption recommendation
9	Project execution and peer review	Draft artifact and review response
10	Defense, transfer, and maintenance	Final artifact, briefing, and continuation package

Graduate Assessment Model

- Architecture and source critiques: 20%
- Research or design proposal: 15%
- Technical or policy artifact: 30%
- Oral defense and stakeholder briefing: 15%
- Peer-review quality and revision record: 10%
- Reproducibility, transfer, and maintenance package: 10%

E.3 Professional Short-Course Outline: Cyber Risk Decisions for Busy Professionals

Length: Eight sessions of sixty to ninety minutes **Audience:** Managers, project leaders, auditors, educators, and professionals who influence security decisions but do not require deep tool training **Course purpose:** Improve risk, governance, communication, and response decisions using realistic scenarios.

Session	Focus	Practical product
1	What cybersecurity risk means to the mission	Asset and dependency map
2	Identity, access, and account lifecycle	Access-review questions
3	Social engineering, verification, and reporting	Communication and escalation plan

Session	Focus	Practical product
4	Cloud, vendors, software, and shared responsibility	Supplier-risk checklist
5	Incident priorities and executive decisions	Tabletop decision log
6	Privacy, legal obligations, and ethical tradeoffs	Stakeholder impact map
7	Metrics, evidence, and misleading certainty	Executive dashboard critique
8	Improvement plan and continuing governance	Ninety-day action plan

Short-Course Assessment

Use completion evidence, scenario decisions, briefing quality, and the final action plan. Avoid high-stakes testing that rewards terminology recall without improving workplace decisions.

E.4 Syllabus Checklist

Identity and Purpose

- [ ] Course title, audience, prerequisites, and delivery mode are accurate.
- [ ] The course purpose describes capability rather than broad topic exposure.
- [ ] Learning outcomes are measurable and limited to what the course can reasonably achieve.

Learning and Assessment

- [ ] Each major outcome has planned evidence.
- [ ] Grading weights match the importance of outcomes.
- [ ] Practical activities include documentation and debriefing.
- [ ] Late, revision, collaboration, and academic-integrity expectations are explicit.
- [ ] AI-use expectations distinguish permitted assistance, required disclosure, prohibited substitution, and verification duties.

Safety, Privacy, and Access

- [ ] Authorization and prohibited activities are stated.
- [ ] Learners know how to report mistakes, unsafe conditions, or suspected incidents.
- [ ] Required accounts, software, hardware, bandwidth, and costs are disclosed.
- [ ] Accessibility and accommodation processes are stated.
- [ ] Data handling, screenshots, recordings, and use of employer or personal information are controlled.

Course Operation

- [ ] Schedule includes preparation, practice, feedback, and recovery time.
- [ ] Contact methods, response expectations, office hours, and support paths are clear.
- [ ] Volatile modules and named tools can be replaced without rewriting the entire course.
- [ ] Version, release date, source date, and next review are recorded.

E.5 Modular Schedule Template

Module ID	
Outcome	
Enduring concept	
Replaceable example or tool	
Practice	
Assessment	
Accessibility alternative	
Source/review date	

Appendix F: Lab Setup, Safety, Accessibility, Reset, and Recovery Guides

A cybersecurity lab is an instructional system, not merely a collection of machines. It must connect outcomes, authorization, isolation, learner access, evidence, reset, support, accessibility, and maintenance.

F.1 Lab Authorization and Safety Checklist

Approval and Scope

- [ ] The activity has a defined learning outcome.
- [ ] The systems, networks, accounts, data, and techniques in scope are listed.
- [ ] Written institutional approval and responsible contacts are known.
- [ ] Prohibited targets and actions are stated in learner-facing language.
- [ ] Licensing, terms of service, and data-handling requirements have been reviewed.

Environment and Isolation

- [ ] The activity runs in an institutionally approved, isolated, or explicitly authorized environment.
- [ ] External connectivity is disabled or restricted to what the exercise requires.
- [ ] Test data are fictional, synthetic, public, or properly authorized.
- [ ] Real credentials, regulated data, employer data, and personal secrets are excluded.
- [ ] Snapshots, templates, or redeployment methods are available.

Learner Operation

- [ ] Instructions explain the start condition, allowed actions, evidence, stop condition, and help path.
- [ ] Learners receive only the privileges required for the activity.
- [ ] The instructor can pause or terminate the environment.
- [ ] Support is available for account, device, and accessibility issues.
- [ ] The activity does not reward unsafe experimentation outside the environment.

Recovery and Evidence

- [ ] Reset and recovery have been tested from a clean state.
- [ ] Evidence collection avoids exposing secrets or sensitive data.
- [ ] The instructor knows how to preserve relevant logs after a problem.
- [ ] A non-lab alternative can assess the essential outcome when the environment is unavailable.
- [ ] The environment has an owner, version, last test date, known issues, and next review.

F.2 Environment Selection Worksheet

Decision factor	Questions	Requirement or decision
Outcome	What must the learner demonstrate that cannot be assessed adequately through a lower-risk method?	
Learner context	What prior skills, devices, bandwidth, assistive technologies, and support are available?	
Isolation	What could the activity reach, alter, transmit, or expose?	

