IT Capstone Topic Approval Form

The purpose of this document is to help you clearly explain your capstone topic, project scope, and timeline and to ensure that they align with your degree emphasis. Without clearly addressing each of these areas, you will not have a complete and realistic overview of your project, and your course instructor cannot accurately assess whether your project will be doable for the purposes of these courses.

Of course, if this a project that you have already completed at work or elsewhere, this should be easy to fill in! Most students use a project that they have already completed in the past year or two. In that case, you will write the proposals (Tasks 1 and 2) as if the project has not been done yet, and Task 3 as the complete post-implementation report.

Complete this form and send it (via UGCapstoneIT@WGU.edu) to your course instructor for approval. Once approved, you will receive a signed document in PDF format that you can upload as part of Task 1.

DEGREE EMPHASIS: IT-Security

ANALYSIS:

Project Topic – Small Town Family Medicine, a small doctor's office offering general medical care to local patients, is looking to sell the practice to the local hospital. In preparation for the offer, the practice needs to evaluate and improve its information security configuration, specifically regarding patient Personal Health Information (PHI).

Problem Statement or Project Purpose – Small Town Family Medicine started with a single doctor and a support staff of 2 nurses and 2 front office employees. As the doctor approaches retirement, he has decided to sell the practice to the local hospital in order to bring his patients under the larger care umbrella the hospital and its affiliated practices provide. In preparation, the practice must ensure that its patients' PHI is properly secured. Currently, the PHI is stored on a server kept in the office. The office has a single SOHO router providing two wireless networks, one internal network for staff devices and a guest network for patients to access during their visit. The practice needs to identify and remediate vulnerabilities in the network that could potentially allow for unauthorized access to the PHI. They have hired Small Town Security Experts to test the network, make recommendations, and perform the system improvements.

DESIGN and DEVELOPMENT:

Project Scope

a. Project Goal(s) and Supporting Objectives –
    i. Perform a network audit to identify weaknesses in configurations and vulnerabilities within the network and attached system, including a penetration test to specifically investigate how vulnerable the PHI server is to outside access.
    ii. Install necessary network and infrastructure improvements based on audit findings to improve PHI security.

b. Project Outcomes and Deliverables –

i. Upgrade network infrastructure with new, more secure devices including a physical firewall device, separate routers for wireless networks, and a managed switch to orchestrate the network.
ii. Segment the network by creating VLANs for the following:
    1. The PHI Server
    2. Office devices authorized to access the PHI Server
    3. Wireless network for employee personal devices
    4. Wireless network for patient and other visitor devices
iii. Configure a VPN for the authorized staff to access the server remotely when needed.
iv. Implement an automated patch management solution to ensure the server and office machines are kept patched with up-to-date security patches.

c. Projected Project End Date –

IMPLEMENTATION and EVALUATION:

Describe how you will approach the execution of your project –

1. Perform a black box penetration test on the PHI server by accessing the wireless network, then moving laterally through the network until obtaining access. Document vulnerabilities along the way to be addressed during remediations.
2. Perform in depth vulnerability scans on the network and server to discover vulnerabilities not encountered during the penetration test. Prepare a summary of the discovered vulnerabilities and determine appropriate mitigation strategies to implement during the network redesign and upgrade.
3. Create an inventory of the existing networking devices and office computers, including the PHI server and any computers used in daily operations, and a diagram of the current network layout.
4. Identify which current devices will remain, which will be disposed of, and what new devices will be needed. Acquire the new devices and evaluate any maintenance needs of the devices being retained. Properly and securely dispose of any devices being removed.
5. Install and securely configure the new devices, VLANs, and other mitigations and remediations across the network.
6. Verify network availability and performance for office machines, employee devices, and patient devices.
7. Re-scan network for vulnerabilities and attempt another penetration test of the server to verify security improvements meet or exceed expectations.

✓This project does not involve human subjects research and is exempt from WGU IRB review.

COURSE INSTRUCTOR SIGNATURE: 

COURSE INSTRUCTOR APPROVAL DATE: 1/30/2025