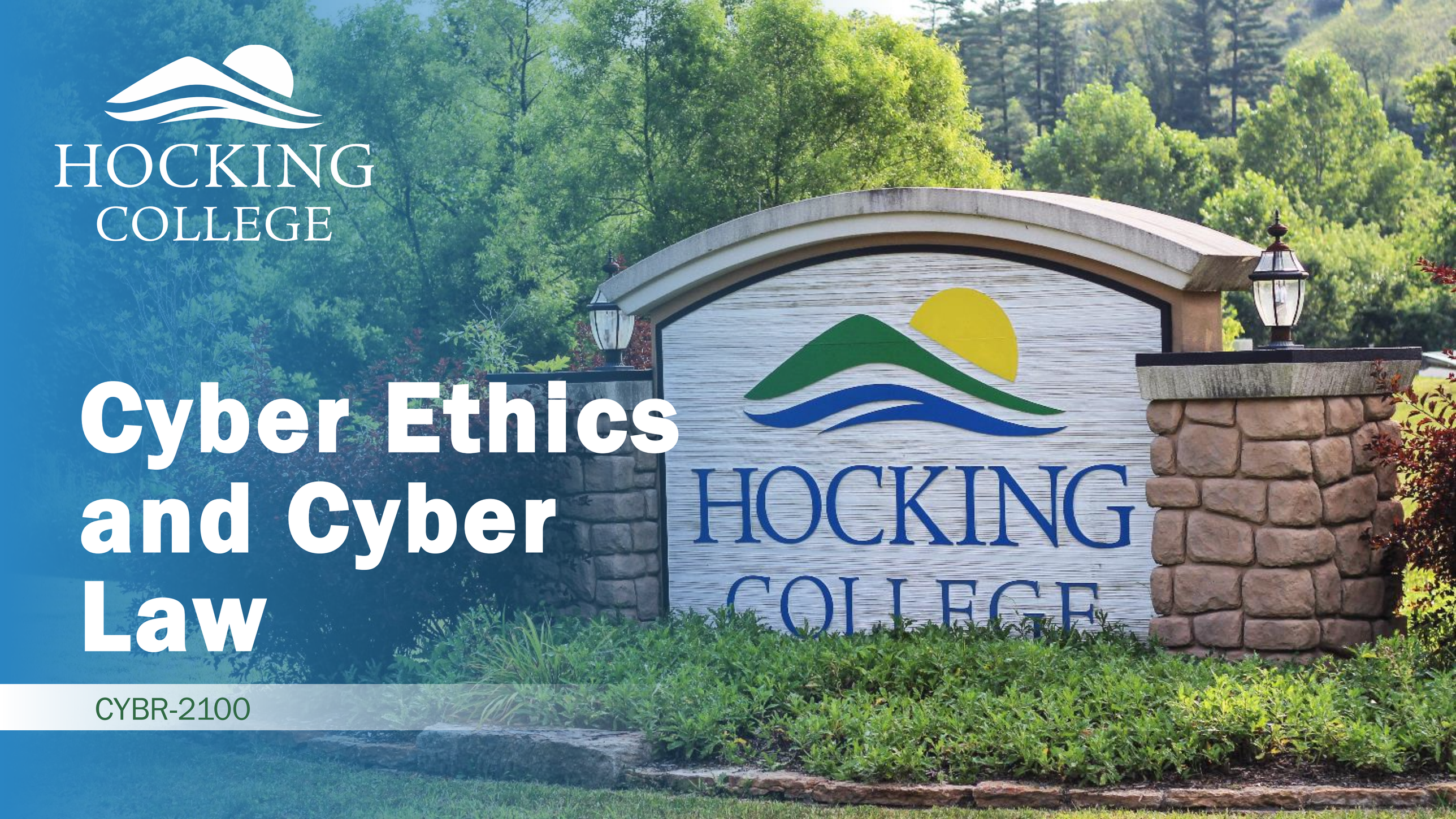
HOCKING COLLEGE

Cyber Ethics and Cyber Law

CYBR-2100



HOCKING COLLEGE

Governance, Risk & Compliance

Week 5 - A

Why this matters?

HOCKING COLLEGE

- Security practice lives or dies on **clear roles**, **policy fit**, and **accountability**.
- This week you'll connect ethical principles to **GRC** (governance, risk, compliance) and draft a **Rules of Engagement (ROE)** so testing stays **authorized, proportionate, and safe**.
- Outcomes:
  - Explain **policy/standard/procedure/guideline** and assign **owners/approvers/review cadence**.
  - Draft a concise **ROE** (scope, consent, comms, evidence handling, escalation).
  - Justify choices using an **ethical framework** and **law/policy**.

Governance, Risk, Compliance

- **Policy** = management intent & principle (what/why)
- **Standard** = specific control requirements (musts)
- **Procedure** = step by step execution (how/who/when)
- **Guideline** = recommended practices/templates (shoulds).