Decision factor	Questions	Requirement or decision
Identity and access	How are accounts created, reviewed, recovered, and removed?	
Data	What data are used, where are they stored, and how are they deleted?	
Cost	What licensing, cloud, hardware, labor, and support costs recur?	
Scale	How many simultaneous learners and sessions must be supported?	
Reset	How quickly and reliably can the environment return to a known state?	
Evidence	What artifacts demonstrate learning without collecting excessive data?	
Accessibility	Can every essential task be completed with required accommodations or an equivalent method?	
Maintenance	Who owns images, scripts, documentation, sources, and patch decisions?	
Continuity	Can another qualified educator deploy and operate the lab?	

F.3 Instructor Runbook Template

Identification

- Lab ID and title:
- Version and release date:
- Owner and backup owner:
- Related chapter, course, and outcome:
- Intended learner level:
- Expected duration:

Architecture

- Components and relationships:
- Network and trust boundaries:
- Required accounts and roles:
- External services or dependencies:
- Data set and classification:
- Expected starting state:

Authorization and Safety

- Approved actions:
- Prohibited actions:
- Isolation controls:
- Stop conditions:
- Escalation contacts:
- Privacy and evidence restrictions:

Deployment

1. Verify host, cloud, or range capacity.
2. Deploy the approved image or template.
3. Apply the required configuration and access policy.
4. Load fictional or sanitized data.
5. Run the instructor verification steps.
6. Record the release identifier and learner assignment.

Instructor Verification

Check	Expected result	Pass/Fail	Notes
Learner login			
Required service state			
Network restriction			
Data availability			
Intended event or vulnerability			
Evidence collection			
Reset process			
Accessibility path			

Facilitation

- Opening explanation:
- Common learner errors:
- Hints and intervention thresholds:
- Indicators of unsafe or out-of-scope behavior:
- Debrief questions:
- Required evidence:

Reset and Closeout

- Preserve required evidence.
- Remove learner-generated secrets or personal data.
- Revert snapshots or redeploy the environment.
- Verify account and access removal.
- Confirm that external connectivity and resources are terminated.
- Record defects, cost, time, and recommended changes.

F.4 Reset and Recovery Checklist

Routine Reset

- [ ] Learner work is collected or exported as authorized.
- [ ] Required logs are preserved and protected.
- [ ] Temporary accounts, keys, tokens, and sessions are removed.
- [ ] Systems are reverted or redeployed from the approved source.
- [ ] Data are restored to the known baseline.
- [ ] Network and access controls match the approved design.
- [ ] The verification script or checklist passes.

Failed or Suspect Environment

- [ ] Stop learner access and preserve the current state when investigation is required.
- [ ] Notify the designated technical and security contacts.
- [ ] Record time, users, observed behavior, scope, and actions already taken.
- [ ] Do not destroy evidence through an automatic reset until authorized.
- [ ] Determine whether the condition is an instructional defect, misuse, or actual incident.
- [ ] Recover from a trusted source rather than repairing an unknown state when appropriate.
- [ ] Document the decision to return the environment to service.

Continuity Alternative

Prepare a nontechnical or low-technology version using sanitized logs, screenshots, diagrams, configuration excerpts, or decision cards. The alternative should preserve the essential reasoning or communication outcome when the live environment is unavailable.

F.5 Lab Accessibility Review

Area	Review question	Possible response
Visual access	Can text, diagrams, terminal output, status indicators, and error states be perceived without relying only on color or tiny text?	Scalable text, high contrast, text alternatives, structured data, verbal description
Keyboard access	Can essential tasks be completed without a mouse?	Keyboard-operable interface, command alternative, accessible remote desktop

Area	Review question	Possible response
Audio	Is important information presented only through sound?	Captions, transcript, visual alert, written instruction
Motor and timing	Does success depend on rapid clicking or unnecessary time pressure?	Extended time, pause function, partner role, untimed equivalent
Cognitive load	Are instructions, interfaces, and failure states unnecessarily complex?	Chunked steps, checklist, stable layout, worked example, reduced distractions
Language	Does the activity require language complexity unrelated to the outcome?	Glossary, plain language, annotated examples, alternative response format
Device and bandwidth	Does the lab assume equipment or connectivity not available to all learners?	Institution-hosted environment, scheduled access, offline evidence set
Evidence	Can learners demonstrate the outcome through an equivalent format?	Written, oral, recorded, diagrammatic, or instructor-observed evidence

Lab Acceptance Rule: A lab is ready only when it can be deployed, completed, assessed, stopped, reset, recovered, and handed to another qualified educator using documented procedures.

Appendix G: Assessment Blueprints, Rubrics, and Feedback Forms

The templates below support consistency without pretending that every cybersecurity task has one correct process. Each numbered G.x item is a separate reusable template or form. Bold labels beneath a numbered item are component sections of that resource, not additional templates. Adapt criteria to the outcome, learner level, and evidence available, and publish the rubric before learners begin whenever possible.

