Rules of Engagement (ROE) Outline

Purpose & Approvals

- **Purpose**: Assess designated systems to reduce security risk without disrupting normal service, in line with ethical and legal standards.
- **Authorization**:
    - Authorized by: [Approver role, e.g., Dean or CIO]
    - Testing performed by: [Testing Team]
    - Effective dates: [Start UTC] - [End UTC]
    - Authorization may be paused or revoked at any time by [Approver role]
- **Explicit Authorization Statement:**
  "[Approver role] authorizes [Testing Team] to test the listed systems under this ROE. All activity outside this scope is prohibited."

Scope (In-Scope / Out-of-Scope)

- **In-Scope**:
    - Named hosts/URLs and IP ranges
    - Synthetic/test accounts
    - Read-only or controlled actions, including:
        - Port scanning
        - Authenticated web/app testing
        - Input validation checks
        - Password policy checks
        - Role-based access attempts
        - Controlled exploit use
- **Out-of-Scope**:
    - Social engineering unless explicitly approved
    - Physical intrusion or after-hours entry without law enforcement coordination
    - DoS/DDoS or service-degrading load tests during business hours
    - Real PII exfiltration; use only test/synthetic accounts
    - Third-party/vendor systems without written vendor consent

Timing & Deconfliction

- **Testing window**: [Dates/times UTC]
- **Restrictions:** No testing during business-critical hours (e.g., 8am-6pm weekdays).
- **Change freeze**: No system changes during testing.

- **Helpdesk routing**: All tickets related to target systems routed to Security during testing.
- **Traffic thresholds**: Test traffic must remain below agreed thresholds to avoid service degradation.
- **Schedule**: Documented start/end times with detailed test schedule.

Communications & Escalation

- **Real-Time Contacts**:
  - Test Lead (cell)
  - SecOps On-Call (bridge)
  - Application/System Owner (with backup)
- **Notification Windows**:
  - Critical = 15 minutes
  - High = 1 hour
  - Medium/Low = by end of day
- **Stop-Test Conditions**:
  - Service impact or outage
  - Unauthorized access to third-party or out-of-scope systems
  - Law enforcement interaction
  - Safety risk or any deviation from scope
- **Escalation Authority**: Only the Approver or System Owner may authorize resumption after a stop-test.

Data Handling

- Collect **minimum-necessary evidence** only
- Store in encrypted repository with role-limited access
- Retain evidence for **90 days**, unless extension approved
- Document deletion after retention period
- Redact personal identifiers; never include passwords (even hashed)
- Hash exported evidence for chain-of-custody

Reporting & Handoff

- **Draft Report**: Delivered within 5 business days
- **Final Report**: Delivered within 15 business days, including executive summary and technical details
- **Report Includes**:
  - Scope tested (note deviations)

    - Attack vectors used
    - Timeline of activity
    - Findings with sanitized evidence
    - Remediation plan
- **Handoff**: Fix-plan meeting with stakeholders, followed by retest window