- Policies drive standards
- Standards are executed by procedures
- Guidelines add some flexibility
- **Review cadence**: typical **annual** policy review; standards may update quarterly.

HOCKING
COLLEGE

Roles

- Data Owner (e.g., Registrar, Department head): sets access needs, accepts risk
- Security Lead: writes standards/policy, advises, monitors.
- Security Operations: alerts, monitors metrics
- Incident Response Lead: declares incidents, runs IR
- System Owner (e.g., Web Portal lead): responsible for uptime/changes.
- Data Custodian (IT Operations): implements controls, runs systems.
- Approver (e.g., Dean/CIO): signs high-risk actions (ROE, exceptions).
- Helpdesk Lead: Intake/escalation bridge; tracks comms.

HOCKING
COLLEGE

Policy Lifecycle

- Draft (owner + stakeholders)
- Review (security + legal/ethics)
- Approve (named approver)
- Publish & train (who must read/sign)
- Enforce (logs, gates, audits)
- Exceptions (who can grant + expiry)
- Review cadence (put a date on the calendar)

HOCKING
COLLEGE

Penetration Testing / Pen test

- Attempt to evaluate the security of IT infrastructures
- Uses controlled environment to safely attack, identify, and exploit vulnerabilities according to rules of engagement
- Uses real-world attack techniques
- Vulnerabilities may exist in operating systems, services, networks, and applications
- May also exist due to improper configurations or risky end-user behavior
- Tests are also useful in validating the efficacy of defensive mechanisms and determining how well end-users adhere to security policies

HOCKING
COLLEGE

Penetration Testing

- **Advantages**
  - Can be fast (and therefore cheap)
  - Requires a relatively lower skill-set than source code review
  - Tests the code that is actually being exposed
- **Disadvantages**
  - Too late in the SDLC
  - Front-impact testing only

HOCKING COLLEGE

No Implied Consent

- Being **reachable on the internet** does **not** grant permission to test
- Public access ≠ consent
- You need **written authorization** (ROE/contract/VDP terms)
- Safer pattern: publish a **VDP** with scope + safe-harbor for good-faith reports.

- Ethical basis: **duty of care & non-maleficence**
- Legal basis: **authorization to access**

HOCKING COLLEGE

AT&T iPad email case

- **Why public ≠ consent**
- Attackers enumerated a **publicly reachable** endpoint to harvest iPad subscriber emails. No bypass or stolen creds—just clever guessing.
- Prosecutors still treated it as **unauthorized access/abuse** of AT&T's systems. (The conviction was later vacated on venue, **not** because the conduct was clearly authorized.)
- **Takeaway:** An endpoint being open to the internet does **not** grant permission to probe, enumerate, or harvest. Authorization matters more than cleverness.

HOCKING
COLLEGE

Rules of Engagement Gone Wrong

- 2019 Iowa courthouse test: pen testers with an authorization letter were arrested
- Coordination gaps between state and county stakeholders.
- Commissioning & notification failures -> Arrests/PR damage
- Pre-engagement & law enforcement notification clauses would have prevented it.

HOCKING
COLLEGE

Rules of Engagement Essentials

- Written Authorization – (who signs, effective dates, revocation terms).
- Scope (in/out) — enumerate assets, networks, accounts, test data.
- Timing & deconfliction — windows, freezes, contact hours.
- Data handling — minimum-necessary, storage, retention/deletion, redaction.
- Communications & escalation — real-time contacts, stop-test conditions.
- Reporting & handoff — format, timelines, remediation path.

HOCKING
COLLEGE

Authorization Snippet

- [Approver role/name] authorizes [Testing Team] to test **[systems/URLs/IPs]** from **[start UTC]** to **[end UTC]** under this ROE. Authorization may be paused or revoked at any time by [role]. Critical/high findings will be reported immediately to [role]. All testing will follow this document’s boundaries, communications, and data-handling terms.

HOCKING
COLLEGE

In-Scope

- Draw the **authorization boundary** from the system security plan; test only what's **in-scope.**
- [Named hosts/URLs]
- Synthetic accounts
- Read-only actions
- **May Include:**
  - Port scanning
  - Authenticated web/app testing
  - Input-validation checks
  - Controlled exploit use
  - Password-policy checks
  - Role-based access attempts

HOCKING
COLLEGE

Out-of-scope

- **Social engineering** of students/faculty unless explicitly approved.
- **Physical intrusion**, lock bypass, tailgating, after-hours entry without law-enforcement coordination.
- **DDoS or service-degrading load tests** during class hours.
- **Data exfiltration of real PII**; use synthetic/test accounts only.
- **Modification of production data**; read-only wherever possible, Altering user/system files
- **Third-party/vendor systems** without **written vendor consent**.
- Could restrict tool usage/attack vectors:
  - Password spraying on SSO
  - Destructive exploits
  - Intentional malware

HOCKING COLLEGE

Timing and deconfliction

- All helpdesk tickets referencing target system routed to Security during window.
- Traffic thresholds to avoid degradation
- No testing during business critical times
- Detailed test schedule (start/end times; windows).

