### **Rules of Engagement (ROE) - External Passive Penetration Test**

**Engagement Title:** Stamford Hospital – External Penetration Test

**Document Version:** 1.0

**Date:** Monday, April 7, 2025

**Client:** Stamford Hospital

**Vendor:** Quinnipiac University, Group 2

**Project:** External Penetration Test & Vulnerability Assessment

**NDA:** Required prior to assessment

**Client Website:** [https://www.stamfordhealth.org](https://www.stamfordhealth.org/)

## **1. Introduction & Purpose**

This document defines the **scope**, **methodology**, **authorized activities**, and **limitations** for the execution of an external passive penetration test and vulnerability assessment against Stamford Hospital’s public-facing digital infrastructure.

This passive assessment will focus on identifying publicly accessible information and vulnerabilities without active interference or exploitation. The objective is to strengthen Stamford Hospital's external security posture while maintaining operational integrity and compliance.

## **2. Objectives**

* Identify publicly accessible systems, services, and information related to Stamford Hospital.
* Evaluate externally exposed assets for potential vulnerabilities.
* Enumerate digital infrastructure to understand attack surface.
* Perform non-disruptive, controlled web application scanning for known weaknesses.
* Document findings with severity ratings and provide clear remediation guidance.

## **3. Scope of Engagement**

### **In-Scope Assets:**

* **Target:** Stamford Hospital's publicly accessible systems, domains, and applications.
* **Subdomains** under \*.stamfordhealth.org.
* **Public IP addresses** owned or operated by Stamford Hospital.
* **Web applications** hosted on target infrastructure.
* **Open-source intelligence (OSINT)** including:
  + WHOIS records, SSL/TLS certificates.
  + Public repositories and file shares.
  + Social media and job postings.
  + DNS records, cached pages, metadata leaks.

### **Permitted Activities (Passive):**

* DNS, WHOIS, and IP registration lookups
* Subdomain enumeration (e.g., via Amass, Sublist3r)
* Banner grabbing for service identification (without intrusion)
* Web application fingerprinting (e.g., WhatWeb, Wappalyzer)
* Passive vulnerability scanning tools (e.g., Nikto, Burp Suite Passive Scanner)
* Certificate analysis (e.g., Censys, crt.sh)
* Metadata analysis on public documents (e.g., FOCA, ExifTool)
* OSINT collection from social media, job boards, public code repositories, and archived pages

### **Out of Scope / Prohibited Activities:**

* **No social engineering** (phishing, vishing, etc.).
* **No active exploitation** (RCE, privilege escalation, etc.).
* **No denial-of-service (DoS)** or stress testing.
* **No internal network access**.
* **No interaction with staff or systems not explicitly listed in scope**.
* **No brute force attacks or credential stuffing.**

## **4. Methodology**

The engagement will follow industry best practices and methodologies, including those outlined by **OWASP**, **NIST** SP 800-115, and **PTES**. Tools and techniques will include:

* **OSINT tools:** Maltego, Spiderfoot, Shodan, Google dorks.
* **Enumeration tools:** Amass, Sublist3r, DNSRecon, Nmap (for banner grabbing only).
* **WebApp Scanning tools:** Nikto, WhatWeb, Wappalyzer, Burp Suite (passive scanning).
* **Certificate analysis:** CRT.sh, Censys.
* **Metadata analysis:** FOCA, ExifTool.
* **Passive Recon:** GitHub dorking, Archive.org, job postings, social media insights.

## **5. Communication Plan**

### **Client Point of Contact:**

* **Name:** [Client Contact Name]
* **Title:** [Title]
* **Email:** [Email Address]
* **Phone:** [Phone Number]

### **Vendor Point of Contact:**

* **Name:** [Professor or Student Name]
* **Title:** [Professor or Student Title]
* **Email:** [Professor or Student Email]
* **Phone:** [Professor or Student Phone]

### **Reporting:**

* Preliminary findings shared as needed in real time (in case of critical issues).
* Final report will include:
  + Executive summary.
  + Detailed technical findings with evidence.
  + Severity rating per issue (Informational → High).
  + Remediation steps and best practices.
  + Methodologies and tools used.
* **Format:** PDF
* **Delivery:** Secure email or file transfer
* **Report Delivery Date:** [Pending]

## **6. Confidentiality**

* All data gathered is confidential under the NDA.
* No data will be shared externally without written consent.
* Data will be securely deleted upon engagement completion unless otherwise agreed.

## **7. Legal and Ethical Considerations**

* All activities will be conducted within legal boundaries.
* The client confirms that Stamford Hospital has authorized this assessment.
* The vendor will not engage in any unethical behavior or illegal testing methods.

## **8. Timeline**

* **Start Date:** [Pending Start Date]
* **End Date:** [pending End Date]
* **Report Delivery Date:** [Pending Report Date]

## **9. Signatures**

### **Client**

* **Name:**
* **Title:**
* **Signature:**
* **Date:**

### **Vendor**

* **Name:**
* **Title:**
* **Signature:**
* **Date:**