NCFM – COURSE OUTLINE

Information Security Services Professional (ISSP)

1. **Security Policy**

Security policy is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.

2. Security Models

A computer security model is a scheme for specifying and enforcing security policies. A security model may be founded upon a formal model of access rights, a model of computation, a model of distributed computing, or no particular theoretical grounding at all.

3. Physical Security

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

4. Communications and operations security

Information technology systems process large quantities of university data. These systems – which include computers, networking equipment, mobile devices, storage media, and other IT components – must be managed so as to protect information

5. Business Continuity Planning

The business continuity planning (BCP) is the creation of a strategy through the recognition of threats and risks facing a company, with an eye to ensure that personnel and assets are protected and able to function in the event of a disaster.

6. Compliance

In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that organisations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws and regulations.

7. Access Control

In the fields of physical security and information security, access control is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

8. Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

9. Software development and maintenance

Software development and maintenance in software engineering is the modification of a software product after delivery to correct faults, to improve performance or other attributes. A common perception of maintenance is that it merely involves fixing defects. However, one study indicated that over 80% of maintenance effort is used for non-corrective actions.

10. Security Tools

A variety of **tools** are available to administer **security** and address ongoing threats to your computers and network. To help you find the right **tool** for the job, the following **security tools** are grouped by task: Manage user accounts, groups, and credentials.