1. Purpose & Approvals

- **What/Why**: Define boundaries, expectations, and safeguards for conducting security testing, training, or exercises.
- **Authority**: Only activities covered by this ROE are permitted.
- **Approvals**:
    - Authorized by: *Program Director / Instructor / System Owner*
    - Reviewed by: *Cybersecurity Faculty or Designated Approver*
    - Signed by: *Instructor + Student/Tester + System Owner (if applicable)*

---

2. Scope

- **In-Scope Activities**:
    - Systems, networks, or applications explicitly listed in appendix/authorization letter.
    - Approved testing techniques (e.g., vulnerability scanning, simulated phishing, penetration testing).
- **Out-of-Scope Activities**:
    - Any system not explicitly listed.
    - Production systems critical to business/college operations unless specifically approved.
    - Denial-of-service (DoS), social engineering against staff, or physical attacks unless stated.
- **Authorization Statement**:
    - Activities outside this ROE are **unauthorized** and may result in disciplinary or legal action.

---

3. Timing & Deconfliction

- **Testing Windows**:
    - Only during designated lab times or approved schedules.
- **Maintenance Freezes**:
    - No testing during exam weeks, system upgrades, or black-out periods.
- **Contact Hours**:
    - Approved testing hours: *e.g., Monday–Thursday, 8:00 AM–5:00 PM (local)*.
- **Deconfliction**:
    - Testing must be paused/rescheduled if it conflicts with legitimate college operations.

---

4. Communications & Escalation

- **Real-Time Contacts**:
    - Primary: *Instructor or Lab Supervisor*
    - Secondary: *System/Network Owner*
- **Notification Windows**:
    - Notify stakeholders at least *24 hours before* testing begins.
- **Stop-Test Conditions**:
    - Immediately halt if:
        - Unexpected service degradation or outage occurs.
        - Unauthorized data access is detected.
        - Stakeholder issues “Stop Test” command.
- **Escalation Path**:

- Student → Instructor → Program Director → IT/College Leadership.

---

5. Data Handling

- **Minimum-Necessary Principle**:
  - Collect only the data required for the test.
- **Storage Location**:
  - Store test data only in designated secure repositories (e.g., GitHub private Playbook, approved college storage).
- **Retention/Deletion**:
  - Retain raw test data for **30 days** (or as defined by policy).
  - Securely delete data after retention period or project completion.
- **Redaction**:
  - Sensitive information (PII, credentials, keys) must be masked before inclusion in reports.

---

6. Reporting & Handoff

- **Format**:
  - Final report includes: Executive summary, methodology, findings, evidence, and recommendations.
- **Timeline**:
  - Draft report due within *5 business days* of test completion.
  - Final polished report delivered within *10 business days*.
- **Remediation Handoff**:

    - Findings handed to system owner and instructor/program lead.
    - Students provide **mitigation recommendations** but system owners are responsible for implementation.

- **Closure**:
    - Exercise formally closed when all parties confirm receipt and sign-off.