CYBR2100 Rules of Engagement (ROE) Outline

# Purpose & Approvals

- **Purpose**: Define clear rules of engagement for cybersecurity testing and monitoring activities at Hocking College.  
- **Why**: Ensure ethical, legal, and professional standards while protecting systems and stakeholders.  
- **Approvals**: Engagement must be approved in writing by the CIO, IT Security Manager, and project sponsor. Signatures from authorized leadership are required before any test begins.

# Scope & Authorization

- **In-Scope**: Hocking College servers, designated lab systems, approved faculty/staff workstations, and network monitoring tools.  
- **Out-of-Scope**: Student personal devices, third-party cloud services without contract authorization, and production systems during critical operations.  
- **Authorization Statement**: This engagement is explicitly authorized by Hocking College IT leadership and is limited to the systems and timelines stated.

# Timing & Deconfliction

- **Testing Windows**: Monday–Friday, 6:00 p.m.–10:00 p.m. (off-peak hours).  
- **Maintenance Freezes**: No testing during final exams, enrollment periods, or other blackouts identified by IT.  
- **Contact Hours**: Primary contacts available 8:00 a.m.–5:00 p.m. for coordination; emergency hotline for after-hours incidents.

# Communications & Escalation

- **Real-Time Contacts**: Incident Commander (IT Security Manager) and Deputy Lead (Network Engineer).  
- **Notification Windows**: All major findings reported within 24 hours; critical issues reported immediately.  
- **Stop-Test Conditions**: Testing halts immediately upon detection of critical service disruption or request from authorized leadership.

# Data Handling

- **Minimum Necessary**: Only data required for investigation is collected.  
- **Storage Location**: Encrypted storage on Hocking College secure servers.  
- **Retention/Deletion**: Data retained no longer than 30 days after report handoff unless extended by written approval.  
- **Redaction**: All personally identifiable information (PII) and sensitive data are redacted in reports.

# Reporting & Handoff

- **Format**: Formal written report with executive summary, technical findings, and remediation recommendations.  
- **Timeline**: Draft report delivered within 5 business days of engagement; final report within 10 business days.  
- **Remediation Handoff**: Findings handed to Hocking College IT Security Manager for assignment and tracking.