G.1 Assessment Blueprint

Outcome	
Cognitive or performance level	Recognition / explanation / application / analysis / creation
Assessment method	
Evidence	
Weight	
Accessibility and fairness check	
Review data	

Blueprint Review Questions

- Does the assessment sample the most important outcomes rather than the easiest material to grade?
- Does it require appropriate reasoning, performance, communication, or reflection?
- Is any unrelated skill becoming an accidental barrier?
- Are time, tools, language, and collaboration rules appropriate?
- Can the evidence distinguish partial understanding from guessing?

- Is the scoring method reliable enough for the decision being made?
- What evidence will trigger reteaching, revision, or retirement of an item?

G.2 Practical Lab Rubric

Score each criterion from 4 to 1. A score of 0 may be used when required evidence is absent or the activity violates authorization or safety rules.

Criterion	**4 - Strong independent performance**	**3 - Competent performance**	**2 - Developing performance**	**1 - Limited performance**
Authorization and safety	Confirms scope, protects data, follows stop conditions, and reports unexpected conditions promptly	Follows required boundaries with minor prompting	Needs repeated reminders or misses a control without causing harm	Disregards or cannot explain essential boundaries
Method	Uses a logical, repeatable process and adapts appro-priately when evidence changes	Uses an appropriate process with small gaps	Process is incomplete, inefficient, or overly dependent on hints	Acts without a coherent method
Technical execution	Completes the essential task accurately and verifies the result	Completes the task with minor correctable errors	Completes only part of the task or verification	Cannot produce the required result
Evidence	Captures relevant, accurate, protected evidence with clear labels and timestamps where needed	Captures sufficient evidence with minor omissions	Evidence is incomplete, unclear, or excessive	Evidence is absent or unreliable

Criterion	4 - Strong independent performance	3 - Competent performance	2 - Developing performance	1 - Limited performance
Troubleshooting	Tests hypotheses, records changes, and recovers from errors	Resolves common issues with limited guidance	Tries unstructured changes or needs substantial guidance	Cannot explain actions or recover safely
Communication and reflection	Explains decisions, limitations, alternatives, and lessons learned for the intended audience	Communicates the result and major reasoning clearly	Explanation is mostly descriptive or omits important limitations	Cannot connect actions to the outcome

G.3 Case-Study Analysis Rubric

Criterion	Exemplary	Proficient	Developing	Beginning
Facts and sources	Distinguishes confirmed facts, claims, inference, and missing information; uses credible sources	Uses credible information with minor gaps	Mixes fact and assumption or relies on weak sources	Repeats unsupported claims
Timeline and causality	Constructs a coherent timeline and avoids unsupported causal conclusions	Identifies major sequence and contributing factors	Timeline or causal reasoning is incomplete	Events are disconnected or inaccurate
Technical analysis	Explains relevant systems, weaknesses, attack paths, and controls at the appropriate depth	Identifies main technical issues and safeguards	Analysis is superficial or tool-centered	Misunder-stands core technical relationships
Human and organizational analysis	Integrates incentives, communica-tion, governance, workload, and decision context	Addresses several nontechnical factors	Mentions human factors without analysis	Treats the event as purely technical

Criterion	Exemplary	Proficient	Developing	Beginning
Recommen-dations	Prioritized, feasible, evidence-based, and linked to root causes and recovery	Reasonable and mostly linked to findings	Generic, unprioritized, or weakly connected	Unsupported or impractical
Communica-tion	Clear, audience-appropriate, concise, and transparent about uncertainty	Understand-able with minor organization issues	Excessive jargon, missing context, or unclear structure	Difficult to follow or misleading

G.4 Teamwork and Communication Rubric

Criterion	4	3	2	1
Role clarity	Roles, handoffs, and decision authority are explicit and adjusted when needed	Roles are generally clear	Roles overlap or leave gaps	Work is uncoordinated
Contribution	Consistent, substantive contribution documented through artifacts and peer evidence	Completes assigned work reliably	Contribution is uneven or late	Contribution is minimal or obstructive
Information sharing	Shares relevant information promptly, verifies understanding, and preserves records	Communicates necessary information	Communication is incomplete or delayed	Withholds, loses, or misstates critical information
Technical-to-nontechnical translation	Adapts language, consequence, and requested action to the audience	Mostly clear and audience-aware	Uses unexplained jargon or omits consequences	Communication is unusable for the audience

Criterion	4	3	2	1
Conflict and judgment	Uses evidence, respectful challenge, escalation, and documented decisions	Resolves ordinary disagreement constructively	Avoids or personalizes conflict	Conflict prevents progress or harms participation
Reflection	Identifies team strengths, weaknesses, and specific process improvements	Identifies useful lessons	Reflection is general or defensive	No meaningful reflection

G.5 Learner Feedback Form

Use anonymous collection where appropriate and avoid asking for sensitive personal disclosures.

Rate from 1, **strongly disagree**, to 5, **strongly agree**:

- I understood what I was expected to learn.
- Activities helped me practice the stated outcomes.
- I knew which actions were authorized and prohibited.
- Instructions and tools were accessible enough for me to participate.
- Feedback helped me improve rather than only explaining a grade.
- Workload and pacing were challenging but manageable.
- I could ask for help or report mistakes without unnecessary embarrassment.
- Assessments reflected what we practiced.
- I can explain how the learning connects to real decisions or work.

