**UNIT IV**

**SESSION 1**

**Topic:**

* + Introduction
  + Policy, standards & practices, & principles

**Date:** 23.8.13

**Period:** 5

**Web links:**

<http://jwfiles.net/99avpz4zmhyn/IS_notes-ppt_s.rar.html>

<http://www.csudh.edu/Eyadat/classes/CIS378/handouts/information%20Security%20Blueprint.ppt>

<http://www.iup.edu/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=81011>

**Suggested Activity: pick ‘n’ learn**

The learners are grouped into 2. A grid is formed with numbers or alphabets. The learners or the group are asked to select an alphabet and then answer the question under it.

|  |  |  |
| --- | --- | --- |
| **A** | **B** | **C** |
| **D** | **E** | **F** |
| **G** | **H** | **I** |

**Question A** : Define policy

It is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters

**Question B:** What do you mean by standards?

Standards, on the other hand, are more detailed statements of what must be done to comply with policy

**Question C:** List policy types

* General or security program policy
* Issue-specific security policies
* Systems-specific security policies

**Question D :** Expand SPP

Security program policy (SPP)

**Question E :** Purpose of SPP?

Sets the strategic direction, scope, and tone for all security efforts within the organization

**Question F:** Expand ISSP

Issue-Specific Security Policy (ISSP)

**Question G**: Purpose of ISSP

It addresses specific areas of technology

**Question H:** List the approaches

* Create a number of independent ISSP documents
* Create a single comprehensive ISSP document
* Create a modular ISSP document

**Question I:** List any 2 structure of ISSP

* Statement of Policy
* Authorized Access and Usage of Equipment

**Conclusion :**

By the above activities the students got an idea about policy, standards and principles

**SESSION 2**

**Topic:**

* System specific policy

**Date:** 27.8.13

**Period:** 5

**Web links:**

<http://jwfiles.net/99avpz4zmhyn/IS_notes-ppt_s.rar.html>

<http://www.iup.edu/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=81011>

**Suggested Activity: crossword**

The learners are grouped into 2. Crossword is displayed and the learners or the group are asked to solve the crossword and they are scored.

****

**Suggested Activity: Buzz round**

The learners are grouped into 2. The group number 1 will answer the question and ask a question to group number 2. The question by group 1 should be related to the answer. Group 2 answers the question and asks a question to Group 1 based on their answer and so on.

Answers could be a one word answer or an explanation of not more than one or two sentences.

Sample questions are:

1. Expand ACL

Access Control List

1. What is the role of ACL?

ACLs allows configuration to restrict access from anyone and anywhere

1. Define rule policies.

Rule policies are more specific to the operation of a system than ACLs

1. Define policies.

Policies are living documents that must be managed and nurtured, and are constantly changing and growing

1. What do you mean by clean desk policy?

Clean desk policy stipulates that at the end of the business day, all classified information must be properly stored and secured.

**Conclusion :**

By the above activities the students got an idea about system specific policy

**SESSION 3**

**Topic:**

* Information security blueprint

**Date:** 29.8.13

**Period:** 4

**Web links:**

<http://jwfiles.net/99avpz4zmhyn/IS_notes-ppt_s.rar.html>

**Suggested activity: Match the words**

1. ACL - living documents
2. Policies - all information must be properly stored and secured
3. Clean desk policy - restrict access
4. Role of ACL - Access Control List

Answers: 1-4, 2-1,3 -2,4-3

**Suggested activity: recall by keywords**

The students are asked to recall a keyword from the topic and they have to answer for the same.

Sample keywords are:

1. Framework

Framework is the basic skeletal structure within which additional detailed planning of the blueprint can be placed as it is developed of refined

1. ISO

Indian Standards organization

1. IEC

International Electrotechnical Commission

1. NIST

National Institute for Standards and Technology

1. NIST Special publications

NIST SP 800-12 - The Computer Security Handbook

NIST SP 800-14 - Generally Accepted Principles and Practices for Securing IT Systems

NIST SP 800-18 - The Guide for Developing Security Plans for IT Systems

**Conclusion :**

By the above activities the students got an idea about Information security blueprint

**SESSION 4**

**Topic:**

* VISA model

**Date:** 29.8.13

**Period:** 6

**Web links:**

<http://jwfiles.net/99avpz4zmhyn/IS_notes-ppt_s.rar.html>

**Suggested activity: rapid fire quiz**

Thelearners are divided into 2 groups. In this quiz questions and answers are exchanged very fast and they are scored. Sample questions are as follows

1. Blueprint

Basic plan or structure

1. Framework

Additional detailed planning of the blueprint can be placed as it is developed.

