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 assure that they align with your degree emphasis. Without clearly naming each of these areas, you will not have a complete and realistic overview of your project, and it cannot be accurately assessed 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 do use a project they have already completed in the past year or two. In that case, you will write the proposal as if it has not been done yet, and the report is the complete after-implementation report. If you have *not* yet done your project, this document can help us make sure the scope is doable.

DEGREE EMPHASIS: Cybersecurity and Information Assurance

ANALYSIS:

Project Topic – Social Alliance Ltd., a small software company focused on analytics and social value of non-profit clients, seek to improve cloud performance and security by upgrading their endpoint protection.

Problem Statement or Project Purpose – What started as a project to help a local non-profit boost their social value in the community turned into a small software company that provides services to select non-profits. After Social Alliance outgrew their on-premise infrastructure, they shifted towards the cloud to leverage the clouds elasticity and cost savings. Social Alliance is currently using a traditional endpoint protection solution that is not suited for a virtualized cloud environment. The current endpoint protection is costing Social Alliance in cloud resources attributing to a high monthly bill. This problem needs to be addressed by deploying an endpoint protection solution that will leverage cloud abilities, reduce consumed resources, and increase security. They have hired STS Cloud Consultants to undertake the deployment of the new endpoint protection.

DESIGN and DEVELOPMENT:

Project Scope

a. Goals and Objectives –
    1. Conduct an inventory of cloud resources at Social Alliance for use in licensing and specialized configurations.
    2. Provision the virtual infrastructure for the deployment of the Symantec Endpoint (SEP) Manager, the SEP Console, and the Insights Cache.
    3. Install and configure the SEP Manager, Console, and Insights Cache.
    4. Prepare updated master images with the old endpoint protection removed and the SEP client installed and deploy them.
    5. Remove the old endpoint protection and install the SEP client on the persistent systems.
    6. Handover the management and response to Social Alliance's IT staff.

b. Project Outcomes and Deliverables –

1. Improved security for the cloud utilizing endpoint protection design for operation in a virtualized cloud environment.
2. Centralized management server for administering all endpoint protection and configuration.
3. Reduced cost for running endpoint protection in the cloud by leveraging the cloud specific features.
4. Improved compute infrastructure performance from the reduction of consumed resources.
5. Layered protection from host-based intrusion prevention and host-based firewalls.
6. Trained IT staff to manage and respond to endpoint alerts and events.

c. Projected Project End Date – The project should be completed within two weeks of the project start date. Approximately April 19, 2019. This will give STS Cloud Consultants the necessary time to inventory the existing cloud infrastructure, provision the needed resources, install the SEP administrative programs, deploy the endpoint protection, and train the IT staff at Social Alliance.

IMPLEMENTATION and EVALUATION:

Describe how you will approach the execution of your project – I will approach the execution of this project in several stages:

1. Inventory and document Social Alliance's compute infrastructure in the Microsoft Azure platform.
2. Provision two (2) additional Windows servers in the Azure platform. The first for the SEP Manager and SEP Console. The second for the Insights Cache.
3. Configure the SEP Manger with the inventory, licensing, and policies to govern the virtualized cloud environment.
4. Remove all instances of the old endpoint protection from Azure by updating and deploying new master images and pushing SEP to persistent instances.
5. Train the IT staff to administer and respond to SEP alerts and events.

COURSE MENTOR NAME: Joe Barnhart

____

COURSE MENTOR APPROVAL DATE:

____