Open responses:

1. Which activity produced the strongest evidence of your learning?
2. Where did an instruction, tool, example, or assessment create avoidable confusion?
3. What should be kept, changed, added, or retired?
4. What support would make the next version more accessible or effective?

G.6 Instructor After-Delivery Review

Area	Evidence reviewed	Finding	Action	Owner	Target release
Outcome achievement					
Assessment validity					
Learner access and participation					
Lab reliability and support burden					
Safety, privacy, and ethical issues					
Currency of cases, tools, standards, and law					
Workload and sustainability					
Partner or advisory feedback					

G.7 Feedback Quality Checklist

Effective feedback is:

- Tied to the stated outcome and rubric
- Specific about evidence rather than personality
- Clear about what was successful
- Clear about the highest-priority improvement
- Timely enough to affect future performance
- Proportionate to the assignment
- Accessible and understandable
- Protective of student privacy
- Open to correction when the evaluator misunderstood the evidence

Appendix H: Ethical Discussion Prompts and Role-Playing Cards

Ethics activities should assess reasoning, stakeholder awareness, evidence, and professional responsibility rather than reward one predetermined opinion. Each numbered H.x section is a separate prompt set, role-play tool, or debrief resource; bold labels beneath it belong to that resource. Explain the boundaries of the discussion, distinguish legal requirements from ethical judgments, and protect learners from pressure to disclose personal experiences.

H.1 K-6 Discussion Prompts

1. A classmate shares a photo of another student without asking. What should happen next, and why?
2. A game offers a reward for entering a parent's email address. What questions should the player ask before continuing?
3. Someone discovers a friend's password written where others can see it. What is the kind and safe response?
4. A student receives an unkind message and wants to repost it so everyone can see what happened. What are safer choices?
5. An app asks to use the camera even though the activity does not need it. What should the learner do?
6. A student accidentally clicks something suspicious and is afraid of getting in trouble. How should adults and classmates respond?

K-6 Debrief Questions

- Who could be helped or harmed by each choice?
- What information is private or sensitive?
- Which trusted adult or reporting path should be used?
- How can the problem be addressed without blaming the person who asks for help?

H.2 Grades 7-12 Discussion Prompts

1. A student finds a weakness in a school-approved practice site. May the student test it further without asking?
2. A friend sends screenshots of a private conversation as evidence of bullying. How should the evidence be protected and reported?
3. A popular account posts a dramatic security claim without a source. Is sharing it "just in case" responsible?
4. A team member wants to use an AI tool to complete a security report but does not plan to disclose the assistance. What are the concerns?
5. A school proposes extensive monitoring of student devices to improve security. What benefits, risks, and safeguards should be considered?
6. A competition rewards the fastest team, but one member completed nearly all the work. What would fair recognition and assessment look like?
7. A student receives access to information that was not intended for that student. What should the student do before viewing, copying, or sharing it?
8. A club wants to demonstrate phishing by sending an unexpected fake message to students. What approvals, protections, and alternatives are needed?

Grades 7-12 Reasoning Frame

Learners should identify:

- The authorized purpose and scope
- Affected people and organizations
- Information that is known, assumed, or missing
- Relevant duties, rules, or policies
- Reasonable alternatives
- Likely benefits and harms
- A decision and the conditions that could change it

H.3 Postsecondary and Professional Dilemmas

1. **Responsible disclosure:** A researcher identifies a serious vulnerability in a widely used product. The vendor does not respond. What disclosure path is proportionate, and what evidence should be preserved?
2. **Ransomware decision:** A public-service organization faces prolonged disruption. Leaders are considering payment. What technical, legal, ethical, operational, and societal factors belong in the decision?
3. **Insider monitoring:** An organization proposes expanded behavior analytics after a suspected insider incident. How should need, privacy, transparency, bias, retention, and oversight be balanced?
4. **AI-generated security advice:** A team uses a generative system to recommend cloud controls. The recommendations appear plausible but cite nonexistent sources. Who is accountable for verification and approval?
5. **Student research data:** A class project uses security telemetry that may contain personal information. What minimization, consent, access, retention, and publication controls are required?
6. **Supply-chain warning:** A component has a severe vulnerability, but immediate replacement could interrupt a critical service. How should temporary controls, communication, acceptance, and retirement be handled?
7. **Conflict of interest:** An advisory partner donates a platform and asks that the curriculum emphasize that product. What boundaries preserve academic independence?
8. **Public incident communication:** Investigators have incomplete evidence, but customers demand immediate certainty. How should leaders communicate what is known, unknown, and changing?
9. **Accessibility versus speed:** A time-critical security training rollout is not usable by several employees with disabilities. Is partial deployment acceptable, and under what conditions?
10. **Portfolio confidentiality:** A learner wants to include internship work in a public portfolio. What evidence can be shown without exposing organizational information?

H.4 Stakeholder Role Cards

Incident Coordinator

Primary responsibility: Coordinate priorities, decisions, owners, and update rhythm. **Information needed:** Scope, mission impact, current actions, dependencies, and unresolved decisions. **Common tension:** Acting quickly without allowing urgency to erase documentation or consultation.

