**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 4**

Names of team members: Corey Cooley, Taylor Payne, Will Brown, and John Hopson

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

Explain the differences between a hot site, warm site, cold site and use of a service bureau for business continuity. (8 pts.)

***Hot Site****: A fully configured computing facility that includes all services, communications links, and physical plant operations. The site can be operational within minutes creating a seamless fail-over. This real-time recovery will be the most expensive option for business continuity due to the required doubling of equipment, maintenance, and security required.*

***Warm Site****: A facility that provides many of the same services and options as a hot site, but typically without installed and configured software applications. The recovery time is not as quick compared to a Hot Site, due to applications not being installed and configured. The cost falls between a hot site and cold site and can be a great option for companies.*

***Cold Site****: A facility that provides only rudimentary services, with no computer hardware or peripherals. The facility will be an empty room with only heating, air condition, and electricity offered. This option is the cheapest to maintain business continuity; however, it is only slightly better than having nothing. It can take up to weeks to be up and running. Some companies have started to take it out as an option opting to do a short term lease then pay maintenance fees at a cold site.*

***Service Bureaus****: A strategy in which an organization contracts with a service agency to provide a facility to maintain business continuity for a fee. Some agencies also offer companies data storage depending on the contract. Contracts will guarantee space and depending on the disaster the company is experience will acquire more to accommodate. Contracts will have to be renegotiated periodically and depending the agency and requirements can be very costly.*

**Problem 2**

Explain the difference between full, differential, and incremental backup schemes. Be sure to mention what gets backed up each time and how restoration of data would work. (7 pts.)

*A* ***full*** *backup is the complete backup of the entire system, including the OS components. A restoration of a full backup will restore all data that was apart of the initial backup, including operating system and operating system components.*

*A* ***Differential*** *backup backs up all the data that has been changed or added since the last full backup. For a differential backup, you recover the last changes that had been made since backing up. For a differential restore, you must have the full backup as well as the differential backups since the full backup was last run.*

*An* ***incremental*** *backup is the backup of files that have been modified since the last incremental backup. For restoration of data, the data restored would be the data that was included in the last incremental backup, but everything since that backup would be lost.*

**Problem 3**

The University of Louisville’s [Information Security Office](http://louisville.edu/security) maintains the University’s information security policies, standards, and procedures. See the overview here:

<http://louisville.edu/security/policies/overview-of-policies-and-standards>

The current list of policies and standards is here:

<http://louisville.edu/security/policies/iso-policies/policies-standards-index>

1. From the above list, look for which policy is serving as the Enterprise Information Security Policy (EISP) as discussed in your text. What is its policy number (ISO PSxxx) and name? When did it take effect? How often is it supposed to be reviewed? When was it last reviewed? Is this consistent with the policy’s stated timeline for review? (5 pts.)

*The ISO PS0001 which is the Information Security Responsibility is considered an Enterprise Information Security Policy, because it covers what each individual who uses the system needs to do in regards to information security. It discusses how admins need to ensure compliance with university guidelines, how providers need to implement security measures to mitigate threats, how users need to be knowledgeable on information security requirements, and many more for each individual type.   
  
It was created on July 23, 2007.   
  
It is supposed to be reviewed annually.  
It was last reviewed on March 8, 2016. It is not compliant with its stated review timeline, since it is past March 8, 2017. After it was published in 2007, it was not looked at again until 2013.*

1. From the above list, look for a policy that would be an example of a Systems-Specific Policy (SysSP). What is the policy number (ISO PSxxx) and name? Is this of the Managerial Guidance, Technical Specifications, or Combination SysSP type? (3 pts.)

*ISO PS013, Server Computing Devices, would be considered a Systems-Specific Policy. It discusses the administrative standards and technical standards for any of the University servers. It covers the everything from the implementation of a server to the data backup and recovery.*

*Since ISO PS013 discusses both technical standards and administrative standards it would be considered a combination SysSP type.*

1. From the above list, look for a policy that would be an example of an Issue –Specific Policy (ISSP). What is the policy number (ISO PSxxx) and name? Is this of the independent, comprehensive, or modular ISSP type? (2 pts.)

*ISo PS008: Passwords is an Issue-Specific Policy because it concerns routine operations in relation to user passwords.*

*This is a comprehensive ISSP because the University ISO is responsible for the development, modification, publication, and oversight of this policy.*