**Project 6 - Cloud Computing Security Policy**

This week you will prepare a cloud security policy. The first CIO of the US mandated that cloud services be implemented in organizations whenever possible. Review the scenario below and prepare a cloud security policy for the organization. Complete the following section readings from “***Challenging Security Requirements for US Government Cloud Computing Adoption,”***

NIST Cloud Computing Public Security Working Group, NIST Cloud Computing Program,

Information Technology Laboratory, sections 1.1, 1.3, 1.6, 1.8, and 1.9;prior to starting your work on the policy:

**PROCESS-ORIENTED SECURITY REQUIREMENTS**

1.1 NIST SP 800-53 SECURITY CONTROLS FOR CLOUD-BASED INFORMATION SYSTEMS: page 10

1.3  CLOUD CERTIFICATION AND ACCREDITATION: page 17

1.6 CLARITY ON CLOUD ACTORS SECURITY ROLES AND RESPONSIBILITIES: page 27

1.8 BUSINESS CONTINUITY AND DISASTER RECOVERY: page 31

1.9 TECHNICAL CONTINUOUS MONITORING CAPABILITIES: page 34

**Background**:
A small non-profit organization (SNPO-MC) has received a grant which will pay 90% of its cloud computing costs for a five year period. But, before it can take advantage of the monies provided by this grant, it must present an acceptable cloud computing security policy to the grant overseers.

**Tasking**:
You are a cybersecurity professional who is “on loan” from your employer, a management consulting firm, to a small non-profit organization (SNPO-MC). You have been tasked with researching requirements for a Cloud Computing Security Policy and then developing a draft policy for the non-profit organization, SNPO-MC. The purpose of this policy is to provide guidance to managers, executives, and cloud computing service providers. This new policy will supersede (replace) the existing Enterprise IT Security Policy which focuses exclusively upon enterprise security requirements for organization owned equipment (including database servers, Web and email servers, file servers, remote access servers, desktop computers, workstations, and laptop computers) and licensed software applications. The enterprise IT security policy also addresses incident response and disaster recovery.

As part of your policy development task you must take into consideration the issues list which was developed during brainstorming sessions by executives and managers in each of the three operating locations for the non-profit organization.

**Your deliverable** for this project is a 5 to 8 page, single spaced, professionally formatted draft policy. See the following resources for suggested formats.

<https://it.tufts.edu/cloud-pol>

<https://www.american.edu/policies/upload/IT-Security-Policy-2013.pdf>

**Organization Profile**:
The organization is headquartered in Boston, MA and has two additional operating locations (offices) in New Orleans, LA and San Francisco, CA. Approximately 50 employees work in a formal office setting at one of these locations. These employees use organization owned IT equipment. The remaining 1,000 staff members are volunteers who work from their home offices using personally owned equipment.

The organization provides a variety of management consulting services for its clients (charities and non-governmental organizations) on a fee for service basis. Fees are set on a sliding scale based upon the client’s ability to pay. The organization receives additional funding to support its administrative costs, including IT and IT security, through grants and donations from several Fortune 500 companies.

The non-profit organization is in the process of hiring its first Chief Information Officer. The organization has a small (3 person) professional IT staff that includes one information security specialist. These staff members are located in the Boston headquarters office.

**Definitions**:
Employees of the organization are referred to as employees.

Executives and other staff who are “on loan” from Fortune 500 companies are referred to as loaned staff members. Loaned staff members usually telework for the organization one to two days per week for a period of one year.

Volunteers who perform work for the organization are referred to as volunteer staff members. Volunteer staff members usually telework from their homes one to two days per week.

Cloud Computing includes but is not restricted to:

* Platform as a Service
* Infrastructure as a Service
* Software as a Service

**Issues List**:

* Who speaks with authority for the firm?
* Who monitors and manages compliance with laws and regulations?
* Ownership of content
* Privacy and confidentiality
* Enforcement
* Penalties for violations of policy
* Use by sales and marketing
* Use by customer service / outreach
* Use by public relations and corporate communications (e.g. information for shareholders, customers, general public)
* Use for advertising and e-commerce
* Use by teleworkers
* Review requirements (when, by whom)
* Use of content and services monitoring tools
* Content generation and management (documents, email, cloud storage)
* Additional issues listed in <http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf>

**Resources (suggested by the organization’s IT Staff for your consideration)**:

1. <http://www.nsa.gov/ia/_files/support/Cloud_Computing_Guidance.pdf>
2. <http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf>
3. <http://www.sans.org/reading-room/whitepapers/analyst/cloud-security-compliance-primer-34910>
4. <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>

**The documents below are useful resources in planning your cloud security policy:**

Cloud Security: A Comprehensive Guide to Secure Cloud Computing by [Ronald L. Krutz](http://library.books24x7.com.ezproxy.umuc.edu/SearchResults.aspx?qdom=author&scol=%7ball%7d&qstr=Ronald%20L.%20Krutz) and [Russell Dean Vines](http://library.books24x7.com.ezproxy.umuc.edu/SearchResults.aspx?qdom=author&scol=%7ball%7d&qstr=Russell%20Dean%20Vines) [John Wiley & Sons](http://library.books24x7.com.ezproxy.umuc.edu/books.aspx?imprintid=35) © 2010(384 pages), ISBN: 9780470589878 Chapter 3: Cloud Computing Software Security Fundamentals <http://common.books24x7.com.ezproxy.umuc.edu/toc.aspx?bookid=34770>

NIST Guide to Information Technology Security Services at <http://www.nist.gov/customcf/get_pdf.cfm?pub_id=906567>

25 point implementation plan to reform information technology <http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>

Understanding Cloud Computing (NIST SP 500-291) and (NIST SP 500-292) <http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024> 500-291 - Standards: Chapter 3 and Chapter 5.5

White Paper:***“Challenging Security Requirements for US Government Cloud Computing Adoption,”***NIST Cloud Computing Public Security Working Group, NIST Cloud Computing Program, Information Technology Laboratory