**Chad Ballay**

**CYBR450-342N**

**Week 2 Assignment**

* **Policies**

**a) What are policies?** Statements of what should be done, not the how it should be done. Sets the direction and importance but not the implementation.

**b) Distinguish between the corporate security policy, major security policies, and behavioral-based (aka acceptable use) policies**. Corportate policy is typically big picture type goals. Major policy is where the first bucketing of concepts starts to happen. The Acceptable Use policies is the first line of defense in assuring that the end user has postively affirmed that they agree to follow a policy.

**c) What are the purposes of requiring users to sign an Acceptable Use Policy (AUP)?** It is where the rubber hits the road for a company. It acts as the first place for showing that a user had fair warning about a policy. It gatekeeps an entity so that if the user is accessing that entity then they have had to agree to how to use it within the range of criteria that have been established by the company.

**d) Why are policies for specific controls, countermeasures or resources needed?**  Each entity may have very unique attributes that require specialization. In detailing them down to this level, the company is able to fine tune as they need.

**e) Provide an example of a Security Policy.** No unescorted guest policies seem to be a common one. That once a person is within the secured area they either have a some visible bona fide like a badge or they have someone with them who is responsible for them that has a visible bona fide. It is understandable the need for this but I've yet to find an Unescorted Guest policy that deals with bathroom policy for escort.

* **Implementation Guidance**

**a) Distinguish between standards, guidelines and procedures. In your explanation, include when each should be used within an organization.** One of the best ways to show this is to show the interrelation graphically. (<https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/images/EA_470psgs.jpg>)



They work to culmatively narrow down the focus to actionable steps from broad goals. The next best example of the interaction between these is this guide. It is amazing in how it helps communicate which of these handle what layers of operations. (<http://examples.complianceforge.com/ComplianceForge%20Hierarchical%20Cybersecurity%20Governance%20Framework.pdf>)



**b) For standards, what is mandatory?** They themselves must contain mandatory minimums on what is acceptable. They should be tied to specific control and objectives so as to ensure alignment.

**c) When are guidelines appropriate?** The focus of these are to ensure time saving configurations, setups, and other best practices are shared. These things may be situational and are not required to adhered to.

**d) Provide examples of security standards, guidelines and procedures you have personally seen.** Security standard I have seen has been the requirement to have all OS patches applied within 30 days of vendor release. A guidline I have seen has been a checklist style list of things to consider when configuring a new system. (disabling open ports. Removing unneeded accounts.) The procedure that I have used walked me through configuring my phone to be in compliance with my workplace's BYOD policy.

* **Policy Document Example**

You are tasked with creating the policies, standards, and guidelines for a small online retail business on the use of removable media (e.g., USB drives) and personal storage services. The intent is to (a) be compliance with regulations (e.g., PCI DSS) and (b) to ensure data isn’t compromised using personal storage (physical or online).   
For this section, you need to create the policy, standards and guidelines statements and correlate applicable regulations. You should use the most recent version of the Payment Card Industry Data Security Standard (PCI DSS): <https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml>.

**a) Policies:** All removable media and personal storage devices are to be not used without existing authorization of the device and approval of use by the indvidual.

**b) Standards:** All employees must store the removable media and personal storage devices upon their person or within lockable storage containers when not in use. Failure to do so may result in action up to and including termination.

**c) Guidelines:** When traveling overseas no removable media or personal storage devices shall be brought. Instead indviduals are required to use our hosted data storage solution. This can be accessed by supplying your login credentials to the XXXXXX website.

**d) Specific regulations and controls that apply:**

PCI-DSS 3: Protect cardholder data.

PCI-DSS 4 Encrypt transimission of cardholder data across open, public networks.

PCI-DSS 7 Restrict access to cardholder data by business need to know

PCI-DSS 9 Restrict physical access to cardholder data.

PCI-DSS 10 Track and monitor all access to network resources and cardholder data.