Security Analyst

Primary responsibility: Interpret technical evidence and propose testable hypotheses. **Information needed:** Logs, configurations, timelines, system context, and known-good baselines. **Common tension:** Communicating uncertainty without making the analysis sound unhelpful.

IT or Service Owner

Primary responsibility: Maintain and restore reliable operations. **Information needed:** Dependencies, change history, recovery options, user impact, and support capacity. **Common tension:** Restoring service quickly while preserving evidence and avoiding reinfection or recurrence.

Privacy or Records Lead

Primary responsibility: Protect information about people and manage collection, use, disclosure, retention, and notification concerns. **Information needed:** Data types, affected populations, jurisdiction, access, and evidence of exposure. **Common tension:** Supporting investigation without unnecessary collection or indefinite retention.

Legal or Compliance Advisor

Primary responsibility: Explain applicable duties, contractual commitments, and legal risk. **Information needed:** Jurisdiction, data, sector, timeline, contracts, and confirmed facts. **Common tension:** Providing actionable guidance while facts and law may still be uncertain.

Communications Lead

Primary responsibility: Deliver accurate, timely, audience-appropriate information. **Information needed:** Confirmed facts, user impact, approved actions, next update, and contact path. **Common tension:** Pressure for certainty, reassurance, or blame before evidence supports it.

Executive Sponsor

Primary responsibility: Make mission, resource, risk, and stakeholder decisions. **Information needed:** Consequence, options, tradeoffs, cost, obligations, and recommendation. **Common tension:** Avoiding both technical micromanagement and uninformed decision-making.

Affected User or Community Representative

Primary responsibility: Surface practical harm, access needs, trust concerns, and communication gaps. **Information needed:** What happened, what actions are required, available support, and how information will be used. **Common tension:** The organization may focus on systems while people experience financial, emotional, educational, or professional consequences.

External Partner or Regulator

Primary responsibility: Protect shared interests and verify that obligations are met. **Information needed:** Scope, impact, evidence, controls, notification, and remediation. **Common tension:** The organization may fear reputational damage while the partner requires transparency.

H.5 Role-Play Procedure

1. Provide a short scenario and a common evidence packet.
2. Assign roles and allow learners to identify missing information.
3. Require each role to state its priority, concern, and requested action.
4. Introduce one new fact that changes the decision environment.
5. Require a documented decision and dissent or unresolved issue.
6. Rotate roles in a second round so learners experience a different perspective.

H.6 Debrief Guide

- Which facts were most important, and which assumptions were treated as facts?
- Which stakeholder was easiest to ignore?
- Where did legal permission, policy, ethics, and operational need point in different directions?
- What alternative caused less harm while still meeting the purpose?
- How did uncertainty affect communication?
- What evidence would have changed the decision?
- What should be documented for accountability and future learning?

Ethical Reasoning Rubric

Criterion	Strong evidence	Developing evidence	Weak evidence
Stakeholder awareness	Identifies affected groups, unequal impacts, and duties	Identifies obvious stakeholders	Focuses only on the decision-maker
Facts and uncertainty	Separates facts, inference, and missing information	Notes some uncertainty	Treats assumptions as facts
Principles and obligations	Applies relevant ethical principles, authorization, policy, and law appropriately	Names rules without integrating them	Uses personal preference as the only basis
Alternatives	Compares feasible options and safeguards	Provides more than one option	Presents a false binary or no alternative
Justification	Gives a clear decision, reasoning, limitations, and review conditions	Gives a decision with partial reasoning	Gives an answer without defensible reasoning

Appendix I: Mini-Labs, Logic Challenges, and Capture-the-Flag Activities

These activities are deliberately bounded. Each numbered I.x entry is a separate activity or reusable form; labels such as Setup, Learner Task, Evidence, Assessment Focus, Scoring, and Debrief are components of that entry. No activity requires testing public systems, real accounts, or live targets. Review each activity against the lab controls in Chapter 10 and Appendix F before use.

I.1 Mini-Lab: Suspicious Message Triage

Audience: Grades 4-6 through adult, with language adjusted **Time:** 25 to 40 minutes **Outcome:** Identify evidence in a fictional message and choose a safe verification and reporting action.

Setup

Create three fictional messages: one legitimate, one deceptive, and one ambiguous. Use invented organizations, links, names, and phone numbers. Provide screenshots or printed cards so no one can click or reply.

Learner Task

For each message, record:

- Claimed sender and purpose
- Requested action
- Pressure or emotion used
- Information or access at risk
- Evidence that can be checked independently
- Safest next action
- Reporting path

Evidence

A completed triage sheet and a two-sentence explanation of the most uncertain case.

Debrief

A professional appearance, encrypted connection, familiar logo, or correct name can coexist with deception. The goal is not to memorize one visual cue but to verify identity, purpose, and action through a trusted path.

I.2 Mini-Lab: Account Recovery Map

Audience: Grades 7-12, postsecondary, or professional **Time:** 35 minutes **Outcome:** Analyze how an approved fictional service proves identity and restores access without exposing actual credentials.

