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.
   - Form the BC Team
   - Develop the BC planning policy statement
   - Review the BIA
   - Identify preventative controls
   - Create relocation strategies
   - Develop the BC plan
   - Ensure BC plan, testing, training, and exercises
   - Ensure BC plan maintenance

2. Identify major BCP components (at least five) and develop a high-level plan.

I. 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

II. High Level Business continuity plan for Bank

Purpose of the Plan:

Unplanned events can have devastating effect on any business. The intent of this plan is to establish operational concepts and identify tasks and responsibilities required to carry emergency management and recovery. It defines the duties and responsibilities of employees and key positions to provide response and recovery actions. The plan is intended to provide flexibility of methods, operations and actions needed to help ensure a return to normal operation.

Scope:

The plan is intended to address events that can be classified as emergencies. This includes,

1. Natural disasters including fire, hurricane, flooding and severe weather.

2. Technology incidents including telecommunication disruptions and severe weather.
3. Geographical/Proximity incidents including truck or rail chemical spills, petrochemical plant explosion, radioactive releases from nuclear power plants and Bio Lab hazardous material incidents.
4. Human incidents including major crimes rioting, terrorist threats and political incidents.

Roles and Responsibilities**:**

A. Administration: Administrative support, defined as the Administrative Council, includes the full endorsement, support, and approval of the plan, ensuring necessary financial, human, and physical resources are available.

B. Directors, Managers, and Supervisors: Required to be knowledgeable of and adhere to the procedures in this plan, to the extent possible, and ensure communication to and the participation of staff in planning, recovery, and training.

C. Branch Safety & Security Committee: 1. Serves as the Plan Administrator and has the responsibility for overseeing the development, implementation, and maintenance of the Branch's Emergency Management Plan in support of the plan objectives. 2. Serves as the advisory committee responsible for providing recommendations and advice to the President and Administrative Council, as assistance is needed.

D. Employees: Employees are responsible for knowing and understanding their individual roles in the plan and having the ability and willingness to carry out that role in the event of an emergency.

Alternate Sites:

The Bank guarantees the availability of alternate sites for conducting business. The operations of affected branches will be performed in nearby branch (located within 30 miles) until the original site operations been resumed.

Communications:

Once the decision has been made to declare an emergency by the President (or designee), the communication process begins. The Director of Marketing & Communications (or designee) will initiate mass notification for staffs, customers and stakeholders through the Emergency Alert System.

A. Marketing & Communications will keep current emergency call lists for VC. Key employees are required to provide as appropriate, home phone and cell phone numbers, and email contact information.
B. All staffs and customers are encouraged to provide telephone numbers or other means of contact for emergency communications.

C. Each Branch Manager shall maintain a current phone and email listing of all key employees.

Plan Maintenance:

The Bank Safety & Security Committee is the Plan Administrant and shall coordinate the review of the plan. Each Recovery Team shall be responsible for reviewing its team responsibilities and making necessary changes. The plan can also be updated as a result of any post-incident review process and as a result of information gained from plan training exercises.

Plan Training Exercises:

Plan training and reviews should be completed prior to April 30 of review years, so that any major changes can be considered during the budget development process. All key employees should be included in the exercises. The exercise objectives are to:

- Ensure that the Emergency Operations Center Team, and other bank Administrators, are knowledgeable of their roles and responsibilities.
- Ensure that branch employees are knowledgeable of their roles and responsibilities and have a good understanding of the Bank's Business Continuity Plan.
- Ensure that individual Recovery Teams, both leaders and members, are knowledgeable of team roles and responsibilities.
- Provide assurance that the plan will be effective, current, and viable in the event of an emergency interruption of operations.

Distribution:

- The plan should be available in electronic format to all employees of bank
- It is the responsibility of each branch to maintain a hard copy version, readily accessible in the event of an emergency since Internet access may not be available during an emergency.
- Marketing & Communications will provide one hard copy to each member of the Administrative Council and each Recovery Team Leader.

2. 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?

Chief Information Officer

ITSO is responsible for the assessment, management and implementation of the policy that assures the safe use of EHR.

Responsibilities:

1. Understanding the information associated with EHR and understanding the nature and justification of all information flows to and from university.
2. Knowing who has access to these EHR
3. Understand trusts information usage and risk management policy.
4. Asses' risks to EHR as defined by this policy in accordance with established procedures.

Information Technology Administrators and Technicians

IT Administrators and Technicians are members of staff who understand and are very familiar with the risk in handling and maintaining the EHR.

Responsibilities:

1. Provide regular reports to senior management about effectiveness of information security policy.
2. Design access controls for the EHR database.
3. Classify and provide access privileges to users.
4. Revoke the access privilege when there is no more need. (Eg., Professors may have higher privilege compared to the students in record usage)

IT Database Staffs

IT database staffs are members of staff who monitors intrusion-controls, monitor e-mail accounts and perform other routine administrative roles.

Responsibilities:

1. Ensuring EHR handling procedures are fit for purpose and properly applied.
2. Ensure that the records are securely archived when there is no further requirement for it.

Authorized Users of EHR

Users include Faculty, staff and students who are authorized to access the system for research purpose.

Responsibilities:

They are responsible for following established policies and procedures and also for alerting managers, data owners or security officers of security breaches.

2. What are the existing ISSPs and laws related to the development of this policy?

ISSUES

Access of EHR:

The records can be accessed within department systems and can't be accessed in personal devices. Access to EHR may be provided when the access request is approved by Department Dean and if the user has cleared the following test:

- Background check.
- Drug screen test
- Completion of CITI training
- Completion of HIPAA CBL's training
- Signed protocol specific HIPAA authorization form obtained prior to accessing individual patient information.

Usage of EHR:

Users are prohibited from copying the EHR to their personal electronic devices.

Renewal of access privilege every semester:

User access privileges will be revoked at the end of every semester. New request needs to be submitted for getting access every semester.

Manipulating of EHR:

Users are prohibited from manipulating the original records. The personal details of the patients will not be disclosed to the users. The user has only read permission to access the EHR.

LAWS

1. HIPAA – Health Insurance Portability and Accountability Act
2. ePHI – electronic Protected Health Information

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

Security Objectives

It is the policy of University of Kansas to protect the privacy and security of evert patient's Protected Health Information. This policy defines the technical controls and security configurations users and IT administrators are required to implement in order to ensure the trustworthiness, authentication, responsibility, confidentiality, integrity and availability of data at KU. It serves as the central policy document with which all employers and users must be familiar and defines actions and prohibitions that all user

must follow. The policy provides IT managers within the practice with policies and guidelines concerning the acceptable use of EHR.

Actions and Operations

1. Any workforce member, upon discovering a potential breach of EHR, will inform the university privacy officer, in addition to reporting the incident in accordance with the KU computer security incident response policy, if applicable. Examples of possible breaches of EHR:
    - Any access to EHR out of curiosity or that is unauthorized.
    - Loss or theft of any device containing patient information
    - Finding hard copy of the EHR in the trash
    - Manipulating of EHR.
2. The privacy official, in consultation with the Director of IT Security and General Counsel's office, is responsible for reviewing incidents to determine whether notification is required and directing responsible departments in complying with the applicable notification obligation.
3. If a 'Breach of EHR' has occurred, timely notice to security officer, federal authorities and the public media (for large scale breaches) must be made as required.
4. The privacy officer or the Director of IT Security may take immediate action, when necessary to mitigate harm to the person who is subject of a potential/alleged unauthorized access, but before an investigation is complete.
5. In addition to the notification required under federal law, any breach analysis and/or notification determination under this policy shall include an evaluation of any applicable state breach notification law.