1. ISO

Indian Standards organization

1. IEC

International Electrotechnical Commission

1. NIST

National Institute for Standards and Technology

**Suggested activity: factual questions**

1. What is VISA model

VISA International promotes strong security measures and has security guidelines

1. What at the 2 documents proposed?

* Security Assessment Process
* Agreed Upon Procedures

1. Define baselining

Baselining and best practices are solid methods for collecting security practices

**Conclusion :**

By the above activities the students got an idea about VISA model

**SESSION 5**

**Topic:**

* Design of security architecture

**Date:** 30.8.13

**Period:** 6

**Web links:**

<http://jwfiles.net/99avpz4zmhyn/IS_notes-ppt_s.rar.html>

**Suggested activity:match the words**

1. VISA - improve and regulate information systems
2. Security Assessment Process - provide best practices for public agencies
3. The Federal Agency Security Practices- International promotes strong security measures

Answers: 1-3, 2-1, 3-2

**Suggested activity: summary**

Information, at the core of the sphere, is available for access by members of the organization and other computer-based systems. “sphere of protection” overlays each of the levels of the “sphere of use” with a layer of security, protecting that layer from direct or indirect use through the next layer.

Information security is therefore designed and implemented in three layers

* + policies
  + people (education, training, and awareness programs)
  + technology

**Conclusion :**

By the above activities the students got an idea about Design of security architecture

**SESSION 6**

**Topic:**

* Security Education Training & Awareness(SETA)

**Date:** 31.8.13

**Period:** 5

**Web links**

<http://jwfiles.net/99avpz4zmhyn/IS_notes-ppt_s.rar.html>

**Suggested activity:crossword**



**Suggested activity: Tit for tat**

1. SETA

Security Education Training Awareness

1. SETA goal

Control measure designed to reduce accidental security breaches

1. Security education and training purpose

Builds on the general knowledge the employees must possess to do their jobs

1. SETA elements
   * security education
   * security training
   * security awareness
2. Security Awareness

Designed to keep information security at the forefront of the users’ minds

**Conclusion :**

* By the above activities the students got an idea about Security Education Training & Awareness(SETA)

**SESSION 7**

**Topic:** Security awareness program

**Date:** 19.09.13

**Period:** 4

**Web links**

<http://www.csudh.edu/Eyadat/classes/CIS378/handouts/information%20Security%20Blueprint.ppt>

**Suggested activity: recall by keywords**

1. Security education and training

Builds on the general knowledge the employees must possess to do their jobs

1. SETA elements
   * security education
   * security training
   * security awareness

**Suggested activity: choose & defend**

|  |  |
| --- | --- |
| **A** | **B** |
| **C** | **D** |

1. Security Perimeter

The point at which an organization’s security protection ends, and the outside world begins

1. Defense in Depth

Requires that the organization establish sufficient security controls and safeguards

1. Firewall

Device that selectively discriminates against information flowing into or out of the organization

1. DMZ -De-Militarized Zone

**Conclusion :**

By the above activities the students got an idea about Security awareness program

**SESSION 8**

**Topic:** Attack success scenario

**Date:** 24.9.13

**Period:** 5

**Web links**

<http://jwfiles.net/99avpz4zmhyn/IS_notes-ppt_s.rar.html>

<http://www.csudh.edu/Eyadat/classes/CIS378/handouts/information%20Security%20Blueprint.ppt>

**Suggested activity:puzzle**



**Suggested activity: tit for tat**

1. What is potential damage assessment?

BIA planning team must estimate the cost of the best, worst, and most likely cases

2. Attack scenario

Final result is referred to as an attack scenario end case

3.Subordinate plans

Will take into account the identification of, reaction to, and recovery from each attack scenario

**Conclusion :**

By the above activities the students got an idea about Attack success scenario

**SESSION 9**

**Topic:**

* IRP
* BCP
* Model for CP

**Date: 25.9.13**

**Period: 2**

**Web links**

<http://www.csudh.edu/Eyadat/classes/CIS378/handouts/information%20Security%20Blueprint.ppt>

S**uggested activity: rubik cube**

A: Incident -an attack against an information asset

B: IR -is more reactive, than proactive

C: Storage -The plan should be protected as sensitive information

D: Testing strategies –

* + - * Checklist
      * Structured walk-through
      * Simulation
      * Parallel
      * Full-interruption

E: Incident classification- is the process of examining a potential incident

F:Possible indicators of incidents:

* + Presence of unfamiliar files
  + Unknown programs or processes
  + Unusual consumption of computing resources
  + Unusual system crashes

Probable indicators of incidents:

* + Activities at unexpected times
  + Presence of new accounts
  + Reported attacks
  + Notification from IDS

**Conclusion :**

By the above activities the students got an idea about IRP & BCP