Setup

Provide a fictional account with these recovery elements:

- Primary password or passkey
- Registered device
- Backup authentication method
- Recovery code
- Support process
- Session revocation
- Notification to the account owner

Learner Task

1. Draw the normal sign-in path.
2. Draw the lost-device or forgotten-credential path.
3. Identify two ways an attacker might abuse recovery.
4. Recommend safeguards for proofing, notifications, rate limits, support staff, and session revocation.
5. Identify one accessibility or continuity concern.

Evidence

An annotated recovery diagram and prioritized recommendations.

Boundary

Do not inspect or change real account recovery settings during the activity. A supervised extension may use institutionally approved test accounts.

I.3 Mini-Lab: Log Triage Without Exploitation

Audience: Grades 9-12, postsecondary, or professional **Time:** 45 to 60 minutes **Outcome:** Build an event timeline from sanitized logs and distinguish confirmed evidence from hypotheses.

Setup

Provide a small text or spreadsheet data set containing:

- Successful and failed sign-ins
- One unusual source location or device
- File-access events
- Administrative change
- Benign background activity
- Incomplete or missing fields

All data must be invented or thoroughly sanitized.

Learner Task

1. Normalize timestamps and sort events.
2. Identify the five events most relevant to the investigation.
3. Label each statement as fact, inference, or unknown.
4. Develop two competing hypotheses.
5. Identify the next evidence needed to distinguish them.
6. Prepare a one-minute status update.

Evidence

Timeline, hypothesis table, and status update.

Assessment Focus

Reward evidence discipline, not dramatic conclusions. A learner who says "insufficient evidence" with a strong next step may demonstrate better judgment than a learner who names an attacker without support.

I.4 Logic Challenge: Sequence the Incident

Cut the following events into cards and ask teams to create the most defensible sequence. Some events may remain uncertain.

- User reports an unfamiliar authentication prompt.
- Monitoring records a successful sign-in from an unusual device.
- A help-desk ticket requests a password reset.
- A privileged group membership changes.
- A shared file is downloaded.
- The user confirms the prompt was not expected.
- Security revokes active sessions.
- The team preserves authentication and administrative logs.

Challenge Questions

- Which events are observations, actions, or interpretations?
- What sequence is supported by timestamps?
- What alternative sequence remains possible?
- Which containment action might destroy useful evidence?
- What should be communicated to the affected user?

I.5 Logic Challenge: Choose the Control Portfolio

A fictional organization has limited funds and these conditions:

- Shared administrator accounts
- Incomplete device inventory
- Reliable backups that have not been restored recently
- Frequent phishing reports
- A critical public service with little downtime tolerance
- Several unsupported applications

Teams receive a fixed budget of ten points. Possible actions cost one to four points. Examples include inventory improvement, privileged account redesign, restore testing, phishing-report workflow, network segmentation, emergency patching, application retirement, logging improvement, and awareness training.

Learner Task

Select a portfolio, explain the sequence, identify residual risk, and state what evidence would cause the priorities to change. There is no single correct portfolio; scoring focuses on risk relationships, dependencies, feasibility, and justification.

I.6 Beginner CTF: Metadata and Evidence Hunt

Audience: Grades 7-12 or introductory postsecondary **Time:** 45 minutes **Format:** Offline evidence challenge **Outcome:** Inspect approved files and records for clues without exploiting a system.

Challenge Design

Prepare a folder with fictional documents, images, and text files. Embed flags in safe locations such as:

- Document properties
- File names and timestamps
- Image metadata created specifically for the exercise
- A text file encoded with a simple substitution
- A log entry requiring correlation with a provided timeline

Rules

- Only the supplied folder may be examined.
- No external upload or public decoding service may be used unless explicitly approved.
- Files may be copied within the lab but not modified if evidence preservation is part of the outcome.
- Learners record the method and evidence for every flag.

Scoring

Award points for the flag, method, evidence, and explanation. A guessed flag without method evidence earns little or no credit.

Debrief

Discuss metadata reliability, chain of custody, tool limitations, and the difference between a clue and a conclusion.

I.7 Beginner CTF: Configuration Review

Audience: Grades 9-12, postsecondary, or professional **Time:** 60 minutes **Format:** Sanitized configuration analysis **Outcome:** Identify weaknesses in an invented configuration and recommend prioritized fixes.

Challenge Design

Provide an approved text configuration containing several issues, such as:

- Excessive permissions
- Unused account that remains active
- Logging disabled for a critical action
- Broad network rule
- Unprotected backup location
- Default or insecure setting
- Missing owner or review date

Flags correspond to issue identifiers, not exploitation steps.

Learner Task

For each issue:

1. Identify the evidence.
2. Explain the risk.
3. Recommend a proportional change.
4. State a possible operational consequence.
5. Describe how the change should be tested and rolled back.

Scoring

Use technical accuracy, prioritization, consideration of consequences, and verification plan.

I.8 Activity Evidence Template

Activity ID	
Outcome	
Evidence collected	
Learner explanation	
Instructor finding	
Revision or follow-up	

I.9 Post-Activity Debrief

- What was the intended capability?
- Which action or clue produced the strongest evidence?
- Where did the environment encourage guessing or unsafe shortcuts?
- Which assumptions proved wrong?
- What would a professional document or communicate differently?
- What should be changed before the activity is offered again?

