1. **Security Planning**

Suppose you are in the InfoSec program of a large bank with several branches, and tasked to handle contingencies and plan for Business Continuity.

1. identify main steps to develop the BC program.
2. Form the BC Team
3. –Develop the BC planning policy statement
4. –Review the BIA
5. –Identify preventative controls
6. –Create relocation strategies
7. –Develop the BC plan
8. –Ensure BC plan, testing, training, and exercises
9. –Ensure BC plan maintenance
10. identify major BCP components (at least five) and develop a high-level plan.

The **BC policy** contains the following key sections:

–Purpose

–Scope

–Roles and responsibilities

–Resource requirements

–Training requirements

–Exercise and testing schedules

–Plan maintenance schedule

–Special considerations

1. **Security Policy**

Management focuses on and decides policy issues for a specific system. Such SysSPs are often codified as standards and procedures. Imagine you are the Chief Information Security Officer of KU, and responsible for developing a policy regarding to the use and protection of electronic health records in KU research projects. Please read KU Information Technology Security Policy and related issue-specific security policies, and identify/discuss:

1) what are the roles responsible for the development and implementation of this policy?

2) what are the existing ISSPs and laws related to the development of this policy?

3) what are the security objectives (please be more specific than CIA) for such system using EHRs? Describe security actions and/or operational rules.