Module 4 Topic 4

Worksheet

First you…

Define each of the information security policies listed in the slide 5 from the lecture (above) and select what aspect of the CIA triad each seeks to address.

Policy	Definition	C	I	A
Acceptable use policy	It restricts the acceptable use of a particular service or resource (for example mobile data, university network connection). Universities will often require you to accept an AUP before you are allowed to use Uni computers or before you can browse the Internet from those computers. It sets out guidelines for how you should behave and defines the limits of what's acceptable.		X	X
Mandatory vacations				

Separation of duties				
Job rotation				
Clean desk policy				
Policies related to the least privilege principle	Bear in mind that a singular “LEAST PRIVILEGE POLICY DOCUMENT” does not normally exist, however many policies implement the principle of least privilege (why do you think that matters?) You can focus on cloud environments and review the sort of policies we see there, to try and answer, which of them look at the PoLP (principle of least privilege). Remember that a policy often doesn’t require a PDF document, it can be managed online through a dashboard. Example cloud PoLP policy: IAM Policies (for example in AWS cloud)			
Account disablement policy				
Never use shared accounts				
Require admin to use two accounts				
Storage and retention policy				
Social media policy				

Privacy policy				
Configuration management				
Disaster recovery				
Incident response policies	Outline how are you detecting incidents? (Specify the details of your IDS = an intrusion detection system). How will the systems by restored, how will the issues be solved.What are the lessons learned from this incident? How are we going to be alerting the relevant staff, who is going to get which type of alerts (different of levels incidents), how quickly do they have to react.	X	X	X

Recommended reading: Gibson (2014) CompTIA SECURITY + Get Certified Get Ahead, YCDA, LLC