Appendix J: Capstone and Project Idea Bank

Projects should have a clear audience, authentic decision or product, bounded scope, evidence, feedback, and a defined safety or privacy control. The same project can be scaled by changing depth, independence, source requirements, and stakeholder complexity.

J.1 Project Selection Criteria

Choose projects that:

- Support defined outcomes rather than novelty alone
- Can be completed with available time, access, and supervision
- Produce evidence that can be assessed consistently
- Avoid real credentials, sensitive data, unauthorized testing, or unsafe publication
- Include communication and reflection
- Have a sponsor or audience who can provide useful feedback without controlling the academic conclusion
- Can be maintained, transferred, or retired responsibly

J.2 K-12 Projects

Learner band	Project	Main deliverable	Safety or privacy boundary
K-3	Create a “Pause, Ask, Tell” story	Illustrated story or role-play	Fictional characters and situations only
K-3	Design a kindness shield for digital spaces	Poster and explanation	No public sharing of real incidents

Learner band	Project	Main deliverable	Safety or privacy boundary
Grades 4-6	Build a family cyber-safety checklist	Plain-language checklist	Do not record actual passwords or account details
Grades 4-6	Redesign a fictional profile for privacy	Before-and-after profile	Use invented identities and images
Grades 4-6	Create a source-checking game	Card game and instructions	Use age-appropriate fictional claims
Grades 7-8	Conduct a school-approved security awareness campaign	Messages, poster, and evaluation	No deceptive live messages without formal approval
Grades 7-8	Map the lifecycle of a fictional student account	Diagram and control recommendations	No use of real directory or student data
Grades 7-8	Build a phishing evidence workbook	Fictional message set and answer guide	Nonclickable examples only
Grades 9-12	Develop an incident tabletop for a community organization	Scenario, injects, role cards, and debrief	Fictional systems, people, and data
Grades 9-12	Create a secure-design review for a school app concept	Threat model and design recommendations	Design analysis only; no testing of real applications
Grades 9-12	Produce a cybersecurity career evidence portfolio	Curated artifacts and reflection	Remove sensitive information and obtain permission for shared work

J.3 Undergraduate Capstones

Project	Representative deliverables
Security architecture for a fictional small enterprise	Requirements, architecture, threat model, control rationale, recovery plan, and briefing
Identity lifecycle redesign	Current-state analysis, target workflow, access-review model, migration risks, and metrics
Incident detection and response exercise	Sanitized data set, detection logic, response runbook, tabletop, and after-action report
Secure software development review	Threat model, dependency analysis, code-review plan, pipeline controls, and release gate
Cloud shared-responsibility assessment	Architecture, responsibility matrix, configuration findings, evidence, and remediation roadmap
Privacy-aware analytics design	Data inventory, purpose, minimization, access, retention, impact analysis, and prototype
Cybersecurity learning module	Outcomes, lesson, practical activity, assessment, accessibility review, and evaluation data
Community cyber-resilience project	Needs assessment, educational materials, delivery plan, feedback, and sustainability plan
Supply-chain risk assessment	Component or service inventory, dependency mapping, risk analysis, monitoring, and exit plan
Digital forensics process evaluation	Approved evidence set, process, chain-of-custody documentation, findings, and limitations

J.4 Graduate and Research Projects

Project	Research or design focus
Cryptographic agility readiness model	How organizations inventory dependencies, prioritize transition, test compatibility, and govern change
Security and privacy evaluation of agentic AI workflows	Identity, permissions, tool use, data exposure, oversight, logging, and failure containment
Resilience metrics for critical educational services	Measures that connect system recovery, communication, learner impact, and institutional mission
Human-centered phishing reporting study	Which reporting designs reduce delay, shame, and uncertainty while improving useful evidence
Accessibility of cyber ranges	Barriers, accommodations, equivalent evidence, and design recommendations
Software supply-chain transparency study	Practical use and limitations of component inventories, provenance, vulnerability information, and supplier communication
Privacy-preserving student analytics	Data minimization, utility, fairness, governance, and evaluation of a bounded model
Security curriculum maintenance framework	Volatility classification, source governance, release testing, retirement, and succession
Operational technology tabletop design	Stakeholder, safety, availability, and recovery decisions without unsafe live-system testing
Comparative identity architecture evaluation	Usability, phishing resistance, recovery, lifecycle governance, and deployment tradeoffs

J.5 Professional Program Projects

- Develop a ninety-day risk-reduction plan for a fictional organization.
- Evaluate an incident-response plan through a facilitated tabletop.
- Create a role-based security awareness module and measurement plan.
- Review a supplier's security evidence and prepare executive questions.
- Build an identity and privileged-access review checklist.
- Create a secure project-launch checklist for a product or service team.
- Develop a communications plan for account compromise or data exposure.
- Design an annual curriculum or workforce-development review process.

J.6 Capstone Gate Checklist

- [ ] Problem, audience, purpose, and success criteria are defined.
- [ ] Authorization, data, access, intellectual property, and publication boundaries are approved.
- [ ] Sources and methods are appropriate.
- [ ] Milestones include proposal, design review, evidence review, and final defense.
- [ ] Accessibility, ethics, privacy, safety, and operational consequence are addressed.
- [ ] Deliverables include limitations and recommendations.
- [ ] The final package can be transferred, reproduced, or responsibly archived.

