Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The Information Security and Policy Office (ISPO) will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The ISPO is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date):_____

Definitions

Data Custodian - The technical contact(s) that have operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software platforms.

Business Owner - The senior official(s) within a college or departmental unit (or his/her designee) that are accountable for managing information assets.

Penetration Testing Component Descriptions:

1. Gathering Publicly Available Information - Researching the environment using publicly available data sources, such as search engines and web sites.
2. Network Scanning – Performing automated sweeps of IP addresses of systems provided and/or discovered, from on-campus and off-campus.
3. System Profiling - Identification of the operating system and version numbers operating on the system, to focus subsequent tests.
4. Service Profiling – Identification of the services and applications as well as their version numbers operating on the system, to further focus testing on vulnerabilities associated with the identified services discovered.
1. Vulnerability Identification - Potential vulnerabilities (control weaknesses) applicable to the system are researched, tested, and identified.
2. Vulnerability Validation/Exploitation - After vulnerabilities are identified, they must be validated to minimize errors (false reports of problems), which involves attempts to exploit the vulnerability.
3. Privilege Escalation - Should exploitation of vulnerability be successful, attempts are made to escalate the privileges to obtain “complete control” of the system.