**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 4**

Grading ID: A7386

**Problem 1**

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

A hot site is, in a lot of ways, a duplicate of the original work site, containing all of the equipment and amenities necessary for an organization to continue operating immediately following a disaster. A cold site is a reserved space that can be used in the event of a disaster, but is not pre-equipped with the amenities and equipment (such as desks and computers) that are necessary for an operation to function. A warm site is a compromise between the two, where it may have all the equipment, but be on a smaller scale, or not have a complete data backup to work with in case of a disaster.

A service bureau is an external operation that can facilitate a process for a company that may not have the resources or scale to manage that process internally. Service bureaus can assist in disaster recovery in instances where scale or operational efficiency is reduced as a result.

**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 scheme is a complete backup that takes a complete copy of the data. This backup is the most resource intensive and time consuming, but it does offer the lowest RTO. Full backups are typically only run periodically, unless a critical application requires daily backup. A differential backup only records and stores changes that occurred following an initial backup. As subsequent backups occur, the data set will grow. Differential backups are typically run daily if incremental backups are not implemented. Incremental backups only record changes that occurred following the previous backup, and as a result, store less data than an incremental back up. These are usually implemented daily unless differential backup is used. This set up has the highest RTO, as the least amount of data is stored.

**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/policies-standards-list>

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.)
2. 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.)
3. 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.)
4. ISO-PS001 v2.0 “Internet Security Responsibility” took effect July 23, 2007 and is to be reviewed annually. However only two review dates are recorded, along with a handful of revision dates, which is not consistent with the policy’s timeline for review. It was last reviewed June 12, 2017.
5. ISO-PS007 v2.0 “User Accounts and Acceptable Use” is a Managerial Guidance SysSP that governs how passwords and account authentication is handled at UofL.
6. ISO-PS006 v2.1 “Security Incidents” is a modular ISSP that offers guidelines for dealing with IT security incidents.