Rules of Engagement (ROE) Class Sandbox Testing

Purpose & Approvals

- **Purpose:** Safely conduct penetration and security testing exercises on the course sandbox network to identify vulnerabilities, practice authorized techniques, and teach incident handling without impacting production systems.

- **Approvals:** All tests must be explicitly approved in writing by the Chief Information Officer (CIO) and the course instructor prior to execution. Tests without written approval are prohibited.

Scope & Authorization

- **In-scope:** The designated course sandbox network (lab VLAN), purpose-built test hosts, and instructor-provisioned test accounts identified in the written approval. Only assets explicitly listed in the approval are authorized targets.

- **Out-of-scope:** Any production college systems (HR, finance, grading), personal devices, and mock student or college data residing on the sandbox (mock PII remains protected and must not be exfiltrated or published).

- **Explicit Authorization Statement:** No testing, scanning, or exploitation may occur outside the approved in-scope assets and time window. Written authorization from the CIO and course instructor is required and must be attached to the ticket/work order.

Timing & Deconfliction

- **Authorized windows:** Testing is allowed only during scheduled class hours (Mon/Thu 08:00–10:50 local time) or other windows explicitly listed in the written approval.

- **Maintenance freezes:** No tests during announced maintenance windows, scheduled backups, or other campus-declared freezes. Instructor/IT will publish freeze dates in advance.

- **Deconfliction:** Test teams must check the shared test calendar before starting. If multiple teams will test simultaneously, coordinate to avoid overlapping disruptive scans.

- **Duration:** Each test run must be scoped to a specific start/end time in the approval.

Communications & Escalation

- **Real-time contacts:**
    - Incident Manager / Instructor
    - IT Support (sandbox custodian): IT Help Desk
- **Notification windows:** Notify the Incident Manager and IT Support at least 24 hours before planned testing; confirm again 1 hour before start.

- **Stop-test conditions:** Immediately halt testing and notify contacts if any of the following occur: signs of impact to systems outside the sandbox, unexpected service outages, evidence of real user data exposure, or any suspected unauthorized escalation.

- **Escalation path:** If stop-test is triggered, Incident Manager will escalate to CIO/IT Security for triage and determine containment steps.

Data Handling (minimum necessary)

- **Minimum-necessary:** Only collect evidence required to validate the test objective (example: vulnerable service banner, exploit success indicator, short log snippets tied to the time window). Avoid capturing full disk images or unrelated files.

- **Prohibited capture:** No capture or retention of mock student/college data, credentials, tokens, or any personal data. If such data is captured accidentally, stop testing, notify Incident Manager, and follow the redaction procedure below.

- **Storage location:** All evidence is stored in `/evidence/CYBR2100_ROE/` on the sandbox custodian's restricted server with IR-team-only access.

- **Integrity:** Compute and record SHA-256 hashes for each evidence file at collection time. Log collection timestamps and operator initials.

- **Retention & deletion:** Retain evidence for a maximum of 14 days unless extended by written approval (e.g., for grading or instructor review). After retention, securely delete

artifacts and confirm deletion in the evidence log.

- **Redaction:** Remove or redact any accidentally captured PII/mock data prior to sharing. The collector must document redaction actions in the chain-of-custody record.

Reporting & Handoff

- **Report format:** Short technical write-up (1–2 pages) per test run: purpose, assets tested, tools/commands used, key findings (no exploit steps), evidence IDs (EV-###), hashes, and recommended fixes.

- **Timeline:** Draft report due within 48 hours of test completion; final report (incorporating instructor/IT feedback) due within 7 days.

- **Remediation handoff:** Provide remediation recommendations and, where applicable, a prioritized action list to the sandbox custodian and instructor. If a vulnerability poses broader risk, the Incident Manager will escalate to CIO/IT Security.

- **Grading notes:** Instructor will annotate reports for course feedback but will not circulate raw evidence containing sensitive information.

Compliance & Legal Considerations

- Tests must comply with institutional AUP, applicable laws (e.g., avoid actions that could violate CFAA), and ethical codes (ACM/IEEE/(ISC)²). Collect only what is authorized and minimize risk to people and systems.

Signatures (required prior to testing)

- CIO: _____ Date: _____

- Course Instructor / Incident Manager: _____ Date: _____

- Test Lead (student/team): _____ Date: _____