Appendix K: Mentoring, Internship, Partnership, Office-Hour, and Grant Templates

The templates in this appendix capture decisions and expectations that are often left informal. Each numbered K.x item is a separate reusable template; bold labels beneath it are sections of that template rather than new activities. Adapt every template to institutional policy, labor requirements, student protections, contracts, and applicable law.

K.1 Mentoring Agreement

Field	Agreement
Mentor and learner	
Purpose of the relationship	
Intended duration and meeting frequency	
Learner goals	
Mentor commitments	
Learner commitments	
Preferred communication channels and response expectations	
Confidentiality and limits of confidentiality	
Boundaries: academic decisions, employment promises, personal support, and conflicts of interest	
How feedback will be requested and given	
What happens when a meeting is missed	

Field	Agreement
Midpoint review date	
Closing and continuation plan	

Mentoring Conversation Prompts

- What capability is the learner trying to develop?
- What evidence already shows progress?
- What obstacle is technical, instructional, organizational, or personal?
- Which next action is small enough to complete before the next meeting?
- Which connection, resource, or perspective can the mentor offer without taking ownership of the learner's work?

K.2 Internship Learning Plan

Element	Description
Student, institution, and host	
Dates, hours, location, and supervision	
Role purpose	
Learning outcomes	
Authorized systems, data, and activities	
Prohibited activities	
Required training and access approval	
Work products and evidence	
Confidentiality and portfolio restrictions	
Accessibility and support	
Academic and workplace contacts	
Check-in schedule	
Evaluation method	
Incident, safety, or concern-reporting path	

Internship Reflection Questions

1. Which classroom concept became more complex in practice?
2. What evidence demonstrates growth?
3. How did communication, documentation, or teamwork affect the outcome?
4. What information may not be included in a public portfolio?
5. What capability should be developed next?

K.3 Partnership Outreach and Memorandum Checklist

Initial Outreach

- Organization and contact
- Shared problem or opportunity
- Value to learners
- Value to the partner
- Proposed contribution from each party
- Time, cost, data, access, and staffing assumptions
- First small pilot rather than an indefinite commitment

Memorandum or Agreement Review

- [ ] Purpose and scope
- [ ] Roles and decision authority
- [ ] Student eligibility, supervision, safeguarding, and accessibility
- [ ] Data ownership, confidentiality, privacy, and retention
- [ ] Intellectual property and publication
- [ ] Systems access and security requirements
- [ ] Costs, equipment, licenses, and insurance
- [ ] Communication and issue escalation
- [ ] Evaluation and reporting
- [ ] Conflict of interest and academic independence
- [ ] Term, renewal, modification, and termination
- [ ] Handoff and continuity contacts

K.4 Office-Hour Plan

Decision	Plan
Purpose	Concept clarification, troubleshooting, feedback, mentoring, or another stated purpose
Schedule and modality	
Appointment and drop-in process	
Accessibility and alternative contact	
Preparation requested from learners	Error message, attempted steps, question, or draft - never passwords or sensitive data
Privacy	What can be discussed in a group and what requires a private channel
Boundaries	Academic support, crisis referral, employment advice, and response-time expectations
Documentation	What action or follow-up is recorded and where
Pattern review	How repeated questions improve teaching materials

Technical Help Request Template

- What were you trying to do?
- What environment or approved activity were you using?
- What happened?
- What did you expect?
- What steps did you already try?
- What error or evidence can be shared safely?
- Did you change anything after the error?
- Is the environment still running, and is any stop condition present?

K.5 Grant Concept Worksheet

Section	Planning notes
Need	What learner, community, workforce, or institutional problem is supported by evidence?
Population	Who benefits, and what barriers do they face?
Outcome	What observable change will occur?
Approach	What instruction, lab, partnership, support, or resource will produce the outcome?
Evidence	How will progress and impact be measured without overstating causation?
Accessibility and equity	How will design, equipment, language, disability, schedule, and cost barriers be addressed?
Safety and privacy	What approvals, data controls, lab boundaries, and safeguarding are required?
Budget	Personnel, equipment, licensing, cloud, training, support, evaluation, and indirect costs
Sustainability	What continues after the grant, who owns it, and what recurring cost remains?
Risks	What could prevent delivery, and what is the mitigation or fallback?
Partners	What will each partner contribute, and how will academic independence be protected?
Timeline	Design, approval, pilot, delivery, evaluation, and handoff milestones

Grant Readiness Gate

Do not submit until the proposal can answer:

- Why this problem, for these learners, now?
- What capability will improve?
- What evidence supports the approach?
- What resources and people are actually available?
- How will the project remain safe, accessible, ethical, and maintainable?
- What will continue when the funding ends?

Sharing and reuse

Please do not resell this resource. You may repost or share it with other educators. Please keep the Bare Metal Cyber Educators Hub URL below intact when you repost or share the resource.

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

Free educator resource from Bare Metal Cyber. Please preserve this notice when sharing.