HOCKING
COLLEGE

Data handling clauses

- Minimum-necessary
- Storage (encrypted repo; role-limited),
- Retention (e.g., 90 days),
- Redaction (mask student identifiers)
- Hash on export.
- Reports sanitize sensitive data and never include passwords (even hashed)

- “Collect **minimum-necessary** evidence; store encrypted in [location] with access limited to [roles]. Retain **90 days** unless extended by [role]; document deletion. Redact student identifiers; preserve domains/timestamps.”

HOCKING
COLLEGE

Mini cases

- **Case A:** Out-of-scope API hit during crawl
- **Case B:** Helpdesk calls: users seeing latency
- **Case C:** Vendor-hosted component touched

HOCKING COLLEGE

Escalation & Communications

- **Named technical points-of-contact + backups** for each subsystem.
- **Real-time contacts:** Test Lead (cell), SecOps on-call (bridge), App owner., Test lead, Security on-call, IT Ops bridge.
- **Notification windows** (Critical=15 min, High=1 hr, others by EOD).
- **Stop-test conditions:** service impact, unapproved data access, third-party touch, Law Enforcement interaction, safety risk, any deviation from scope.
- **Notify path for critical/high vulnerabilities**

HOCKING
COLLEGE

Reporting and Handoff

- All transferred/stored securely
- Draft w/in ? business days
- Include in the report:
  - Scope actually tested (note deviations).
  - Attack vectors exercised.
  - Timeline of activity.
  - Tests performed + results.
  - Findings with evidence (hashed, mask sensitive details; no passwords in reports).
  - Access paths (chain from foothold → impact)
- Remediation Plan
- Retest Window

HOCKING
COLLEGE

Reporting

- A typical reports consists of two major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences.
- **Executive Summary:**
  - Specific goals of the Penetration Test and the high level findings of the testing exercise.
  - The intended audience will be those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization which may be impacted by the identified/confirmed threats.
- **Technical Report:**
  - Technical details of the test and all of the aspects/components agreed upon as key success indicators
  - The technical report section will describe in detail the scope, attack path, impact and remediation suggestions of the test.

HOCKING COLLEGE

ROE outline

- Purpose: Assess [app] to reduce risk without disrupting service.
- Authorization: [Approver] authorizes testing by [team] on [dates/times] for [targets].
- In-scope: [hosts/URLs], test accounts, read-only data.
- Out-of-scope: prod data writes, student mailboxes, social engineering, after-hours physical access.
- Timing & deconfliction: [window], change freeze, helpdesk route to SecOps.
- Data handling: minimum-necessary; encrypted storage; 90-day retention; redaction rules; hash evidence.
- Communications & escalation: contacts; notification windows; stop-test triggers.
- Reporting & handoff: draft within 5 business days; fix-plan meeting; retest window.

HOCKING
COLLEGE

Measuring ROE Effectiveness

- Scope deviations per test (Number, % with corrective actions).
- Time-to-escalation from alert to human (mean/median to notify)
- Stop-test events (invoked? why? recovery time).
- Evidence hygiene (% findings with chain-of-custody, redaction + hash).
- % policies reviewed on time
- % exceptions with expiry dates.

HOCKING
COLLEGE

Frameworks you can cite

- NIST SP 800-115 (testing & assessment planning; authorization/consent emphasis).
- PTES — Pre-engagement (scope, objectives, constraints).
- OWASP WSTG (test planning/reporting best practices).
- CISA/DoD VDPs (public templates for lawful testing boundaries).
- FedRAMP ROE template

HOCKING COLLEGE

Policy Mapping Lab

- Given a small-org scenario, map policy set (AUP, Access Control, Incident Response, Monitoring, ROE). Identify **owners**, **approvers**, **review periods**, and **enforcement**. Deliverable: 1-page map.

Document (type)	Purpose	Owner	Approver	Review Period	Enforcement
AUP (Policy)					
Access Control (Standard)					
Incident Response (Procedure)					
Monitoring & Logging (Standard)					
ROE (Guideline/Template)					

HOCKING COLLEGE

Policy Mapping

Document (type)	Purpose	Owner	Approver	Review Period	Enforcement
AUP (Policy)	Define acceptable IT use	Security Lead	Vice-President	Annual	Discipline, Block user
Access Control (Standard)	Who gets what, MFA, recert	IT Ops Mgr	Security Lead	Quarterly	Redo Logins
Incident Response (Procedure)	Monitor→containment→ recovery	SecOps Lead	Security Lead	Annual	Ticketed Response
Monitoring & Logging (Standard)	What to log/retain/review	SecOps Lead	Vice-President	Semiannual	Weekly Meetings
ROE (Guideline/Template)	Safe, authorized testing	SecOps Lead	Dean IT + Counsel	Per test	Remediation

HOCKING COLLEGE